Кенин Александр Михайлович, автор более 10 книг компьютерной тематики, вышедших общим тиражом более 500 тыс. экземпляров, специалист с богатым опытом проектирования и управления информационными системами.

Настольная книга администратора

САМОУЧИТЕЛЬ СИСТЕМНОГО АДМИНИСТРАТОРА

7-е издание

Есть области человеческой деятельности, где фактор личного опыта и мастерства играет решающую роль. Как ни парадоксально, вышедшее из самых точных наук компьютерное дело относится к таковым. Дружественность интерфейсов часто бывает столь же обманчива, как дружелюбие страховых агентов, а инструкции для сисадминов написаны в расчете на профессионала, ответы так называемых специалистов еще более неясны.

К счастью, исключения есть. В этой книге сконцентрирован опыт специалистов, которые не только знают свое дело, но и умеют рассказать о нем легко и доходчиво, охотно делятся своим опытом, консультируют, объясняют, обучают.

КАТЕГОРИЯ: операционные системы

ISBN 978-5-9775-1910-6

191036, Санкт-Петербург,
Гончарная ул., 20
Тел.: (812) 717-10-50,
339-54-17, 339-54-28
E-mail: mail@bhv.ru
Internet: www.bhv.ru

А. КЕНИН

САМОУЧИТЕЛЬ СИСТЕМНОГО АДМИНИСТРАТОРА

bhv

АЛЕКСАНДР КЕНИН

bhv

САМОУЧИТЕЛЬ СИСТЕМНОГО АДМИНИСТРАТОРА

7-е издание

Системы высокой доступности и их построение

Оптимизация производительности

Выбор оборудования и его характеристики

Использование облачных технологий

Объединение компьютеров Windows, macOS и Linux

Контроль и управление. Утилита monit для перезапуска сетевых сервисов

Надежная защита данных

Виртуализация средствами KVM

Практические рекомендации по выбору DLP-системы

Информационные системы на основе Windows 10/11/Server 2016/2019/2022

СИСАДМИН
СИСТЕМНЫЙ АДМИНИСТРАТОР

Александр Кенин

САМОУЧИТЕЛЬ СИСТЕМНОГО АДМИНИСТРАТОРА

7-е издание

Санкт-Петербург
«БХВ-Петербург»
2024

УДК 004.4
ББК 32.973.26-018.2
К35

Кенин А. М.

К35 Самоучитель системного администратора. — 7-е изд., перераб. и доп. — СПб.: БХВ-Петербург, 2024. — 608 с.: ил. — (Системный администратор)

ISBN 978-5-9775-1910-6

Изложены основные задачи системного администрирования, описаны базовые протоколы, даны рекомендации по выбору оборудования и проведению ежедневных рутинных операций. Подробно раскрыты технологии, используемые при построении информационных систем, описаны средства мониторинга и обслуживания как малых, так и распределённых сетей. Рассмотрены методы централизованного управления, основы создания безопасной среды. Даны рекомендации по поиску неисправностей, обеспечению защиты данных. Параллельно рассмотрены решения на основе операционных систем Windows и Linux с использованием как проприетарных, так и открытых технологий. Книга написана на основе многолетнего опыта разработки и практического администрирования информационных систем.

В 7-м издании весь материал актуализирован для Windows Server 2022 (русская версия), дополнительно рассмотрены файрвол ufw, утилита monit, виртуализация средствами KVM.

Для начинающих системных администраторов

УДК 004.4
ББК 32.973.26-018.2

Группа подготовки издания:

Руководитель проекта	*Евгений Рыбаков*
Зав. редакцией	*Людмила Гауль*
Компьютерная верстка	*Ольги Сергиенко*
Дизайн серии	*Марины Дамбиевой*
Оформление обложки	*Зои Канторович*

Подписано в печать 08.11.23.
Формат 70×100$^{1}/_{16}$. Печать офсетная. Усл. печ. л. 49,02.
Тираж 1500 экз. Заказ № 8041.
"БХВ-Петербург", 191036, Санкт-Петербург, Гончарная ул., 20.

Отпечатано с готового оригинал-макета
ООО "Принт-М", 142300, М.О., г. Чехов, ул. Полиграфистов, д. 1

ISBN 978-5-9775-1910-6

© ООО "БХВ", 2024
© Оформление. ООО "БХВ-Петербург", 2024

Оглавление

Предисловие **17**
Что нового вы найдете в седьмом издании? 18

Глава 1. Системное администрирование **19**
Обязанности системного администратора 19
Выбор операционной системы: Windows vs Linux 20
Участие в тендерах 22
Обновление программного обеспечения 22
О моральных качествах администратора 23

Глава 2. Выбор аппаратных и программных средств **25**
Требования к оборудованию информационных систем 25
Выбор производителя 25
Гарантия и сервис-центры 27
Выбор процессора 28
Выбор шасси 30
Выбор материнской платы 31
Выбор дисков 31
Выбор памяти 33
Дополнительные требования к коммутационному оборудованию 34
Дополнительные требования к аварийным источникам питания 35
Состав программного обеспечения типового предприятия 35
Подсистема аутентификации и контроля доступа 36
Подключение Linux к домену: протокол Kerberos 36
Настройка конфигурации клиента Kerberos 36
Настройка файла *nsswitch.conf* 37
Получение билета Kerberos для учетной записи администратора 37
Подключение к домену 37
Проверка подключения 38
Сервер Linux в качестве контроллера домена 38
Совместно используемые ресурсы 38
Учетная запись для анонимного доступа 39
Работа с Windows-ресурсами в Linux 40
Установка пакета Samba 40

Настройки Samba 40
Подключение к общим ресурсам 41
Браузеры Интернета 42
Защита узлов сети 42
Средства удаленного администрирования 43
Средства резервного копирования 44
Офисный пакет 46
Электронная почта 48
Свободное программное обеспечение 51
Базовые сведения о работе в *NIX-системах 52
Linux-мифы 52
Надежность Linux и Windows 54
Несколько моментов, о которых следует знать пользователям Linux 54
Ядро и дистрибутивы 54
Файловая система 55
Монтирование файловой системы 57
Консоль и графический режим 58
Пользователь root 58
Структура папок Linux 59
Текстовые редакторы: vi и другие 59
Выполнение команд с правами другого пользователя 63
Прикладные программы в Linux 64
Кросс-платформенный запуск программ 65
Установка Linux 66
Загрузка нескольких операционных систем 67
Тестирование Linux на виртуальной машине 67

Глава 3. Структура сети 69
Структурированные кабельные сети 69
Категории СКС 72
Волоконно-оптические сети 74
Сети 10G, 40G и 100G 75
Схема разъема RJ-45 76
Варианты исполнения СКС 78
Удлинение кабеля 78
Прокладка силовых кабелей 78
Питание по сети Ethernet (PoE) 79
Требования пожарной безопасности 79
Топология сети 80
Размеры сегментов сети на витой паре 80
Уровни ядра, распределения и доступа 80
Топология каналов распределенной сети предприятия 81
Сеть управления 82
Документирование структуры каналов связи 83
Качество сетей связи предприятия 83
Проверка кабельной системы 83
Проверка качества передачи данных 85
Приоритизация трафика 85
Варианты приоритизации: QoS, ToS, DiffServ 86
Классификация, маркировка, правила приоритизации 88

Как работает приоритизация: очереди ... 88
Ограничение полосы пропускания трафика (Traffic shaping) ... 89
Беспроводные сети ... 90
Стандарты беспроводной сети ... 92
Проектирование беспроводной сети предприятия ... 93
Безопасность беспроводной сети ... 97
Шифрование трафика беспроводной сети ... 97
Аутентификация пользователей и устройств Wi-Fi ... 97
Безопасность клиента ... 98
Настройка транспортных протоколов ... 99
Протоколы ... 99
Модель OSI ... 100
Стек протоколов TCP/IP ... 101
Протоколы UPD, TCP, ICMP ... 102
Протокол IPv6 ... 102
Параметры TCP/IP-протокола ... 103
IP-адрес ... 103
Групповые адреса ... 103
Распределение IP-адресов сети малого офиса ... 104
Подсети и маска адреса ... 105
Шлюз (Gateway, default gateway) ... 106
Таблицы маршрутизации ... 106
Автоматическое присвоение параметров IP-протокола ... 111
Серверы DHCP ... 111
Адресация APIPA ... 112
Назначение адресов при совместном использовании подключения к Интернету ... 112
Порт ... 113
Протокол ARP ... 114
Имена компьютеров в сети TCP/IP ... 115
Доменные имена Интернета ... 116
Соотношение доменных имен и IP-адресов компьютеров ... 117
Серверы доменных имен (DNS) ... 117
WINS ... 118
Статическое задание имен ... 118
Последовательность разрешения имен ... 119
Настройка серверов DHCP и DNS ... 120
Настройка DHCP ... 120
Создание и настройка зоны ... 120
Авторизация DHCP-сервера ... 121
Настройка параметров области ... 122
Фиксированные IP-адреса ... 123
Подстройка DHCP под группы клиентов ... 124
Отказоустойчивость DHCP-сервера ... 125
Обслуживание DHCP-сервером других сегментов сети ... 126
Порядок получения IP-адресов клиентами DHCP ... 127
Первичное получение адреса ... 127
Продление аренды ... 127
Диагностика и обслуживание DHCP-сервера ... 128

Интеграция DHCP и DNS ... 128
DNS ... 129
Термины DNS ... 129
Порядок разрешения имен в DNS ... 132
Основные типы записей DNS ... 133
Установка сервера DNS ... 134
Записи домена Windows ... 136
Разделение DNS ... 136
Настройка DNS в удаленных офисах ... 138
Обслуживание и диагностика неисправностей DNS-сервера ... 138
Перенос записей зон ... 141

Глава 4. Информационные системы предприятия ... 143
SOHO-сети ... 143
Одноранговые сети ... 145
Сеть с централизованным управлением ... 145
Управление локальными ресурсами ... 145
Возможность добавлять рабочие станции в домен ... 146
Удаление устаревших записей о компьютерах и пользователях ... 148
Изменение настроек системы при подключении ее к домену ... 148
Локальный администратор против доменного ... 149
Исключение компьютера из домена ... 149
Отключение совместного использования административных ресурсов ... 149
Исключение администратора домена из группы локальных администраторов ... 150
Блокировка администратора домена на уровне файловой системы ... 150
Блокирование групповой политики ... 150
Проблема аудитора ... 151
Методы управления локальной системой ... 151
Служба каталогов ... 152
Служба каталогов Windows (Active Directory) ... 153
Домены Windows ... 154
Подразделение ... 155
Лес ... 156
Сайты ... 156
DN и RDN ... 156
Управление структурой домена предприятия ... 157
Создание нового домена ... 157
Функциональный уровень домена ... 159
Компоненты Active Directory ... 160
Создание контроллеров домена «только для чтения» ... 162
Удаление контроллера домена ... 162
Переименование домена ... 164
LDAP и Active Directory ... 164
Подключаемся к каталогу по протоколу LDAP ... 164
Синтаксис поисковых запросов LDAP ... 165
Команда *ldifde* ... 167
Делегирование прав ... 168
Корзина Active Directory: просмотр и восстановление удаленных объектов каталога ... 169

Учетные записи и права ... 171
Понятие учетной записи ... 171
Локальные и доменные учетные записи ... 173
Группы пользователей ... 174
Ролевое управление ... 176
Результирующее право: разрешить или запретить? ... 176
Разрешения общего доступа и разрешения безопасности ... 177
Наследуемые разрешения: будьте внимательны ... 178
Восстановление доступа к ресурсам ... 179
Обход перекрестной проверки ... 180
Изменение атрибутов объектов при операциях копирования и перемещения ... 180
Результирующие права и утилиты ... 181
Рекомендации по применению разрешений ... 182
Создание и удаление учетных записей ... 182
Права учетной записи ... 184
Восстановление параметров безопасности по умолчанию ... 185
Автоматически создаваемые учетные записи ... 187
Встроенные учетные записи пользователей ... 187
Предопределенные учетные записи пользователя ... 187
Учетная запись *Администратор* ... 188
Учетная запись *Гость* ... 188
Другие встроенные учетные записи пользователей ... 188
Встроенные группы ... 189
Специальные группы ... 191
Рекомендации по использованию операции *Запуск от имени Администратора* ... 192
Включение сетевого обнаружения в Windows Server 2016/2019/2022 ... 193

Глава 5. Работа в глобальной сети ... 195
Организация доступа к ресурсам Интернета ... 195
Сетевая адресация ... 195
Введение в IPv6 ... 198
NAT — трансляция сетевого адреса ... 199
Реализация NAT средствами службы маршрутизации Windows Server ... 199
Аппаратный NAT ... 203
Реализация NAT средствами Linux ... 204
Фильтрация трафика ... 204
Демилитаризованная зона ... 205
Межсетевой экран (брандмауэр) ... 205
Выбор межсетевого экрана ... 206
Нужен ли прокси-сервер? ... 207
Системы обнаружения вторжений ... 207
Варианты межсетевых экранов ... 208
Программное решение ... 208
Аппаратные решения ... 209
Настройка параметров межсетевого экрана при помощи групповой политики ... 209
Межсетевой экран Linux ... 211
Настройки запуска ... 211
Цепочки и правила ... 212

Задание правил брандмауэра 214
Пример настройки брандмауэра 217
Брандмауэр UFW 222
Установка и базовая настройка 222
Создание правил для сетевых сервисов 223
Разрешаем IP-адреса 224
Запрещаем IP-адреса и службы 224
Сброс правил 224
Оптимизация доступа в Интернет 224
Основные мероприятия оптимизации 224
Прокси-сервер 225
Прозрачный прокси 227
Настройка использования полосы пропускания 228
Блокировка рекламы, сайтов «для взрослых» и т. п. 230
Поддержка SSL 233
Удаленная работа 235
Виртуальные частные сети 235
Удаленное подключение к Linux 236
Протокол SSH 236
«Тонкие» клиенты 238
Использование графических утилит для подключения к Linux 239
Подключение филиалов 239
Контроллер домена «только для чтения» 240
Решение DirectAccess 241
Терминальный доступ 242
Терминальные серверы от Microsoft 242
Терминальные клиенты 242
Режимы терминальных служб 243
Лицензирование терминальных служб 244
Особенности использования приложений на терминальном сервере 245
Безопасность терминальных сессий 245
Подключение к консоли терминального сервера 246
Подключение администратора к сессии пользователя 247
Публикация приложений в терминале 247
Веб-доступ к терминальному серверу 250
Шлюз терминалов 250
Создание локальных копий данных 251
История файлов 251
Технология BranchCache 252
Доступ из-за межсетевого экрана 253

Глава 6. Управление информационной системой 255
Состав информационной системы 255
Построение топологии существующей СКС 255
Инвентаризация физических каналов связи 256
Учет компьютеров и программ 257
Мониторинг функционирования ПО 258
Управление с помощью групповых политик 258
Порядок применения множественных политик 259

Совместимость версий групповых политик 259
Места хранения и условия применения групповых политик 260
Последствия отключений политик 262
Редактирование групповых политик 262
Начальные объекты групповой политики 265
«Обход» параметров пользователя 266
Фильтрация объектов при применении групповой политики 266
Фильтрация при помощи WMI-запросов 267
Настройка параметров безопасности групповых политик 267
Предпочтения групповых политик 267
Рекомендации по применению политик 268
Блокирование запуска нежелательных приложений с помощью компонента AppLocker 269
Некоторые особенности политики установки программного обеспечения 270
Административные шаблоны 272
Утилиты группового управления 272
Средства поддержки пользователей 273
Удаленный помощник 273
Утилиты подключения к рабочему столу 274
Средства автоматизации — сценарии 276
Использование командной строки 276
Сценарии Visual Basic 277
Интерфейс IPMI 278
Интерфейс WMI 278
Язык запросов WMI Query Language 279
Варианты применения WMI 279
Примеры WMI-сценариев 280
PowerShell 281
Утилиты администрирования третьих фирм 282
Утилиты от компании Sysinternals 282
Снифферы 283
Ideal Administrator 284
Hyena 284
Автоматизация установки программного обеспечения 284
Развертывание Windows 8 285
Развертывание Windows 10/11 285
Клонирование Windows-систем 285
Подводные камни процесса клонирования 286
Утилита sysprep 287
Создание установочного образа системы при помощи утилиты sysprep 287
Подготовка диска для существенно отличающейся системы 288
Дублирование жесткого диска 289
Образы клонируемого диска и их модификация 290
Клонирование компьютеров — членов домена 290
Клонирование Linux-систем 290
Средства клонирования Linux 290
Использование Clonezilla 291
Подготовка программ для «тихой» установки 297
Файлы ответов (трансформаций) 298

Использование ключей «тихой» установки 300
Переупаковка 301
Административная установка 303
Развертывание программы в Active Directory 303

Глава 7. Мониторинг информационной системы 309
Основные способы мониторинга 309
Журналы системы и программ 309
Протокол SNMP 310
Опрос служб 310
Мониторинг с использованием агентов 311
Мониторинг на основе протокола SNMP 312
Простейшие варианты мониторинга 314
Контроль журналов Windows 314
Привязка задачи 314
Подписка на события 316
Создание собственных событий в журналах Windows 316
Настройка журналирования в syslog 317
Простейший мониторинг Apache 317
Утилиты мониторинга 317
Система мониторинга Nagios 318
Необходимость мониторинга сети 318
Установка Nagios 318
Настройка Nagios 320
Мониторинг в Nagios серверов Windows 324
Мониторинг Windows-систем на основе WMI 327
Мониторинг в Nagios серверов Linux 328
Мониторинг систем с использованием протокола SNMP 328
Сервер протоколов 329
Постановка задачи 329
Настройка основного (центрального) сервера 330
Настройка остальных серверов сети 333
Протоколирование системой инициализации в Linux 334
Системы мониторинга трафика 337
Простейшая система мониторинга трафика: darkstat 337
Система NeTAMS 339
Утилита monit 343
Мониторинг жестких дисков. Коды S.M.A.R.T. 344

Глава 8. Виртуализация и облачные технологии 351
Секрет популярности виртуализации 351
Глоссарий 352
Вендоры виртуальных решений 352
Выбор гипервизора 353
Программное обеспечение и виртуальная среда 356
Особенности сетевых подключений виртуальных машин 356
Лицензирование программного обеспечения виртуальных машин 357
Создание виртуальных машин 358
Создание виртуальной машины путем чистой установки операционной системы 358

Клонирование виртуальной машины 359
Снятие образа физического сервера 360
Миграция между решениями различных производителей 360
Некоторые замечания к устройству виртуальных машин 362
Жесткие диски 362
Типы виртуальных дисков 362
Необходимость блочного доступа к виртуальному диску 363
Варианты подключения виртуального диска 363
Обслуживание файлов виртуального диска 363
Сохранение состояния виртуальной машины 363
Распределение вычислительных ресурсов 364
Оперативная память 364
Сервисные операции 365
Резервное копирование и антивирусная защита 365
Обмен данными 365
Копирование данных с машины на машину 365
Общие папки 365
Миграция виртуальных машин 367
Подключение к виртуальным машинам 368
Особенности выключения виртуальных машин 368
Виртуальные рабочие станции 369
Сравниваем VDI-решения с терминальными клиентами 369
Немного об экономике VDI 370
Структура VDI-решений 371
Некоторые особенности VDI-решений 372
KVM и Virtuozzo (OpenVZ) 373
Разница между KVM и Virtuozzo 373
Виртуализация на основе технологии KVM 374
Установка KVM 374
Создание виртуальной машины 375
Полезные команды 377
Советы по оптимизации виртуальных систем 378
Виртуализация в сетях передачи данных 379
Виртуальные частные сети 379
Зачем нужны виртуальные сети? 379
Маркировка кадров 380
Порты и VLAN 381
Практика настройки VLAN на коммутаторах Cisco 382
Другие производители оборудования 384
Настройка VLAN в Linux 384
Выбор сервера: физический или виртуальный 386
Нужен ли вашему проекту сервер? 386
Стоимость физического сервера 386
Стоимость виртуального сервера 387
Стоимость содержания физического сервера 388
Выбор облачного провайдера 390
Площадка 390
Сертификация ЦОД 390

Где расположен ЦОД: в России или за границей? ... 391
Кому принадлежит ЦОД? Можно ли войти и посмотреть, как все устроено? ... 392
Облачная платформа ... 392
Как можно подключиться к «облаку»? Есть ли панель управления? ... 393
Что представляет собой виртуальное ядро? ... 393
Какие используются дисковые ресурсы? Соответствует ли скорость ресурсов заявленной? ... 393
Есть ли сервис резервного копирования? ... 394
Какова пропускная способность интернет-соединения и сколько будет стоить ее расширение? ... 394
Входит ли в стоимость услуги лицензия на программное обеспечение? ... 394
Как выполняется тарификация? ... 394
Есть ли тестовый режим? ... 395
Сколько стоит собственная VPN-сеть и какие есть ограничения? ... 395
Есть ли какие-либо скрытые платежи — например, за панель управления сервером и т. п.? ... 395
Поддержка ... 395
Виртуализация физического сервера ... 395
Установка панели управления на виртуальный Linux-сервер ... 398
Настройка терминального Windows-сервера ... 404
Создание виртуального сервера ... 404
Оптимальная конфигурация виртуального сервера для бухгалтерской программы «1С:Предприятие» ... 405
Установка службы удаленных рабочих столов ... 406
Настройка сервера лицензирования для удаленных рабочих столов ... 411
Установка лицензий службы удаленных рабочих столов ... 417
Безопасный запуск программы «1С:Предприятие» ... 420
Песочница Windows ... 421

Глава 9. Безопасность ... 425
Безопасность и комфорт ... 425
Попытаемся разложить по полочкам ... 426
Как будем защищать? ... 427
Три «кита» безопасности ... 428
Организационное обеспечение информационной безопасности ... 429
План обеспечения непрерывности функционирования информационной системы ... 430
Безопасность паролей ... 430
Токены и смарт-карты ... 432
Rainbow-таблицы ... 433
Блокировка учетной записи пользователя ... 433
Восстановление пароля администратора ... 434
Методы социальной инженерии ... 435
Меры защиты от внешних угроз ... 436
Физическая безопасность ... 436
Ограничение доступа к рабочим станциям ... 437
Межсетевые экраны ... 438
Ограничения подключения нового оборудования ... 438
Обеспечение сетевой безопасности информационной системы ... 439
Контроль проходящего трафика ... 439

Контроль устройств по MAC-адресам 440
Протокол 802.1x 441
Особенности применения протокола 802.1x 442
Настройка протокола 802.1x 443
Выдача сертификатов компьютерам 444
Настройка службы каталогов 445
Настройка службы RADIUS 445
Настройка автоматического назначения VLAN для порта коммутатора 445
Настройка клиентского компьютера 446
Настройка коммутатора 447
Технология NAP 447
Обнаружение нештатной сетевой активности 448
Контроль состояния программной среды серверов и станций 449
Индивидуальная настройка серверов 449
Security Configuration Manager 449
Security Compliance Manager 450
Исключение уязвимостей программного обеспечения 450
Уязвимости и эксплойты 450
Как узнать об обновлениях? 451
Проверка системы на наличие уязвимостей 451
Тестирование обновлений 452
Обновления операционных систем Linux 453
Индивидуальные обновления Windows-систем 454
Обновление Windows-систем на предприятии 455
Установка обновлений через групповые политики 456
Защита от вредоносных программ 456
График обновления антивирусных баз 459
Внимательность пользователя 459
Обезвреживание вирусов 460
Защита от вторжений 461
Программы-шпионы: «троянские кони» 461
Редактирование списка автоматически загружаемых программ 465
Безопасность приложений 466
Основные принципы безопасности приложений 466
Единый фонд дистрибутивов и средства контроля запуска программного обеспечения 467
Неизменность системы 467
Защита от утечки данных 468
Шифрование данных 468
Шифрование данных на устройствах хранения 468
Шифрование архивов 468
Бесплатные программы шифрования данных 468
Шифрование дисков: коммерческие программы 470
Шифрование в Linux 472
Шифрование файловой системы Windows 475
Шифрование диска при помощи BitLocker 477
Использование BitLocker на компьютерах без TPM 478

Включение шифрования 479
Режим восстановления 479
Шифрование почты 480
Получение открытого ключа для защищенной переписки 481
Получение цифрового сертификата для защищенной переписки 481
Работа с подписанными и зашифрованными сообщениями в ОС Android 484
Шифрование в базах данных 490
Стеганография 491
Анализ поведения пользователей 491
DLP-технологии 492
Инструменты анализа безопасности Windows Server 495
MBSA, Microsoft Baseline Security Alalyzer 495
Microsoft Windows Server Best Practice Analyzer 497
SekCheck Security Auditing 498
Скрипт Windows SEC-Audit 499
Анонимность работы в глобальной сети 499

Глава 10. Отказоустойчивая информационная система 503
Территориальная распределенность 503
Центры обработки данных (дата-центры) 504
Требования к помещениям 504
Поддержание в помещении постоянной температуры 505
Резервное электроснабжение 505
Системы пожаротушения 506
Сетевая инфраструктура 506
Выбор правильной топологии сети передачи данных 506
Построение отказоустойчивой сети на основе протоколов второго уровня модели OSI 507
Протокол STP 507
Протокол MSTP 508
Отказоустойчивая сеть на основе протоколов третьего уровня модели OSI 508
Протокол VRRP 508
Агрегированные каналы 509
Проприетарные технологии восстановления структуры сети 510
Фермы серверов 510
Отказоустойчивые решения для приложений 511
DNS-серверы 511
DHCP-сервер 512
Кластер Oracle RAC 512
Распределенная информационная база программы «1С:Предприятие» 513
Дублирование данных 513
Зеркалирование серверов баз данных 513
Зеркалирование (репликация) данных SQL-серверов 513
Снимки баз данных 514
Настройка клиентских подключений 514
Распределенная файловая система 515
Создание DFS 515
Репликация DFS 516
Поддержка DFS в Linux-системах 518

Кластеры ... 518
Кластер Microsoft ... 519
Распределенные каталоги ... 521
Репликация данных каталогов ... 521
Хозяева операций ... 522
Смена хозяев операций ... 523
Сервер глобального каталога (GC) ... 524
Отказоустойчивые решения и виртуальные системы ... 525

Глава 11. Порядок выявления неисправностей и их устранения ... 527
Если отказ уже произошел ... 527
Максимальный аптайм ... 528
Восстановление с нуля, или полное фиаско ... 528
Запасные детали ... 529
Где получить помощь? ... 530
Сбор информации об отказе ... 530
Анализ журналов системы ... 531
Средства просмотра журналов системы ... 532
Журналы в Linux: демон syslogd ... 533
Централизованное ведение журналов ... 537
Установка триггеров на события протоколов ... 538
Настройка аудита событий безопасности ... 538
Особенности отказов различных компонентов ... 539
Мониторинг отказоустойчивой структуры ... 540
Неисправности подсистемы передачи данных ... 540
Обнаружение неисправностей сетевой инфраструктуры ... 540
Диагностика IP-протокола ... 541
Проверка параметров настройки IP-протокола ... 541
Проверка достижимости ближайших компьютеров сети ... 544
Проверка функционирования серверов имен ... 544
Проверка доступности приложений на удаленном компьютере ... 546
Проверка качества канала связи ... 547
Объективные показатели качества канала связи ... 547
Программа Observer ... 548
Утилита pathping ... 549
Неисправности аппаратной части компьютера ... 550
Контроль жестких дисков ... 551
Восстановление данных с жестких дисков ... 553
Проверка оперативной памяти ... 553
Контроль теплового режима работы системы ... 555
Ошибки программного обеспечения ... 556
Восстановление «упавших» систем ... 556
Восстановление из резервной копии ... 556
Восстановление загрузчика системы ... 557
Восстановление загрузки Windows 8 ... 557
Восстановление загрузки Windows 10/11 ... 562
Восстановление загрузки Linux-систем ... 565
Если опции восстановления недоступны ... 565

Загрузка в специальных режимах ... 566
Загрузка Windows в безопасном режиме ... 566
Загрузка *NIX-систем в однопользовательском режиме ... 566
Откат к предыдущим состояниям системы ... 567
Загрузка последней удачной конфигурации Windows ... 567
Загрузка конфигурации из точек восстановления Windows ... 567
Восстановление Windows путем переустановки ... 568
Восстановление удаленных данных ... 570
Корзины ... 570
Восстановление из теневых копий ... 570
История файлов ... 572
Оптимизация настроек компьютера ... 577
Что такое «медленно»? ... 578
Основные «узкие места» системы ... 578
Оценка производительности процессора ... 579
Оценка использования оперативной памяти ... 581
Оценка дисковой подсистемы ... 582
Показатели производительности дисков ... 582
Пути оптимизации дисковой подсистемы ... 585
Оценка работы сетевого адаптера и пути оптимизации системы передачи данных ... 585
Некоторые советы по анализу показаний производительности ... 587
Оптимизация приложений ... 588
Диагностика службы каталогов и обнаружение ее неисправностей ... 589
Средства тестирования AD ... 590
Проверка разрешения имен ... 591

Глава 12. Плановые задачи обслуживания ... 593
Ежедневные задачи ... 593
Еженедельные задачи ... 594
Прочие плановые операции ... 595

Предметный указатель ... 597

Предисловие

Эта книга пригодится всем, кто занимается созданием и эксплуатацией информационных систем. Главное внимание в ней уделено оценке различных технологий, на которых эти системы основаны: в большей степени с учетом практического опыта авторов и в меньшей — с точки зрения менеджера по продажам.

Многолетняя практика администрирования, развития компьютерных систем и оказания технической поддержки пользователям и специалистам показывает, что проблемы и вопросы у них возникают, как правило, однотипные. Именно поэтому в книге простыми и доходчивыми словами объяснены основы, на которых построена современная информационная система и понимая которые можно успешно контролировать ситуацию.

Цель книги заключается в том, чтобы пользователь выработал собственную позицию, а не шел на поводу у рекламных материалов и заказных статей.

В большинстве книг подобной тематики материал излагается по принципу: задача — решение. Возможно, в них приводится несколько вариантов решения, но в любом случае предлагается точная последовательность действий. Эта книга организована несколько в ином ключе. Последовательность действий описана в технической документации, и ознакомиться с ней — не проблема. Здесь же представлено наше ви́дение решения той или иной задачи. Мы указываем различные направления ее решения, не предлагая конкретной последовательности действий, а также описываем основные технологии, чтобы вы, как системный администратор, получили общее представление об их использовании. При этом предполагается, что наш читатель знаком с основами компьютерных технологий.

Если вас больше интересуют практические советы, то их можно найти в книге А. Кенина «Практическое руководство системного администратора» (2-е изд.) издательства «БХВ-Петербург»[1]. Обе книги хорошо дополняют друг друга.

---

[1] См. **https://bhv.ru/product/prakticheskoe-rukovodstvo-sistemnogo-administratora-2-e-izd/**.

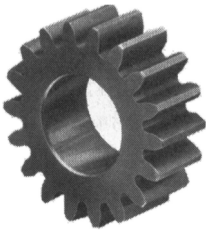
Что нового вы найдете в седьмом издании?

Во-первых, переработан и обновлен весь материал книги в целом — теперь он ориентирован на новейшую версию серверной операционной системы от Microsoft — Windows Server 2022. Нужно отметить, что большая часть материала применима и к предыдущим версиям Windows: 2019 и 2016, однако все иллюстрации выполнены в русской версии Windows Server 2022.

Во-вторых, обновлению подверглись и все без исключения главы. Где-то изменений больше, где-то — меньше, но без нововведений не осталась ни одна глава.

В-третьих, традиционно появились дополнительные практические примеры. Однако цель книги — задать правильное направление поиска информации, а не объяснять подробно каждую затронутую тему. Поэтому в книге читатель найдет множество ссылок на самые разные ресурсы, в том числе и на официальную документацию Microsoft. Что же касается конкретных практических примеров, то в *главе 5* показано, как настроить простой брандмауэр — UFW, в *главе 7* — как использовать утилиту monit, а в *главе 8* уделяется внимание настройке гипервизора KVM для создания виртуальных машин.

Теперь же самое время перейти от слов к делу.



ГЛАВА 1

Системное администрирование

Так кто же такой системный администратор? Ответить на этот вопрос мы сейчас и постараемся. Коротко говоря, системный администратор — это специалист, объединивший в сеть все компьютеры предприятия и поддерживающий работоспособность созданной системы. Однако часто на системного администратора возлагаются и некоторые дополнительные обязанности. И тут уже не знаешь, как все это понимать: или перед нами не системный администратор, или все же он, но с «расширенными» функциями.

Обязанности системного администратора

К огромному сожалению, в нашей стране отсутствует понимание задач и обязанностей системного администратора. В большинстве случаев под системным администратором имеют в виду универсального IT-специалиста, выполняющего (часто в одиночку) обязанности по обслуживанию компьютерного парка предприятия: создать и настроить сеть, установить/переустановить программу или операционную систему, отремонтировать/модернизировать компьютер, заправить картридж принтера, участвовать в закупке нового оборудования и т. п. Считается, что системный администратор должен заниматься всем этим. Хотя здесь как минимум нам видится должность «специалист по обслуживанию компьютерного парка», но никак не системный администратор.

В более «продвинутых» случаях (в крупных компаниях, например) системным администратором считается специалист по сопровождению рабочих мест пользователей. Он же, кроме того, отвечает за функционирование тех или иных отдельных информационных систем предприятия (сервер Active Directory, сетевые хранилища и принтеры, сервер баз данных, сетевое оборудование). Однако выделенного технического специалиста, отвечающего за работу информационной системы предприятия в целом, как правило, нет и здесь. Обычно эти обязанности возлагают на руководителя IT-отдела (IT-директора), что в корне неправильно. Руководство подразделением (отделом) и системное администрирование — это два разных направления работы.

И поскольку выделенного специалиста нет, техническая политика предприятия в части развития его информационной системы осуществляется так называемыми системными интеграторами, которые при этом на собственное усмотрение проводят линию поставщиков оборудования и программного обеспечения, с которыми заключили партнерские соглашения.

Понятно, что один человек не может знать всё про всё. Поэтому на большом предприятии сотрудники IT-службы закреплены за теми или иными системами и в меру своей компетенции осуществляют их поддержку. Имеются там также сотрудники, занимающиеся внедрением новых технологий, взаимодействием с пользователями и т. п. А кто же должен разбираться в работе всей информационной системы предприятия? Для этого есть особая должность — системный администратор. Он и должен знать особенности работы каждого отдельного элемента системы и понимать работу всех ее компонентов в комплексе. А для решения узких задач есть специалисты узкой специализации.

Итак, системный администратор — это специалист, который отвечает за функционирование и развитие информационной системы предприятия. Он координирует работу специалистов технической поддержки, администраторов подразделений, а также всех сотрудников узкой IT-специализации.

Хорошими системными администраторами не рождаются, ими становятся. Настоящим специалистом в этой области нельзя стать сразу после окончания обучения, будь то вуз или центр сертификации, — для этого нужен опыт работы и обретение на его основе комплексного взгляда на систему. Именно комплексного, а не в разрезе рекламы тех или иных производителей программного обеспечения, предлагающих свое ви́дение вашей системы, которое не всегда верно именно для конкретно рассматриваемого предприятия.

Одну и ту же задачу можно решить несколькими способами. Полагаем, это всем известно из курса вычислительных методов. Но в одном случае лучше выбрать способ А, в другом — Б. Вот выбор оптимального способа решения возникающих задач как раз и входит в обязанности системного администратора. А реализацией его пусть занимаются специалисты узкого профиля.

Выбор операционной системы: Windows vs Linux

Какую операционную систему выбрать для построения информационной системы? Так уж получилось, что отечественные пользователи привыкли к Windows и ничего, кроме нее, знать не хотят. Однако мир операционных систем Windows не исчерпывается — есть еще Linux, FreeBSD, macOS. А современные информационные системы, как правило, объединяют решения, основанные на различных операционных системах.

Хуже всего, что к Windows привыкли не только пользователи, но и сами администраторы, которые в массе своей ни с чем, кроме Windows, не знакомы.

Да, для Windows создано огромное количество всевозможных приложений, и эта ОС до сих пор остается доминирующей, особенно на универсальных рабочих мес-

тах, где заранее неизвестно, какие программы могут понадобиться, поскольку под Windows найти нужную программу проще.

Однако в то же время существует множество задач из области редактирования документов, работы с электронной почтой, просмотра веб-страниц. Такие задачи можно с успехом решить с использованием бесплатного программного обеспечения, предлагаемого Linux и FreeBSD. Именно поэтому если на предприятии начинают считать деньги, то задумываются о переходе на бесплатное ПО.

Правда, это не всегда возможно. В некоторых случаях требуется именно сертифицированное программное обеспечение, а для Linux его не так уж и много — из сертифицированных ФСТЭК[1] дистрибутивов можно упомянуть только ALT Linux, Astra Linux Special Edition и SLED (SUSE Linux Enterprise Desktop). И хотя для этих дистрибутивов разработано достаточно много самых разнообразных программ, может оказаться, что нужных вам как раз и не найдется. Да и сертифицированы эти дистрибутивы всего лишь по четвертому классу защищенности. А в некоторых случаях требуется третий или более высокий класс. Поэтому хочешь не хочешь, а придется использовать Windows — только из-за наличия сертифицированных программ.

Тем не менее UNIX-системы (Linux и FreeBSD) — не только бесплатные. Они, как правило, отличаются надежностью и стабильностью и могут работать без перезагрузки многие месяцы, чего не скажешь о Windows-системах, которые иногда приходится перезагружать по нескольку раз в день.

Какой дистрибутив Linux выбрать? Все они хороши. Если нужен сертификат ФСТЭК, то особо не разгуляешься: малоизвестный дистрибутив Astra Linux, SUSE Linux или ALT Linux[2]. Нам представляется, что ALT Linux предпочтительнее, но если вы привыкли к SUSE Linux (например, ранее использовали openSUSE), то выбор очевиден.

Если наличие сертификата ФСТЭК не требуется, выбирайте тот дистрибутив, который лично вам больше нравится. Мы могли бы порекомендовать Debian, CentOS и openSUSE — именно в такой последовательности. В «немилость» сейчас попал дистрибутив Ubuntu — раньше он был более надежен, но последние его версии оставляют желать лучшего.

При выборе операционной системы нужно учитывать еще и стоимость владения ею. Как таковой стоимости владения ОС не существует. Однако не нужно забывать, что если в настоящее время на предприятии нет администратора UNIX-системы, придется его нанять, а это дополнительные расходы. Конечно, любому квалифицированному пользователю не составит особого труда разобраться с основами UNIX, а вот для решения серьезных задач понадобится тщательная подготовка. Не скажем, что найти специалиста по UNIX слишком сложно (на дворе уже далеко не

---

[1] ФСТЭК — Федеральная служба по техническому и экспортному контролю.

[2] Полный список сертифицированного ФСТЭК программного обеспечения можно найти по адресу: **https://reestr.fstec.ru/reg3**.

2000 год, когда таких специалистов можно было пересчитать по пальцам), но их меньше, чем администраторов Windows-систем.

Не нужно обходить стороной и macOS. Это качественная операционная система, которая может работать в Windows-инфраструктуре. Без особых проблем компьютер под управлением этой ОС может стать членом домена Active Directory[1], причем «танцевать с бубном» для этого не придется — все решается путем использования Службы каталогов и специального плагина[2].

Участие в тендерах

Периодически возникает необходимость внедрения новых технических решений. Как правило, такое внедрение происходит на основе тендеров — открытых конкурсов. Системный администратор может и даже должен участвовать в тендерах. На основании своего опыта он может оказать серьезное влияние на результаты тендера путем формулирования технических требований. Самое интересное, что даже в открытом конкурсе можно заранее выбрать победителя, если «заточить» техническое задание под определенную модель оборудования и конкретное программное обеспечение. С другой стороны, системный администратор может сформулировать лишь основные требования проекта, что в результате позволит рассмотреть все предложения участников и выбрать оптимальный для предприятия вариант.

Обновление программного обеспечения

Многие системные администраторы стараются как можно чаще обновлять установленное программное обеспечение. Определенная логика в этом есть — каждое обновление несет исправление имевшихся ошибок и, возможно, новые функции.

Мы же придерживаемся иной политики. Применять обновления следует выборочно — если обновление несет в себе необходимый функционал (нужные пользователям функции, исправление «дыр» в безопасности и т. п.). В противном случае с применением обновлений лучше не торопиться. Как говорится, не мешайте компьютеру работать! Если все программы функционируют нормально и пользователи ни на что не жалуются, то зачем что-то менять? Конечно, это правило не касается антивирусных баз, а также обновлений безопасности (так называемых security updates).

Что же касается перехода на новые версии программного обеспечения (например, с Windows 10 на Windows 11), то тут хорошо бы оценить экономическую целесообразность такого решения. Переход только ради перехода нерационален. Переход должен быть оправданным.

---

[1] Active Directory (Активный каталог, AD) — службы каталогов корпорации Microsoft для операционных систем семейства Windows Server.

[2] См. **https://support.apple.com/ru-ru/guide/directory-utility/diru39a25fa2/mac**.

Зачем осуществляется переход? Предположим, что у вас есть парк компьютеров под управлением Windows 10 с установленными последними обновлениями. Если бы речь шла о Windows 7, поддержка которой давно прекращена, то однозначно нужно обновляться, т. к. многое современное ПО уже не работает в «семерке». Но у вас же Windows 10. И если сейчас всё работает, а пользователей и администраторов устраивает функционал этой ОС, есть ли смысл переходить на Windows 11? Это будут впустую потраченные деньги. Переход на новую версию Windows нужно производить по мере необходимости. Приведем некоторые примеры:

- необходимо установить какое-то ПО, которое несовместимо с Windows 10 и требует более новой версии Windows. Что ж, если нельзя использовать аналог этого ПО, работающий в «десятке», придется перейти на 11;
- компонент ПК вышел из строя. Представим, что сгорела видеокарта. Вы покупаете новую и обнаруживаете, что для нее нет драйвера под Windows 10. Тогда тоже — хочешь не хочешь, а обновиться придется. Хотя эта ситуация сегодня более чем надуманна: если бы речь шла о Windows 7, то она имела бы место быть. В случае же с Windows 10 и Windows 11 драйверы обычно взаимно заменяемы, и проблем с этим сейчас не наблюдается;
- появилась необходимость в использовании каких-либо функций, предоставляемых только новыми версиями Windows.

Итак, прежде чем обновляться и выкладывать деньги за обновление, нужно оценить выгоды, которые вы от него получите. Ведь очень часто обновление не заканчивается покупкой новых версий программных продуктов — приходится «подтягивать» «железо» до уровня нового программного обеспечения. Когда речь идет о целом парке компьютеров (как правило, на больших предприятиях такой парк покупается за один раз и все они примерно одинаковой конфигурации), то модернизировать придется все компьютеры сразу, а это может обойтись в круглую сумму.

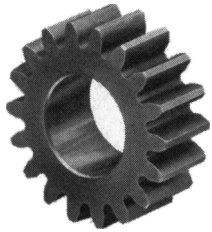
О моральных качествах администратора

Системный администратор — это пользователь с практически неограниченными правами, благодаря которым он может получить на своем предприятии доступ к любой информации (например, выяснить, у кого какая зарплата), перехватывать передаваемый трафик и даже читать почту сотрудников. На некоторых предприятиях ведется даже учет паролей — не только к учетным записям, но также и к ключам электронной подписи. Такая практика в корне неправильна, но она существует. Легко понять, что, имея пароли пользователей, администратор получает неограниченную власть над данными этих пользователей. Да, администратор может и без паролей пользователей получить доступ к любой информации, но система все равно запишет, что доступ получал именно администратор. А если он воспользуется паролем пользователя, система запротоколирует лишь доступ определенного пользователя к своим данным. Следовательно, доказать факт изменения данных администратором будет очень трудно.

Учитывая все сказанное, системный администратор должен обладать высокими моральными качествами, чтобы не подвергнуться соблазну совершить должностное преступление в виде несанкционированного доступа к чужим данным, их хищения и т. п.

Если вы собственник бизнеса и хотите хоть как-то обезопасить себя от нечистых на руку сотрудников, вам в помощь — DLP-системы[1]. Но и здесь есть нюансы. Ведь DLP-система будет устанавливаться и настраиваться тем же администратором, которому вы, возможно, не доверяете. Как быть в этом случае? Привлекать к ее установке и настройке третьих лиц? Не на каждом предприятии это возможно, да и есть ли доверие к ним? Вопрос доверия вообще весьма сложен, но в любом случае DLP хотя и не дает 100%-ной гарантии отслеживания утечек данных, однако предоставляет больше контроля над действиями пользователей.

[1] DLP-система (от англ. Data Leak Prevention) — специализированное ПО, которое защищает организацию от утечки данных.



ГЛАВА 2

Выбор аппаратных и программных средств

Одна из обязанностей системного администратора — выбор аппаратных и программных средств, используемых в составе информационной системы. Именно от администратора зависит правильный и оптимальный выбор оборудования и ПО. В этой главе мы постараемся помочь вам сделать такой выбор и попытаться найти оптимальное решение — как по стоимости, так и по функционалу.

Требования к оборудованию информационных систем

Сами понимаете, на рынке представлено множество аналогичного по своим параметрам и цене оборудования. Такое многообразие рождает проблему выбора. Ранее проблема выбора решалась отсутствием самого выбора — выбирать было не из чего и приходилось использовать то, что оказывалось доступно. Сейчас же эта задача — не из легких.

Выбор производителя

Не станем здесь углубляться в тонкости, а представим, что перед нами стоит очень простая задача — выбор для офиса маршрутизатора Wi-Fi, поскольку старый вышел из строя. Продукцию какого производителя: TP-Link, ZyXEL, D-Link или Cisco — выбрать? У всех этих производителей есть как дешевые, так и дорогие модели, но понятно, что модели одинакового уровня от ZyXEL и Cisco будут дороже, чем от TP-Link и D-Link. Стоит ли переплачивать за бренд?

Некоторые из читателей возмутятся: мол, как можно ставить «иконы» — ZyXEL и Cisco — в один ряд с бюджетными вендорами? Однако ни для кого не секрет, что подавляющее большинство всей электроники сейчас делается в Китае. Другими словами, качество сборки что того же ZyXEL, что TP-Link примерно одинаковое. Тем более что TP-Link — вполне приличный производитель, и его маршрутизаторы неровня прочим китайским устройствам No-Name.

При этом мы не советуем покупать самые дешевые модели — будь то ZyXEL или D-Link. Оптимальный выбор — это оборудование среднего ценового диапазона.

Дешевые модели работают не так хорошо и стабильно, как хотелось бы, вероятность отказа (из-за того, что производитель экономит на всем) у них выше. С другой стороны, в топовых моделях вы, как правило, не воспользуетесь и половиной предоставляемого функционала, — так зачем платить больше?

Теперь сравним две модели: Zyxel LTE3301 Plus Nebula (более $200) и TP-LINK Archer AX1500 ($50–60). Мы абсолютно случайно выбрали две модели от этих брендов с существенной разницей в цене. Оба устройства являются двухдиапазонными, т. е. могут работать на частотах 2,4 и 5 ГГц (диапазон 5 ГГц в последнее время является более предпочтительным из-за большого числа устройств, работающих на 2,4 ГГц). У обоих устройств по 4 Ethernet-порта, работающих на скорости 1 Гбит/с. А теперь о различиях. У Archer четыре антенны (рис. 2.1), у Nebula — всего две, следовательно, при использовании Archer большему количеству устройств будет обеспечена комфортная работа. К тому же модель от TP-Link поддерживает стандарт IEEE 802.11ax (он же Wi-Fi 6), что обеспечивает передачу данных внутри сети со скоростью 1,5 Гбит/с, в то время как Zyxel поддерживает только IEEE 802.11ac (Wi-Fi 5), работающий на скорости 1,3 Гбит/с[1]. Конечно, у модели Nebula есть «изюминка» — в нее можно установить SIM-карту, которая может использоваться в качестве резервного интернет-канала, если основной окажется недоступен. Но давайте будем честными — готовы ли вы переплатить за этот функционал в четыре раза больше? В крайнем случае, для домашнего применения «расшарить» Интернет можно с любого смартфона, а для предприятия все равно скорости мобильного оператора будет недостаточно.

Примечание

Не нужно думать, что TP-Link, ASUS и подобные бренды выпускают только дешевые устройства. Стоимость некоторых их домашних моделей (например, ASUS ROG Rapture) удивит даже бывалых администраторов — домашняя модель по цене решения для предприятия.

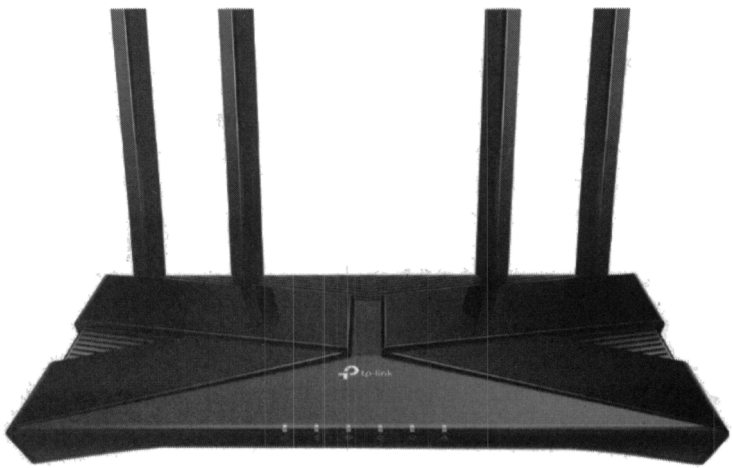


Рис. 2.1. Маршрутизатор TP-LINK Archer AX1500

[1] Заявленная производителем теоретическая максимальная скорость.

Как видите, переплачивать за бренд и покупать именитое устройство с примерно такими же характеристиками смысла нет.

Кстати, в брендах тоже нужно ориентироваться. Если хочется купить именитое устройство и при этом не платить много, обратите внимание на марку Linksys. Компания Linksys поглощена Cisco в 2003 году, но под торговой маркой Linksys до сих пор выпускается оборудование. Видимо, в Cisco решили таким образом разделить линейки устройств: для домашних и небольших офисных сетей — Linksys, для сетей предприятий среднего и большого размера — Cisco.

Примечание

При сравнении оборудования пользуйтесь только официальными источниками информации (сайтами производителей). На сайтах интернет-магазинов информация может оказаться неточной, и использовать ее для сравнения устройств не рекомендуется.

Гарантия и сервис-центры

Гарантийный срок — немаловажный фактор: одно дело — 12 месяцев, а 24 месяца или 36 — совсем другое.

Обратите внимание и на территориальное расположение сервисных центров. Если в вашем городе нет полноценного сервисного центра (иногда есть только представители, которые лишь принимают оборудование, а ремонт осуществляется в другом городе), то лучше поискать другого производителя. В случае отказа оборудования (и если не заключен сервисный контракт, о котором будет сказано далее) такой удаленный ремонт может занять длительное время — на одну только пересылку оборудования туда-сюда уйдет как минимум от 2 до 4 дней.

При выборе оборудования нужно также не только позаботиться о наличии и сроке гарантии и расположении сервис-центров, но еще и разобраться в сервисных обязательствах производителя. Чем дороже и сложнее оборудование, тем важнее его роль в информационной системе и тем дороже обойдется предприятию его простой на время ремонта. В случае с маршрутизатором можно на временную подмену вышедшему из строя устройству купить хоть самый дешевый. Такой выход, конечно, не очень приятен, но не сильно отразится на бюджете конечного пользователя, тем более на бюджете предприятия. Однако для дорогого и сложного оборудования следует заключать сервисные контракты, которые гарантируют восстановление оборудования (или предоставление подменного оборудования) в течение оговоренного срока. Сервисный контракт особенно важен, если предприятие находится вдали от региональных центров.

Любое оборудование рано или поздно устаревает. Поэтому постарайтесь купить к нему запасные части. Бывает так, что выходит из строя какой-то компонент, найти который спустя 4–5 лет после покупки оборудования крайне сложно и дорого. Типичный пример — оперативная память для ПК. Попробуйте сейчас найти модули DDR SDRAM. Максимум — бывшие в употреблении. Да и цена не порадует. Так что если вы сейчас закупили парк компьютеров, озаботьтесь запасными частями.

Через четыре года найти к этим компьютерам комплектующие можно будет разве что на так называемых компьютерных разборках.

Вот примерный список того, что нужно закупить (конкретные спецификации приводить не станем, т. к. они зависят от имеющегося у вас компьютерного парка):

- модули оперативной памяти;
- жесткие диски;
- блоки питания;
- вентиляторы CPU.

Выбор процессора

Характеристики процессора зависят от требований проекта (частота, количество ядер и т. п.). А если планируется использовать виртуализацию, необходимо улучшить конфигурацию примерно на 30%.

Организовывать сервер на базе процессоров AMD из-за их повышенного тепловыделения мы не рекомендуем — даже несмотря на то, что они дешевле процессоров Intel. И, выбирая процессор для сервера, мы бы остановили свой выбор или на Intel Xeon, или на Intel Core i9. Решая, какой именно процессор вам подходит, нужно исходить из задач и финансов, — чтобы не купить устройство, всем потенциалом которого вам не суждено будет воспользоваться (вы просто переплатите), или же, наоборот, которое окажется не соответствующим вашим ожиданиям.

При выборе процессора надо ориентироваться не только на количество ядер, но и на частоту каждого ядра. Например, характерная черта семейства процессоров Xeon Phi — большое количество ядер, но при этом частота каждого ядра от 1 до 1,7 ГГц. Так, на борту Xeon Phi 3120A целых 57 (!) ядер с частотой 1,1 ГГц каждое. Такие процессоры используются на суперкомпьютерах. Что же касается цены, то мы не просто так его упомянули. Этот процессор появился в 2013 году и считается устаревшим, новым его уже не купить, но на eBay в варианте б/у его легко можно приобрести за $40–50. Вы только вдумайтесь: 57 ядер за 50 долларов!

Но вернемся к более приземленным вариантам. В предыдущем издании книги мы рекомендовали процессор Xeon X-3275. Он и на сегодняшний день с его 28 ядрами остается достойным вариантом. Но есть модели и получше — например, W-3365, — у него 32 ядра с частотой 2,7 ГГц каждое (у модели 3275 частота ядер 2,5 ГГц). Есть и еще лучше — W-3375 с 38 ядрами (2,5 ГГц). Вот только его цена вас не порадует — на сайте Intel она официально заявлена в $4951[1].

Если цены в 4–5 тысяч долларов только за процессор вас выводят из равновесия, не отчаивайтесь — можно посмотреть на Intel Xeon E5 2697vE52697v2 (12 ядер по 2,7 ГГц каждое), цена на б/у варианты которого начинается от $30.

---

[1] См. **https://www.intel.com/content/www/us/en/products/sku/217246/intel-xeon-w3375-processor-57m-cache-up-to-4-00-ghz/specifications.html**.

Совет

Очень рекомендуем вам посетить страницу https://www.cpu-world.com/info/Intel/server-processor-number.html — здесь вы сможете ознакомиться со списком серверных процессоров Intel и их характеристиками (рис. 2.2).

Processor numbers of Intel server CPUs

Processor number	Family	Tech. (micron)	CPU speed (GHz)	Bus speed (MHz)	L2 cache size (KB)	L3 cache size (MB)	Cores	EM64T	HT	VT	XD	SS	Notes
1403	Pentium Dual-Core	0.032	2.6		512	5	2	+	-	+	+	+	
1405	Pentium Dual-Core	0.032	1.2		512	5	2	+	-	+	+	+	Uni-processing
1407	Pentium Dual-Core	0.032	2.8		512	5	2	+	-	+	+	+	Uni-processing
3040	Xeon	0.065	1.867	1066	2048		2	+	-	+	+	+	Uni-processing
3050	Xeon	0.065	2.133	1066	2048		2	+	-	+	+	+	Uni-processing
3060	Xeon	0.065	2.4	1066	4096		2	+	-	+	+	+	Uni-processing
3065	Xeon	0.065	2.333	1333	4096		2	+	-	+	+	+	Uni-processing
3070	Xeon	0.065	2.667	1066	4096		2	+	-	+	+	+	Uni-processing
3075	Xeon	0.065	2.667	1333	4096		2	+	-	+	+	+	Uni-processing
3085	Xeon	0.065	3	1333	4096		2	+	-	+	+	+	Uni-processing
3104	Xeon	0.014	1.7		6144	8.25	6	+	-	+	+	+	Dual-processing
3106	Xeon	0.014	1.7		8192	11	8	+	-	+	+	+	Dual-processing
3120A	Xeon Phi	0.022	1.1		29184		57	-	+	-	+	-	Multi-processing
3120P	Xeon Phi	0.022	1.1		29184		57	-	+	-	+	-	Multi-processing
31S1P	Xeon Phi	0.022	1.1		29184		57	-	+	-	+	-	Multi-processing
3204	Xeon	0.014	1.9		6144	8.25	6	+	-	+	+	+	Dual-processing
3206R	Xeon	0.014	1.9		8192	11	8	+	-	+	+	+	Dual-processing
3408U	Xeon	0.01	1.8		16384	22.5	8	+	-	+	+	+	

Рис. 2.2. Начало списка серверных процессоров на сайте **http://www.cpu-world.com**

Серверы на базе процессоров Intel Xeon могут позволить себе лишь крупные компании, поскольку, как отмечено ранее, стоимость только одного процессора может составлять несколько тысяч долларов (так, цена уже упомянутого Intel Xeon W-3275 на момент его презентации составляла $4449). И если бюджет ограничен (как это часто бывает), следует обратить внимание на процессоры семейства Core i7/i9.

Некоторые особо придирчивые читатели могут возразить: мол, что это за сервер с десктопным процессором, которыми являются Core i7 и Core i9? Однако все зави-

сит от того, что мы вкладываем в понятие «сервер». Серверы, которые помещаются в стойку, как правило, поставляются с процессором линейки Xeon. А вот серверы, выполненные в традиционном корпусе Tower, часто комплектуются процессорами Core i7/i9. Конкретный пример — Dell Precision (Intel Core i9), а сервер HPE (Hewlett-Packard Enterprise) Gen10 X3418 вообще выполнен на базе процессора AMD Opteron X3418. Тем не менее, если нужен недорогой сервер в форм-факторе 1U для помещения в стойку, можно остановиться на вариантах от Supermicro — модель 5019S-L оснащена процессором Xeon E3-1220 и памятью с поддержкой ECC[1]. Основной недостаток десктопных процессоров — отсутствие поддержки ECC (даже в 10-м поколении Core i9 поддержки ECC нет). Впрочем, процессоры Intel — это не единственный выбор. Вполне возможно, что вам придется использовать совсем другие процессоры и даже совсем иную архитектуру. Все зависит от используемых приложений.

Выбор шасси

В большинстве случаев серверы устанавливаются в стойку или шкаф, поэтому обычные корпуса, привычные многим пользователям, для серверов не подойдут. Серверы должны поставляться в специальном шассийном исполнении, что позволяет выдвигать их из стойки для упрощения обслуживания. При этом само шасси должно иметь два блока питания, допускающих их «горячую» замену.

На рис. 2.3 приведен типичный серверный корпус. При выборе корпуса обратите внимание на то, чтобы он мог быть установлен в серверную стойку (также называемую телекоммуникационной стойкой). Если серверная стойка еще не покупалась, то вы можете выбирать любой тип серверного корпуса — потом подберете под него стойку. Если же стойка уже куплена, то придется подбирать корпус с возможностью установки в имеющуюся стойку.

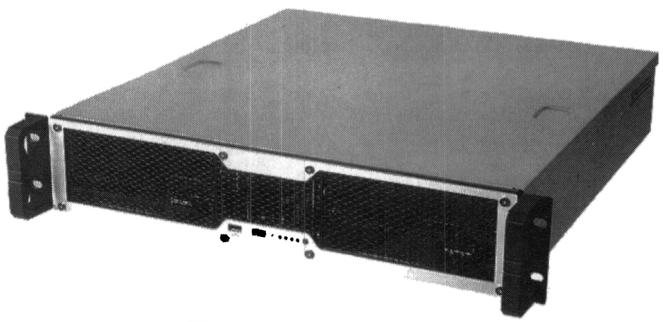


Рис. 2.3. Типичный серверный корпус

[1] ECC-память (от *англ.* Error-Correcting Code Memory, память с коррекцией ошибок) — тип компьютерной памяти, которая автоматически распознает и исправляет спонтанно возникшие изменения (ошибки) битов памяти.

Выбор материнской платы

Выбор материнской платы не менее важен, чем выбор процессора. При выборе материнской платы нужно учитывать следующие ее характеристики:

- **форм-фактор** — важно, чтобы выбранная материнская плата могла быть установлена в выбранный корпус. Иначе придется что-то менять: или корпус, или материнскую плату. Учитывая, что корпус подбирался под стойку, материнскую плату в случае несовпадения придется заказывать другую;
- **тип сокета процессора** — типы сокета процессора и материнской платы должны совпадать. Полагаем, это понятно;
- **максимальный объем оперативной памяти** — учитывая, что мы выбираем материнскую плату для сервера, максимальный поддерживаемый объем ОЗУ должен быть не менее 128 Гбайт. Конечно, если вы создаете сервер начального уровня, то хватит и 64 Гбайт (речь идет о максимальном объеме ОЗУ, а не об объеме «на борту» сервера, — здесь во многих случаях сегодня хватит 16–32 Гбайт), но не нужно забывать о возможной последующей его модернизации. Память — очень критичный ресурс, и очень скоро вы обнаружите, что вам ее недостаточно. Также помните, что максимальный объем может зависеть от типа памяти. Например, при использовании памяти ECC 3DS LRDIMM материнская плата может поддерживать до 1 Тбайт памяти, а при использовании ECC RDIMM — «всего» 256 Гбайт. И хорошо, когда есть возможность расширения;
- **количество слотов памяти** — на серверной материнской плате должно быть не менее 4 слотов под ОЗУ (типичная серверная плата обычно содержит 8 слотов оперативной памяти);
- **поддержка RAID** — эта характеристика даже важнее, чем максимальный объем оперативной памяти. Если на рабочей станции RAID не нужен, то на сервере это обязательное требование;
- **количество разъемов SATA II/III** — чем больше, тем лучше. Скорее всего, на вашем сервере будет установлено несколько жестких дисков. Например, на борту материнской платы Supermicro X10SRH-CF имеется десять слотов SATA-III.

Для упрощения ее обслуживания материнская плата должна быть совместима с используемой на предприятии системой мониторинга.

Выбор дисков

Перед покупкой жестких дисков нужно определиться, где будут храниться данные — на сервере или на внешней системе хранения данных. Предпочтительно использовать внешнее устройство, благо на рынке представлены самые разные варианты различных ценовых категорий. В этом случае для сервера понадобится всего два жестких диска — чтобы построить на их основе отказоустойчивый массив (зеркала).

Совсем другое дело, если данные предполагается хранить на сервере. Тогда надо установить в сервер максимальное число дисков, что ограничивается форм-

фактором корпуса. Следовательно, при выборе корпуса необходимо учитывать и это. Количество дисков зависит от выбранного уровня RAID. Так, для RAID 5 требуется три, а для RAID 5E — четыре диска. Общая информация о некоторых уровнях RAID представлена в табл. 2.1.

***Таблица 2.1.** Основные уровни RAID*

Уровень	Избыточность	Полезная емкость, %	Резервный диск	Мин. кол-во дисков	Макс. кол-во дисков
RAID 0	–	100	–	1	16
RAID 00	–	100	–	2	60
RAID 1	+	50	–	2	16
RAID 1E	+	50	–	3	16
RAID 5	+	67–94	–	3	16
RAID 5E	+	50–88	+	4	16
RAID 50	+	67–94	–	6	60
RAID 15	+	33–48	–	6	60
RAID 6	+	50–88	–	4	16

Из всех уровней, представленных в табл. 2.2, наиболее часто используется RAID 5. Это самый экономный уровень — он требует всего лишь три диска, при этом поддерживается избыточность данных, а полезная емкость достигает 67% (для 3 дисков). Общий размер массива вычисляется по формуле

$$S \times (K - 1),$$

где S — размер меньшего диска в массиве, а K — число дисков. Если у вас есть четыре диска по 1 Тбайт каждый, то полезный размер массива будет

$$1 \times (4 - 1) = 3 \text{ Гбайт},$$

что равно 75% от общей емкости всех накопителей. То есть чем больше дисков, тем выше полезный размер массива.

При выборе дисков, кроме интерфейса их подключения и емкости самих дисков, нужно также учитывать размер буфера диска и скорость вращения шпинделя. Сами понимаете — чем эти параметры выше, тем лучше.

От скорости вращения шпинделя зависит параметр IOPS (Input/Output operations Per Second) — число операций ввода/вывода в секунду. Этот параметр практически одинаков для всех моделей всех производителей и зависит от скорости вращения шпинделя — чем выше скорость, тем больше IOPS. Зависит также IOPS и от размера блока. Понятно, что чем больше размер блока, тем ниже IOPS. В среднем при объеме блока до 4 Кбайт включительно IOPS составляет 170 операций в секунду при скорости вращения шпинделя (RPM) 15 тыс. оборотов в минуту. Если скорость вращения равна 10 тыс. RPM, то IOPS будет равен 120. Да, именно такие жесткие

диски нужны для серверов. Для сравнения — на рабочих станциях обычно устанавливаются жесткие диски с частотой вращения шпинделя 7200–7500 RPM. В этом случае их IOPS равен всего 70.

Разумеется, какой тип массива RAID, исходя из ваших задач, рекомендуется применить, какой размер блока использовать и т. д., следует выяснить до покупки сервера.

Существенно повысить производительность можно путем использования твердотельных дисков (SSD). Однако необходимо иметь в виду, что время наработки на отказ у них ниже, чем у обычных жестких дисков, и заменять такие диски придется чаще. Имея в виду стоимость SSD-дисков большого размера (от 500 Гбайт), это удовольствие не из дешевых.

Учитывать также нужно и интерфейс диска. Начиная с Windows Server 2016, интерфейс PATA (ATA/IDE/EIDE) более не поддерживается. Конечно, в 2023 году мало кому придет в голову покупать PATA-диск для использования на сервере, но вы должны знать, что если у вас не очень новый сервер, построенный с использованием PATA-дисков, — без модернизации «железа» проапгрейдить такой сервер до Windows Server 2016/2019/2022 уже не получится. Последней версией, поддерживающей интерфейс PATA, является Windows Server 2012.

Выбор памяти

Вот мы и добрались до очень важного элемента любой системы — оперативной памяти. Считается, что увеличение объема оперативной памяти — самый простой и относительно дешевый способ увеличения производительности системы. Но это не всегда так.

При выборе оперативной памяти, кроме емкости самих модулей и их типа (DDR3, DDR4), нужно учитывать еще и следующие параметры:

- **эффективную пропускную способность** — она обычно указывается в спецификации модуля как PC4-<число>. Например, стандарт PC4-19200 означает, что эффективная пропускная способность составляет 19 200 Мбайт/с. Все модули должны быть одного стандарта;
- **частоту памяти** — она измеряется в мегагерцах, и обычно можно сказать, что чем больше этот параметр, тем лучше, но и это не всегда так. Надо, чтобы материнская плата поддерживала выбранную вами частоту. Если, например, вы купите модули памяти, работающие на частоте 3200 МГц, но поскупитесь на соответствующую материнскую плату (или просто не обратите внимание на этот параметр при ее выборе), и окажется, что она поддерживает только частоту 2133 МГц, ничего хорошего из этого не выйдет. Ваши высокоскоростные модули будут работать, но на частоте материнской платы — 2133 МГц;
- **коррекцию ошибок** — серверная оперативная память, в отличие от обычной «настольной» памяти, должна быть с коррекцией ошибок (ECC). Память с коррекцией ошибок может исправлять изменения одного бита в одном машинном слове. Это значит, что при чтении одного машинного слова из памяти будет

прочтено то же значение, что было до этого записано, даже если в промежутке между записью и чтением один бит был случайно изменен. Обычная оперативная память на такое не способна. Как уже было отмечено ранее, поддержка ECC есть только у серверных процессоров вроде Xeon, десктопные процессоры Core i7/9 ECC не поддерживают;

- **режим работы оперативной памяти** — это характеристика не модулей памяти, а материнской платы (лучше уточнить это в документации на нее). Например, материнская плата у вас может иметь два слота для оперативной памяти и режим работы — двухканальный (Dual-channel architecture). Следовательно, для получения полной отдачи вам нужно будет установить в нее два одинаковых модуля — одинакового стандарта, емкости и частоты и желательно одного производителя. Если вы установите один модуль емкостью 16 Гбайт, то он будет работать медленнее, чем два по 8 Гбайт.
- **наличие регистра** — если вы собираете серьезный сервер, вам нужна регистровая память (Registered DIMM, RDIMM). Модули этой памяти содержат регистр между микросхемами памяти и системным контроллером памяти. Наличие регистров уменьшает электрическую нагрузку на контроллер и позволяет установить больше модулей памяти в одном канале. Такая память стоит дороже и поддерживается не всеми материнскими платами, но, как правило, на материнских платах, предназначенных для серверов, такая поддержка есть. Также стоит заметить, что модулей RDIMM без ECC не существует, так что выбирая RDIMM, вы автоматически получаете ECC.

  Аналогично бывают материнские платы и с трехканальным, и четырехканальным режимом работы. Для работы, например, в трехканальном режиме вам потребуются три одинаковых модуля памяти, которые, возможно, нужно будет установить в определенные слоты — обычно они отмечены на материнской плате одним цветом (для уточнения этого момента лучше обратиться к документации на вашу материнскую плату). Здесь тоже могут иметь место подводные камни — например, у вас установлены три модуля по 4 Гбайт суммарным объемом 12 Гбайт. И вы хотите сделать благое дело, добавив еще один модуль, увеличив тем самым объем ОЗУ до 16 Гбайт. Однако на сервере перестанет работать трехканальный режим, и вы получите замедление скорости работы подсистемы памяти вместо ожидаемого прироста ее производительности.

Дополнительные требования к коммутационному оборудованию

Коммутационное оборудование нужно выбирать с учетом поддержки технологий, которые используются при построении инфраструктуры сети. Здесь никаких конкретных советов дать нельзя, поскольку каждое решение будет индивидуальным.

Можно разве что посоветовать покупать оборудование с поддержкой протокола SNMP (Simple Network Management Protocol, простой протокол сетевого управления). Этот протокол упростит управление оборудованием и его мониторинг. Обо-

рудование без поддержки SNMP допустимо выбирать в самых простых случаях и для самых малых предприятий.

Дополнительные требования к аварийным источникам питания

Источники бесперебойного (аварийного) питания, или, попросту, UPS-ы, должны быть оснащены сетевыми интерфейсами, по которым можно получать данные о состоянии батарей, уровне заряда и оставшемся времени автономной работы.

Состав программного обеспечения типового предприятия

Теперь рассмотрим вопросы выбора программного обеспечения. Если для инфраструктуры сети нужен индивидуальный подход, то о программном обеспечении говорить намного проще. Прикладное программное обеспечение мы обсуждать не станем — оно зависит от специфики вашего предприятия. Например, если вы не занимаетесь проектированием, то и САПР вам не нужна. Одни предприятия могут использовать популярную бухгалтерскую программу «1С:Предприятие», другие — нет. Одним предприятиям требуется CRM[1], другим — нет и т. д.

В этом разделе речь пойдет об инфраструктурном программном обеспечении. В любой информационной системе можно выделить следующие классы программного обеспечения:

- операционные системы;
- подсистемы аутентификации и контроля доступа;
- подсистемы DNS (рассмотрены в *главе 3*);
- файловые сервисы;
- средства доступа к Интернету;
- средства защиты информации: антивирусное ПО, межсетевые экраны, IDS/IPS и т. п.;
- средства резервного копирования;
- офисное программное обеспечение (как правило, офисные пакеты используют все предприятия);
- подсистему электронной почты.

Операционные системы были рассмотрены в *главе 1*, поэтому начнем сразу с подсистемы аутентификации и контроля доступа.

---

[1] CRM-система (от *англ.* Customer Relationship Management, система управления взаимоотношениями с клиентами) — прикладное программное обеспечение для организаций, предназначенное для автоматизации стратегий взаимодействия с заказчиками.

Подсистема аутентификации и контроля доступа

Для упрощения администрирования используются централизованные системы управления. При этом учетные записи пользователей хранятся на серверах, также на серверах осуществляется аутентификация и принимается решение о предоставлении доступа к тем или иным ресурсам.

В Windows-сетях задействована служба каталогов Active Directory, а в Linux-системах — OpenLDAP. В общем-то, можно Linux-сервер превратить в контроллер домена Active Directory и сэкономить немаленькую сумму на покупке лицензионного Windows Server 2022. Возможно участие Linux-систем и в домене Active Directory. Поэтому, если на вашем предприятии используются разные операционные системы, проблем с этим возникнуть не должно. Надо будет только потратить определенное время на их правильную настройку.

Подключение Linux к домену: протокол Kerberos

Linux-систему можно подключить к Windows-домену по-разному: или с применением NTLM-аутентификации, или по протоколу Kerberos. Поскольку в современных версиях Windows используется именно Kerberos, то для подключения Linux-клиентов рекомендуется задействовать именно его.

Далее мы рассмотрим настройку гипотетического Linux-клиента. В вашем дистрибутиве настройки могут быть несколько иными — например, может отличаться расположение файлов конфигурации в каталоге /etc.

Для протокола Kerberos очень важно минимальное рассогласование времени между компьютером пользователя и контроллером домена — оно не должно превышать пяти минут. Поэтому перед настройкой Kerberos следует синхронизировать время на компьютерах и проверить идентичность установленных часовых поясов.

Чтобы подключиться к домену, нужно отредактировать конфигурацию клиента Kerberos, получить билет Kerberos для учетной записи администратора и выполнить команду подключения к домену.

Настройка конфигурации клиента Kerberos

В Linux практически все можно настроить с помощью графических конфигураторов. Вот только делать это мы не рекомендуем, поскольку в каждом дистрибутиве свои конфигураторы, которые редактируют одни и те же конфигурационные файлы. Если вы привыкнете к одному дистрибутиву, вам потом в случае необходимости будет сложно перейти на другой. Когда же вы будете знать, что и в каком конфигурационном файле находится, графические конфигураторы вам вообще не понадобятся.

Файлом конфигурации Kerberos обычно является файл /etc/krb5.conf. В этом файле нужно изменить параметры доменной зоны (realm) и службы Kerberos — центра выдачи ключей KDC (Key Distribution Center):

```
[realms]
EXAMPLE.COM = {
kdc = tcp/dc1.example.com:88 tcp/dc2.example.com:88
```

```
admin_server = dc1.example.com
default_domain = example.com
}
[domain_realm]
.example.com = EXAMPLE.COM
example.com = EXAMPLE.COM

[kdc]
enable-kerberos4 = false
```

Назначения параметров, думаем, понятны по их названиям — вам нужно указать собственный домен (вместо `example.com`) и имена контроллеров домена[1]. Помните, что имена в этом файле чувствительны к регистру.

Настройка файла *nsswitch.conf*

Файл /etc/nsswitch.conf содержит список источников, которые будут использоваться для получения данных о пользователях. Обычно вам не придется изменять его содержимое, однако проверьте, чтобы было указано не только `files`, но `winbind` в каждой строке. Вот пример этого файла:

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

Получение билета Kerberos для учетной записи администратора

Отредактировав конфигурацию Linux-клиента, нужно получить билет Kerberos на Linux-компьютере для учетной записи администратора домена. Это делается командой:

```
kinit administrator@EXAMPLE.COM
```

Имя домена должно быть указано прописными буквами, а слева от символа `@` следует указать учетную запись администратора домена. Проверить полученный билет можно с помощью команды `klist`. Вы увидите параметры полученного билета, в том числе и срок его действия.

Подключение к домену

Осталось дело за малым — подключить Linux-клиент к домену Windows по протоколу Kerberos. Для этого выполните команду:

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

---

[1] В этом примере DNS-имя домена — `example.com`, а контроллеры домена имеют имена `dc1` и `dc2`.

При этом будет осуществлено подключение к домену, указанному в файле конфигурации Kerberos. Параметры `administrator` и `password` замените на реальные имя пользователя и пароль. Если вы не ошиблись и все сделали правильно, то получите сообщение об успешном подключении к домену.

Проверка подключения

Как проверить подключение? Просто просмотрите список компьютеров — членов домена — в нем вы увидите ваш Linux-клиент.

Это можно сделать как в Windows, так и в самой Linux. Сначала проверим наличие безопасного подключения с помощью команды:

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

Такой вывод команды означает, что все в порядке. Далее нужно ввести:

```
wbinfo -u
```

для отображения списка пользователей или:

```
wbinfo -g
```

для отображения списка групп.

Также следует проверить (командой `getent passwd`), что служба winbind[1] успешно получает пароли с контроллера домена — в списке паролей вы увидите записи, относящиеся к домену.

Сервер Linux в качестве контроллера домена

Операционная система Linux позволяет неплохо сэкономить деньги предприятия — на базе Linux вы можете так настроить контроллер домена, что рабочие станции Windows не заметят никакой разницы. При этом отпадет необходимость приобретать лицензионный Windows Server, стоимость которого зависит от количества рабочих станций в вашей сети.

К сожалению, такое решение практикуется не очень часто — обычно администраторы знакомы с Windows Server и не желают изучать что-либо для них новое. А зря. Учитывая стоимость Windows Server и дополнительных лицензий (например, лицензий терминального доступа), можно реально сократить расходы.

Всевозможных статей и руководств по настройке Linux в режиме контроллера домена Active Directory предостаточно, поэтому этот вопрос мы здесь рассматривать не станем.

Совместно используемые ресурсы

На любом предприятии не обойтись без общих папок с документами. В Windows для доступа к общим папкам и принтерам служит протокол SMB (Server Message

[1] Winbind — это демон («служба» в терминах Windows), работающий на клиентах Samba.

Block, блок серверных сообщений), разработанный компаниями Microsoft, Intel и IBM.

Компьютеры под управлением Linux также могут работать по протоколу SMB. Для этого в Linux имеется специальная служба — Samba. Пакет Samba входит в состав всех дистрибутивов Linux и в большинстве случаев установлен по умолчанию. Проект Samba — это не просто OpenSource-проект. К нему подключилась и Microsoft, что говорит о важности этого направления и о значимости проекта.

Для работы с общими документами, кроме общих папок, можно использовать и облачные сервисы — например, тот же Google Drive. Преимущества этого решения таковы:

- ваши документы будут доступны в любой точке земного шара, где есть соединение с Интернетом;
- вам не придется настраивать VPN-сервер для доступа мобильных клиентов к ресурсам вашей корпоративной сети;
- серверы Google «переехали» в Россию, что дает возможность использовать Google Drive даже для хранения персональных данных и прочей конфиденциальной информации;
- работать с документами, расположенными в Google Drive, можно не только из Windows или Linux, но и с мобильных устройств под управлением Android. И, вообще, получить доступ к общим документам можно через веб-интерфейс с любого устройства, на котором возможен запуск браузера;
- если вы боитесь, что к вашим данным получит доступ кто-либо посторонний, то сможете воспользоваться программами облачного шифрования.

Третье решение для доступа к общим документам — распределенная файловая система — подробно рассмотрено в *главе 10*.

Учетная запись для анонимного доступа

В Windows используется гостевая учетная запись — учетная запись **Гость**. Эта запись служит для предоставления общего доступа всем, когда ОС не контролирует права доступа. По умолчанию эта учетная запись отключена.

В Linux учетной записи **Гость** соответствует учетная запись **nobody**. По умолчанию анонимный доступ к ресурсам Linux также запрещен. Если вам нужно его разрешить, проверьте, чтобы в вашей системе существовала учетная запись **nobody**, и отредактируйте конфигурацию Samba так:

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

[share_definition]
 guest ok = yes
```

Есть и второй способ, который заключается в использовании параметра `security = share`. При этом доступ к ресурсу будет осуществляться только с параметрами гостевой учетной записи.

Работа с Windows-ресурсами в Linux

Как уже отмечалось ранее, в Linux для работы в составе домена Windows необходим пакет Samba, который часто бывает установлен по умолчанию. Если он почему-либо оказался не установлен, установить его не составит особого труда, т. к. он в любом случае входит в состав дистрибутива.

Установка пакета Samba

Следующая команда в Debian/Ubuntu устанавливает пакет Samba, поддержку протокола Kerberos и службу winbind:

```
sudo apt-get install install samba krb5-user winbind
```

После установки сервис smb настраивается на автоматическую загрузку. Управлять запуском/перезапуском службы можно с помощью команды `services`:

```
services smb start
services smb stop
services smb restart
```

Настройки Samba

Основным файлом конфигурации Samba является файл /etc/samba/smb.conf. Файл состоит из нескольких секций:

- `[globals]` — содержит глобальные настройки;
- `[homes]` — описывает домашние папки пользователей;
- `[public]` — содержит описание публичных ресурсов;
- `[printers]` — описывает сетевые принтеры.

Рассмотрим на примере практическую настройку Samba. Во-первых, поставим задачу, чтобы Linux-клиент интегрировался в домен Active Directory `EXAMPLE.COM`. Во-вторых, «расшарим» папку /var/samba так, чтобы все пользователи домена могли записывать в нее файлы, читать из нее файлы и просматривать ее содержимое. В листинге 2.1 приведен готовый пример конфигурации Samba.

Листинг 2.1. Пример конфигурации Samba

```
[global]
   # Имя рабочей группы и домена нужно указывать заглавными буквами
   workgroup = EXAMPLE
   realm = EXAMPLE.COM

   # Указываем, что авторизация будет через AD
   security = ADS
```

```
   # Пароли будем шифровать
   encrypt passwords = true

   # Прокси DNS не используется
   dns proxy = no

   # Ускоряем работу Samba
   socket options = TCP_NODELAY

   # Следующие параметры нужны, чтобы Samba
   # НЕ работала в режиме контроллера домена
   domain master = no
   preferred master = no
   os level = 0
   domain logons = no
   local master = no

   # Поддержка принтеров не нужна
   load printers = no
   show add printer wizard = no
   printcap name = /dev/null
   disable spoolss = yes

[public]
   # Описываем публичный ресурс
   comment = Public Folder
   # путь к публичному ресурсу
   path = /var/samba
   # разрешаем запись
   read only = no
   # еще раз разрешаем запись
   writable = yes
   # разрешаем гостевой доступ
   guest ok = yes
   # разрешаем просмотр содержимого каталога
   browseable = yes
```

Правильность составления файла конфигурации Samba вы можете проверить с помощью программы testparm.

Подключение к общим ресурсам

В предыдущем разделе было показано, как предоставить ресурс, находящийся на Linux-машине, в общее пользование. Здесь мы покажем, как подключиться к ресурсам, которые предоставляют Windows-машины.

Как правило, если запущен графический интерфейс, то доступ к общим ресурсам Samba осуществляется через файловый менеджер — просто нужно открыть раздел **Сеть**, выбрать в нем компьютер и общий ресурс, — все так же, как и в Windows.

Если графический интерфейс не запущен, вам следует воспользоваться командой `smbmount`, которой передать имя монтируемого ресурса, точку монтирования, имя пользователя и пароль (если нужно):

```
smbmount ресурс точка_монтирования -o username=пользователь,password=пароль
```

Подключение будет сохранено до перезагрузки системы. Обратиться к файлам ресурса можно через указанную точку монтирования.

Отобразить список доступных ресурсов определенного компьютера можно так:

```
smbclient -L hostname
```

Браузеры Интернета

В составе Windows поставляются браузеры Internet Explorer и Microsoft Edge. Браузер Internet Explorer долго считался одним из самых популярных, но это не его заслуга — своей популярностью Internet Explorer был обязан тому, что изначально поставлялся в составе Windows.

Начиная с Windows 10Windows 10, разработка браузера Internet Explorer прекращена, а ему на смену пришел Microsoft Edge. Поддержка же самого Internet Explorer в Windows 10 прекращена 15 июня 2022 года, а с 14 февраля 2023 года все ссылки в Internet Explorer стали по умолчанию перенаправлять пользователей в Microsoft Edge. Окончательно же поддержка браузера в лице его одиннадцатой версии прекратится 13 января 2032 года вместе с окончанием поддержки Windows 10 IoT Enterprise LTSC 2021.

Существует множество других бесплатных браузеров: Google Chrome, Firefox, Opera и пр. Как правило, пользователи устанавливают себе сторонние браузеры, выбор которых определяется личными предпочтениями.

Защита узлов сети

Каждый узел сети должен быть защищен от вирусов, вредоносного программного обеспечения, сетевых атак и т. п. Именно поэтому крайне важно наличие программы защиты узла. Подробно защита информации будет рассматриваться в *главе 9*, а сейчас лишь отметим, что обычно относится к функциям защиты узла:

- антивирусная защита;
- межсетевое экранирование;
- обнаружение атак (IDS, Intrusion Detection System) и/или предотвращение атак (IPS, Intrusion Prevention System);
- контроль приложений (блокировка запуска нежелательных приложений) и устройств (блокировка доступа к устройству).

В Linux используется ряд систем контроля доступа, таких как LIDS, Tomoyo, SELinux. Эти системы могут даже ограничить полномочия самого суперпользователя root. Собственно, для этого они и предназначены — на случай, если учетная запись суперпользователя окажется скомпрометированной.

Многие антивирусы для Windows-станций также сегодня включают функции межсетевого экрана и проактивной защиты (контроль запуска приложений), а некоторые содержат еще и средства обнаружения атак.

Для больших предприятий среды можно отметить и сугубо корпоративные решения — например, Symantec Endpoint Protection (рис. 2.4).

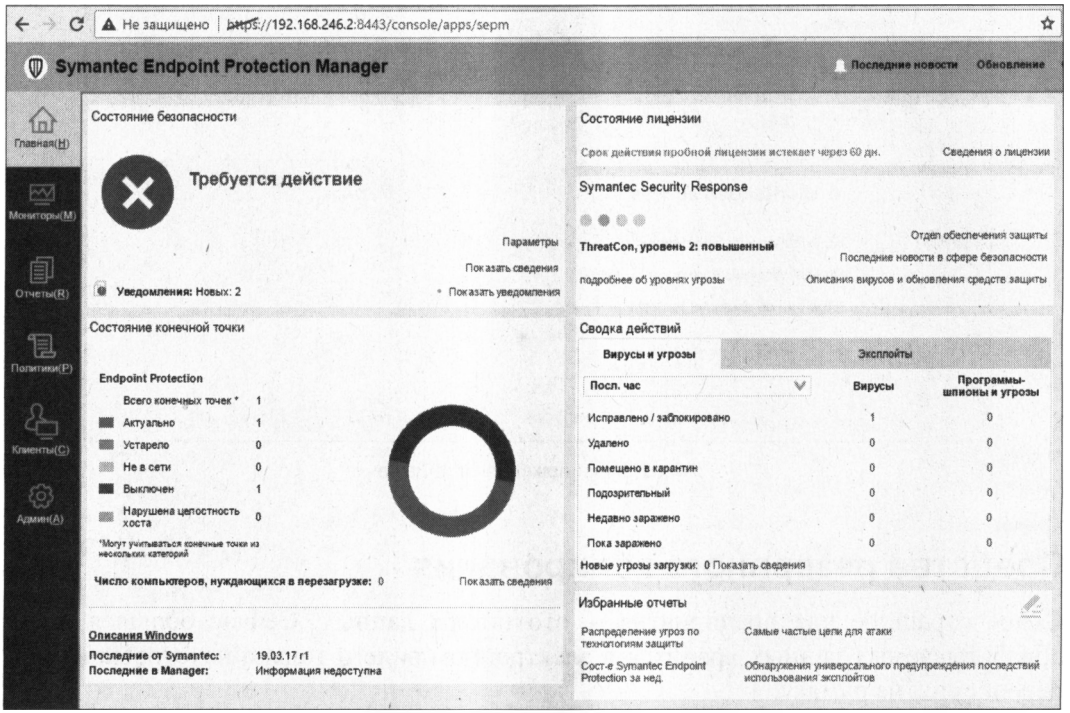


Рис. 2.4. Symantec Endpoint Protection Manager

Средства удаленного администрирования

В компаниях средних и больших размеров администратору гораздо удобнее настраивать компьютеры пользователей удаленно. Поскольку при удаленной настройке администратору не требуется лично подходить к компьютеру, это значительно повышает оперативность его работы и оптимизирует использование рабочего времени.

Для удаленного администрирования можно применять различные средства, в том числе и протокол RDP (Remote Desktop Protocol, протокол удаленного рабочего стола). Вместо широко использовавшейся ранее коммерческой программы TeamViewer, прекратившей сейчас работу в России и Белоруссии, вы можете задействовать совершенно бесплатный UltraViewer (рис. 2.5). Принцип работы UltraViewer такой же, как у TeamViewer, только платить за него не придется.

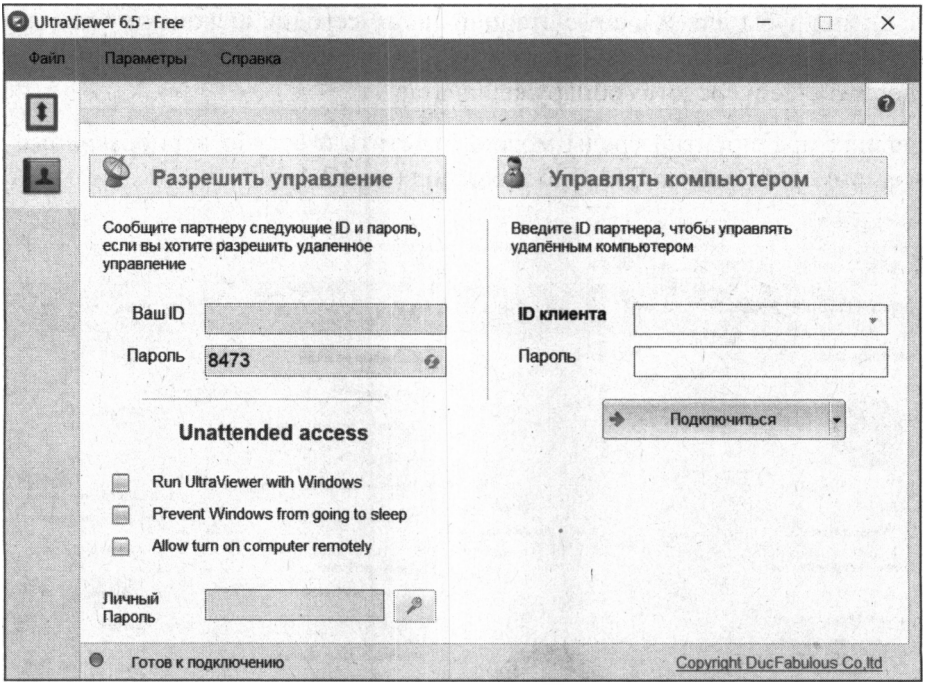


Рис. 2.5. Приложение UltraViewer

Средства резервного копирования

Самое страшное для предприятия — это потеря данных. Сейчас бóльшая часть обрабатываемых данных хранится в электронном виде и только некоторые из них переносятся на бумагу.

Именно поэтому важна система резервного копирования, которая копировала бы информацию с серверов на внешнее хранилище. Внешнее хранилище должно находиться вдали от сервера — как минимум в другом помещении. В случае пожара в серверной останутся шансы, что уцелеет сетевое хранилище.

Непосредственно для самого резервного копирования применяется различное программное обеспечение — например, Symantec NetBackup или Acronis Backup & Recovery. Не стоит забывать и о стандартных средствах Windows (рис. 2.6) — системе архивации данных Windows Server (Windows Server Backup), что позволит не тратиться на приобретение приложений сторонних разработчиков. Существует также возможность резервного копирования в облако — необходимую информацию об этом можно получить по следующей ссылке: **https://azure.microsoft.com/en-us/blog/protecting-windows-server-2016-using-azure-backup/**.

При выборе программного обеспечения резервного копирования нужно учитывать следующие его характеристики:

- **возможность восстановления всей системы с нуля и на новое оборудование** — программа резервного копирования должна позволить администратору

быстро и путем простых операций подготовить и восстановить систему на новом оборудовании. Понятно, что подобные ситуации не будут встречаться часто, но эта возможность сведет к минимуму возможные простои;

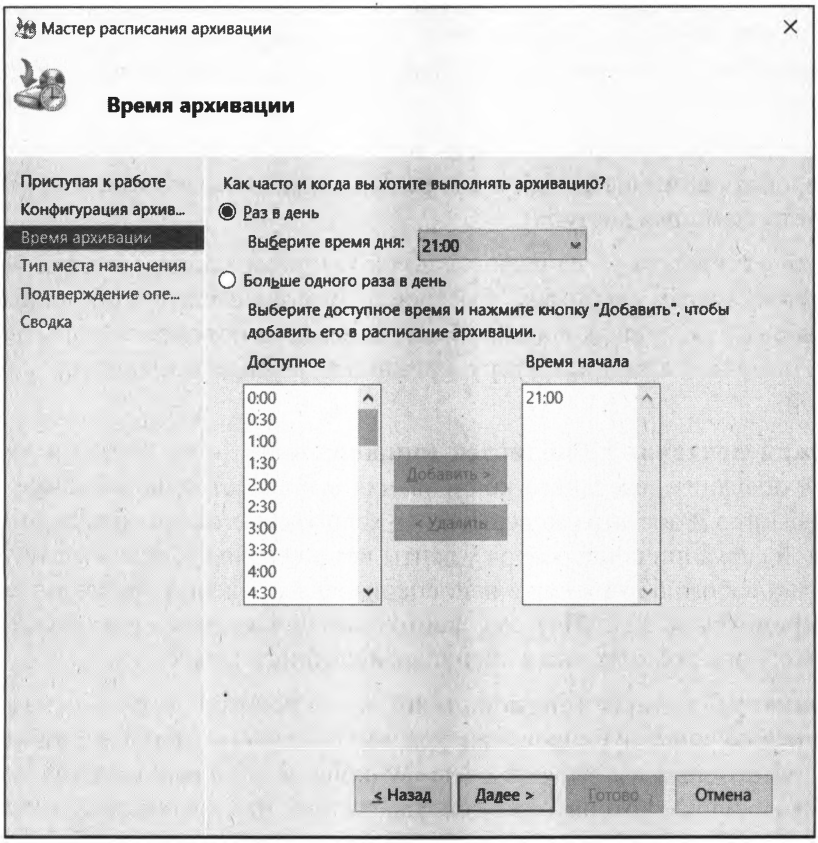


Рис. 2.6. Система архивации данных Windows Server

- **поддержка прикладных программ, эксплуатируемых на предприятии**, — корпоративная программа резервного копирования должна выполнять задачу сохранения данных для всех программ, которые используются на предприятии. Это касается серверов баз данных, почтовых программ различных производителей, ERP-систем[1], если таковые присутствуют в системе, и т. д.;
- **возможность создавать гибкий график операций** — администратор должен достаточно просто настраивать график полного и частичного резервного копирования для каждого продукта и быть уверенным, что в случае сбоя (например, временной недоступности сервера) операция будет повторена через заданные промежутки времени.

[1] ERP-система (от *англ.* Enterprise Resource Planning System, система планирования ресурсов предприятия) — это интегрированная система на базе ИТ для управления внутренними и внешними ресурсами предприятия.

Кроме того, администратор не должен выполнять несколько последовательных операций при восстановлении данных — программа должна самостоятельно объединять полные и промежуточные копии на требуемый момент времени;

- **возможность гранулярного восстановления** — на практике резервные копии данных часто используются для того, чтобы восстановить случайно удаленные пользователями отдельные файлы или вернуть информацию к предыдущему состоянию.

  Удобно, если эта функциональность доступна самим пользователям, чтобы они не привлекали администраторов для решения таких задач (конечно, с необходимым контролем прав доступа);

- **развитая отчетность** — отчетность по результатам выполнения операций является немаловажным свойством. Быстрое получение сведений об ошибках операций, о составе резервных копий, об использовании объемов устройств хранения и т. п. помогает администратору принимать верные решения по управлению системой;

- **поддержка ленточных библиотек (опционально)** — на большей части предприятий операция резервного копирования выполняется на дисковые устройства. Это быстро и достаточно дешево. Но если требуется хранить данные годами, то в такой ситуации конкурентов у ленты нет и сегодня. Однако магнитная лента требует и особого обращения с ней: специальных условий хранения, периодических перемоток и т. п. Поэтому ленточные библиотеки организуются только в крупных организациях или в специализированных целях;

- **дедупликация данных (опционально)** — технология дедупликации подразумевает исключение дублирования хранимых данных. Данные разбиваются на блоки, для которых вычисляется хеш-функция. И если выполняется попытка записи нового блока, который уже совпадает с тем, что хранится в системе (совпадают значения хеш-функций), то вместо повторной записи всех данных блока записывается только указатель на существующие в системе блоки.

  Дедупликация может сократить размер хранимых данных, особенно если по регламенту резервного копирования предприятия должно создаваться и храниться много промежуточных копий (например, если требуется сохранять ежедневные копии в течение месяца).

Такие возможности специфичны для каждого продукта.

Офисный пакет

Любому предприятию нужен пакет офисных приложений: текстовый процессор, электронная таблица, средство для создания презентаций и т. п. Наличие офисного пакета стало стандартом. При покупке ПК уже никто и не задумывается, приобретать офисный пакет или нет, — его покупают вместе с операционной системой.

Тем не менее тот же функционал можно получить совершенно бесплатно, поскольку существует множество бесплатных офисных пакетов. Самые популярные из них:

Apache OpenOffice, скачать который для Windows, Linux и macOX можно по адресу: **https://www.openoffice.org/download/**, и LibreOffice, который для тех же операционных систем предлагает скачать сайт **https://ru.libreoffice.org/**. Надо также отметить, что офисный пакет LibreOffice входит в состав большинства дистрибутивов Linux и обычно устанавливается по умолчанию вместе с установкой ОС.

По составу компонентов, поддерживаемым функциям и даже по виду интерфейса оба пакета практически идентичны и различаются лишь нюансами лицензий их поставки, впрочем, как уже подчеркивалось ранее, бесплатных, поэтому далее мы рассмотрим офисный пакет LibreOffice, в состав которого входят следующие приложения:

- текстовый процессор LibreOffice Writer (аналог Microsoft Word);
- редактор формул LibreOffice Math (в пакете Microsoft Office для этих целей используется встроенный объект Microsoft Equation);
- редактор рисунков LibreOffice Draw;
- редактор электронных таблиц LibreOffice Calc (аналог Microsoft Excel);
- редактор презентаций LibreOffice Impress (аналог Microsoft PowerPoint).

Интерфейс LibreOffice (рис. 2.7) напоминает интерфейс старого доброго Microsoft Office 2003. На наш взгляд, этот интерфейс более удобен и привычен пользователям, чем интерфейс Microsoft Office 2007/2021, и эти строки сейчас написаны именно в LibreOffice.

LibreOffice поддерживает форматы даже самого последнего MS Office 2021. Впрочем, здесь не все так гладко. Если ваши документы содержат сценарии, написанные на Visual Basic, то вам все же придется приобрести и установить MS Office.

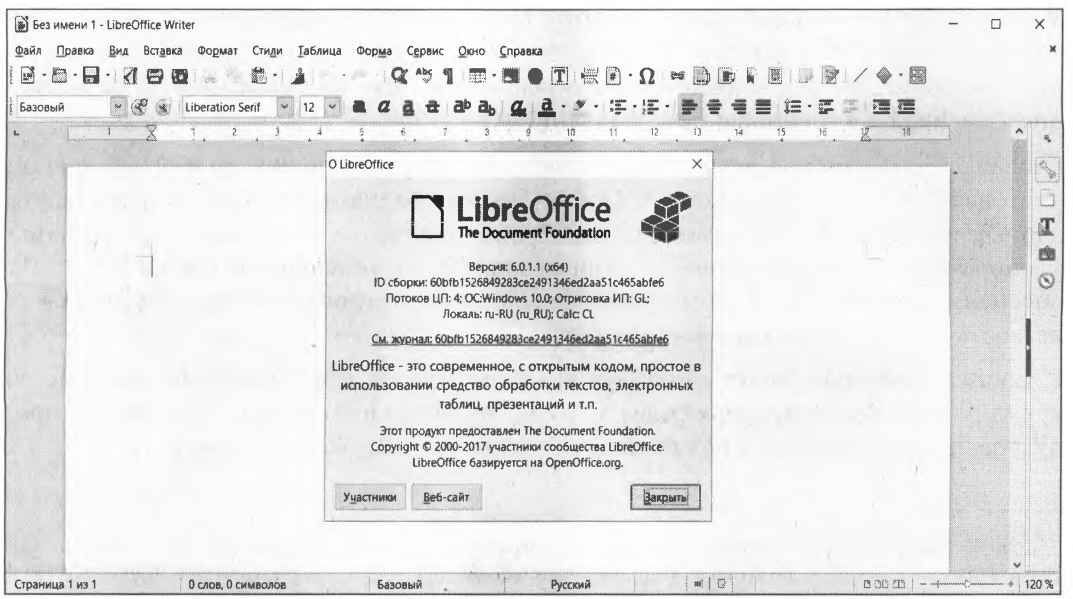


Рис. 2.7. Интерфейс LibreOffice

Электронная почта

Если для индивидуального пользователя часто достаточно почтового ящика на любом из бесплатных серверов Интернета, то серьезность предприятия проявляется и в наличии собственного почтового домена, указываемого в правой части ее электронного адреса.

Самый простой способ организации подобного почтового обслуживания заключается в размещении сервера на ресурсах интернет-провайдера. После регистрации собственного доменного имени достаточно доплатить еще небольшую сумму и оформить услугу почтового обслуживания. Преимущества такого варианта: надежность (решения провайдера выполнены в отказоустойчивом варианте), доступность из любой точки Интернета, возможность простейшей обработки сообщений (например, фильтрация спама и т. п.).

Однако в последнее время от почтового сервера ждут не только обмена сообщениями, но и поддержки функциональности организации групповой работы: наличия календаря и возможности планирования встреч, общих папок хранения сообщений и документов, единых списков контактов и т. п. Частично такой функционал можно реализовать и на бесплатных почтовых ящиках — например, в почте Gmail[1] можно вести календарь, а если в качестве клиента использовать обозреватель Google Chrome[2], то и получать на рабочий стол оповещения о предстоящих событиях и т. п. Однако более функциональными являются локальные решения, которые можно выбрать и настроить под конкретные пожелания.

Среди коммерческих решений для корпоративной работы можно отметить Lotus от IBM и Exchange Server от Microsoft.

Сервер и клиенты Lotus присутствуют в версиях как для Linux-систем, так и для Windows. Отличительной особенностью Lotus является построение продукта как распределенной базы данных. В результате, используя Lotus как транспортную систему, можно легко реализовать такие приложения, как, например, учет и регистрация входящей корреспонденции, заявлений и пр.

Exchange Server можно установить только на серверы Windows, да и его основной почтовый клиент — Microsoft Outlook — также предназначен только для стационарных и мобильных Windows-систем. Преимущество этого варианта организации корпоративного обслуживания — в интеграции всей линейки продуктов Microsoft, обеспечивающей единый интерфейс всех продуктов офиса, типовое управление и легкость обмена данными.

И Lotus, и Exchange Server — продукты коммерческие, и их внедрение часто не по карману небольшим предприятиям. В то же время существует ряд бесплатных продуктов, поддерживающих возможности групповой работы, в частности:

---

[1] Gmail (от Google Mail) — бесплатный сервис электронной почты от американской компании Google. Предоставляет доступ к почтовым ящикам через веб-интерфейс и по протоколам POP3, SMTP и IMAP.

[2] Google Chrome — браузер, разработанный компанией Google на основе свободного браузера.

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

Один из авторов этих строк уже много лет эксплуатирует в различных организациях систему корпоративной работы Zimbra Collaboration Suite Open Source Edition (ZCS). Архитектура этого продукта представлена на рис. 2.8.

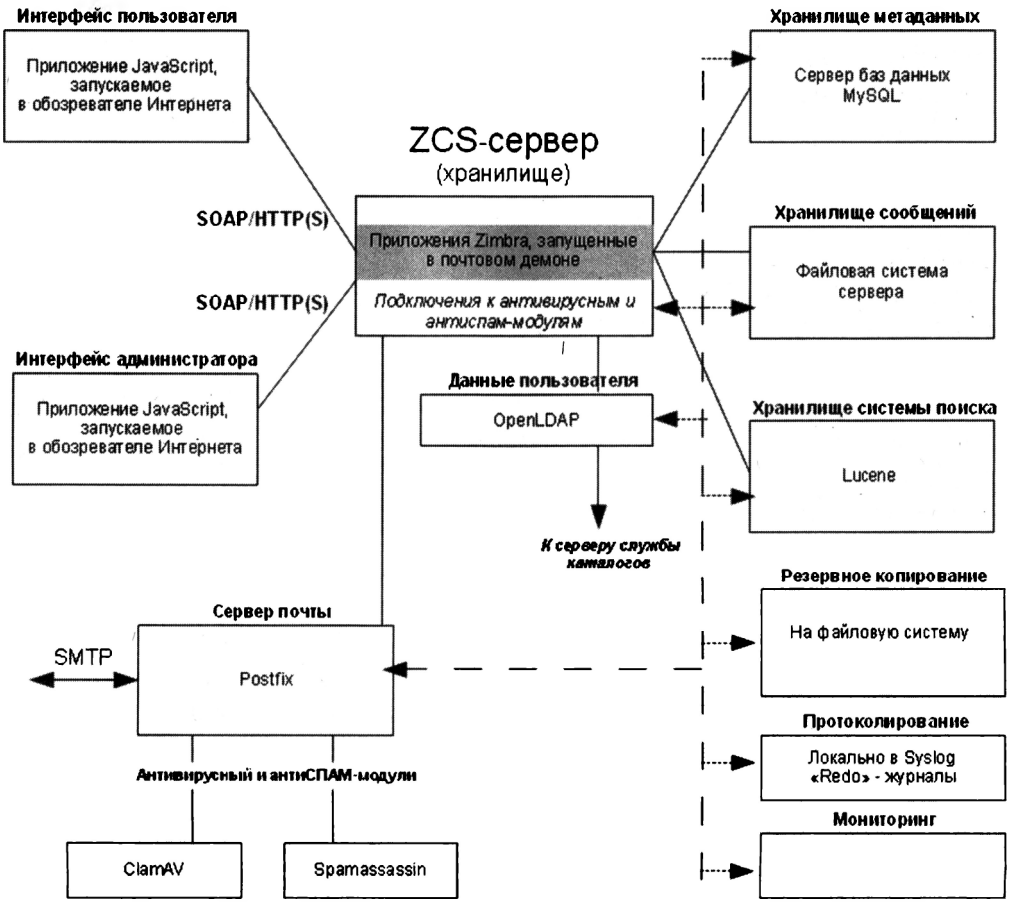


Рис. 2.8. Архитектура ZCS

В Zimbra Collaboration Suite Open Source Edition реализованы, например, следующие возможности (рис. 2.9):

- функция **Электронная почта**, позволяющая создавать и отправлять почтовые сообщения, отслеживать сообщения с помощью функции **Разговор**, присоединять вложения, осуществлять поиск сообщений и вложений по конкретным характеристикам или указанному тексту, создавать собственные папки и теги для систематизации почты, создавать фильтры для направления входящей почты по различным папкам;
- функция **Адресная книга**, позволяющая создавать собственные списки контактов и использовать контакты пользователей из службы каталогов домена Windows;
- функция **Ежедневник** с возможностью создания и управления несколькими ежедневниками, позволяющая планировать встречи и собрания, а также просматривать расписания занятости других пользователей;
- функция **Задачи**, позволяющая создавать списки задач, устанавливать их приоритеты и отслеживать выполнение;
- функция **Папки документов**, позволяющая хранить в почтовом ящике документы пользователя и предоставлять их в совместный доступ с назначением прав для конкретных пользователей;
- функция **Портфель**, позволяющая создавать документы средствами ZCS и т. д.

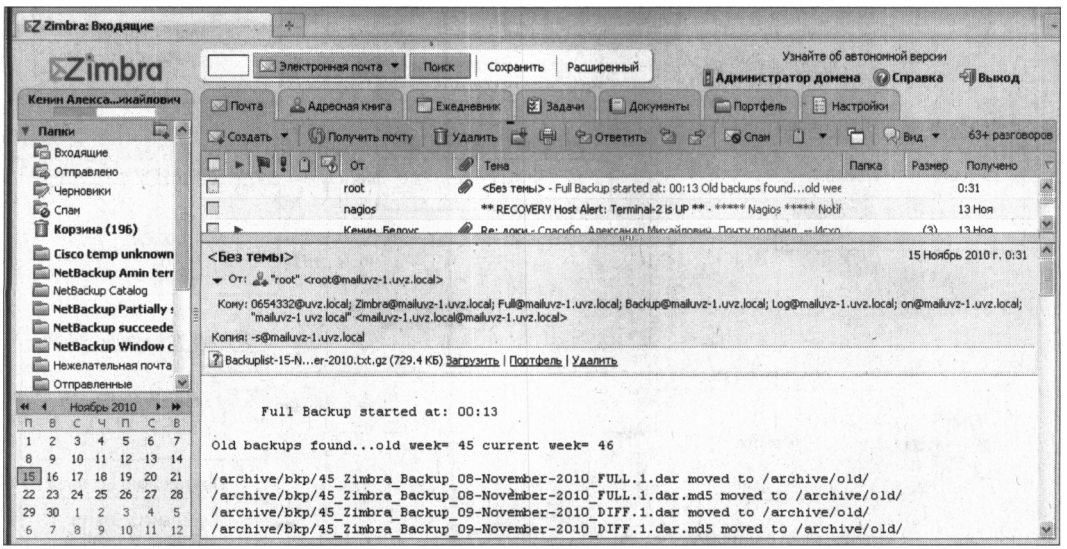


Рис. 2.9. Пример веб-интерфейса ZCS

Отметим также, что все почтовые сообщения в ZCS проверяются на сервере антивирусной программой и программой блокировки спама. И весь этот комплект функций абсолютно бесплатен!

Работать с ZCS по стандартным почтовым протоколам (POP3, IMAP, HTTP/HTTPS, SMTP/SMTPS) можно посредством любого почтового клиента.

Свободное программное обеспечение

Как уже стало понятно, совсем необязательно выбирать коммерческое программное обеспечение. Можно неплохо сэкономить, если использовать бесплатные аналоги, — никаких проблем с лицензиями и вирусами (разве что вдруг кому-то захочется скачать нелицензионные программы с пиратских ресурсов).

В табл. 2.2 приведен список некоторых бесплатных программ. В большинстве случаев свободное программное обеспечение является кросс-платформенным, т. е. существуют его версии как для Windows, так и для Linux, что позволяет сэкономить не только на прикладном программном обеспечении, но и на системном — на самой операционной системе. Вы можете установить на некоторых рабочих станциях Windows (где по условиям работы требуются программы, для которых нет Linux-аналогов), а на остальных — Linux, и при этом пользователи, несмотря на разные ОС, будут использовать одинаковое программное обеспечение: OpenOffice, Firefox, GIMP и т. д.

Таблица 2.2. *Перечень некоторых бесплатных программ для Windows*

Название и соответствующий сайт	**Описание**
LibreOffice, **https://ru.libreoffice.org/**	Популярный офисный пакет, включающий текстовый процессор, электронную таблицу, средства для создания презентаций и работы с базами данных. Является аналогом Microsoft Office и поддерживает форматы документов Microsoft Office
Firefox, **https://www.mozilla.org/ru/firefox/** Google Chrome, **https://www.google.ru/chrome/?hl=ru**	Бесплатные браузеры, являющиеся самыми популярными браузерами в мире и доступные для разных операционных систем
GIMP, **https://www.gimp.org/**	Мощный графический редактор, многие пользователи считают его аналогом Adobe Photoshop, поскольку с его помощью можно решить те же задачи
ImageBurn, **http://www.imgburn.com/** InfraRecorder, **http://infrarecorder.org/**	Бесплатные программы для записи, копирования CD- и DVD-дисков. Программы также работают с ISO-образами дисков
NanoCAD, **http://www.nanocad.ru/**	Бесплатная САПР-платформа для различных отраслей
FreeCommander, **https://www.freecommander.com/**	Двухпанельный файловый менеджер, созданный по образу и подобию широко известного в недавнем прошлом Norton Commander
7Zip, **https://www.7-zip.org/**	Архиватор, поддерживающий форматы: ARJ, CAB, CHM, CPIO, DEB, DMG, HFS, ISO, LZH, LZMA, MSI, NSIS, RAR, RPM, UDF, WIM, XAR и Z

Таблица 2.2 (окончание)

Название и соответствующий сайт	Описание
CCleaner, **https://www.ccleaner.com/ru-ru**	Очень мощная программа для чистки реестра
Avast Free Antivirus, **https://www.avast.com/** AVG, **https://www.avg.com/ru-ru/free-antivirus-download** Avira, **https://www.avira.com/ru** PCTools Antivirus, **https://us.norton.com/**	Бесплатные антивирусы, вполне способные заменить коммерческие продукты. Бесплатны не только сами программы, но и обновления антивирусных баз. Мы рекомендуем на Windows-компьютерах использовать Avast как наиболее оптимальный по производительности антивирус
ZoneAlarm, **https://www.zonealarm.com/**	Межсетевой экран для личного использования
COMODO Internet Security, **https://www.comodo.com/**	Система обеспечения безопасности, состоящая из антивируса и межсетевого экрана
PDF creator, **https://sourceforge.net/projects/pdfcreator/** PDF converter, **https://www.dopdf.com/**	Программы для конвертирования документов любого формата в формат PDF. Позволяют обойтись без программы Adobe Acrobat
Babiloo, **http://babiloo-project.org/** GoldenDict, **http://goldendict.org/**	Программы для перевода текста
Inkscape, **https://inkscape.org/**	Редактор векторной графики, способный заменить программы Illustrator, Freehand, CorelDRAW
Collabtive, **http://collabtive.o-dyn.de** dotProject, **http://www.dotproject.net** eGroupWare, **https://www.egroupware.org/en/** и др.	ПО для управления проектами. Поддерживает управление ресурсами, обмен сообщениями и т. д.
SugarCRM, **https://www.sugarcrm.com/crm/community/sugarcrm-community.html**	Бесплатная версия коммерческого пакета управления отношениями с клиентами (CRM) — лишний повод сэкономить на Microsoft Dynamics CRM
Alfresco, **https://www.alfresco.com/**	Система управления документами (Enterprise Content Management)

Базовые сведения о работе в *NIX-системах

Трудно себе представить информационную систему предприятия без серверов, работающих под управлением UNIX-подобной операционной системы. Еще бы — UNIX изначально проектировалась для серверов, и серверы работают под управлением UNIX и ее вариантов с 1971 года. Чего не скажешь ни об одной из других операционных систем.

Linux-мифы

Сообщество OpenSource (т. е. программного обеспечения с открытым и бесплатно распространяемым исходным кодом) буквально перевернуло мир информационных

технологий. И это не удивительно — современные OpenSource-программы бесплатны и по функционалу ничем не отличаются от коммерческих собратьев, код которых закрыт, вследствие чего могут возникать подозрения на наличие в таких программах всякого рода «закладок».

В этой книге не будет полного руководства по работе с Linux. Таких руководств написано немало, в том числе и авторами этой книги. Однако ранее было сказано, что системный администратор должен хотя бы поверхностно ориентироваться во всех системах и технологиях, применяемых на предприятии. Вполне вероятно, что эта книга может попасть в руки администратору, который всю жизнь работал только с серверными и настольными версиями Windows, а на обслуживаемом им предприятии используется Linux — хотя бы на сервере. Поэтому сейчас мы осуществим краткий экскурс в мир Linux.

Не нужно бояться Linux. Многие считают Windows венцом развития операционных систем только потому, что не работали с другими операционными системами. Взять ту же macOS — по мнению многих, она гораздо лучше, чем настольные версии Windows. А вы знаете, что у нее UNIX-корни? Если вы никогда не сталкивались с macOS, то будете удивлены этому факту.

В качестве серверной операционной системы UNIX появилась в конце 1960-х годов. В то время никто не знал ни о Windows, ни о macOS, ни о каких-либо других

Рис. 2.10. Веб-интерфейс Webmin

операционных системах. А вот UNIX в тех или иных инкарнациях дожила до наших дней.

Linux — несложная операционная система. В ней так же, как и в Windows, присутствуют графический интерфейс и графические конфигураторы, упрощающие процесс настройки ОС, что особенно актуально для начинающих администраторов. Продвинутые же администраторы предпочитают администрировать Linux-серверы удаленно: или по SSH, или с использованием веб-интерфейса — обычно это Webmin (рис. 2.10).

Надежность Linux и Windows

Какая система надежнее? Однозначно — Linux. Уж поверьте администраторам с многолетним опытом. Серверы на базе Linux работают по принципу: установил и забыл. Сервер может напомнить о себе лишь в случае выхода из строя «железа» — например, при отказе жесткого диска или блока питания.

Для Linux сама перезагрузка системы является нештатной ситуацией. Такое явление, как фрагментация памяти, из-за которой в некоторых других операционных системах происходит эффект торможения, в Linux практически отсутствует. Благодаря этому компьютеры под управлением Linux могут работать долгие месяцы и годы без перезагрузки. В идеале перезагрузка/выключение Linux осуществляется только в связи с обслуживанием оборудования.

Этого не скажешь о Windows, которую иногда нужно перезагружать по нескольку раз в день, чтобы она не подтормаживала. Конечно, надежность серверных версий Windows выше, чем настольных, но посмотрите на ведущих вендоров, предлагающих готовые серверные решения. Много ли вы найдете серверов, работающих под управлением Windows Server? В большинстве случаев предлагается один из вариантов Linux (Red Hat Enterprise Linux, SUSE Linux и др.) или какой-то собственный дистрибутив Linux. Так что результат, как говорится, налицо.

Конечно, при выборе ОС для сервера нужно учитывать решаемые задачи. Но об этом уже говорилось ранее.

Несколько моментов, о которых следует знать пользователям Linux

Ядро и дистрибутивы

Эта книга, как отмечалось и ранее, посвящена не Linux, но все-таки кое-что здесь будет сказано об этой операционной системе — в рамках общего развития. Если вам нужна дополнительная информация, вы сможете найти ее в Интернете или в других книгах, посвященных Linux (например, в книге Д. Колисниченко «Linux. От новичка к профессионалу» (8-е изд.) издательства «БХВ-Петербург»[1]).

[1] См. **https://bhv.ru/product/linux-ot-novichka-k-professionalu-8-izd/**.

Итак, что же представляет собой операционная система Linux? Сама Linux — это только ядро. Дистрибутив Linux — это уже и ядро, и программы. Ядро Linux — одно и то же для всех дистрибутивов, разве что могут отличаться его версии. Четные версии (2.6, 3.0 и т. д.) — стабильные, нечетные (2.5, 3.3) — экспериментальные. Экспериментальные версии предназначены только для энтузиастов, их нельзя использовать на производстве: ни на серверах, ни на рабочих станциях.

Различных дистрибутивов создано много: Fedora, CentOS, Debian, Ubuntu, OpenSUSE, Slackware, Denix, ALT Linux, Mandriva и т. д. Они появляются и «умирают» по тем или иным причинам.

Файловая система

В Linux используется собственная файловая система, и из-под Windows вы не сможете прочитать содержимое разделов Linux без установки специального программного обеспечения. Также в Linux предусмотрена строгая структура размещения информации. Например, все пользовательские файлы хранятся только в разделе /home/<имя_профиля>. Пользователь не может создать в корне диска свои папки и хранить там данные, как это можно в Windows.

Максимальная длина имени файла в Linux — 254 символа. Имя может содержать любые символы (в том числе и кириллицу), кроме следующих: / \ ? < > * « |. Но кириллицу в именах файлов Linux мы бы не рекомендовали вовсе. Впрочем, если вы уверены, что не будете эти файлы передавать Windows-пользователям (на флешке, по электронной почте), используйте для себя на здоровье. А при обмене файлами по электронной почте (кодировка-то у всех разная, поэтому вместо русскоязычного имени пользователь может увидеть абракадабру) имя файла лучше писать латиницей.

Разделение элементов пути осуществляется символом / (прямой слеш), а не \ (обратный слеш), как в Windows.

Для каждого каталога и файла вы можете задать права доступа. Точнее, права доступа автоматически задаются при создании каталога/файла, а вам при необходимости можно их изменить. Какая может быть необходимость? Например, вам нужно, чтобы к вашему файлу-отчету смогли получить доступ пользователи — члены вашей группы. Или вы создали обычный текстовый файл, содержащий инструкции командного интерпретатора. Чтобы этот файл стал сценарием, вам нужно установить право на выполнение для этого файла.

Существуют три права доступа: чтение (r), запись (w), выполнение (x). Для каталога право на выполнение означает право на просмотр содержимого каталога.

Вы можете установить разные права доступа для владельца (т. е. для себя), для группы владельца (т. е. для всех пользователей, входящих в одну с владельцем группу) и для прочих пользователей. Пользователь root может получить доступ к любому файлу или каталогу вне зависимости от прав, которые вы установили.

Чтобы просмотреть текущие права доступа, введите команду:

```
ls -l <имя файла/каталога>
```

Например,

```
ls -l video.txt
```

В ответ программа выведет следующую строку:

```
-r--r----- 1 den group 300 Apr 11 11:11 video.txt
```

В этой строке фрагмент: `-r--r-----` описывает права доступа:

- первый символ — это *признак каталога*. Сейчас перед нами файл. Если бы перед нами был каталог, то первый символ был бы символом `d` (от directory);
- последующие три символа (`r--`) определяют *права доступа владельца файла или каталога*. Первый символ — это чтение, второй — запись, третий — выполнение. Как можно видеть, владельцу здесь разрешено только чтение этого файла, запись и выполнение запрещены, поскольку в правах доступа режимы `w` и `x` не определены;
- следующие три символа (`r--`) задают *права доступа для членов группы владельца*. Права такие же, как и у владельца: можно читать файл, но нельзя изменять или запускать;
- последние три символа (`---`) задают *права доступа для прочих пользователей*. Прочие пользователи не имеют права ни читать, ни изменять, ни выполнять файл. При попытке получить доступ к файлу они увидят сообщение **Access denied**.

> ***Примечание***
>
> После прав доступа команда `ls` выводит имя владельца файла, имя группы владельца, размер файла, дату и время создания, а также имя файла.

Права доступа задаются командой `chmod`. Существуют два способа указания прав доступа: *символьный* (когда указываются символы, задающие право доступа: `r`, `w`, `x`) и *абсолютный*.

Так уж заведено, что в мире UNIX чаще пользуются абсолютным методом. Разберемся, в чем он заключается, и рассмотрим следующий набор прав доступа:

```
rw-r-----
```

Этот набор предоставляет владельцу право чтения и модификации файла (`rw-`), запускать файл владелец не может. Члены группы владельца могут только просматривать файл (`r--`), а все остальные пользователи не имеют вообще никакого доступа к файлу.

Теперь разберем отдельный набор прав — например, для владельца: `rw-`.

Чтение разрешено — мысленно записываем 1, запись разрешена — запоминаем еще 1, а вот выполнение запрещено, поэтому запоминаем 0. Получается число 110. Если из двоичной системы перевести число 110 в восьмеричную, получится число 6. Для перевода можно воспользоваться табл. 2.3.

Аналогично произведем разбор прав для членов группы владельца. Получится двоичное 100, т. е. восьмеричное 4. С третьим набором (`---`) все вообще просто — это 000, т. е. 0.

Таблица 2.3. Преобразование чисел из двоичной системы в восьмеричную

Двоичная система	Восьмеричная система	Двоичная система	Восьмеричная система
000	0	100	4
001	1	101	5
010	2	110	6
011	3	111	7

Записываем полученные числа в восьмеричной системе в порядке: владелец-группа-остальные. Получится число 640 — это и есть абсолютный вариант записи прав доступа. Для того чтобы установить эти права доступа, выполните команду:

```
chmod 640 <имя_файла>
```

Наиболее популярные права доступа:

- 644 — владельцу можно читать и изменять файл, остальным пользователям — только читать;
- 666 — читать и изменять файл можно всем пользователям;
- 777 — всем можно читать, изменять и выполнять файл.

Иногда символьный метод оказывается проще. Например, у нас есть файл script, который нужно сделать исполнимым, — для этого можно применить команду:

```
chmod +x script
```

Для того чтобы снять право выполнения, указывается параметр `-x`:

```
chmod -x script
```

Подробнее о символьном методе вы сможете прочитать в руководстве по команде `chmod`, выполнив в терминале Linux команду: `man chmod`.

Монтирование файловой системы

В Windows стоит вам открыть Проводник, и вы сразу же увидите все файловые системы вашего ПК — как стационарных жестких дисков, так и сменных носителей. Исключения составляют ситуации, когда одна из файловых систем скрыта посредством реестра.

В Linux, чтобы увидеть содержимое файловой системы, отличной от корневой, ее сначала нужно *подмонтировать*. В результате монтирования файловая система станет доступной через *точку монтирования* — специальный каталог, указанный при монтировании. Монтирование осуществляется или вручную (с помощью команды `mount`), или при загрузке системы (через файл /etc/fstab и файлы конфигурации systemd), или автоматически (с помощью демона `automountd` или аналогичного). Обычно файловая система монтируется к одному из подкаталогов каталога /mnt (или /media — для съемных носителей в некоторых дистрибутивах), но изменив или

параметр команды `mount`, или конфигурационные файлы средства автоматического монтирования, вы можете подмонтировать ее к любому другому каталогу.

Консоль и графический режим

По умолчанию в современных дистрибутивах при входе в систему запускается графический менеджер регистрации, в окне которого требуется указать имя пользователя и пароль.

После этого загрузится установленная в вашем дистрибутиве по умолчанию графическая среда — обычно это KDE или GNOME. Конечно, может быть загружена и какая-либо другая графическая среда по вашему выбору. Для этого надо нажать соответствующую кнопку выбора типа сеанса, имеющуюся в окне регистрации. В зависимости от дистрибутива она может называться **Тип сеанса** или **Сеанс** (в Fedora и некоторых других дистрибутивах), а может быть представлена графической пиктограммой или списком.

Несмотря на то что Linux запустилась в графическом режиме, в любое время вы можете перейти в консоль. Для этого нажмите клавиатурную комбинацию <Ctrl>+<Alt>+<F*n*>, где *n* — номер консоли (от 1 до 6). То есть чтобы перейти на первую консоль, нужно нажать <Ctrl>+<Alt>+<F1>, на вторую — <Ctrl>+<Alt>+ +<F2> и т. д. Обратите внимание, что так можно перейти в консоль только из графического режима. Если вы уже находитесь в консоли, то для переключения между консолями служат комбинации клавиш <Alt>+<F1> ... <Alt>+<F6>, а также <Alt>+<F7> — для возврата в графический режим.

При вводе команд (как в консоли, так и в терминале — графическом эмуляторе консоли) работает автоматическое дополнение команды. Вам нужно ввести начальные буквы команды и нажать клавишу <Tab>, после чего система предложит вам доступные варианты. Набор команд зависит от установленного программного обеспечения и на разных компьютерах может быть различным.

Команды в Linux, как и имена файлов, чувствительны к регистру, т. е. команды `CP` и `cp` — это разные команды.

Пользователь root

Linux, как и UNIX, является многозадачной многопользовательской операционной системой. Это означает, что в один момент с системой могут работать несколько пользователей и каждый пользователь может запустить несколько приложений.

Пользователь root обладает в системе максимальными полномочиями — система полностью подвластна этому пользователю. Любая его команда будет безоговорочно выполнена системой. Поэтому работать под именем пользователя root нужно с осторожностью. Всегда думайте о том, что собираетесь сделать. Если вы дадите команду на удаление корневой файловой системы, система ее выполнит. Если же вы попытаетесь выполнить определенную команду, зарегистрировавшись под именем обычного пользователя, система сообщит вам, что у вас нет на это полномочий.

Структура папок Linux

Файловая система любого дистрибутива Linux содержит следующие каталоги:

- / — корневой каталог;
- /bin — содержит стандартные программы Linux (`cat`, `cp`, `ls`, `login` и т. д.);
- /boot — каталог загрузчика, содержит образы ядра и Initrd (RAM-диска инициализации), может содержать конфигурационные и вспомогательные файлы загрузчика;
- /dev — содержит файлы устройств;
- /etc — содержит конфигурационные файлы системы;
- /home — содержит домашние каталоги пользователей;
- /lib — библиотеки и модули;
- /lost+found — восстановленные после некорректного размонтирования файловой системы файлы и каталоги;
- /media — в некоторых дистрибутивах содержит точки монтирования сменных носителей (CD-, DVD-, USB-накопителей). Хотя файловые системы сменных дисков могут монтироваться и к другим каталогам;
- /misc — может содержать все что угодно, равно как и каталог /opt;
- /mnt — обычно содержит точки монтирования;
- /opt — некоторые программы устанавливаются в этот каталог, хотя в последнее время такие программы встречаются все реже и реже;
- /proc — каталог псевдофайловой системы procfs, предоставляющей информацию о процессах;
- /root — каталог суперпользователя root;
- /sbin — каталог системных утилит, выполнять которые имеет право пользователь root;
- /tmp — каталог для временных файлов;
- /usr — содержит пользовательские программы, документацию (папка /usr/share/doc), исходные коды программ и ядра (папка /usr/src);
- /var — постоянно изменяющиеся данные системы — например, очереди системы печати, почтовые ящики, протоколы, замки и т. д.

Текстовые редакторы: vi и другие

Из первых версий UNIX в современные системы перекочевал текстовый редактор vi. То, что ему больше пятидесяти лет, видно сразу. Более неудобного редактора нам не встречалось! Согласны, что тогда это был прорыв, но сегодня редактор смотрится уж очень архаично.

Некоторые гурманы (мы бы их назвали мазохистами) говорят, что к нему нужно привыкнуть. Может и так, но сначала следует изучить длинную инструкцию (man)

и выучить наизусть команды редактора. Как такового интерфейса пользователя у этого редактора практически нет, можно сказать, что вообще нет — то, что есть, сложно назвать интерфейсом. Однако в этой книге мы рассмотрим vi, хотя бы вкратце. Тому есть две причины. Первая — это критики. Мол, как это в книге, посвященной системному администрированию, не будет «классики». Вторая — некоторые системы, где по непонятным нам причинам до сих пор используется по умолчанию vi, а другие редакторы недоступны. Да, можно изменить переменную окружения `EDITOR`, но нет никакой гарантии, что в системе будет установлен какой-нибудь другой редактор.

Итак, приступим к рассмотрению редактора vi. Он может работать в трех режимах:

- основной (визуальный) режим — в нем и осуществляется редактирование текста;
- командный режим — в нем выполняется ввод специальных команд для работы с текстом (если сравнивать vi с нормальным редактором, то этот режим ассоциируется с меню редактора, где есть команды вроде «сохранить», «выйти» и т. д.);
- режим просмотра — предназначен только для просмотра файла (если надумаете использовать этот режим, вспомните про команду `less`).

После запуска редактора вы можете переключать режимы (как — будет сказано позже), но выбрать режим можно и при запуске редактора:

```
vi файл
vi -e файл
vi -R файл
```

Первая команда запускает vi и загружает файл. Вторая команда запускает vi в командном режиме и загружает файл. Третья команда — это режим просмотра файла. Если указанный файл не существует, то он будет создан. По умолчанию активируется именно командный режим, поэтому в ключе `-e` нет смысла.

После запуска vi главное — знать, как из него выйти. Ведь в нем не будет знакомой строчки меню, редактор также не станет реагировать на привычные комбинации клавиш вроде <Alt>+<X> или <Ctrl>+<C>. На рис. 2.11 представлен редактор vi, в который загружен файл /etc/passwd.

В табл. 2.4 приведены основные команды редактора vi. Команды, которые начинаются с двоеточия, будут отображены в нижней строке окна редактора, остальные просто выполняются, но не отображаются. Как уже было отмечено, у редактора vi есть два основных режима (режим просмотра не считается): режим команд и режим редактирования (визуальный). Переключение в режим команд осуществляется нажатием клавиши <Esc>. Нажатие клавиш <i>, <a> и др. переключает редактор в режим вставки, когда набираемые символы трактуются именно как символы, а не как команды. Для переключения обратно в командный режим служит клавиша <Esc>. В некоторых случаях (например, когда вы пытаетесь передвинуть курсор левее первого символа в строке) переход в командный режим осуществляется автоматически.

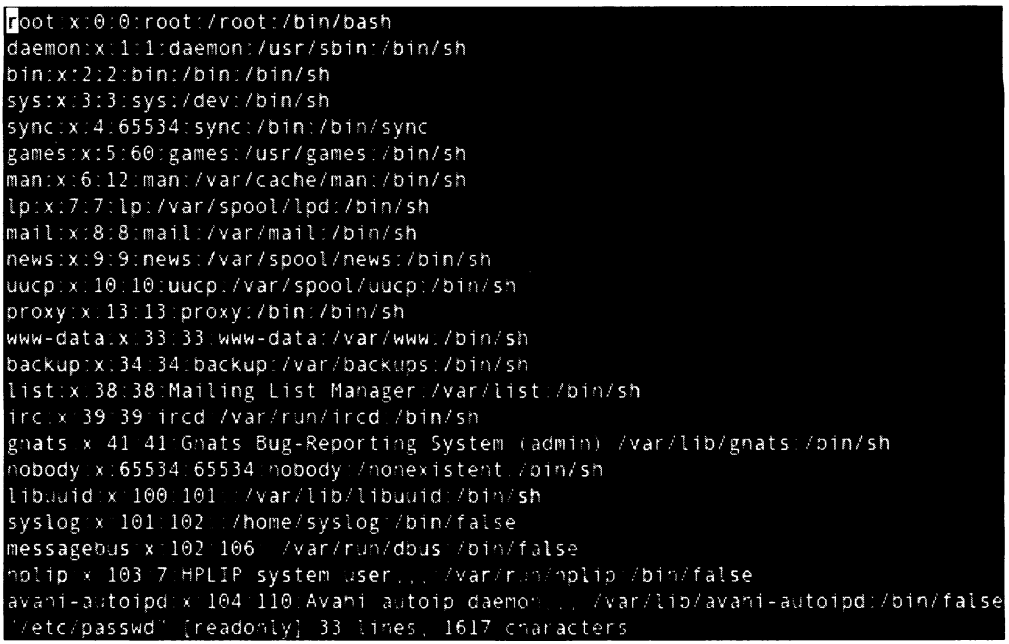


Рис. 2.11. Текстовый редактор vi

Таблица 2.4. *Основные команды редактора vi*

Команда	Описание
:q!	Выход без сохранения
:w	Сохранить изменения
:w <*файл*>	Сохранить изменения под именем <*файл*>
:wq	Сохранить и выйти
:q	Выйти, если нет изменений
i	Перейти в режим вставки символов в позицию курсора
a	Перейти в режим вставки символов в позицию после курсора
o	Вставить строку после текущей
O	Вставить строку над текущей
x	Удалить символ в позицию курсора
dd	Удалить текущую строку
u	Отменить последнее действие

Теперь немного практики — введите команду:

```
$ vi file.txt
```

Далее нажмите клавишу <i>, чтобы переключиться в режим вставки. Наберите любой текст, но постарайтесь не ошибиться, поскольку исправление ошибок в vi — дело, требующее отдельного разговора.

Затем нажмите клавишу <Esc> и введите `:wq`. После выхода из редактора введите команду:

```
cat file.txt
```

Так вы убедитесь, что файл создан и в нем сохранен введенный вами текст.

Продолжим изучать редактор. Если ввести не команду `i`, а команду `a`, то вы тоже перейдете в режим вставки, но с одним отличием — введенный текст будет вставляться не перед символом, в котором находится курсор, а после него. Также в режим вставки можно перейти командами `o` и `O`. В первом случае будет добавлена пустая строка после текущей строки, а во втором — перед текущей строкой, а весь дальнейший ввод будет восприниматься именно как ввод текста, а не команд.

Чтобы удалить символ, нужно перейти в режим команд и над удаляемым символом нажать клавишу <x>. Да, клавиши <Backspace> и <Delete> тут не работают. Точнее, <Backspace> работает, но для удаления последней непрерывно введенной последовательности символов. Например, у вас есть текст: `vi - текстовый редактор`. Пусть вы перейдете в режим вставки и измените текст так: `vi - неудобный текстовый редактор`. Нажатие клавиши <Backspace> удалит слово `неудобный`, но не сможет удалить дефис и другие символы.

Чтобы удалить строку, в которой находится курсор, нужно выполнить команду `dd`. Помните, что vi считает строкой не то, что вы видите на экране, а последовательность символов до первого символа новой строки (`\n`). Если строка длиннее 80 символов, то она переносится на две экранные строки и визуально выглядит как две строки, а не как одна.

Чтобы перейти в конец строки (клавиши <Home> и <End> тоже не работают, как вы успели заметить, если уже запускали vi), нужно ввести команду `$`. При навигации курсор перемещается не по экранным линиям, а как раз по строкам текста.

Для отмены последней операции служит команда `u`. Вот только истории изменений нет, да и по команде `u` отменяется вся предыдущая команда целиком. Например, вы создали файл, перешли в режим вставки (команда `i`) и набрали весь текст Большой медицинской энциклопедии. Если вы введете команду `u`, то она отменит всю предыдущую команду, т. е. удалит весь введенный вами текст. Так что будьте осторожны.

Азы vi мы вам преподали. Но не думаем, что вы будете им пользоваться. Если есть желание продолжить знакомство, введите команду:

```
man vi
```

А мы тем временем познакомимся с другими текстовыми редакторами. Самый удобный из известных нам текстовых редакторов — редактор nano (раньше он назывался pico и входил в состав почтового клиента pine).

Внизу (под текстом) есть подсказка по комбинациям клавиш для управления редактором. Символ `^` означает <Ctrl>. То есть для выхода из редактора нужно нажать комбинацию клавиш <Ctrl>+<X>, а для сохранения текста — <Ctrl>+<O>.

В некоторых системах (например, в FreeBSD) вместо nano используется редактор ee. Он похож на nano, однако подсказки выводятся до текста (вверху экрана), а не после него, но идея та же. Также достаточно удобен редактор joe.

В пакет mc (файловый менеджер) входит довольно-таки удобный редактор mcedit, который запускается при нажатии в mc клавиши <F4>. Но вы можете запустить редактор отдельно:

```
mcedit <имя файла>
```

Кстати, редакторы joe, nano и ee запускаются аналогично:

```
joe <имя файла>
nano <имя файла>
ee <имя файла>
```

Выполнение команд с правами другого пользователя

Запустить любую команду с привилегиями root позволяет команда `sudo`. Использовать ее нужно так:

```
sudo <команда_которую_нужно_выполнить_с_правами_root>
```

Например, вам необходимо изменить файл /etc/apt/sources.list. Для этого следует отдать команду:

```
sudo gedit /etc/apt/sources.list
```

> ***Пояснение***
>
> Программа gedit — это тоже текстовый редактор, мы ему передаем один параметр — имя файла, который нужно открыть.

Если ввести эту же команду, но без `sudo` (просто: `gedit /etc/apt/sources.list`), текстовый редактор тоже запустится и откроет файл, но сохранить изменения вы не сможете, поскольку у вас не хватит полномочий.

Программа `sudo` перед выполнением указанной вами команды запросит у вас пароль:

```
sudo gedit /etc/apt/sources.list
Password:
```

Вы должны ввести свой *пользовательский пароль* — тот, который применяете для входа в систему, но не пароль пользователя root (кстати, мы его и не знаем).

> ***Примечание***
>
> Использовать команду `sudo` имеют право не все пользователи, а только те, которые внесены в файл */etc/sudoers*. Администратор системы (пользователь root) может редактировать этот файл с помощью команды `visudo`. Если у вас дистрибутив, который запрещает вход под учетной записью root (следовательно, у вас нет возможности отредактировать файл *sudoers*), то в файл *sudoers* окажутся внесены пользователи, которых вы добавили при установке системы.

Команда `su` позволяет получить доступ к консоли root любому пользователю (даже если пользователь не внесен в файл /etc/sudoers) при условии, что он знает пароль

root. Понятно, что в большинстве случаев этим пользователем будет сам пользователь root — не будете же вы всем пользователям доверять свой пароль? Поэтому команда `su` предназначена в первую очередь для администратора системы, а `sudo` — для остальных пользователей, которым иногда нужны права root (чтобы они меньше отвлекали администратора от своей работы).

Использовать команду `su` просто:

```
su
```

После этого надо будет ввести пароль пользователя root, и вы сможете работать в консоли как обычно. Использовать `su` удобнее, чем `sudo`, потому что вам не придется вводить `su` перед каждой командой, которая должна быть выполнена с правами root.

Прикладные программы в Linux

В Windows программное обеспечение устанавливается с помощью мастера установки — программы setup.exe или install.exe. Мастер установки свой для каждой программы, т. е. программа setup.exe, предназначенная для установки MS Office, не установит Photoshop.

В Linux все иначе. Здесь используются два основных способа установки программного обеспечения:

- с помощью пакетов;
- из исходных кодов.

Пакет содержит все необходимое для установки программы. Существуют два основных типа пакетов:

- RPM-пакеты — применяются во всех Red Hat-совместимых дистрибутивах (Red Hat, Fedora, CentOS, Mandrake, Mandriva, ALT Linux, ASPLinux и др.);
- DEB-пакеты — применяются в дистрибутиве Debian и в дистрибутивах, основанных на Debian (Ubuntu, Kubuntu, Edubuntu, Denix и др.).

Пакеты хранятся в хранилищах — репозиториях. Репозиторий может быть локальным — например, каталогом на жестком диске или на DVD, или же сетевым — сервером в Интернете или в локальной сети, содержащим соответствующие пакеты. Для чего создаются репозитории? Для централизованного управления обновлением пакетов. Представьте, что у нас нет репозиториев. Тогда, чтобы узнать, вышла ли новая версия нужной вам программы, вам пришлось бы посещать сайт ее разработчика или как минимум сайт разработчика дистрибутива Linux. А это не очень удобно. Один-другой раз вы можете забыть проверить наличие обновлений, а потом вам вообще надоест это делать. Проще дождаться выхода новой версии дистрибутива и обновить все программы за один раз.

Так и было раньше. Вот вышла программа, ее включили в состав дистрибутива, но полностью не протестировали (протестировать все невозможно). Потом оказалось, что программа работает неправильно, но только при определенных условиях, например с определенным форматом файла. Или же Linux была установлена на

сервер и организованы сетевые службы — например, тот же веб-сервер. Через некоторое время обнаружилось, что в этой версии веб-сервера имеется «дыра», поэтому вскоре выпустили новую версию. Пользователь, установивший программу из дистрибутива, ничего не подозревая о том, что вышла новая ее версия, мог бы мучаться минимум полгода или даже год — до выхода следующей версии дистрибутива. А его сервер могли бы взломать уже на следующий день после обнаружения «дыры». Но не тут-то было. Разработчики Linux, заботясь о нас с вами, создали репозитории. И с помощью репозиториев можно быстро и удобно отслеживать обновления тех или иных пакетов. Причем это делает сам менеджер пакетов, а вам лишь остается указать, какие обновления нужно загружать, а какие — нет.

Практически все системы управления пакетами современных дистрибутивов поддерживают хранилища пакетов.

Для установки пакета нужно выполнить одну из следующих команд:

```
# Debian-совместимые дистрибутивы, в том числе Ubuntu
apt-get install <название пакета>
# Fedora, CentOS
yum install <название пакета>
# OpenSUSE
zypper install <название пакета>
```

Дополнительную информацию об этих командах вы можете получить или в справочной системе (команда `man`), или в уже упоминавшейся книге «Linux. От новичка к профессионалу» (7-е изд).

Кросс-платформенный запуск программ

Windows-программы в Linux, увы, просто так не запустишь. Однако способы использования Windows-программ в Linux есть, даже два. Первый заключается в установке виртуальной машины VirtualBox, в которой будет инсталлирована Windows, а в ней, в свою очередь, установлена необходимая программа. При этом виртуальную машину можно настроить так, чтобы она могла взаимодействовать с реальной сетью и получать доступ к ресурсам физической машины и других рабочих станций по сети.

У такого способа есть и преимущества, и недостатки. К преимуществам можно отнести то, что он будет работать в любом случае и подойдет для программ, которые нельзя запустить в Linux другими способами. В общем, универсальный способ запуска программ. Правда, зачем тогда нужна Linux, ведь так?

А недостатки:

- не следует забывать о необходимости законного приобретения ОС Windows, работающей в виртуальной машине;
- виртуальная машина потребляет весьма много ресурсов, поэтому вряд ли производительность Windows-программы, работающей в виртуальной машине, вам понравится.

Второй, наиболее распространенный способ запуска Windows-программ из-под Linux — это использование эмулятора Wine, который входит в состав многих дистрибутивов, а в некоторых даже установлен по умолчанию. Преимущества такого решения очевидны:

- достойная производительность — Windows-программа работает быстрее, чем в виртуальной машине;
- нет нужды лицензировать Windows, поскольку она не требуется для запуска Windows-программы из-под Linux с помощью Wine.

Есть и недостатки:

- далеко не все программы запускаются в Wine (особенно сложно с запуском игр);
- некоторые программы могут работать некорректно;
- некоторые программы могут иметь проблемы с отображением русских шрифтов.

Справедливости ради нужно отметить, что существует также возможность запуска Linux-программ в Windows. Если вы этим заинтересовались, нужную информацию найдете в Интернете.

Установка Linux

Раньше, скажем, лет 20 назад, чтобы установить Linux, нужно было быть настоящим компьютерным гуру. Сейчас же все операции выполняются в графической

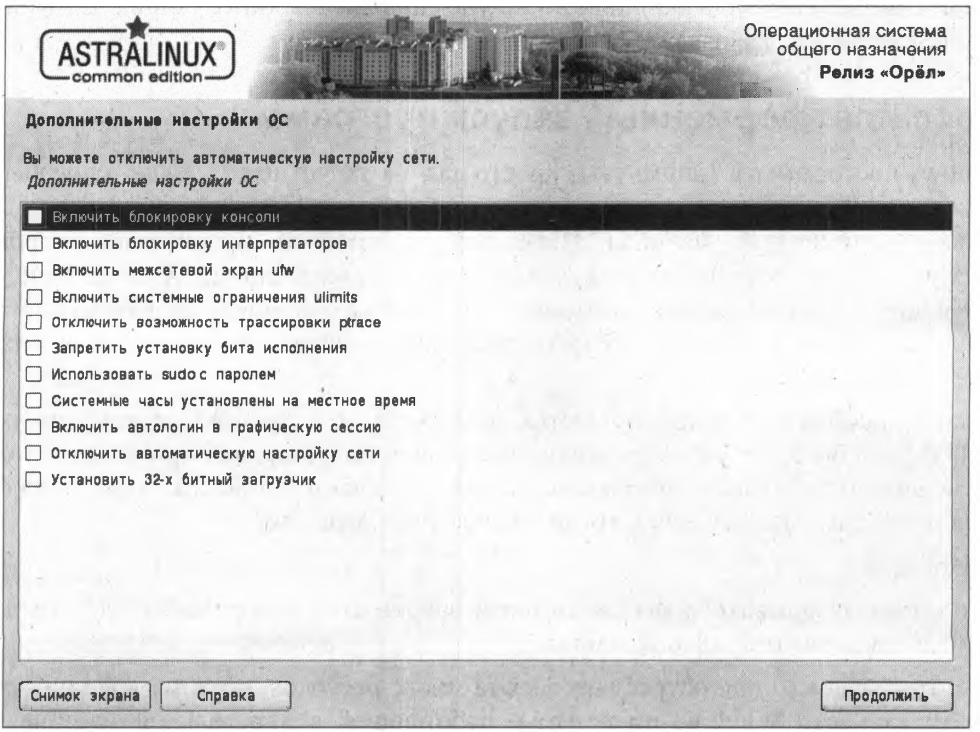


Рис. 2.12. Установка Astra Linux

среде с помощью мастера установки, который сначала запрашивает основные параметры системы, помогает выполнить разметку жесткого диска, а потом сам устанавливает ОС (на рис. 2.12 представлена программа установки дистрибутива Astra Linux, которая как две капли воды похожа на инсталлятор Debian). В большинстве случаев установка Linux не вызывает проблем и каких-либо сложностей.

Загрузка нескольких операционных систем

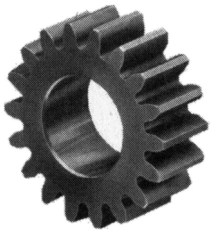
На одном компьютере можно установить несколько ОС, при этом каждая ОС устанавливается в собственный раздел жесткого диска. Как правило, если на компьютере уже установлена Windows, можно без проблем установить еще и Linux. Программа установки Linux может «отрезать» от одного из логических дисков Windows свободное пространство (причем эта операция осуществляется без потери данных) и на этом месте создать разделы Linux.

В процессе установки Linux в главную загрузочную запись (MBR) компьютера будет установлен загрузчик GRUB2, позволяющий загружать как Linux, так и Windows.

Если вы конфигурируете новый компьютер, то сначала следует установить Windows, а уже потом — Linux. Дело в том, что инсталлятор Windows принципиально ничего не хочет знать о других операционных системах, и загрузчик Windows, если ее устанавливать после Linux, просто перезапишет загрузчик Linux в MBR, в результате чего загружаться станет только одна операционная система — Windows.

Тестирование Linux на виртуальной машине

Если вы ни разу не работали с Linux, но очень хочется попробовать, а желания (возможности) установить ее на реальный компьютер нет, можно воспользоваться виртуальной машиной. В качестве виртуальной машины лучше всего выбрать или VMware Workstation, или Oracle VirtualBox — в этих виртуальных машинах Linux работает без проблем.



ГЛАВА 3

Структура сети

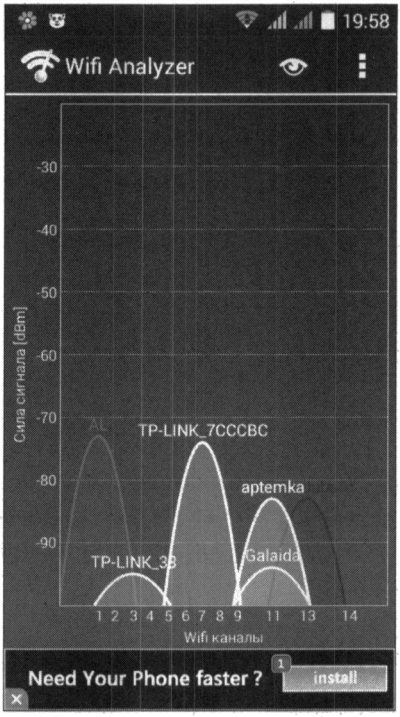
Информационная система не может существовать без сети — каналов связи. А от их качества зависит стабильность работы бизнес-приложений. В этой главе рассмотрена структура сети и даны некоторые рекомендации относительно ее организации.

Структурированные кабельные сети

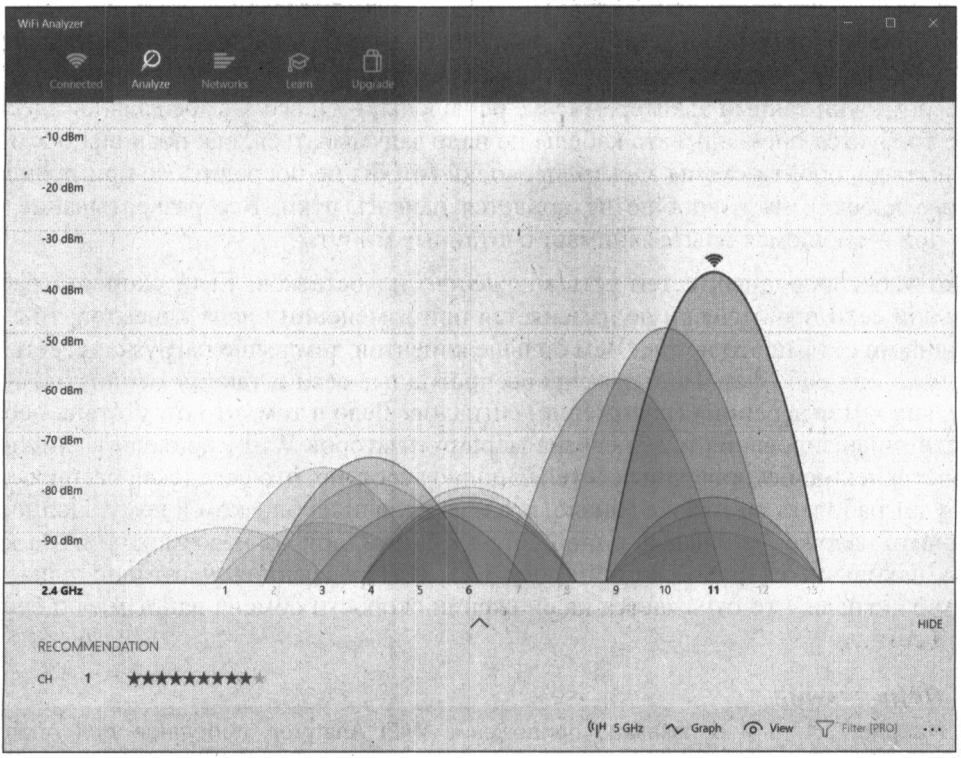
На небольших предприятиях сейчас все чаще организуются беспроводные сети на основе протоколов Wi-Fi. Спору нет, такие сети очень удобны: установить маршрутизатор Wi-Fi, настроить его, подключить адаптеры Wi-Fi к стационарным компьютерам (ноутбуки такими адаптерами уже оснащены) — и все. Самое главное здесь то, что не требуется прокладывать кабель, не надо задумываться, как правильно это сделать, пытаясь обойти схемы электропроводки (чтобы не повредить ее при прокладке сетевого кабеля), да и вообще не придется пачкать руки. Все развертывание сети Wi-Fi при имеющемся опыте занимает считанные минуты.

Однако у беспроводных сетей есть множество недостатков. Если скорость работы кабельной сети практически не изменяется при изменении числа клиентов, то с беспроводными сетями это не так. Чем больше клиентов, тем выше нагрузка на сеть, тем медленнее она работает. Подвержены беспроводные сети и такому неприятному эффекту, как интерференция (наложение) сигналов. Дело в том, что отсутствие необходимости лицензирования и дешевизна маршрутизаторов Wi-Fi привели к широкому распространению беспроводных сетей. Вполне вероятно, что соседская беспроводная сеть будет работать на том же канале, что и ваша, или на близком к нему. Полностью исключить наложение сигнала одной сети на сигнал другой невозможно из-за количества находящихся рядом сетей (рис. 3.1). Интерференция негативно влияет на качество сигнала, что отражается на снижении скорости обмена данными по беспроводной сети.

> ***Примечание***
>
> На рис. 3.1, *а* и *б* показано приложение WiFi Analyzer, доступное для Android и Windows 10, — соответственно его можно загрузить из Google Play и из магазина приложений Microsoft. К сожалению, для iPhone и macOS такого приложения не существует.



а



б

Рис. 3.1. Наложение сигналов беспроводных сетей: *а* — приложение WiFi Analyzer для Android; *б* — WiFi Analyzer для Windows 10

Безопасность беспроводных сетей также находится под вопросом. Появились сведения, что технология шифрования WPA2 уже не справляется со своей функцией, и данные, передаваемые по беспроводному соединению, защищаемому WPA2, можно перехватить. В качестве современной альтернативы рекомендуется использовать WPA3. Подробно о WPA, WPA2 и WPA3 можно прочитать в статье **https://www.kaspersky.ru/resource-center/definitions/wep-vs-wpa**.

Реальная пропускная способность беспроводной сети зачастую оказывается гораздо ниже заявленной. Например, в спецификации домашнего маршрутизатора TP-LINK TL-WR740N заявлена скорость передачи данных до 150 Мбит/с. На практике же больше 72 Мбит/с «выжать» из него не удавалось даже при отсутствии интерференции и одном работающем клиенте. Из-за этого одному из нас пришлось перейти на более дешевый интернет-пакет — со 100 на 70 Мбит/с, — нет смысла платить за 100 Мбит/с, если маршрутизатор «режет» скорость до 72. И это просто домашняя сеть, в которой вместе с мобильными устройствами насчитывается максимум пять работающих клиентов. А как будет работать беспроводная сеть на небольшом предприятии, эксплуатирующем 20–30 клиентов (компьютеров и подключающихся к Wi-Fi смартфонов)?

Многое зависит и от того, как работают с сетью сотрудники предприятия. Если им нужно обмениваться внутри сети большими объемами данных («большие» здесь — это даже не терабайты, а просто сотни мегабайт) или загружать такие объемы данных из Интернета, беспроводная сеть — не вариант. Все станет ужасно «тормозить». С другой стороны, когда беспроводная сеть служит для обычной офисной работы: просмотра страничек в Интернете, переписки по электронной почте, обмена мгновенными сообщениями и даже общения в видеочатах типа Skype или WhatsApp, проблем возникнуть не должно. Да, сеть будет работать медленнее, чем кабельная, но зато это всем удобно. Удобно как администратору, так и пользователям, которые при необходимости могут взять свой ноутбук и перейти в соседний кабинет.

Однако, учитывая все недостатки и особенности сетей Wi-Fi, на некоторых предприятиях наблюдается обратная тенденция — возвращение к кабельным сетям. Возвращаемся к тому, с чего начинали. Это примерно так же, как и с размерами мобильных телефонов, — помните, какими большими были первые мобильники? С хорошую рацию. Потом размер их стал постепенно снижаться. Но в последнее время и это пошло вспять — посмотрите на «лопаты» с размером экрана от 5,5 дюймов и выше.

Кроме того, даже если принято решение использовать беспроводную сеть по всему предприятию, без участков кабельной сети все равно не обойтись. Серверы предприятия должны быть всегда доступны, поэтому к маршрутизатору они так или иначе будут подключаться по кабелю, а не «по воздуху».

В этом разделе главы мы рассмотрим *структурированные кабельные сети* (СКС). Такие сети должны проектироваться и монтироваться специальными организациями, у которых есть государственная лицензия на этот вид деятельности. Тем не менее весьма часто для экономии средств монтаж СКС выполняется собственными силами предприятия. Конечно, такие сети не всегда соответствуют требованиям, предъявляемым стандартами СКС, но это мало кого волнует (к сожалению).

Действующими стандартами СКС в России являются ГОСТ Р 53245-2008 «Информационные технологии. Системы кабельные структурированные. Монтаж основных узлов системы. Методы испытания»[1] и ГОСТ Р 53246-2008 «Информационные технологии. Системы кабельные структурированные. Проектирование основных узлов системы. Общие требования»[2].

Примечание

Опубликованные тексты этих документов содержат опечатки — отнеситесь к их применению с осторожностью.

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
1	0,1	Применяется в телефонных и старых модемных линиях. Кабель несет две жилы. На просторах бывшего СССР кабель используется без скруток, в США — в скрученном виде. Отсюда и пошло название «витая пара». Практически не используется
2	1	Старые терминалы, такие как IBM 3270, сети Token Ring, Arcnet. Представляет собой две пары проводников. Скорость передачи данных до 4 Мбит/с. Не используется
3	16	Телефонные каналы, локальные сети Ethernet 10Base-T, сети Token Ring. Скорость передачи данных до 10 Мбит/с (технология 10Base-T) или 100 Мбит/с (технология 100Base-T4). Сейчас используется в основном для телефонных линий
4	20	Сети Token Ring, 10Base-T, 100Base-T4. Скорость передачи — не более 16 Мбит/с с одной пары. Практически не используется
5	100	Локальные сети со скоростью передачи до 100 Мбит/с (10Base-T, 100Base-T, 100Base-TX). Скорость передачи данных при использовании двух пар — до 10 Мбит/с, четырех пар — до 100 Мбит/с
5e	100	Локальные сети со скоростью передачи до 1000 Мбит/с (1000Base-T). При использовании двух пар достигается скорость передачи данных до 100 Мбит/с, четырех — до 1000 Мбит/с

[1] См. **http://protect.gost.ru/document.aspx?control=7&baseC=6&page=0&month=11&year=2009&search=53245&id=174298**.

[2] См. **http://protect.gost.ru/document.aspx?control=7&baseC=6&page=0&month=11&year=2009&search=53246&id=174287**.

Таблица 3.1 (окончание)

Категория	Максимальная частота сигнала, МГц	Область применения
6	250	Локальные сети со скоростью передачи до 10 Гбит/с (10GBase-T). Максимальная скорость достигается при передаче информации на расстояние до 55 м. Стандарт добавлен в июне 2002 года
6a	500	То же, что и категория 6, но расстояние передачи данных увеличено до 100 м
7	600	Локальные сети со скоростью передачи до 10 Гбит/с, сети ATM, кабельное телевидение. Кабель этой категории имеет общий экран и экраны вокруг каждой пары. Седьмая категория не UTP, а S/FTP (Screened Fully Shielded Twisted Pair)
7a	до 1200	Разработана для передачи данных со скоростью до 40 Гбит/с на расстояние до 50 метров и до 100 Гбит/с на расстояние до 15 метров
8/8.1	1600–2000	Используется в центрах обработки данных (ЦОД) как с топологией Top of Rack (в каждом шкафу устанавливается сетевой коммутатор), так и с топологией End of Row (крайний шкаф в каждом ряду играет роль распределителя). Официально 8-я категория принята в 2014 году и описана стандартом ANSI/TIA-568-C.2-1. Расстояние передачи данных — до 30 метров, скорость — до 40 Гбит/с (40GBase-T). Полностью совместима с кабелем категории 6A.
8.2	1600-2000	Находится в разработке. Полностью совместима с кабелем 7A. Скорость передачи данных — до 40 Гбит/с (40Base_T). Кабель этой категории имеет общий экран и экраны вокруг каждой пары (F/FTP, S/FTP).

Кабельную сеть можно отнести к определенной категории только в том случае, если при ее создании использованы элементы (розетки, разъемы, кабели и т. п.), удовлетворяющие требованиям этой или более высокой категории, а проектирование и монтаж выполнены в соответствии с требованиями стандартов (ограничения на длину, 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, позволяющие использовать каналы передачи данных с гигабитными сетевыми картами. На практике же осуществлять передачу на скорости до 1 Гбит/с позволяет аккуратно выполненная проводка на элементах категории 5. Однако, если вы изначально планируете использовать сетевое оборудование, работающее на таких скоростях, лучше использовать 6-ю категорию.

Кабели витой пары, упомянутые в табл. 3.1, подразделяются на категории, обозначаемые как CAT*cc*, где *cc* — категория кабельной сети, в которой допускается использовать такой кабель. Соответственно CAT5e — витая пара, на основе которой можно прокладывать сети категории 5e.

Волоконно-оптические сети

Если вы внимательно изучили табл. 3.1, то заметили, что максимальное расстояние передачи данных не превышает 100 метров. А что если при построении кабельной системы большого предприятия возникнет необходимость подключить устройства, находящиеся на расстоянии более 100 метров? В этом случае успешно применяются *волоконно-оптические* линии связи.

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

Оптические волокна могут быть одномодовыми и многомодовыми. Диаметр сердцевины *одномодовых* волокон составляет от 7 до 10 микрон. Благодаря столь малому диаметру достигается передача по волокну лишь одной моды излучения, за счет чего исключается влияние дисперсионных искажений.

Многомодовые волокна отличаются от одномодовых диаметром сердцевины, который составляет 50 микрон в европейском стандарте и 62,5 микрона в североамериканском и японском стандартах. Из-за большого диаметра сердцевины по многомодовому волокну распространяется несколько мод излучения — каждая под своим углом, из-за чего импульс света испытывает дисперсионные искажения и из прямоугольного превращается в колоколоподобный.

Многомодовые оптические кабели используются на расстояниях до 200 метров. Стоимость прокладки такой линии не намного дороже стоимости прокладки витой пары.

Одномодовые оптические кабели применяются, когда нужно организовать передачу данных на расстояние свыше 200 метров. Стоимость самого одномодового кабеля, как и стоимость соответствующего оборудования, в несколько раз дороже, чем стоимость многомодового кабеля.

При необходимости передавать данные на расстояния, измеряющиеся десятками километров, используются передатчики повышенной мощности.

Для подключения волоконно-оптических линий применяются так называемые SFP-модули (Small Form-factor Pluggable). Существуют и другие виды подобного оборудования, но SFP-модули (рис. 3.2) используются чаще всего — они подключаются в соответствующие порты активного оборудования.

Сами SFP-модули представляют собой компактные сменные приемопередатчики. В форм-факторе SFP выпускаются модули как для подключения витой пары, так и для оптических каналов.

Волоконно-оптические кабели требуют аккуратного обращения. Так, не допускается резко изгибать кабель, нужно следить за чистотой оптических поверхностей (не трогать их руками, всегда закрывать концы кабеля и гнезда специальными заглушками и т. п.). В случае повреждения кабеля придется воспользоваться услугами

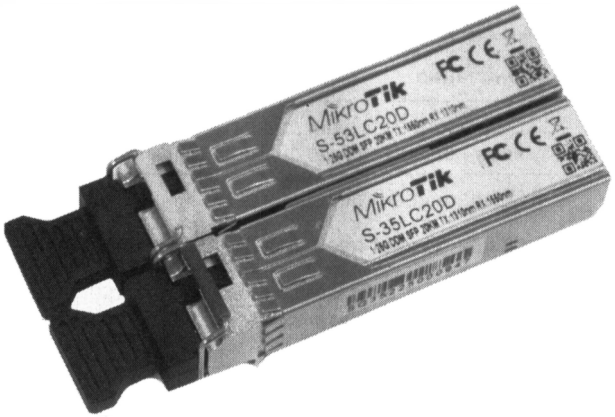


Рис. 3.2. SFP-модули для подключения оптического канала

монтажных фирм, поскольку далеко не все могут позволить себе обзавестись оборудованием для поиска и определения мест неисправности (рефлектометры и пр.).

Сети 10G, 40G и 100G

С увеличением объемов передаваемой информации повышаются и скорости передачи данных. Внедрение мультимедийных приложений (IP-телефония, видеоконференции, системы видеонаблюдения и т. п.) привело к тому, что скорость передачи данных в 1 Гбит/с уже является недостаточной для магистральных каналов предприятия (подробно о них мы поговорим в *главе 10*).

В результате появились технологии передачи данных на скорости до 10 Гбит/с — 10GBase-T (табл. 3.2) и даже выше: 40 Gigabit Ethernet (или 40GbE) и 100 Gigabit Ethernet (или 100GbE). 40-гигабитный Ethernet и 100-гигабитный Ethernet — стандарты Ethernet, разработанные группой IEEE P802.3ba Ethernet Task Force в период с 2007 по 2011 год. Эти стандарты (табл. 3.3) являются следующим этапом развития группы стандартов Ethernet, определявших до 2010 года наибольшую скорость в 10 Гбит/с. В новых стандартах, как следует из их названий, обеспечивается скорость передачи данных в 40 и 100 Гбит/с. Несмотря на то что эти стандарты появились довольно давно, используются они пока редко даже в дата-центрах. А вот сети 10G успешно применяются сейчас для связи коммутаторов уровня ядра предприятия и при оснащении дата-центров, где имеют место самые высокие требования к объемам и скорости передачи данных.

Таблица 3.2. *Технологии Ethernet 10G (IEEE 802.3ae)*

Технология	Описание
10GBase-CX4	Служит для передачи данных на короткие расстояния — до 15 метров. Используется медный кабель CX4 и коннекторы InfiniBand
10GBase-SR	Служит для передачи данных на короткие расстояния — до 26 или 82 метров в зависимости от типа кабеля. В определенных случаях возможна передача на расстояние до 300 метров. Используется многомодовое волокно

Таблица 3.2 (окончание)

Технология	Описание
10GBase-LX4	Дальность передачи данных — от 240 до 300 метров по многомодовому волокну или до 10 км по одномодовому волокну
10GBase-LR	Поддерживает передачу данных на расстояние до 10 км
10GBase-ER	Поддерживает передачу данных на расстояние до 40 км
10GBase-T	Использует витую пару 6-й категории для передачи данных на расстояние до 55 м или витую пару категории 6е для передачи данных на расстояние до 100 м
10GBase-KR	Используется для кросс-плат модульных коммутаторов/маршрутизаторов и серверов

Таблица 3.3. Технологии Ethernet 40G и 100G

Стандарт	Тип	Скорость передачи данных, Гбит/с	Максимальная длина сегмента
IEEE 802.3ba	40GBase-KR4100GBase-KP4	40–100	1 м
	100GBase-KR4	100	1 м
	40GBase-CR4100GBase-CR10	40–100	7 м
	40GBase-T	40	30 м
	40GBase-SR4100GBase-SR10	40–100	100–125 м
	40GBase-LR4100GBase-LR4	40–100	10 км
	100GBase-ER4	100	40 км
IEEE 802.3bg	40GBase-FR	40	2 км

Схема разъема RJ-45

Для подключения компьютера к коммутатору по кабелю витой пары используются коннекторы RJ-45. Таких коннекторов вам понадобится в два раза больше, чем компьютеров, поскольку каждый отрезок кабеля нужно оснастить коннекторами с обоих концов. Но мы рекомендуем покупать коннекторы с запасом, поскольку во время обжатия кабеля они могут быть повреждены.

В «природе» существуют два варианта расшивки витой пары под коннектор RJ-45, различающиеся переменой мест зеленой и оранжевой жил. Один вариант используется в США, другой — в странах Европы. На рис. 3.3 изображен европейский вариант расшивки кабеля.

В общем-то, расшивка никак не сказывается на работе оборудования. Например, одни кабели могут быть обжаты первым вариантом, другие — вторым. Исключение составляют случаи, когда один конец одного и того же кабеля обжат одним вариантом, а второй — другим. Такое может произойти, если один конец кабеля повреж-

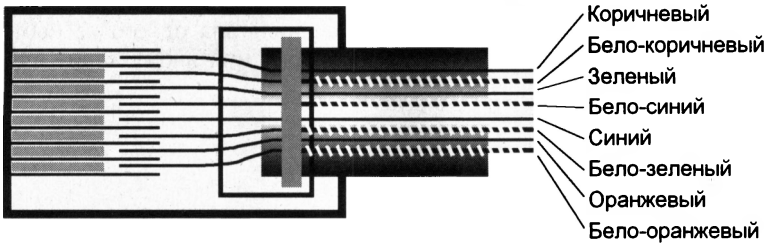


Рис. 3.3. Расшивка разъема RJ-45

ден и его приходится переобжимать. Если специалист, выполняющий обжимку, не обратит внимания на то, как обжат другой конец кабеля, возникнут проблемы.

Для передачи сигналов на линиях связи 100 Мбит/с используются только две пары из четырех, имеющихся в кабеле (в Gigabit Ethernet на скорости 1000 Мбит/с задействованы уже все четыре пары). Хотя это и не предусмотрено стандартами, администратор может на свое усмотрение задействовать оставшиеся пары — например, использовать средние провода (пару голубой — бело-голубой) под телефон, а коричневую пару — в качестве замены одной из сигнальных при обнаружении обрыва в кабеле. При этом следует учитывать, что для питания устройств поверх сети Ethernet (Power over Ethernet, PoE) служит центральная пара проводов (см. о PoE подробнее чуть далее) и что в гигабитных каналах задействованы все провода.

Два компьютера можно объединить в сеть и без коммутатора. Для этого используется *перекрестная обжимка кабеля* (crossover). В этом случае на одной из сторон кабеля меняются местами входные и выходные провода — первая и третья пары (табл. 3.4). Перекрестная обжимка может понадобиться не только при соединении одного компьютера с другим, но и при подключении ADSL-модема непосредственно к компьютеру или при соединении двух коммутаторов ранних моделей выпуска.

***Таблица 3.4.** Перекрестная схема расшивки разъемов RJ-45*

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 этой функции нет, поэтому, например, для соединения двух таких

устройств между собой также необходимо использовать crossover-кабель. На некоторых моделях имеется либо кнопка переключения типа одного из портов, либо два разъема для одного порта, соответствующих тому или иному варианту подключения (называемых MDI и MDIX).

Варианты исполнения СКС

Кабельную систему предприятия можно построить самыми разными способами. Проводка кабеля может быть скрытой, может проходить над навесным потолком, в накладных каналах и т. д. Обычно, если прокладка кабелей выполняется своими силами, все это осуществляется без трудоемких строительных работ. Как правило, используются накладные каналы, а переходы между помещениями осуществляются или через отверстия в стенах, или над навесным потолком.

ВНИМАНИЕ: КОММУТАЦИОННЫЕ КАБЕЛИ (ПАТЧ-КОРДЫ)

По данным одного из производителей патч-кордов, две трети кабелей не проходят тестирования после изготовления в промышленных условиях. Некачественные патч-корды являются причиной снижения скорости передачи данных. Имейте это в виду, если скорость передачи данных оставляет желать лучшего или же вообще появились ошибки при передаче данных.

Удлинение кабеля

Стандартами СКС не предусмотрено удлинение линии передачи данных. А что делать, если сотруднику выделено другое место и нужно перенести его компьютер на несколько метров в сторону, а кабеля не хватает? Конечно, первое, что приходит в голову, — использовать Wi-Fi и забыть как страшный сон все эти СКС.

Как говорится: если нельзя, но очень нужно или сильно хочется, то можно. Конечно, мы не рекомендуем этого делать, но на практике возможны скрутки (или спайки) кабеля витой пары. При этом такой кабель относительно нормально работает даже в 100-мегабитных сетях. Качество контактов скрутки может со временем снизиться, например, из-за окисления. Поэтому нужно позаботиться о надежной изоляции такого соединения.

Прокладка силовых кабелей

В этом разделе мы рассмотрим требования к прокладке силовых кабелей:

- каждое рабочее место пользователя должно быть оборудовано розеткой электропитания с заземлением и информационными розетками;
- расстояние между силовой и информационной розетками одного рабочего места по стандарту не должно превышать 1 м;
- минимальное расстояние между силовым и информационным кабелями зависит от потребляемой мощности, но на практике обычно используется значение 15–20 см;
- если такие расстояния выдержать невозможно, нужно использовать кабели с экранированием.

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 этого источника помех не следует допускать прокладку информационного кабеля ближе 15 см от люминесцентной лампы.

Питание по сети Ethernet (PoE)

Некоторое современное оборудование может получать питание по технологии *питания оборудования по кабелю Ethernet* (Power over Ethernet, PoE). Как правило, запитывают по PoE точки беспроводного доступа, камеры видеонаблюдения, IP-телефоны и прочее не очень мощное оборудование.

Технология PoE основана на том, что в стандартах передачи данных 10/100 Мбит/с задействованы только две пары проводов витой пары из четырех имеющихся, а остальные две можно использовать для питания некоторого не очень мощного оборудования.

Обычно для работы этой технологии устанавливаются специальные PoE-коммутаторы. При этом допускается установка дополнительного блока питания, который будет запитывать PoE-устройства. Администраторы могут использовать управление портами PoE-коммутатора для перезагрузки зависшего устройства — для этого просто нужно снять напряжение с соответствующего порта, а затем заново его подать.

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). Упомянутые ранее устройства обычно потребляют меньшую мощность — например, IP-телефонам достаточно 2 Вт, точкам доступа — около 11 Вт и т. д.

Из соображений безопасности на большинстве моделей коммутаторов суммарно допустимая мощность питания по портам Ethernet должна быть меньше величины:

$$15{,}4 \times \langle \textit{количество портов} \rangle \text{ ватт (Вт).}$$

При превышении допустимого значения потребляемой мощности коммутатор начинает отключать питание отдельных портов. При этом учитываются *приоритеты* портов для PoE, назначенные вручную администратором.

Требования пожарной безопасности

В этом разделе представлены основные требования пожарной безопасности при прокладке кабелей в офисе:

- кабели, каналы, розетки и т. п. должны соответствовать определенной категории пожароустойчивости. Обычно это достигается использованием современных элементов СКС;
- силовые и информационные кабели при прокладке в одном канале должны быть разделены сплошной перегородкой. Минимальное расстояние от силовых кабе-

лей 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.

На монтаж СКС под фальшполом налагаются более строгие ограничения. Например, должно быть обеспечено разделение пространства под фальшполом на зоны, отделяемые друг от друга несгораемыми материалами, и т. п.

Топология сети

Топология сети — это схема расположения и соединения устройств сети. Можно выделить две топологии: физическую и логическую. Физическая топология описывает реальное расположение устройств и наличие каналов связи между ними. Логическая топология создается поверх физической и описывает пути передачи данных.

Размеры сегментов сети на витой паре

Как уже было отмечено ранее, длина кабеля от одного активного сетевого устройства до другого, например от коммутатора к компьютеру, не должна превышать 100 метров (уточним, что сейчас разговор идет о сети Ethernet). При этом обычно считается, что максимальная длина самого кабеля не должна превышать 90 метров, а 10 метров отводится на соединительные кабели.

Минимальная длина сегмента сети — 1 метр. Нет смысла применять более короткие самодельные патч-корды (хотя длина некоторых «фирменных» кабелей может быть и меньше метра, но не менее 60 см) — при малой длине кабеля возрастает уровень помех, возникающих при отражении высокочастотных сигналов от точки соединения кабеля и розетки, что приводит к увеличению числа ошибок в линии.

Ранее, когда сети Ethernet строились на базе концентраторов (хабов), действовало «правило 5/4» — между любыми двумя сетевыми устройствами должно быть не более пяти сегментов сети с четырьмя концентраторами. Современные сети Ethernet строят на базе коммутаторов, и таких ограничений больше нет.

Уровни ядра, распределения и доступа

В идеале проектировать сеть желательно с нуля. При этом в структуре сети принято выделять несколько уровней (рис. 3.4):

- *уровень ядра* (core) — этот уровень должен максимально быстро передать трафик между оборудованием уровня распределения;
- *уровень распределения* (distribution) — здесь реализуется маршрутизация пакетов и их фильтрация (на основе правил маршрутизатора);

- *уровень доступа* (access) — здесь происходит подключение к сети конечных рабочих станций.

На рис. 3.4 представлена типичная трехуровневая схема иерархической структуры сети, которая на практике может быть немного иной. Все зависит от размеров предприятия — если предприятие совсем небольшое, то какой-либо уровень может отсутствовать и сеть станет двухуровневой. Например, маршрутизацию данных можно реализовать на уровне ядра, и оборудование уровня распределения будет только пересылать данные внутри сегмента сети. Также может не быть и серверной фермы (серверная ферма представляет собой обычный узел распределения, однако реализованный на быстродействующем оборудовании). На небольших предприятиях серверы подключаются непосредственно к ядру сети передачи данных.

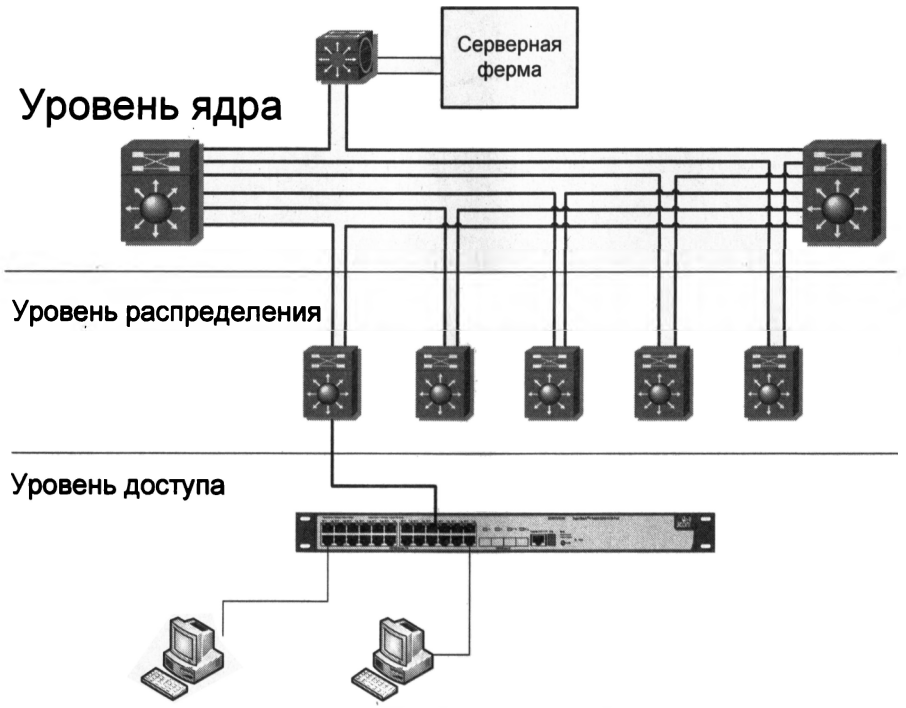


Рис. 3.4. Трехуровневая структура сети

К сожалению, на практике часто приходится использовать уже существующие линии связи. Тут уже ничего не поделаешь — переделывать структуру сети, как правило, никто не разрешит. Для оптимизации имеющейся структуры можно лишь посоветовать сократить количество коммутаторов между двумя точками подключения компьютеров.

Топология каналов распределенной сети предприятия

Часто бывает так, что не все компьютеры предприятия находятся в одном помещении. Некоторые предприятия имеют распределенную топологию каналов сети —

например, как минимум располагаются в нескольких зданиях (не говоря уже про филиалы в других городах).

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 распределенной сети крупного предприятия.

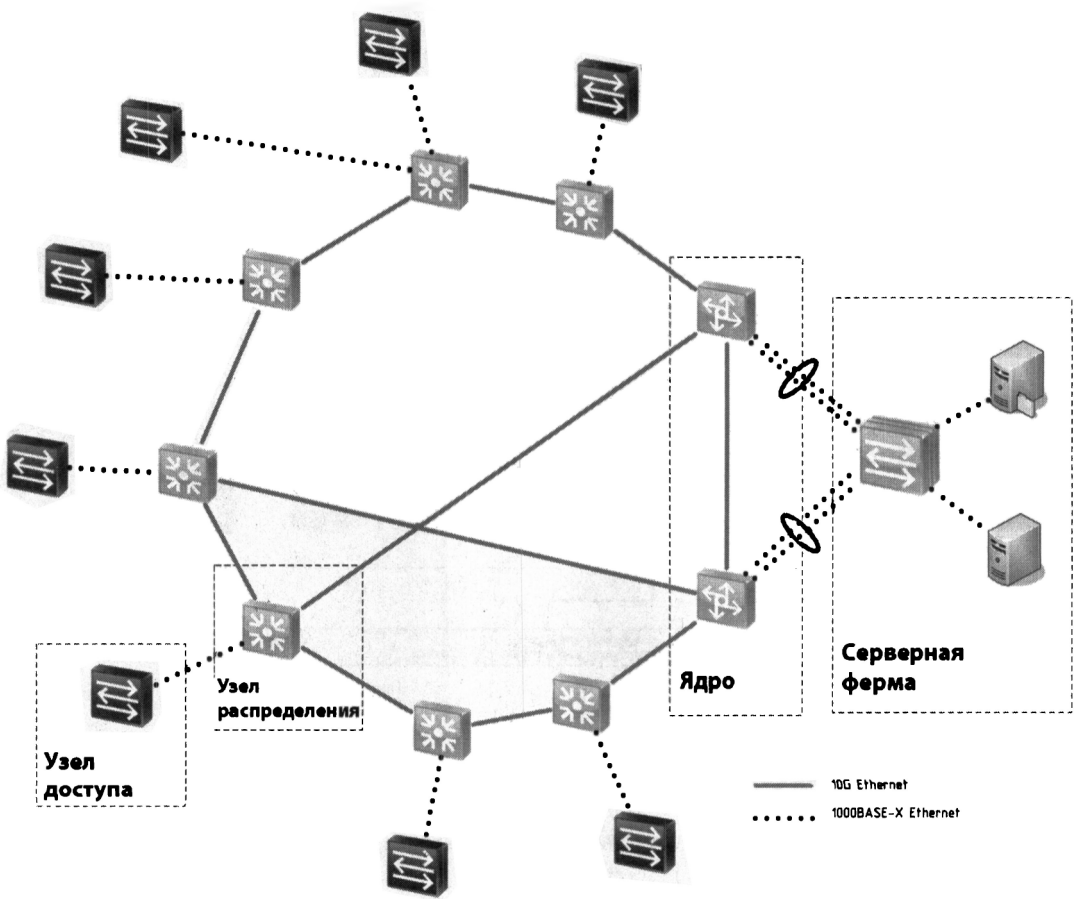


Рис. 3.5. Вариант структурной схемы связей территориально распределенной информационной системы

Сеть управления

Чтобы сохранить управляемость оборудования сети, нужно построить отдельную сеть для подключения интерфейсов управления. Такая сеть должна быть собрана на физически других линиях связи, отличных от тех, что используются для передачи данных. Это могут быть отдельные концентраторы, к которым подключены активные устройства. Да, ошибки тут нет — именно концентраторы. Если у вас где-то

завалялись такие, вы можете использовать их для построения сети управления. И ничего страшного, что скорость передачи данных будет всего 10 Мбит/с — для сети управления не нужно высокой скорости.

Документирование структуры каналов связи

К сожалению, далеко не на всех предприятиях производится документирование их кабельной подсистемы. Объясняется это тем, что многие предприятия работают на оборудовании, не поддерживающем протокол SNMP[1], а без его поддержки нельзя использовать специальные программы, строящие диаграммы структуры сети. В этом случае администратору приходится создавать диаграммы структуры сети вручную, что довольно-таки трудоемко. Тем более что такие диаграммы очень быстро становятся неактуальными — достаточно перевести одного пользователя в другой кабинет или проложить дополнительный канал связи.

Качество сетей связи предприятия

Администратор должен регулярно проверять качество сетей связи предприятия. Цель таких проверок — убедиться, что линии связи не создают препятствий в работе информационной системы.

Проверка кабельной системы

Для построения качественной информационной системы нужны качественные комплектующие. Немаловажную роль играет и правильность построения самой сети. Несмотря на доступность инструментов для расшивки кабеля и монтажа элементов СКС, желательно привлечь к работам фирмы, которые имеют опыт работы в этой области и обладают необходимым уровнем компетенции. Например, даже такая мелочь, как лишний перехлест пары проводов при расшивании гигабитного соединения, может привести к тому, что линия связи 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 лишь после некоторого периода эксплуатации. Выполнение подобного тестирования 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. 3.6 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.

Такие тесты должны быть проведены для всей кабельной системы, а их результаты — храниться в архиве администратора.

---

[1] SNMP (от *англ.* Simple Network Management Protocol, простой протокол сетевого управления) — стандартный интернет-протокол для управления устройствами в IP-сетях на основе архитектур TCP/UDP.

LW LINKWARE
CABLE TEST MANAGEMENT SOFTWARE

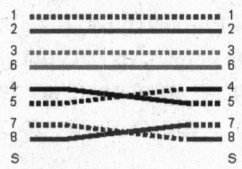
ID кабеля: R530-PP14-P07 **Суммарный результат: FAIL**

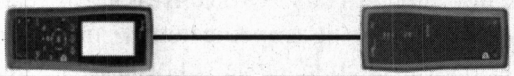
Дата / Время: 12/28/2006 01:16:10pm
Запас: 7.2 dB (NEXT 12-78)
Врем. предел: ISO11801 PL max Class D
Тип кабеля: Cat 5e UTP

Оператор: [redacted]
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

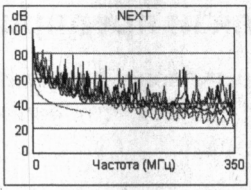
Карта проводов (T568A)
FAIL

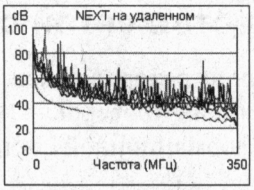




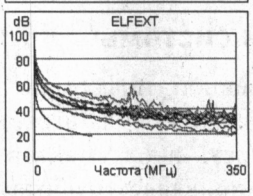
Длина (фт)	[Пара 36]	42
Обосн. задержка (ns), Лимит 498	[Пара 12]	65
Разн. задержок (ns), Лимит 44	[Пара 12]	1
Сопротивл. (ом), Лимит 21.0	[Пара 36]	2.7
Затухание Разница (dB)	[Пара 45]	17.5
Частота (МГц)	[Пара 45]	100.0
предел (dB)	[Пара 45]	20.4

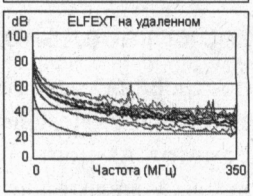
	Наихудш. разн		Наихудш. знач	
Неверн	Глав.	SR	Глав.	SR
Наихудш пара	12-78	36-78	12-78	36-78
NEXT (dB)	7.2	7.4	7.2	7.4
Част. (МГц)	88.8	100.0	88.8	100.0
предел (dB)	33.2	32.3	33.2	32.3
Наихудш пара	12	78	78	36
PSNEXT (dB)	8.2	8.7	8.3	9.3
Част. (МГц)	87.5	90.8	90.3	100.0
предел (dB)	30.3	30.0	30.0	29.3



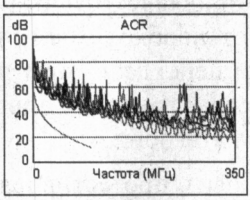


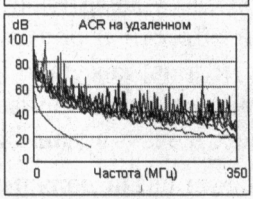
PASS	Глав.	SR	Глав.	SR
Наихудш пара	36-45	45-36	36-45	45-36
ELFEXT (dB)	13.7	13.6	14.2	13.6
Част. (МГц)	89.8	89.8	97.8	90.3
предел (dB)	19.6	19.6	18.8	19.5
Наихудш пара	36	36	36	36
PSELFEXT (dB)	15.9	15.5	16.6	15.9
Част. (МГц)	2.5	88.8	100.0	97.8
предел (dB)	47.7	16.7	15.6	15.8



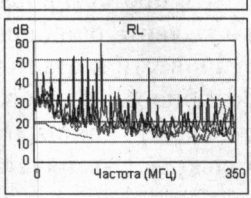


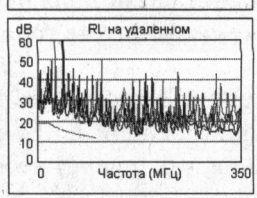
Неверн	Глав.	SR	Глав.	SR
Наихудш пара	12-78	12-78	12-78	36-78
ACR (dB)	13.9	13.3	23.8	25.1
Част. (МГц)	6.9	7.4	88.8	100.0
предел (dB)	46.0	45.4	14.0	11.9
Наихудш пара	12	78	36	36
PSACR (dB)	15.6	15.1	26.8	26.9
Част. (МГц)	6.6	7.4	100.0	100.0
предел (dB)	43.4	42.4	8.9	8.9





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. 3.6. Протокол испытания качества линии связи специализированным оборудованием

Проверка качества передачи данных

Когда сеть уже введена в эксплуатацию, о качестве передачи информации по каналам связи можно судить по показаниям счетчиков коммутационного оборудования. Ясное дело, что такие показания можно получить только на управляемых устройствах, к которым, к сожалению, не относятся так называемые офисные (бюджетные) модели.

В *главе 11* будет рассказано, по каким показаниям счетчиков можно судить о качестве передачи данных, а пока рассмотрим вопросы приоритизации трафика.

Приоритизация трафика

Построить сеть, которая гарантированно пропускала бы весь трафик в случае активной сетевой работы всех пользователей, практически нереально. Параметры пропускной способности рассчитываются по 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 и повсеместного внедрения мультимедийных решений вероятность кратковременной перегрузки сети будет только повышаться.

Сама сеть *не гарантирует* доставку информации. Если пакет с данными не может быть передан, он просто 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, как бы «булькание» речи. В этом случае можно решить проблему, если предоставить передаче голоса более привилегированные условия, чем, например, протоколу пересылки почтовых сообщений. Ничего не случится, если почтовое сообщение будет доставлено чуть позже, — это даже не будет замечено пользователями.

Задача приоритизации трафика решается путем присвоения передаваемым по сети пакетам определенного *класса* обслуживания и обеспечения для каждого класса соответствующего *качества* обслуживания. Часто для простоты все эти технологии называют QoS — Quality of Service. Обращаем внимание читателя, что настраивать QoS имеет смысл только при возникновении подобных ситуаций. В случае достаточности полосы пропускания никаких дополнительных действий предпринимать не нужно. В общем случае эта задача является весьма сложной и решается поразному для локальной и магистральных сетей. 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. Далее мы опишем основные подходы, используемые для решения задачи приоритизации трафика.

Варианты приоритизации: 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 (о модели OSI далее рассказано подробно). 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, принимающее данные о требуемом уровне обслуживания. Впоследствии был разработан новый протокол Differentiated Services (DS, или DiffServ), который и служит 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 задействуют для приоритизации только поле QoS Ethernet-кадра. Коммутаторы уровня предприятия могут приоритизировать трафик с учетом всех действующих стандартов.

Говоря о QoS, нельзя не сказать, как настроить QoS в Windows. Ограничить резервируемую пропускную способность можно посредством *групповой политики*. Для этого в редакторе групповой политики (вызываемом командой `gpedit.msc`) перейдите по меню **Административные шаблоны | Сеть | Планировщик пакетов QoS** и щелкните двойным щелчком на элементе **Ограничить резервируемую пропускную способность** (рис. 3.7). По умолчанию (даже если ограничение, как пока-

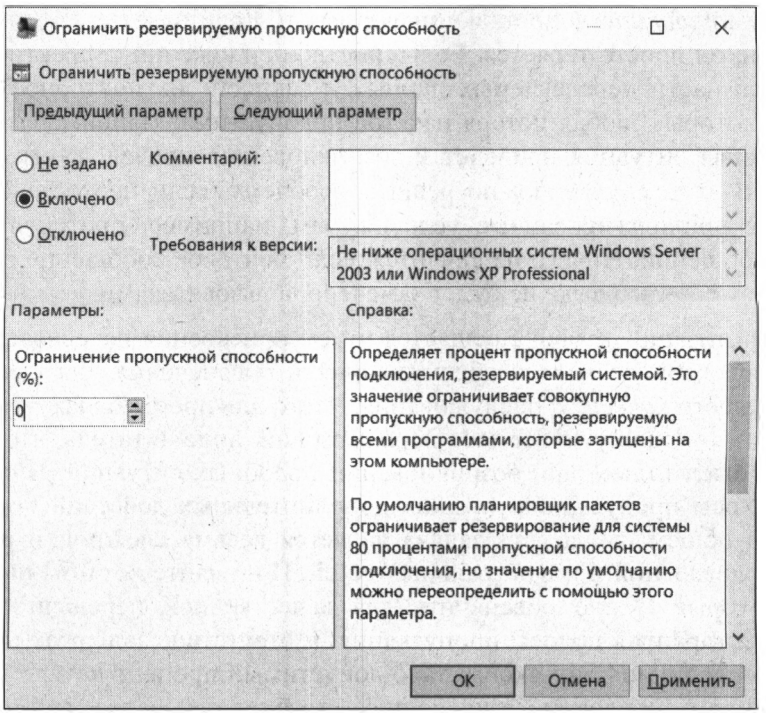


Рис. 3.7. Настройка резервируемой пропускной способности

зано на рис. 3.7, не задано) Windows резервирует 20% пропускной способности. Чтобы повысить полезную пропускную способность, можно установить переключатель **Включить** и задать значение 10%.

Пакеты данных в соответствии с протоколом 802.1p (точнее, само поле определено в протоколе 802.1q, но назначение битов приоритета описано в протоколе 802.1p) имеют специальное поле приоритета из трех битов. Таким образом, данные в локальной сети могут быть промаркированы одним из восьми *классов* обслуживания. Приоритет пакету должна ставить программа, создающая текущий трафик, но значение этого приоритета может быть изменено по пути следования пакета (например, на некоторых моделях коммутаторов). Существуют 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.

В протоколе DiffServ на описание приоритета выделено 6 битов, что позволяет иметь до 64 возможных классификаций приоритизации. Реально используется существенно меньше уровней сервиса. В табл. 3.5 приведены основные применяемые на практике уровни сервиса DiffServ.

Таблица 3.5. *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		Сообщения электронной почты
	AF22 Medium Priority High Drop Precedence		Фоновая репликация данных
	AF31 Low Priority Low Drop Precedence		HTTP

Классификация, маркировка, правила приоритизации

Для настройки приоритизации 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 определенному приложению. Если оно работает по какому-либо протоколу, не используемому другими приложениями, то достаточно создать правило классификации на основе протокола. Так можно, например, 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 каждый описанный — *маркированный* — тип трафика одному из существующих уровней. Промаркированный пакет будет готов к применению правил приоритизации. Часто в целях удешевления коммутаторы, предназначенные для использования на уровне доступа, имеют меньше восьми очередей, используемых при приоритизации трафика. Соответственно сузятся ваши возможности по детализации процесса приоритизации.

Классификацию с последующей маркировкой пакетов можно проводить на любом коммутаторе, поддерживающем управление приоритизацией. 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 на основании ее выполняют приоритизацию 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 приоритизации*. 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 приоритизации 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.

Как работает приоритизация: очереди

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

Количество буферов — это количество очередей, которые поддерживает коммутатор. В идеале количество очередей должно быть равно количеству уровней приоритизации, а именно — восьми. Меньшее их количество не позволит использовать все возможности протокола, большее — не имеет смысла за пределами конкретного коммутатора, хотя и позволяет более точно приоритизировать передачу трафика в нем. Размеры буфера обычно не одинаковы для разных очередей — чем выше приоритет очереди, тем больше памяти отводится для хранения ее пакетов. 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, как правило, не изменяют.

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

При использовании алгоритма SPQ сначала передаются пакеты из очереди, имеющей максимальный приоритет, и только когда она полностью освободится, коммутатор начнет передачу данных из следующей по приоритету. Такой 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. Такой 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.

Ограничение полосы пропускания трафика (Traffic shaping)

Коммутаторы, на которых реализована возможность приоритизации 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.

Такая настройка выполняется в соответствии с правилами конфигурирования конкретной модели коммутатора.

Беспроводные сети

Вот мы и добрались наконец-то до беспроводных сетей. Куда ж без них сейчас! А ведь еще лет десять назад не то чтобы о сетях Wi-Fi никто не знал, но они не были распространены так повсеместно. Ранее в этой книге мы уже начали обсуждать беспроводные сети, но в этом разделе поговорим о них подробно.

Как уже было отмечено, основное преимущество беспроводной сети — простота монтажа. Если сделать качественную СКС дорого (проект, прокладка кабеля и, возможно, ремонт помещений после его прокладки, метры кабеля, множество различных мелочей и, конечно же, активное оборудование), то в случае с беспроводной сетью все гораздо проще и дешевле.

А если учесть, что стоимость точки доступа примерно равна стоимости небольшого коммутатора, то переход на беспроводную сеть может быть экономически оправдан для многих предприятий, и в некоторых случаях (например, при аренде помещения без права выполнения монтажно-строительных работ или наличии мобильных сотрудников — к примеру, официанты могут использовать мобильные устройства для приема заказов, врачи — иметь с собой ноутбуки или планшеты при проведении обхода и т. д.) организация беспроводной сети может стать и единственным приемлемым решением.

Именно поэтому для небольших офисов использование беспроводных сетей является практически идеальным вариантом.

Что нужно для построения беспроводной сети? Маршрутизатор Wi-Fi, совместимый с интернет-соединением вашего провайдера (если Интернет «заходит» к вам в офис по Ethernet-линии, то WAN-порт должен иметь разъем RJ-45, если же у вас ADSL-линия, то маршрутизатор должен быть оснащен ADSL-модемом), и беспроводные адаптеры Wi-Fi. Количество адаптеров должно соответствовать количеству компьютеров в вашем офисе, причем ноутбуки уже с завода оснащены беспроводными адаптерами. Следовательно, беспроводные адаптеры нужно докупить только для стационарных компьютеров.

Стоимость беспроводных адаптеров невысока — несколько сот рублей, т. е. стоят они примерно столько же, сколько и обычные кабельные адаптеры. Существует несколько форм беспроводных сетевых адаптеров. Выбирайте ту, которая вам больше подходит. Например, если компьютеры уже сняты с гарантии, можно купить беспроводные адаптеры, выполненные в виде PCI-платы. На рис. 3.8 изображен адаптер Intellinet Wireless 150N. Такие адаптеры стоят дешевле своих USB-собратьев и оснащены внешней съемной антенной (не у всех USB-адаптеров антенна внешняя и тем более съемная), что позволяет не только изменить угол наклона антенны для лучшего приема, но и заменить ее на более мощную.

Если компьютеры на гарантии и вскрывать корпуса нельзя, приходится обзаводиться USB-адаптерами (рис. 3.9). Мы, как и в случае с PCI-адаптерами, рекомен-

дуем выбирать адаптеры со съемной антенной, что при необходимости позволит заменить саму антенну на более мощную. Не покупайте адаптеры без внешней антенны! Пусть она будет не съемная, но внешняя. При необходимости такую антенну хотя бы можно направить для улучшения приема/передачи.

Рис. 3.8. Беспроводной адаптер Intellinet Wireless 150N

Рис. 3.9. Беспроводной адаптер USB со сменной антенной

Примечание

Для получения лучших результатов рекомендуется покупать маршрутизатор Wi-Fi и сетевые адаптеры одного производителя и не выбирать самые дешевые варианты.

Маршрутизатор Wi-Fi (рис. 3.10) — это многофункциональное устройство, выполняющее следующие основные функции:

- объединение в сеть беспроводных клиентов (точка беспроводного доступа);
- подключение кабельных клиентов. Обычно маршрутизаторы оснащены несколькими портами RJ-45 (Ethernet), позволяющими подключить от 4 до 8 клиентов;

Рис. 3.10. Маршрутизатор Cisco 819

- обеспечение возможностей шлюза и брандмауэра;
- функции ADSL-модема (опционально).

Как видите, самый простой маршрутизатор Wi-Fi выполняет множество функций. Более точный набор функций можно найти в спецификации на конкретное устройство.

Стандарты беспроводной сети

В настоящее время устройства для беспроводной сети выпускаются на основе нескольких стандартов, некоторые параметры которых приведены в табл. 3.6.

Самый современный и оптимальный стандарт — 802.11n. Он не только обеспечивает самую высокую скорость передачи данных, но и работает на двух диапазонах частот: 2,4 и 5,0 ГГц. Это означает, что если в режиме 2,4 ГГц наблюдается высокая интерференция (рядом слишком много соседних сетей), то можно перенастроить маршрутизатор на частоту 5 ГГц. Главное, чтобы все сетевые адаптеры компьютеров поддерживали стандарт IEEE 802.11n. Дело в том, что хотя стандарт 802.11n и поддерживает старые стандарты, но если в сети будет хотя бы один старый адаптер, то скорость всей сети снизится до скорости этого адаптера.

Таблица 3.6. Стандарты беспроводных сетей

Характеристика	Стандарт				
	802.11a	802.11b	802.11g	802.11n	802.11ac
Диапазон частот, ГГц	5	2,4	2,4	2,4 или 5,0	5,0
Максимальная скорость передачи, Мбит/с	54	11	54 (108 с аппаратным сжатием)	600 (150 по одной антенне)	6,7 Гбит/с (при 8 антеннах)
Совместимость	—	g	b	a, b/g	n

Со стандартом 802.11ac еще несколько лет назад было не все так гладко, как с 802.11n. Для его применения нужна была лицензия. Однако с 2016 года государственная комиссия по радиочастотам (ГКРЧ) разрешила работать на частотах, используемых этим стандартом, без обязательного лицензирования. При этом стало возможным задействовать дополнительный диапазон 5650–5850 МГц. Кроме того, для диапазонов 5150–5350 и 5650–5850 МГц была удвоена максимально допустимая мощность (до 10 мВт) на 1 МГц. Переход на новый стандарт позволяет не только повысить максимальную скорость передачи данных, но и избавиться (по крайней мере, на некоторое время — пока этот стандарт не очень популярный) от проблемы интерференции.

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

Проектирование беспроводной сети предприятия

Беспроводные технологии позволяют соединять как компьютеры (по принципу «точка-точка»), так и отдельные сегменты сетей. Чаще всего в локальных сетях устройства беспроводного доступа ставятся в качестве *точки доступа* (Wireless Access Point, AP). В этом случае точка доступа выступает аналогом концентратора локальной сети, т. е. через нее к сети подключаются отдельные компьютеры.

Обратите внимание, что на рынке присутствуют как беспроводные маршрутизаторы Wi-Fi, так и беспроводные точки доступа. Полагаем, вы понимаете в чем разница. Любой маршрутизатор Wi-Fi может работать в режиме точки доступа, но точка доступа не может работать в режиме маршрутизатора. Другими словами, если вы купите просто точку доступа, то объедините все беспроводные клиенты в один сегмент локальной беспроводной сети, но для доступа к Интернету вам понадобится дополнительное устройство. Им может быть как аппаратный маршрутизатор (DSL-модем), так и отдельный компьютер, выполняющий роль шлюза (программный маршрутизатор). Надо также иметь в виду, что точки доступа, как правило, не оснащены Ethernet-портами (максимум они могут нести один Ethernet-порт для управления и питания — многие точки доступа поддерживают технологию PoE).

Так что для небольшого офиса, состоящего как из проводных, так и из беспроводных клиентов, нужен именно беспроводной маршрутизатор.

Несмотря на то что маршрутизатор может работать в режиме точки доступа, строить сеть только на маршрутизаторах нерационально. Если вам нужно покрыть большое расстояние, целесообразно приобрести один маршрутизатор и несколько точек доступа — так будет дешевле.

Выбрав стандарт беспроводной сети, нужно определить *зоны покрытия*. Одна стандартная точка доступа покрывает зону радиусом около 50 м. На практике это значение может быть меньше или больше в зависимости от:

- мощности устройства;
- используемых антенн — хорошо, если антенны съемные, тогда можно установить более мощные, в противном случае при нехватке зоны покрытия нужно будет менять устройство;
- интерференции — наличия рядом беспроводных сетей, работающих на том же (или близком) канале;
- планировки помещения и типа стен.

В спецификациях точек доступа часто указывается такая характеристика, как *максимальный радиус действия*. Однако это значение достижимо только в идеальных условиях — в поле, где рядом нет ни стен, ни деревьев, ни других беспроводных сетей. На практике, поверьте, более чем на 50 метров рассчитывать не нужно.

Лучшим способом определения реальной зоны покрытия является проведение тестовых измерений на местности с использованием соответствующего оборудования. На рис. 3.11 приведен пример программы, которая анализирует замеры параметров радиочастотного сигнала в реальных условиях и формирует карту зоны покрытия (с привязкой к карте с помощью глобальных систем позиционирования).

Как правило, это весьма дорогостоящая операция, поэтому часто ограничиваются тестированием уровня сигнала с помощью имеющегося беспроводного адаптера штатными средствами Windows или с помощью специальных программ — например, Wifi Analyzer (см. рис. 3.1).

При этом нужно учитывать, что помехи беспроводной сети может создать при своей работе и действующее на предприятии производственное оборудование, и предусмотреть необходимые технологические резервы. И даже при отсутствии постоянных помех используемые в беспроводной сети программы должны быть устойчивы к кратковременному исчезновению связи. Так, при работе в бухгалтерской программе «1С:Предприятие» могут наблюдаться случаи аварийного завершения программы из-за кратковременной потери связи с сервером.

Количество устанавливаемых точек доступа зависит не только от зоны покрытия, но и от необходимой скорости доступа к сети. В табл. 3.5 были указаны максимальные скорости передачи данных, но при этом надо учитывать, что полоса пропускания делится между всеми устройствами, которые подключены к тому или

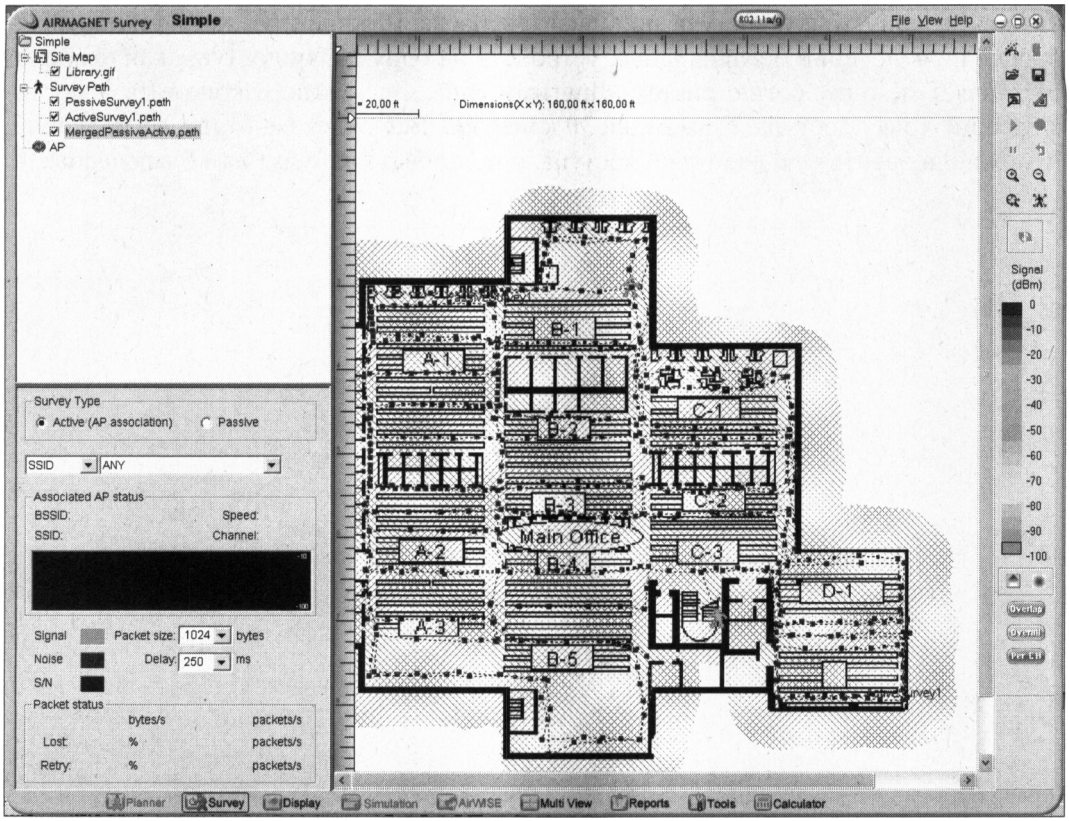


Рис. 3.11. Специализированное программное обеспечение позволяет построить возможные зоны покрытия на основе замеров и анализа параметров радиосигнала (здесь представлен пример от AirMagnet, Inc.)

иному каналу. Рассмотрим для примера устройство стандарта 802.11n. Его максимальная заявленная скорость — 150 Мбит/с (это в теории, а на практике значительно ниже). Если одновременно будут работать пять клиентов, то на каждого из них придется по 30 Мбит/с максимальной теоретической скорости. С учетом практического опыта разделите эти значения еще на 2. В итоге получится 15 Мбит/с, а это всего лишь 1,87 Мбайт/с — маловато на сегодняшний день. Следует также учитывать, что скорость передачи данных снижается при слабом уровне сигнала на максимальных расстояниях.

Учитывая современные тенденции, когда к Wi-Fi подключаются не только компьютеры и смартфоны, но и бытовые устройства (телевизоры, мультиварки и пр.), то даже в совсем небольшой сети может быть весьма много клиентов. Чтобы все они могли комфортно работать, нужно установить маршрутизатор с повышенной пропускной способностью. Конечно, интернет-канал тоже должен всему этому соответствовать. Вторым вариантом может стать установка дополнительных точек доступа — таких, например, как Linksys RE6700 (рис. 3.12).

Установка дополнительных точек доступа позволяет распределить между ними пользователей и повысить скорость обмена данными. Обычно рекомендуется уста-

навливать одну точку доступа приблизительно на 10 клиентов, хотя технический предел подключений беспроводных устройств на одну точку доступа, как правило, составляет не одну сотню систем. Другими словами, можно сэкономить и поставить одну точку доступа, скажем, на 30 клиентов. Все будет работать, но медленно. А можно добавить еще две точки доступа, и пользователи будут вам благодарны.

Рис. 3.12. Ретранслятор Linksys RE6700

Беспроводные решения могут помочь соединить, например, два здания. Для этого созданы специализированные беспроводные *мосты* и направленные антенны. В режиме моста могут работать многие точки доступа, даже не самые дорогие.

Здесь повторимся и снова порекомендуем покупать точки доступа, маршрутизаторы и беспроводные адаптеры со съемными антеннами. Антенны сами по себе стоят недорого, поэтому в случае недостаточного сигнала можно просто установить более мощную антенну, что не ударит по вашим финансам.

Для работы вне помещения нужны специальные наружные (outdoor) точки доступа. Такие устройства устойчивы к перепаду температур, и им не страшна повышенная влажность.

Примечание

Если режим работы системы предполагает мобильность устройств (постоянное перемещение их во время работы с системой с переключением между различными точками доступа), то для исключения прерывания сессий необходимо использовать специальное программное обеспечение.

Безопасность беспроводной сети

Безопасность беспроводной сети оставляет желать лучшего. Представьте только — по умолчанию к вашей беспроводной сети может подключиться любой желающий. Что он станет делать: просто получит доступ к Интернету через вашу беспроводную сеть или же будет перехватывать передаваемые по сети пакеты — никто не знает. Поэтому нужно уделить внимание правильной настройке маршрутизатора и/или точки доступа.

Шифрование трафика беспроводной сети

Для защиты передаваемой по беспроводной сети информации все данные *шифруются*. Существуют следующие стандарты шифрования данных, передаваемых по беспроводной сети:

- WEP (Wireless Encryption Protocol или Wired Equivalent Privacy);
- WPA (Wi-Fi Protected Access);
- WPA2 (усовершенствованный вариант Wi-Fi Protected Access).

Наиболее безопасным считается стандарт WPA2. Стандарт WEP можно сравнить с решетом, а WPA — с голландским сыром. Да, вы все правильно поняли — «дыр» в этих стандартах очень много. Однако и протокол WPA2 также подвержен взлому, что стало известно относительно недавно. Многие думали, что раз они используют WPA2, то полностью защищены. Но это не так. В Сети уже полно руководств по взлому сетей, защищаемых стандартом WPA2. Например, вот одно из них: **https://skillville.ru/electro/kak-vzlomat-wi-fi-s-wpa2-shifrovaniem.html**.

Что же делать? Есть два способа решения этой проблемы:

- если по сети не передаются никакие важные данные, которые даже в случае перехвата не могут быть никоим образом использованы против вас, применяйте WPA2 и не очень беспокойтесь. Ну, для большего спокойствия отключите широковещание идентификатора беспроводной сети (SSID) в настройках маршрутизатора и/или точки доступа — чтобы даже никто не знал, что рядом есть ваша сеть;
- если же по беспроводной сети передаются важные данные, то можно защитить передаваемую информацию путем создания виртуальных частных сетей (VPN) поверх беспроводных каналов связи. В этом случае трафик, даже если и перехватят, то разобраться с ним не смогут, поскольку он будет зашифрован.

Аутентификация пользователей и устройств Wi-Fi

Современные точки доступа и беспроводные маршрутизаторы поддерживают следующие способы проверки пользователей и устройств при их подключении:

- **проверка MAC-адреса подключаемого устройства**. Этот способ подразумевает, что администратор для каждой точки доступа вручную настроит список MAC-адресов устройств, которым разрешено подключение к точке доступа.

Такой подход весьма утомителен и малоэффективен, поскольку MAC-адреса устройств можно перехватить, а изменить MAC-адрес устройства не составит труда даже для не очень подготовленного взломщика;

- **парольная фраза**. Этот способ может использоваться со всеми стандартами шифрования: WEP, WPA, WPA2. Он достаточно оптимален для дома или небольшого офиса, где всем пользователям сети можно доверять. Дело в том, что пароли на клиентах (в настройках операционной системы) хранятся в незашифрованном виде. Любой пользователь может легко их просмотреть и, следовательно, передать кому-либо еще — ведь пароль один на всех, и выяснить, кто именно выдал этот пароль, будет очень сложно. Если же в сети «все свои», то об этом можно не беспокоиться;
- **аутентификация с помощью RADIUS-сервера**. Этот способ следует использовать в корпоративной среде. Наличие RADIUS-сервера подразумевает, что у каждого пользователя будут свои аутентификационные данные;
- **использование PKI** (Public Key Infrastructure, инфраструктура открытых ключей). Настройка беспроводных устройств для аутентификации с использованием сертификатов по протоколу 802.1x практически идентична примеру, описанному в *разд. «Настройка протокола 802.1x» главы 9*. Разница заключается в том, что в мастере создания политики удаленного доступа нужно выбрать вариант **Беспроводной доступ**.

> ***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 клиентского 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 к общественной (публичной) беспроводной сети следует принимать те же меры безопасности, что и при работе в Интернете.

Первым делом нужно включить брандмауэр, если он выключен. Если вы не используете сторонние межсетевые экраны, включите хотя бы стандартный брандмауэр Windows — в последних версиях Windows (8, 8.1, 10, 11) он отлично справляется со своими обязанностями.

Для общественной беспроводной сети следует обязательно запретить входящие подключения к вашему компьютеру (рис. 3.13).

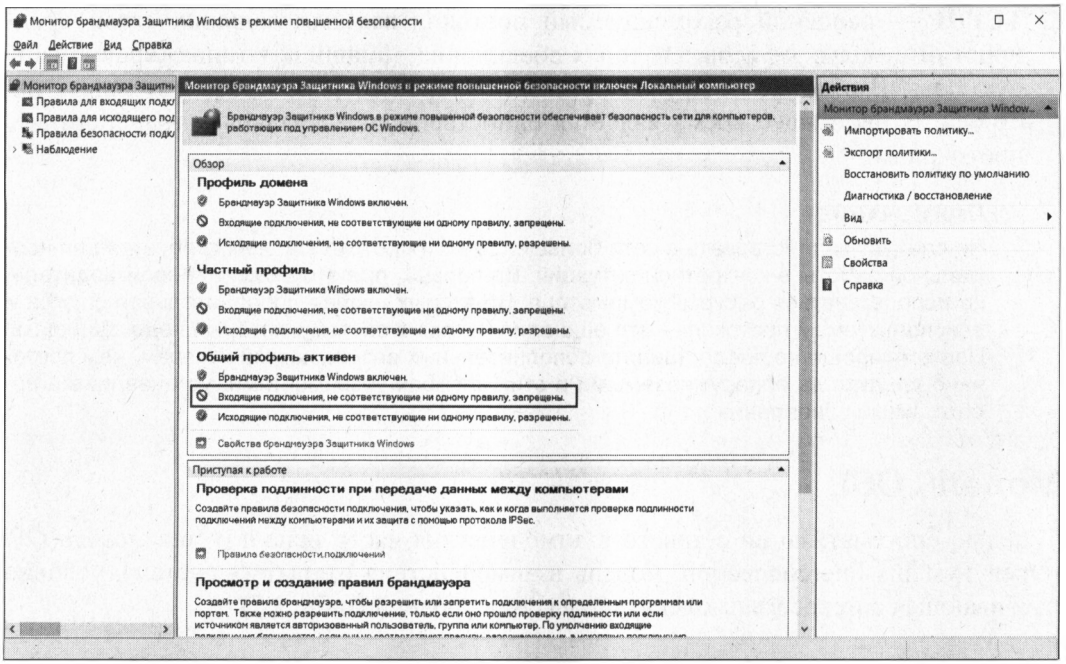


Рис. 3.13. Отключение входящих подключений в публичной сети

Настройка транспортных протоколов

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. Познакомимся с ними подробнее.

- **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). Протокол не является маршрутизируемым. Сети на основе NetBEUI очень трудно расширить. Протокол устарел и больше не используется.
- **NWLink IPX/SPX** — если в сети есть серверы Novell NetWare, то этот протокол необходим для организации связи с ними (в последних версиях Netware по умолчанию задействован протокол TCP/IP). В противном случае этот протокол следует исключить из числа используемых в системе. Сети Novel NetWare давно канули в Лету и больше не актуальны.

- **TCP/IP** — основной рекомендуемый протокол как для больших сетей предприятий и малых офисов, так и для соединения домашних компьютеров в частную сеть. В отличие от других протоколов, требует ряда предварительных настроек. В настоящее время является единственным актуальным транспортным протоколом.

> ***Примечание***
>
> Не следует задействовать 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 сетевого взаимодействия часто используется *модель OSI* (Open Systems Interconnection, модель взаимодействия открытых систем), условно разбивающая сетевое взаимодействие на семь уровней (табл. 3.7).

Таблица 3.7. *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)	—
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

Таблица 3.7 (окончание)

Уровень OSI	Назначение	Примеры	Необходимое сетевое оборудование
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

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 весьма сложно. В маркетинговых целях в описаниях коммутаторов часто указывают, что они работают, например, на уровне 4 или 7. На практике это означает только, что при реализации определенного функционала в коммутаторах осуществляется 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), приоритизации пакетов и т. п.

Стек протоколов TCP/IP

Когда говорят о TCP/IP, то обычно подразумевают под этим именем большое количество различных стандартов, которые определяют те или иные варианты взаимодействия в сети с использованием протокола TCP/IP.

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 по Интернету телефонных переговоров. 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 служат 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.

Протокол IPv6

Бурное развитие Интернета привело к тому, что параметры, заложенные при создании протоколов IP, стали сдерживать дальнейшее развитие глобальной сети. Так появился протокол IPv6 (более подробно о протоколе IPv6 рассказано в *главе 5*).

К основным особенностям IPv6 относятся:

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

Протокол IPv6 устанавливается по умолчанию в новые версии операционных систем Windows (начиная с Windows XP — для включения необходимо выполнить команду `ipv6 install`) и Linux. Некоторые технологии, например DirectAccess (рассматривается в *главе 5*), основаны на возможностях этого протокола. Протокол IPv6 принят в качестве основного при развитии Интернета в некоторых странах (в частности, в Китае).

В нашей стране пока не создана инфраструктура, поддерживающая этот протокол. Поэтому при желании его использовать можно, но только внутри сети предприятия, когда вся его инфраструктура находится под вашим контролем и управлением. Кроме того, следует также учитывать все имеющиеся нюансы (например, что система разрешения имен в DirectAccess построена через сервер корпорации Microsoft).

Параметры TCP/IP-протокола

Здесь и далее мы будем рассматривать характеристики протокола IPv4.

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-провайдеров 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» диапазона IP-адресов. 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.

Для построения *локальных сетей* предприятий выделены специальные диапазоны адресов. Это адреса 10.x.x.x, 192.168.x.x, 10.x.x.x, с 172.16.x.x по 172.31.x.x, 169.254.x.x (под «x» подразумевается любое число от 0 до 254). 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. Такие адреса часто называют *серыми* адресами.

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 5*.

Групповые адреса

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

Для этого компьютеру присваивается еще один IP-адрес из специального диапазона: с 224.0.0.0 по 239.255.255.255[1], причем диапазоны 224.0.0.0–224.0.0.255

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

и 239.0.0.0–239.255.255.255 не могут быть использованы в приложениях и предназначены для протоколов маршрутизации (например, адрес 224.0.0.1 принадлежит всем системам сегмента сети; адрес 224.0.0.2 — всем маршрутизаторам сегмента и т. д). Назначение адресов групповой рассылки производится соответствующим программным обеспечением.

Групповая рассылка поступает *одновременно на все* подключенные устройства. В результате сетевой трафик может быть существенно снижен по сравнению с вариантом передачи таких данных каждому устройству сети независимо.

По умолчанию рассылки передаются на все порты, даже если к ним не подключены устройства, подписавшиеся на эту рассылку. Чтобы исключить такой паразитный трафик, используются специальные возможности коммутаторов: поддержка IGMP snoophing (прослушивание протокола IGMP), PIM DM/PIM SM (PIM-DM, Protocol Independent Multicast Dense Mode и PIM-SM, Protocol Independent Multicast Sparse Mode — протоколы маршрутизации многоадресных сообщений). При включении и настройке этого функционала (поддерживается не всеми моделями оборудования) данные будут передаваться только на нужные порты.

Распределение IP-адресов сети малого офиса

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

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*. Удобно часть динамических адресов выдавать для локального использования, а часть — для внешних клиентов («гостей») сети. Это позволяет проще настраивать ограничения доступа к внутренним ресурсам сети для сторонних систем.

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

Подсети и маска адреса

Понятие *подсети* введено, чтобы можно было выделить часть IP-адресов одному предприятию, часть — другому 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 адреса — это параметр, который сообщает программному обеспечению о том, сколько компьютеров объединено в ту или иную группу (подсеть). Маска адреса имеет такую же структуру, что 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 эту 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. Тогда адрес 192.168.0.255 является адресом широковещательной рассылки для этой 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 служит 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 предприятия используют диапазоны локальных адресов сетей класса C. Сеть класса C имеет маску адреса 255.255.255.0 и может содержать до 254 хостов. Применение сетей класса C при разбиении на подсети VLAN в условиях предприятия связано с тем, что протоколы автоматической маршрутизации используют именно такие подсети.

При создании подсетей на предприятии 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 какому-либо коммутатору подключены подсети 192.168.0.0/255.255.255.0, 192.168.1.0/255.255.255.0 и 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.

---

[1] Значение 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.

Эта рекомендация несущественна для сетей малых и средних предприятий, 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**.

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

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.

Шлюзы бывают аппаратными и программными. В качестве аппаратного шлюза может выступать, например, маршрутизатор Wi-Fi. Программным шлюзом считается компьютер с развернутым на нем программным обеспечением — например, с ОС Linux и брандмауэром iptables. С другой стороны, разделение на программные и аппаратные — весьма условное. Ведь любой маршрутизатор Wi-Fi является небольшим компьютером, на котором запущен урезанный вариант Linux и работает тот же iptables или другой брандмауэр.

Для работы *только* в локальной сети шлюз может не назначаться. И если для доступа в Интернет используется прокси-сервер, то компьютерам локальной сети адрес шлюза также может не назначаться.

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

Предприятие 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 table). 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.

В TCP/IP-сетях информация о маршрутах имеет вид правил. Например, чтобы добраться к сети А, нужно отправить пакеты через компьютер Д. Кроме набора маршрутов есть также и стандартный маршрут — по нему отправляют пакеты, предназначенные для отправки в сеть, маршрут к которой явно не указан. Компьютер, на который отправляются эти пакеты, называется *шлюзом по умолчанию* (default gateway). Получив пакет, шлюз решает, что с ним сделать: или отправить дальше, если ему известен маршрут в сеть получателя пакета, или же уничтожить пакет, как будто бы его никогда и не было. В общем, что сделать с пакетом — это личное дело шлюза по умолчанию, все зависит от его набора правил маршрутизации. Наше дело маленькое — отправить пакет на шлюз по умолчанию.

Просмотреть таблицу маршрутизации протокола TCP/IP можно при помощи команды: `route print` — для Windows или `route` — в Linux. 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).

В Linux кроме команды `route` можно использовать команду `netstat -r` или `netstat -rn`. Разница между командами `netstat -r` и `netstat -rn` заключается в том, что параметр `-rn` запрещает поиск доменных имен в DNS, поэтому все адреса будут представлены в числовом виде (подобно команде `route` без параметров). А вот разница между выводом `netstat` и `route` заключается в представлении маршрута по умолчанию (`netstat` выводит адрес 0.0.0.0, а `route` — метку `default`) и в названии полей самой таблицы маршрутизации.

Какой командой пользоваться — решать вам. Раньше мы применяли `route` и для просмотра, и для редактирования таблицы маршрутизации. Теперь для просмотра таблицы мы используем команду `netstat -rn`, а для ее изменения — команду `route`.

На рис. 3.14 показан вывод команд `netstat -rn` и `route`. Видны две сети: 192.168.181.0 и 169.254.0.0 — обе на интерфейсе eth0. Такая ситуация сложилась из-за особенностей NAT/DHCP виртуальной машины VMware, в которой была запущена Linux для снятия снимков с экрана. В реальных условиях обычно вы увидите по одной подсети на одном интерфейсе. С другой стороны, рис. 3.14 демонстрирует поддержку VLAN, когда один интерфейс может использоваться двумя подсетями. Шлюз по умолчанию — компьютер с адресом 192.168.181.2, о чем свидетельствует таблица маршрутизации.

Поля таблицы маршрутизации объясняются в табл. 3.8.

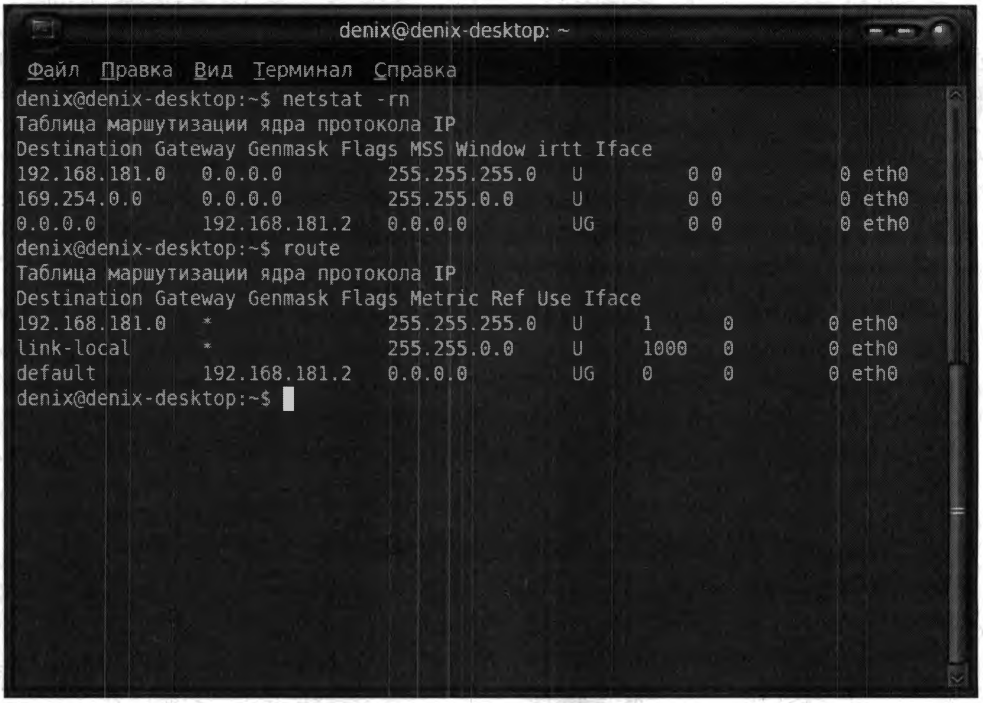


Рис. 3.14. Команды `netstat -rn` и `route`

***Таблица 3.8.** Поля таблицы маршрутизации*

Поле	Описание
Destination	Адрес сети назначения
Gateway	Шлюз по умолчанию
Genmask	Маска сети назначения
Flags	Поле **Flags** содержит флаги маршрута: • U — маршрут активен; • H — маршрут относится не к сети, а к хосту; • G — эта машина является шлюзом, поэтому при обращении к ней нужно заменить MAC-адрес машины получателя на MAC-адрес шлюза (если MAC-адрес получателя почему-то известен); • D — динамический маршрут, установлен демоном маршрутизации; • M — маршрут, модифицированный демоном маршрутизации; • C — запись кеширована; • ! — запрещенный маршрут
Metric	Метрика маршрута, т. е. расстояние к цели в хопах (переходах). Один хоп (переход) означает один маршрутизатор
Ref	Количество ссылок на маршрут. Не учитывается ядром Linux, но в других операционных системах, например в FreeBSD, вы можете столкнуться с этим полем

Таблица 3.8 (окончание)

Поле	Описание
Use	Содержит количество пакетов, прошедших по этому маршруту
Iface	Используемый интерфейс
MSS	Максимальный размер сегмента (Maximum Segment Size) для TCP-соединений по этому маршруту
Window	Размер окна по умолчанию для TCP-соединений по этому маршруту
irtt	Протокол TCP гарантирует надежную доставку данных между компьютерами. Для такой гарантии используется повторная отправка пакетов, если они были потеряны. При этом ведется счетчик времени: сколько нужно ждать, пока пакет дойдет до назначения и придет подтверждение о получении пакета. Если время вышло, а подтверждение-таки не было получено, то пакет отправляется еще раз. Это время и называется rtt (round-trip time, время «путешествия» туда-обратно). Параметр **irtt** — это начальное время rtt. В большинстве случаев подходит значение по умолчанию, но для некоторых медленных сетей — например, для сетей пакетного радио — значение по умолчанию слишком короткое, что вызывает ненужные повторы. Параметр **irtt** можно увеличить командой `route`. По умолчанию его значение 0

Теперь вернемся в Windows. Вывод команды `route print` в Windows выглядит примерно так:

```
IPv4 таблица маршрута
===========================================================================
Активные маршруты:
    Сетевой адрес          Маска сети      Адрес шлюза       Интерфейс  Метрика
          0.0.0.0          0.0.0.0    192.168.43.1    192.168.43.30       25
        127.0.0.0        255.0.0.0         On-link         127.0.0.1      306
        127.0.0.1  255.255.255.255         On-link         127.0.0.1      306
  127.255.255.255  255.255.255.255         On-link         127.0.0.1      306
     192.168.43.0    255.255.255.0         On-link     192.168.43.30      281
    192.168.43.30  255.255.255.255         On-link     192.168.43.30      281
   192.168.43.255  255.255.255.255         On-link     192.168.43.30      281
     192.168.52.0    255.255.255.0         On-link      192.168.52.1      276
     192.168.52.1  255.255.255.255         On-link      192.168.52.1      276
   192.168.52.255  255.255.255.255         On-link      192.168.52.1      276
    192.168.153.0    255.255.255.0         On-link     192.168.153.1      276
    192.168.153.1  255.255.255.255         On-link     192.168.153.1      276
  192.168.153.255  255.255.255.255         On-link     192.168.153.1      276
        224.0.0.0        240.0.0.0         On-link         127.0.0.1      306
        224.0.0.0        240.0.0.0         On-link     192.168.153.1      276
        224.0.0.0        240.0.0.0         On-link      192.168.52.1      276
        224.0.0.0        240.0.0.0         On-link     192.168.43.30      281
  255.255.255.255  255.255.255.255         On-link         127.0.0.1      306
  255.255.255.255  255.255.255.255         On-link     192.168.153.1      276
  255.255.255.255  255.255.255.255         On-link      192.168.52.1      276
  255.255.255.255  255.255.255.255         On-link     192.168.43.30      281
===========================================================================
```

Проверим путь прохождения пакетов на адрес Интернета — например, на **google.com**, с помощью команды `tracert` (в Linux используется команда `traceroute`, можно также применять команду `tracepath`):

```
tracert google.com
```

В итоге получаем примерно такую картину:

```
tracert google.com

Трассировка маршрута к google.com [172.217.13.142]
с максимальным числом прыжков 30:

  1    115 ms    115 ms    115 ms  10.11.18.1
  2    115 ms    114 ms    114 ms  154.6.12.125
  3    116 ms    115 ms    115 ms  98.142.220.58
  4    115 ms    116 ms    120 ms  core1-0-0-8.lga.net.google.com [198.32.118.39]
  5    116 ms    116 ms    128 ms  108.170.248.35
  6    116 ms    115 ms    123 ms  142.250.57.145
  7    140 ms    128 ms    124 ms  142.251.49.201
  8    127 ms    124 ms    123 ms  192.178.75.0
  9    132 ms    123 ms    124 ms  108.170.251.49
 10    125 ms    123 ms    125 ms  108.170.231.55
 11    123 ms    123 ms    123 ms  yul02s05-in-f14.1e100.net [172.217.13.142]

Трассировка завершена.
```

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 нужный нам маршрут:

```
route add 91.203.4.50 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, мы явно указали адрес сетевого интерфейса, через который нужно пересылать пакеты.

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

```
Активные маршруты:
Сетевой адрес        Маска сети        Адрес шлюза       Интерфейс   Метрика
...
91.203.4.50    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 и приведена в этом примере (остальные строки не изменились и опущены для наглядности).

Выполненные изменения маршрутизации действуют до перезагрузки системы или до подачи обратной команды — удаления записей маршрутизации. Для восстановления параметров маршрутизации достаточно подать следующую команду, указав тот маршрут, который требуется удалить:

```
route delete 91.203.4.50
```

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 приходится сталкиваться с ситуациями, когда изменение параметров маршрутизации в операционной системе Windows не сразу «отрабатывается» корректно. Иногда после операций над таблицей маршрутизации для достижения успеха приходится 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. А для того чтобы обеспечить доступ в такие сети, администраторы должны уметь написать правильную таблицу маршрутизации для соответствующей VLAN или создать список доступа — ACL (Access Control List), в котором правила записываются аналогично правилам маршрутизации.

Автоматическое присвоение параметров IP-протокола

Параметры протокола IP индивидуальны для каждого компьютера. Чтобы облегчить процесс настройки компьютеров, были разработаны специальные средства, автоматизирующие процесс настройки.

Серверы DHCP

Сервер DHCP (Dynamic Host Configuration Protocol) осуществляет автоматическую настройку узлов сети. С помощью DHCP компьютер, подключенный к сети, в которой есть DHCP-сервер, может получить IP-адрес, маску сети, IP-адрес шлюза, адреса серверов DNS и другие сетевые параметры.

Особенно удобно использовать DHCP в средних и больших сетях. Вы только представьте, что у вас в сети есть, скажем, 20 компьютеров. Если им назначать IP-адреса статически, то вам придется подойти к каждому компьютеру и прописать

его IP-адрес, а заодно и IP-адрес сети, IP-адрес шлюза и адреса серверов DNS. Понятно, что эту процедуру надо будет выполнить разово — при настройке сети. Но если через некоторое время конфигурация сети изменится (например, вы поменяете провайдера) и потребуется изменить IP-адреса DNS-серверов, то вам придется все повторить заново — снова обойти все компьютеры и прописать для них новые DNS-серверы.

Адресация APIPA

Для облегчения построения небольших сетей предусмотрена возможность автоматического 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. Этот механизм позволяет применять IP-протокол в небольших сетях при минимальных ручных настройках — компьютеры в локальной сети увидят друг друга. 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 протокол NetBIOS поверх TCP/IP, то системы не смогут разрешить имена других компьютеров сети и т. п.

> ***Примечание***
>
> Использование адреса из указанного здесь диапазона (проверяется командами `ipconfig` или `winipcfg`) при наличии в сети сервера DHCP свидетельствует либо о неисправности последнего, либо о проблемах кабельного подключения 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 подключение, начинает выполнять роль сервера DHCP с единственным ограничением — его адрес *жестко фиксирован*: 192.168.0.1. Клиенты, которые получают от этого 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 является для небольших предприятий оптимальным. Настройте подключение к Интернету, включите его совместное использование — и вы получите у себя в сети корректное назначение параметров TCP/IP-протокола для компьютерных систем.

> ***Примечание***
>
> Из-за того, что в этой технологии используется один и тот же диапазон адресов, организовать канал соединения двух таких локальных сетей невозможно.

Порт

При передаче данных пакет информации, кроме IP-адресов отправителя и получателя, 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 от 1024 до 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 той или иной программы.

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

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

```
netstat -a
Активные подключения
  Имя    Локальный адрес        Внешний адрес          Состояние
  TCP    0.0.0.0:135            acer:0                 LISTENING
  TCP    0.0.0.0:445            acer:0                 LISTENING
  TCP    0.0.0.0:554            acer:0                 LISTENING
  TCP    0.0.0.0:902            acer:0                 LISTENING
  TCP    0.0.0.0:912            acer:0                 LISTENING
  TCP    0.0.0.0:2869           acer:0                 LISTENING
  TCP    0.0.0.0:5357           acer:0                 LISTENING
  TCP    0.0.0.0:10243          acer:0                 LISTENING
  TCP    0.0.0.0:49152          acer:0                 LISTENING
  TCP    0.0.0.0:49153          acer:0                 LISTENING
```

```
  TCP    0.0.0.0:49154          acer:0                 LISTENING
  TCP    0.0.0.0:49156          acer:0                 LISTENING
  TCP    0.0.0.0:49157          acer:0                 LISTENING
...
```

В этом примере на компьютере готовы к подключению несколько портов (состояние `LISTENING`).

> ***Примечание***
>
> Для получения информации по удаленному компьютеру используются специальные программы *сканирования портов*. Наиболее известный бесплатный продукт — nmap. Если нужно сертифицированное решение, можно порекомендовать программу XSpider. Данные по отдельному порту можно получить штатными средствами системы (например, с помощью команды `telnet` или утилиты PortQry из состава Support Tools). Обратите внимание, что хотя использование подобных программ не запрещено стандартами, тем не менее многие системы оценивают сканирование портов как попытку вторжения и блокируют источник на некоторый период времени.

Протокол ARP

В сети Ethernet пакеты адресуются не по именам и не по IP-адресам компьютеров — 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 устройства.

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

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 этой системы, после чего просмотреть кеш ARP (командой `arp -a`) и скопировать значение MAC-адреса в настройки DHCP.

MAC-адреса часто используются для идентификации систем при создании фильтров. Однако такой способ не отличается надежностью, поскольку изменить MAC-адрес программно, как правило, не составляет труда. Например, вот как просто можно изменить MAC-адрес в Linux:

```
# ifconfig eth1 down
# ifconfig eth1 hw ether a1:b2:c3:d4:e5:f6
# ifconfig eth1 up
```

Здесь `eth1` — имя интерфейса, для которого производится замена MAC-адреса, а `a1:b2:c3:d4:e5:f6` — его новый MAC-адрес.

В Windows изменить MAC-адрес можно с помощью редактора реестра (рис. 3.15). Для этого нужно перейти в раздел:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class\
{4D36E972-E325-11CE-BFC1-08002BE10318}
```

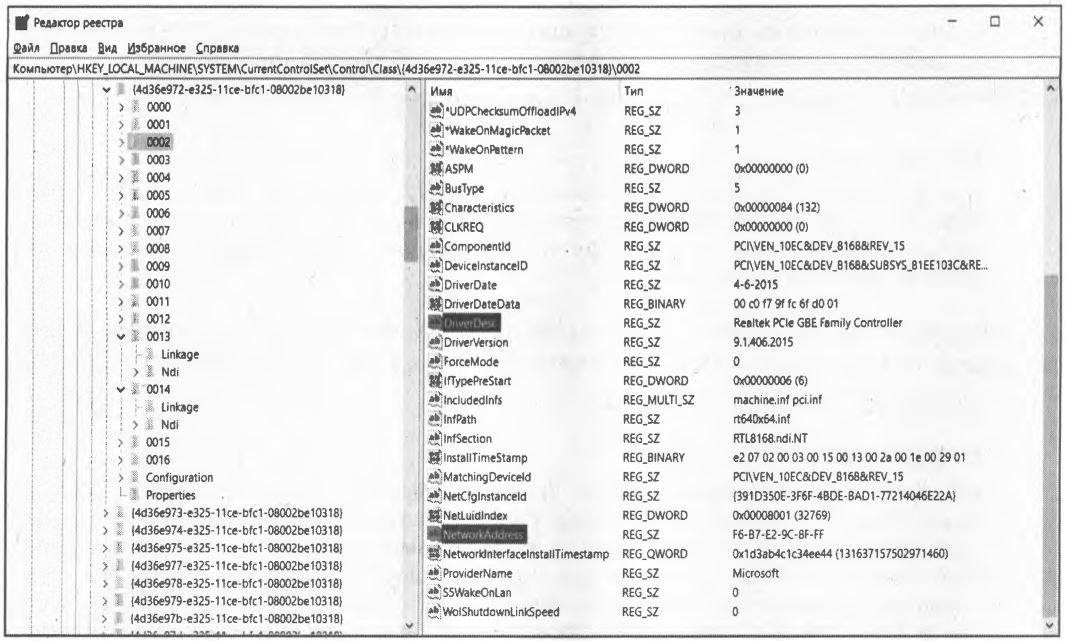


Рис. 3.15. Изменение MAC-адреса сетевого адаптера с помощью реестра

Затем выбрать подраздел с интересующим вас адаптером (наименование адаптера в подразделе содержится в параметре **DriverDesc**) и соответствующим образом изменить значение параметра **NetworkAddress**. После проделанных манипуляций компьютер лучше перезагрузить.

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. Однако эти имена могут быть и 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 этому хосту другое имя.

Имя хоста составляется из нескольких имен, разделяемых при написании точкой, — например, так: **www.ask.ru**. Первая слева группа символов (до точки) — в нашем примере это **www**, является собственным именем компьютера (точнее, его *псевдонимом* — см. об этом в табл. 3.8 далее). Следующая группа символов — от точки до точки — это имя группы компьютеров, которой принадлежит система. Следующая группа символов — имя группы компьютеров, которой, в свою очередь, принадлежат группы компьютеров, имена которых находятся левее. Такую цепочку можно продолжать сколь угодно долго, но для удобства обычно ограничиваются тремя-четырьмя группами символов.

На практике под *именем домена* понимают всю группу символов справа от полного 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_предприятия>.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 используют без перевода, русский же 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 вебсайта 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 то или иное доменное имя свободно, то его можно получить. Приобретение доменного имени — это платная услуга, кроме того, ежегодно действие имени необходимо продлевать. 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 организации. 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 предприятия.

В России «географические» домены имеют имена **ru** и **рф** (последний — для названий домена на кириллице). Сохранился также домен **su**, закрепленный ранее за

СССР. 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**.

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

В настоящее время список доменов, присваиваемых по типу деятельности, существенно расширен — в их число 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 же доменного имени для работы не обязательно). При необходимости в строках адреса программ, предназначенных для работы в Интернете, вместо доменного имени можно набирать IP-адрес.

Доменное имя может существовать, но не иметь IP-адреса (естественно, работа с этими узлами невозможна). Такая ситуация может возникнуть, если, например, предприятие заранее зарегистрировало за собой доменное имя, но не располагает в настоящий момент какими-либо ресурсами в сети Интернет. В этом случае говорят, что домен *не делегирован*.

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 веб-серверов, соответствующих различным предприятиям).

IP-адреса, соответствующие тому или иному доменному имени, могут меняться. Например, предприятие 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, как уже отмечалось ранее, 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 такого

метода, поскольку он приводит к значительному росту излишнего 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. 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 ресурсах.

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

WINS

Служба регистрации имен в сети Windows (Windows Internet Naming Service, WINS) использовалась для регистрации сетевых имен компьютеров в локальных сетях до Windows 2000. Эта служба позволяла корректно разрешать имена в сетях с наличием маршрутизаторов. Сейчас эта служба считается устаревшей, и вы с ней можете встретиться разве что в очень старых сетях, спроектированных в конце 1990-х—начале 2000-х годов. Такие сети — настоящие динозавры. Честно говоря, трудно представить себе сеть, которая за последние 20 лет не модернизировалась бы.

Статическое задание имен

Ранее, когда еще не было службы DNS, IP-адреса в сети задавались вручную — с помощью файла hosts. В нем прописывались IP-адреса и символьные имена компьютеров. Затем этот файл тиражировался по всем компьютерам сети, чтобы все они могли разрешать доменные имена/IP-адреса друг друга.

Недостаток этого способа — необходимость вручную контролировать состав сети. В небольшой сети со статическими IP-адресами это сделать относительно просто, особенно если учесть, что состав таких сетей часто не меняется.

Но если в вашей сети используется DHCP-сервер (а где он сейчас не используется?), вряд ли вы будете вручную задавать имена узлов через файл hosts.

Тем не менее 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.).

Все три файла (lmhosts, hosts и networks) находятся в папке %systemroot%\system32\drivers\etc. При установке системы обычно создаются файлы примеров (имеют расширение sam), по образцу которых и следует редактировать соответствующие файлы.

Изменять эти 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 такие 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 работают в сети, а на других отображается сообщение, что вход в сеть не может быть осуществлен, 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 20*xx*/XP/7/8/10/11) нуждаются в информации DNS.

При необходимости разрешения имени сначала предпринимается попытка его поиска в локальных ресурсах. Прежде всего, это локальный кеш имен, который для увеличения производительности создают все системы (кеш имен NetBIOS или кеш имен DNS). Если нужное имя компьютера там не найдено, то система пытается найти его в host-файлах. Если и эта попытка неудачна, то системы с ОС 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 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.

С помощью DNS-системы на базе Windows 20*xx*/XP/7/8/10/11 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.

Настройка серверов DHCP и DNS

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

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 (в Windows Server 2012/2016/2019/2022 указанные шаги предлагает выполнить мастер установки роли):

- 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 клиентами, а также облегчит ситуацию восстановления сервера (например, после полной очистки его баз).

Создание области обеспечивает соответствующий мастер (рис. 3.16). Для IPv4-адресов доступны четыре типа областей:

- *обычные области* — используются для назначения адресов в сетях классов A, B и C;
- *многоадресные области* — используются для назначения IP-адресов в сетях IPv4 класса D;

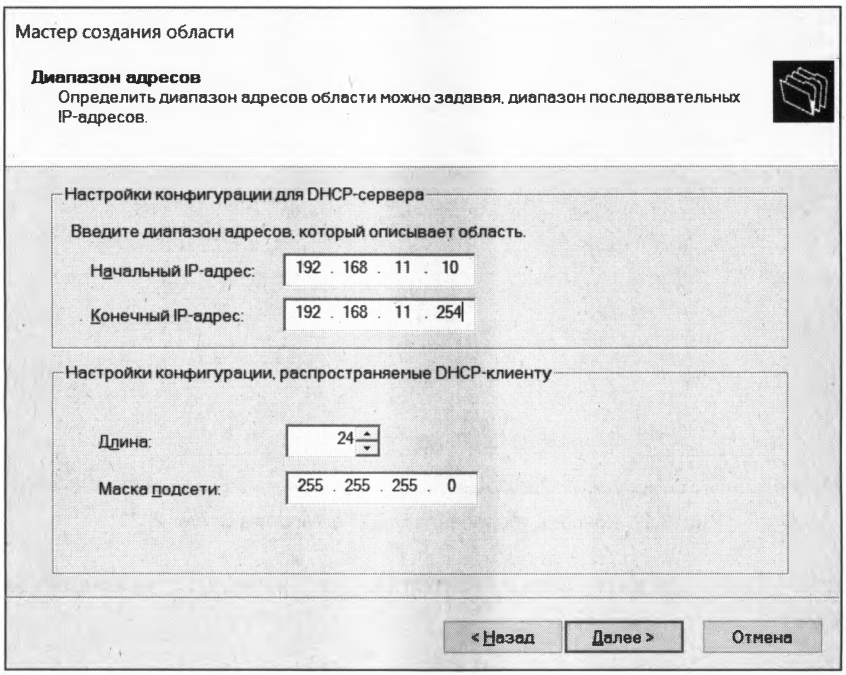


Рис. 3.16. Мастер создания области

- *суперобласти* — являются контейнерами для других областей, упрощающими управление несколькими областями;
- *области отказоустойчивости* — создаются между двумя DHCP-серверами для повышения отказоустойчивости, предоставления избыточности и включения балансировки нагрузки.

В случае с протоколом IPv6 поддерживаются только обычные области.

Авторизация DHCP-сервера

Прежде чем использовать DHCP-сервер в домене, его необходимо авторизовать в Active Directory, поскольку назначать динамические IP-адреса в домене могут только авторизированные серверы. Авторизация требуется для обслуживания клиентов неавторизованными DHCP-серверами.

Чтобы авторизовать DHCP-сервер, щелкните правой кнопкой мыши на элементе сервера в дереве консоли DHCP (рис. 3.17) и выберите команду **Авторизовать**

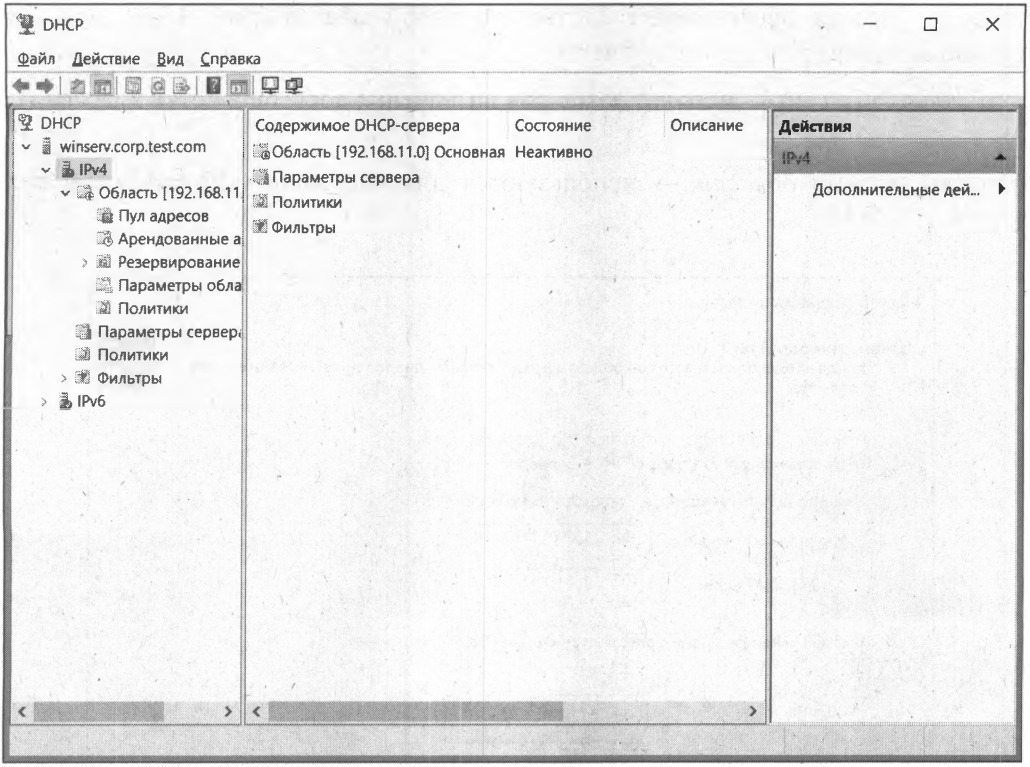


Рис. 3.17. Консоль управления DHCP в Windows Server 2022

(Authorize). Чтобы лишить сервер авторизации, выберите команду **Запретить** (Unauthorize).

> ***Примечание***
>
> Если в вашей сети есть DHCP-сервер, работающий под управлением другой операционной системы, например Linux или старых версий Windows (NT 4.0), то он будет обслуживать клиентов независимо от настроек в службе каталогов.

Настройка параметров области

Для полноценной работы в составе компьютерной сети обычно недостаточно получения только IP-адреса и маски сети — клиентам также минимально необходимы 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. Чтобы это происходило, необходимо определить *опции* (параметры) области/сервера (рис. 3.18).

> ***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.

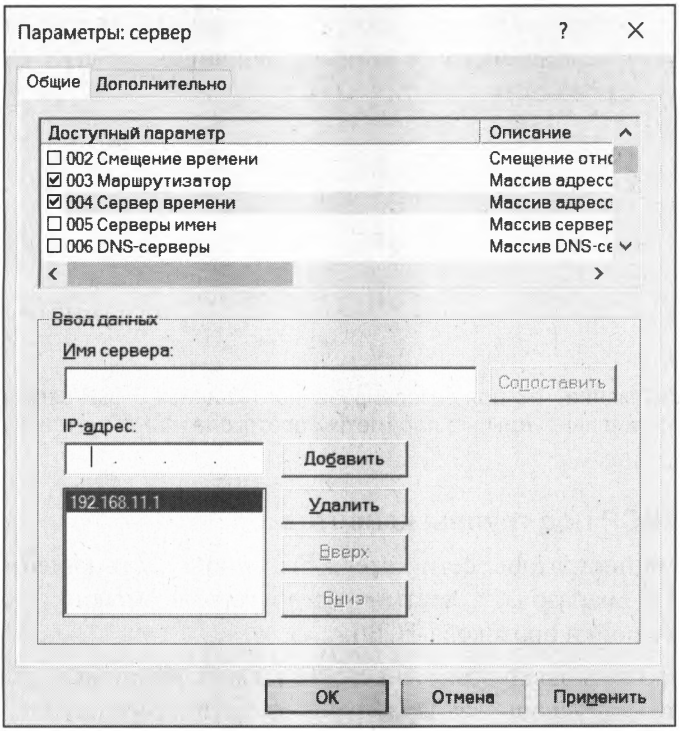


Рис. 3.18. Изменение опций сервера (Windows Server 2022)

Вы можете определить любые параметры области (как минимум следует указать те величины, которые запрашиваются мастером создания новой зоны), а при необходимости и создать собственные. Описание дополнительных параметров обычно включается в документацию прикладного программного обеспечения, которому необходимы дополнительные настройки DHCP.

Фиксированные IP-адреса

В некоторых случаях DHCP-сервер нужно настроить так, чтобы он выдавал клиентам не случайный IP-адрес, а заранее определенный (фиксированный). Например, такую конфигурацию могут потребовать серверы сети, IP-адреса которых должны оставаться неизменными.

Серверы можно настроить или вручную, присвоив им статический IP-адрес, или же настроить DHCP-сервер должным образом.

Чтобы DHCP-сервер одному и тому же компьютеру выдавал определенный IP-адрес, нужно знать MAC-адрес сетевого адаптера этого компьютера. Для определения MAC-адреса можно или использовать команду `ipconfig /all`, введенную непосредственно на сервере, MAC-адрес которого нужно получить, или же попытаться определить его 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.

В Linux для назначения компьютеру с определенным MAC-адресом определенного IP-адреса в блок описания опции (в конфигурационном файле DHCP-сервера) добавляется следующая область:

```
host server {
  option host-name "server";
  option routers 192.168.1.1;
  hardware ethernet AA:BB:CC:DD:EE:FF;
  fixed-address 192.168.1.2;
}
```

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

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.

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*: класс вендоров (vendor class) и класс пользователей (user class). Для клиентов того или иного класса администратор может настраивать индивидуальные опции DHCP-сервера. Например, в DHCP вендором считается производитель соответствующего программного обеспечения операционной системы. В результате можно разделить клиентов с операционными системами разных версий и вендоров.

> ***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 Windows 2000 и выше. Основное их 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, на больших предприятиях подобную настройку можно включить в образы операционной системы, которая потом будет тиражироваться раздельно по

структурам предприятия. Но для малых предприятий применение пользовательских классов обычно не востребовано.

Отказоустойчивость DHCP-сервера

Впервые поддержка отказоустойчивости DHCP-сервера появилась в Windows Server 2012 и только для протокола IPv4.

Отказоустойчивость предполагает высокую доступность DHCP-сервисов путем синхронизации информации об аренде IPv4-адресов между двумя DHCP-серверами в одном из двух режимов:

- **режим балансировки нагрузки (Load Balance)**. В этом режиме можно указать процентное соотношение загрузки каждого сервера. Обычно используется соотношение 50/50, чтобы нагрузка на каждый сервер была одинаковой. Но администратор может указать и другое значение — например, 70/30;
- **режим горячего резервирования (Hot Standby)**. В этом режиме один из серверов действует как основной сервер и обрабатывает DHCP-запросы. Второй сервер используется только в случае сбоя основного сервера.

Отказоустойчивые области создаются на основном DHCP-сервере. Если один из серверов станет недоступным, его место займет другой сервер — он продолжит назначать IP-адреса и возобновит существующие аренды. Также второй сервер начнет работать, если основной сервер просто окажется перегруженным, т. е. такие области используются и для балансировки нагрузки.

Создать отказоустойчивую область можно так:

1. Откройте консоль DHCP (выберите одноименную команду из меню **Средства диспетчера серверов**) и подключитесь к основному DHCP-серверу.
2. Разверните узел **IPv4**. Область, с которой вы будете работать, уже должна быть создана. В противном случае — создайте ее. Щелкните на области или суперобласти правой кнопкой мыши и выберите команду **Настройка отработки отказа** — откроется одноименное окно, в котором нужно нажать кнопку **Далее**.
3. Нажмите кнопку **Добавить сервер**, чтобы добавить вторичный DHCP-сервер, который будет использоваться с этой отказоустойчивой областью. Снимите флажок **Повторно использовать отношения отработки отказа, настроенные для этого сервера** и нажмите кнопку **Далее**.
4. Выберите в списке **Режим** тип отработки отказа: **Балансировка нагрузки** или **Горячая замена**.
   - Если вы выбрали первый вариант (**Балансировка нагрузки**), укажите, как должна распределяться нагрузка между серверами: например, 50/50 — когда нагрузка между двумя серверами распределяется одинаково, или 80/20 — когда основной сервер станет обрабатывать большую часть нагрузки, а потом уже будет подключаться второй сервер.
   - Если вы выбрали режим **Горячая замена**, установите роль партнера: **Активный** или **Резервный**, и укажите, сколько процентов адресов нужно зарезер-

вировать. По умолчанию для резервного сервера используется 5% диапазона адресов.

5. Заполните поле **Общий секрет** — это пароль, который серверы используют при синхронизации базы данных DHCP.
6. Нажмите кнопку **Готово**, а затем кнопку **Закрыть**.

Дополнительную информацию о настройке отказоустойчивых областей можно найти на сайте Microsoft по короткой ссылке: **https://bit.ly/3a5xuVU**.

Обслуживание DHCP-сервером других сегментов сети

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

> ***Примечание***
>
> 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.

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). Обычно используется агент ретрансляции, установленный на коммутационном оборудовании. Но можно задействовать и агент, 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 этом сегменте сети есть свой DHCP-сервер, который и обслужит клиента, — таким образом можно повысить отказоустойчивость сегмента сети, дублируя локальный DHCP-сервер соответствующей областью на удаленном DHCP-сервере). Если запрос клиента остается необслуженным, то агент ретранслирует запрос в соседние сегменты сети. Если в соседних сегментах есть DHCP-сервер, то он получает этот 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.

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

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 (запрос идет от адреса 0.0.0.0 с маской 255.255.255.255). 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 клиент 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 этот 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, то текущие настройки IP-адреса также освобождаются. Такая ситуация может свидетельствовать о переносе компьютера в другой сегмент сети, поэтому он и освобождает свой адрес.

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

Сервер сам 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.

Параметры DHCP-сервера находятся в ключе реестра:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DHCPServer\Parameters
```

Регистрацией событий DHCP-сервера управляют следующие параметры:

- `DhcpLogFilesMaxSize` — максимальный размер всех журналов. По умолчанию — 70 Мбайт;
- `DhcpLogDiskSpaceCleanupInterval` — задает частоту проверки использования диска и очистки журнала. По умолчанию — 60 минут;
- `DhcpLogMinSpaceOnDisk` — порог свободного пространства, необходимый для записи в журнал. Если на диске осталось меньше места, запись в журнал прекращается, пока не освободится дополнительное дисковое пространство. По умолчанию — 20 Мбайт.

Интеграция DHCP и DNS

В Windows Server 2012 появилась новая функция — *защита имен*. Эта функция разрешает DHCP-серверу регистрировать записи от имени клиента, только если никакой другой клиент с этой DNS-информацией не зарегистрирован. Можно на-

строить защиту имени, как для IPv4, так и для IPv6, — на уровне сетевого адаптера или на уровне области.

Защита имен предназначена для предотвращения *занятия имен*. Занятие имен происходит, когда компьютер с ОС, отличной от Windows, регистрирует в DNS имя, которое уже используется на компьютере под управлением Windows. Благодаря защите имен можно предотвратить занятие имени компьютерами, работающими под управлением другой ОС, отличной от Windows.

Включить защиту имен можно с помощью оснастки DHCP в свойствах IPv4/IPv6 (рис. 3.19).

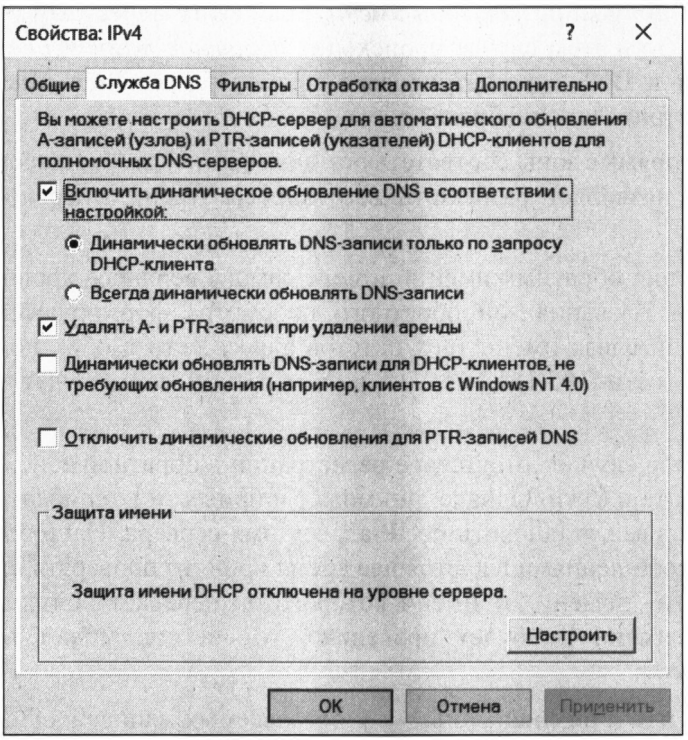


Рис. 3.19. Свойства IPv4 в оснастке DHCP

DNS

В доменах Windows информацию о службах, необходимых для работы систем, 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. И прежде всего вам нужно ознакомиться с основными терминами, связанными с DNS.

- **Зона DNS** — это часть пространства имен, для которого DNS-сервер может выполнять операции разрешения имен. Важно понимать разницу между доменом и зоной. Зона — это не домен. Зона — это часть домена, которая управляется определенным DNS-сервером. Если домен небольшой, то зона — это и есть домен. Именно поэтому эти два понятия часто путают. Существуют зоны прямого и обратного просмотра, которые на практике для удобства называют *прямой* и *обратной зонами.*

  Прямая зона служит для разрешения доменного имени системы в ее IP-адрес, *обратная* — для обратного разрешения, т. е. позволяет определить доменное имя по IP-адресу. Поэтому когда 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.

  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 для первичной зоны. В случае домена Windows 20*xx* и использования зоны DNS, интегрированной со службой каталогов, изменения можно вносить на любом DNS-сервере такой 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 осуществляться 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 создаются 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 тогда 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 старые 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 кеша* для соответствующей зоны — в консоли управления сервером включить опцию отображения дополнительных параметров, найти нужную зону среди структуры кеша и осуществить ее очистку. Однако и эта операция также не гарантирует получение актуальной копии записей, поскольку при следующем запросе данных из этой зоны сервер загрузит копию с того сервера DNS, на который настроена пересылка запросов. Поэтому при рассмотрении проблемных ситуаций следует выяснить на официальных ресурсах адреса NS-серверов нужного домена и проверить записи с по-мощью 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 кеш DNS-записей командой: `ipconfig /flushdns`.

- **Передача зон** — так называется специальная операция копирования всех записей той или иной 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 со-

держаться 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 проведено 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 станет отправлять запросы на уже несуществующий адрес, и в результате будет формироваться неверный ответ).

  Для исправления подобной ситуации в DNS-сервере, начиная с 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 указывалось ранее, принято называть именем «точка». Если в DNS создать зону «точка» (зона с таким именем создается при установке службы каталогов с одновременной установкой и настройкой сервера DNS), то это будет фактически означать, что этот 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 сообщит, 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

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 осуществить все операции для разрешения имени. Обычно для этой цели необходимо выполнить несколько запросов к различным серверам DNS.

Процесс определения имени с использованием итеративных запросов весьма трудоемок — необходимо найти NS-сервер нужного 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 кеш 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, далее 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 кешировано на исходном сервере. Этим резко снижается нагрузка на сеть и уменьшается время ответа на запрос. 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 (как правило, это DNS-сервер провайдера). Тем самым вся процедура разрешения имен будет выполняться уже другим сервером. Поскольку мощные серверы Интернета обычно имеют существенно больший кеш 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 добавление некоторых специальных *записей ресурсов* (resource records), приведенных в табл. 3.9.

Таблица 3.9. *Ресурсные записи DNS*

Запись	Описание
SOA (Start of Authority)	Содержит серийный номер зоны, который увеличивается при любом изменении записей зоны. На практике этот номер формируется в формате год-месяц-день — например: 20181005
NS (Name Server)	Содержит «официальные» серверы DNS текущей зоны. Только эти серверы могут возвращать авторизированные ответы
RP (Responsible Person)	Содержит e-mail лица, ответственного за внесение изменений в записи зоны. Желательно поддерживать этот адрес всегда в актуальном состоянии. Помните, что символ @ в нем заменяется точкой. Например, если адрес ответственного лица **admin@example.com**, то его нужно указать так: **admin.example.com**
A (Host Address)	Содержит информацию об имени системы и ее IP-адресе. Эта запись добавляется в DNS-сервер при регистрации узла
PTR (Pointer, указатель)	Запись обратной зоны. Обычно DNS-сервер автоматически создает/изменяет эту запись при создании/изменении записи A в прямой зоне
CNAME (Canonical NAME)	Определяет псевдоним узла. Обычно названия узлов: **www**, **ftp**, **mail** — являются псевдонимами

Таблица 3.9 (окончание)

Запись	Описание
MX (Mail eXchanger)	Служит для задания почтового сервера. Чтобы на нужный 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)	Используется для обнаружения в домене различных служб. Обычно такие записи автоматически создаются службой каталогов

Примечание

Кроме приведенных здесь 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

DNS-сервер можно установить только на компьютер со статическим IP-адресом. Очень важно, чтобы DNS-сервер мог разрешать как полные (**server.example.com**), так и неполные (**server**) доменные имена. Для этого нужно, чтобы DNS-суффикс компьютера, на котором вы установили DNS-сервер, совпадал с суффиксом имени домена предприятия. Необходимые настройки можно выполнить в параметрах TCP/IP-протокола, статически устанавливаемых для сетевого адаптера сервера DNS.

Настроить параметры DNS можно на вкладке **DNS** окна **Дополнительные параметры TCP/IP**. Для открытия этого окна выполните следующие действия:

1. Откройте Центр управления сетями и общим доступом и щелкните на ссылке **Изменение параметров адаптера**.
2. В окне **Сетевые подключения** щелкните правой кнопкой мыши на подключении, которое вы хотите настроить, и выберите команду **Свойства**.
3. Щелкните двойным щелчком на протоколе **TCP/IPv4** (или **TCP/IPv6**) — в зависимости от того, какой протокол вы хотите настроить.
4. Если нужно, чтобы адрес DNS-сервера был задан по DHCP, установите переключатель **Получить адрес DNS-сервера автоматически**. Иначе установите переключатель **Использовать следующие адреса DNS-серверов**, а затем введите адреса основного и дополнительного DNS-серверов в соответствующие поля.
5. Нажмите кнопку **Дополнительно** — откроется окно **Дополнительные параметры TCP/IP**. Перейдите на вкладку **DNS** и настройте необходимые параметры:

- **Адреса DNS-серверов, в порядке использования** — здесь указываются IP-адреса каждого DNS-сервера, которые используются для разрешения доменных имен. Если указать несколько серверов DNS, их приоритет определяется очередностью в списке. Если первый сервер не может ответить на запрос о разрешении имени хоста, запрос будет отправлен следующему DNS-серверу, и т. д.;
- **Дописывать основной DNS-суффикс и суффикс подключения** — обычно по умолчанию этот параметр установлен. Его нужно включить для разрешения неполных имен компьютеров. Основной домен задается на вкладке **Имя компьютера** диалогового окна **Свойства системы**;
- **Добавлять родительские суффиксы основного DNS-суффикса** — по умолчанию этот параметр установлен. Он используется для разрешения неполных имен компьютеров в иерархии родительских/дочерних доменов;
- **Дописывать следующие DNS-суффиксы (по порядку)** — этот параметр может использоваться для задания особых DNS-суффиксов вместо имени родительского домена;
- **DNS-суффикс подключения** — содержит DNS-суффикс подключения, который переопределяет DNS-имена, уже настроенные на использование с этим подключением. Напомним, что имя домена DNS указывается на вкладке **Имя компьютера** диалогового окна **Свойства системы**;
- **Зарегистрировать адреса этого подключения в DNS** — параметр используется, если нужно зарегистрировать все IP-адреса для этого соединения в DNS с FQDN-именами компьютеров. Включен по умолчанию;
- **Использовать DNS-суффикс подключения при регистрации в DNS** — включите этот параметр, если вам нужно, чтобы все IP-адреса для этого подключения регистрировались в DNS родительского домена.

Для установки службы DNS-сервера достаточно выбрать соответствующую опцию среди добавляемых компонентов (выбрать роль). В целях отказоустойчивости информационная система должна быть настроена на использование нескольких серверов DNS.

После запуска службы DNS следует уточнить некоторые параметры настройки. Во-первых, если сервер должен разрешать имена сети Интернет, то следует удалить зону «точка» (если она 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.

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 применена действующая в Windows система безопасности).

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. Эти записи создаются автоматически через некоторое время после установки службы каталогов.

Разделение DNS

Все большее число сотрудников начинают использовать мобильные компьютеры для доступа к ресурсам предприятия 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:

- **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. 3.20).

  На сервере DNS, обслуживающем домен Интернета этого же предприятия, необходимо настроить A-запись соответствующего ресурса на *внешний адрес* брандмауэра предприятия, а на брандмауэре настроить публикацию внутреннего ресурса таким образом, чтобы запрос, приходящий на брандмауэр и адресованный на то или иное имя, перенаправлялся на локальный адрес ресурса.

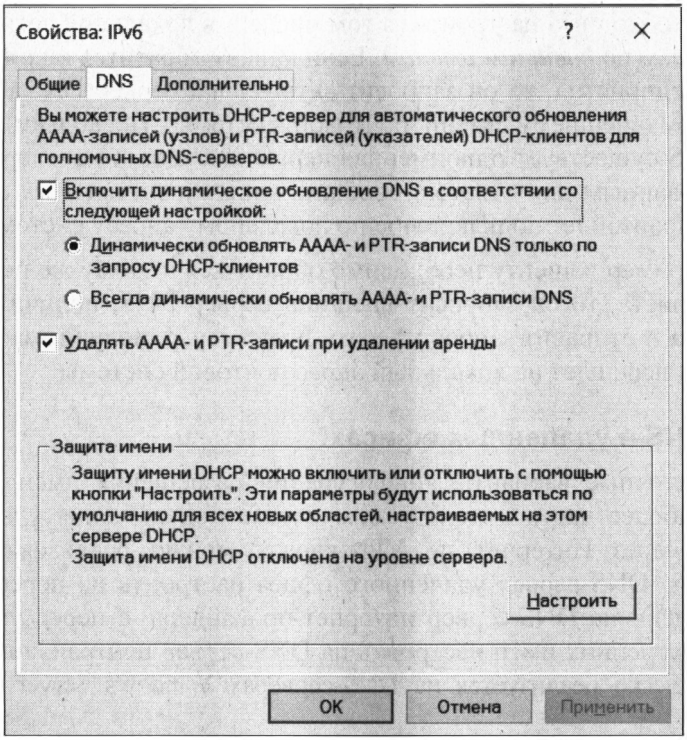


Рис. 3.20. Разделение DNS (Windows Server 2022)

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 станут обращаться к различным DNS-серверам. При этом локальный клиент будет обращаться по локальному адресу, а клиент Интернета перешлет запрос на брандмауэр предприятия, который и перенаправит его на локальный адрес запрашиваемого ресурса;

- **различные имена локального домена и домена Интернета** — если внутреннее и внешнее имена домена предприятия не совпадают, то на внутреннем сервере DNS необходимо создать первичную зону для домена с внешним именем. Затем в этой зоне следует создать записи, соответствующие именам систем, предоставляющих необходимые службы (естественно, что изменение записей этой зоны должно выполняться только вручную), 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 предприятия.

Клиентов необходимо настроить (в том числе и в локальной сети) на подключение к ресурсам по *внешним именам*. Если клиент обратится к почтовому серверу *изнутри* предприятия, 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, сообщит клиенту *внутренний адрес* почтовой системы и 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 DNS в удаленных офисах

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 2012/2016/2019/2022.

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, которая вызывается одноименной командой. 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 утилиты nslookup (строки, вводимые пользователем, отмечены в начале строки знаком >).

```
>nslookup
Default Server: ack
Address: 192.168.0.10
```

Пояснение

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
```

Пояснение

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
```

Пояснение

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
```

Пояснение

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) с помощью команды `dnsdiag`.

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.

Пояснение

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).

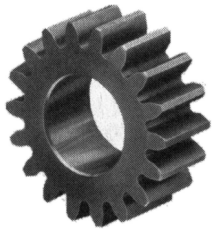
```
c:\WINNT\system32\inetsrv>dnsdiag mail.ru -v 1
mail.ru is an external server (not in the Exchange Org).
No external DNS servers on VSI. Using global DNS servers.
Created Async Query:
------------
QNAME = mail.ru
Type = MX (0xf)
Flags =  UDP default, TCP on truncation (0x0)
Protocol = UDP
DNS Servers: (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).



ГЛАВА 4

Информационные системы предприятия

Эта глава посвящена построению информационной системы предприятия. Задача весьма не простая, поскольку нужно учитывать множество факторов: местоположение офисов, количество сотрудников, бизнес-процесс и т. п.

SOHO-сети

Домашние сети и сети небольших предприятий называют *SOHO-сетями* (Small Office Home Office). В таких сетях к функционированию сети не предъявляются особые требования: установили маршрутизатор Wi-Fi, настроили немногочисленных клиентов, возможно, «расшарили» ресурсы (папки, принтеры) — и сеть готова к употреблению. Самое главное, что у всех пользователей сети есть доступ к Интернету, они могут открывать общие документы и печатать на общем принтере. Все пользователи хорошо знают друг друга, поэтому нет смысла в каком-либо разделении прав доступа к ресурсам.

Создать такие системы очень просто. Как уже было отмечено ранее, можно использовать беспроводной маршрутизатор, а можно выполнить прокладку кабельной сети. Из оборудования понадобится только коммутатор (если сеть кабельная) и устройство, которое будет предоставлять доступ к Интернету (ADSL-модем, аппаратный маршрутизатор или же компьютер, являющийся программным шлюзом). Для создания такой сети не нужна особая квалификация и какие бы то ни было специальные знания — достаточно знания основ работы сети и минимальных навыков работы с сетевым оборудованием.

Как уже отмечалось, для доступа к Интернету лучше приобрести отдельный маршрутизатор. Дело в том, что если настроить в качестве шлюза стационарный компьютер, он должен будет работать постоянно, иначе другие пользователи сети не смогут получить доступ к Интернету. О разнице в потребляемой электроэнергии между стационарным компьютером (с блоком питания на 400–450 Вт) и маленькой «коробочкой», полагаем, говорить не стоит. Кроме всего прочего, аппаратный маршрутизатор не только является шлюзом, но и предоставляет услуги DHCP-сервера. Другими словами, вам нужно лишь установить и включить эту «коробоч-

ку», выполнив минимальную настройку (вроде задания пароля доступа к Wi-Fi). На настройку стационарного компьютера вы потратите гораздо больше времени.

У настройки SOHO-сетей есть несколько особенностей. Первая связана с группой **Все** в Windows. Наверняка все знают о наличии такой группы. Однако нужно понимать, что слово «все» означает здесь не в прямом смысле «все» (т. е. кто угодно), а «все учетные записи, зарегистрированные на этом компьютере». В системе должны быть созданы пользователи, соответствующие текущим пользователям *каждой* рабочей станции сети (с идентичными именами и паролями). Другими словами, если на одном компьютере есть пользователь `Андрей` с паролем `123`, а на втором — пользователь `Маша` с паролем `321`, то на первом компьютере нужно создать пользователя `Маша` (пароль `321`), а на втором — пользователя `Андрей` (пароль `123`). И если на рабочей станции Windows нет учетной записи с именем и паролем пользователя, пытающегося подключиться к ней с другой станции (а обычно операция производится от имени того, кто работает на компьютере), то в подключении будет отказано.

При этом, если пароль одного из пользователей изменится, его нужно будет поменять на всех рабочих станциях сети. Согласитесь, не очень удобно, но, увы, пока в сети не будет службы каталогов (Active Directory), работать с этой сетью придется именно так. Можно, конечно, пренебречь требованиями безопасности и создать на всех компьютерах одну и ту же учетную запись пользователя с пустым паролем... На практике так часто и поступают.

Есть и другой способ решения этой проблемы — включить учетную запись **Гость**, которая по умолчанию заблокирована. Это самый простой способ, но он не позволяет выборочно контролировать или как-либо ограничивать доступ к ресурсам, поскольку все подключения к компьютеру будут осуществляться от имени одной учетной записи. При этом предоставленный в общее пользование ресурс станет доступен любому пользователю.

Вторая особенность SOHO-сетей — искусственное ограничение на количество подключений. Максимальное количество подключений по такой сети — всего 10. А это означает, что если к какому-либо сетевому ресурсу — например, к общей папке — попытаются одновременно подключиться 11 пользователей, то соединение 11-го будет сброшено.

Имеются в SOHO-сетях ограничения и по количеству одновременно открытых по сети файлов. К сожалению, это условие становится критичным при использовании популярной бухгалтерской программы «1С:Предприятие» — даже при работе в ней трех-четырех пользователей уже возникают проблемы.

Самый простой способ обойти эти ограничения (и на количество файлов, и на количество подключений) — установить на один из компьютеров операционную систему Linux и разместить на нем все общие ресурсы, настроив пакет Samba.

Какие операционные системы использовать в SOHO-сетях? Учитывая, что пользователи, как правило, чаще всего более знакомы с Windows, нет смысла предлагать им нечто иное. Windows — оптимальный вариант для таких сетей. Не стоит приобретать и топовые выпуски Windows — для SOHO-сети вполне достаточно Win-

dows 10/11 Home. Стоимость ее существенно ниже профессиональных выпусков: разница в цене домашнего (Home) и профессионального (Windows 10 Pro) выпуска приближается к 15 тыс. рублей. Умножьте это на количество компьютеров в сети и подсчитайте общую сумму выигрыша. Различие между выпусками касается в основном вопросов безопасности при работе в составе домена и несущественно в рассматриваемом случае. Нет смысла переплачивать за функционал, которым вы не будете пользоваться.

Одноранговые сети

Рассмотренные в предыдущем разделе SOHO-сети являются частным случаем *одноранговой сети.* В одноранговой сети отсутствуют какие-либо централизованно реализуемые правила и каждый компьютер в ней управляется автономно. Управлением ресурсами компьютера в такой сети занимается локальный администратор.

Чтобы объединить компьютеры в одноранговую сеть, достаточно всего лишь создать структуру сети: провести кабели или обзавестись беспроводным маршрутизатором. Далее администратор должен определить, какие ресурсы локальной системы будут предоставляться в общее пользование, с какими правами и т. д.

Одноранговую сеть имеет смысл организовывать, если количество компьютеров не превышает двух десятков. В противном случае администрирование такой сети становится слишком сложным. При росте числа компьютеров целесообразно организовывать сети на основе централизованного управления.

Сеть с централизованным управлением

В сетях среднего и большого размера (от 20 компьютеров) принято использовать систему централизованного управления. При этом параметры учетных записей хранятся централизованно в службе каталогов, что дает возможность не дублировать все учетные записи на каждом компьютере.

В случае с Windows службой каталогов является Active Directory, в Linux — LDAP[1]. Справедливости ради нужно отметить, что Linux может работать в составе домена Active Directory и даже быть контроллером домена Active Directory.

При использовании Active Directory каждый компьютер может управляться не только локальным администратором, но и администратором домена.

Управление локальными ресурсами

Чтобы централизованно управлять компьютером, его нужно включить в домен. Включить в домен можно как компьютер под управлением Windows, так и Linux.

---

[1] LDAP (от *англ.* Lightweight Directory Access Protocol, облегченный протокол доступа к каталогам) — относительно простой протокол, использующий TCP/IP и позволяющий производить операции аутентификации, поиска и сравнения, а также операции добавления, изменения или удаления записей.

Обычно систему добавляют в домен с локальной консоли. Эта 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 командой:

```
netdom join ComputerName /Domain DomainName /UserD DomainUserUPN
/PasswordD * /User0 ComputerAdminUser /Password0 * /Reboot
```

Эта команда позволяет осуществить операцию подключения и *удаленно*. Однако первоначальная установка Windows имеет политику безопасности, разрешающую *только* локальное выполнение такой операции.

Возможность добавлять рабочие станции в домен

Начиная с ОС 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 **Организационное 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 **Редактирование ADSI** и установить желаемое значение (рис. 4.1). Установка значения этого параметра в 0 предоставляет пользователям право добавлять в домен *неограниченное* количество компьютеров.

Чтобы добраться до атрибута **ms-DS-MachineAccountQuota**, нужно выполнить следующие действия:

1. Запустите оснастку **Редактирование ADSI** (Adsiedit.msc).
2. Выберите команду **Действие | Подключиться к**. В открывшемся окне выберите службу каталогов, к которой хотите подключиться.
3. Щелкните правой кнопкой мыши на узле, который начинается символами **DC=**, и выберите команду **Свойства**.
4. В открывшемся окне на вкладке **Редактор атрибутов** выберите атрибут **ms-DS-MachineAccountQuota** и нажмите кнопку **Изменить**.
5. Введите новое значение, нажмите кнопку **OK**, а затем — **Применить**.

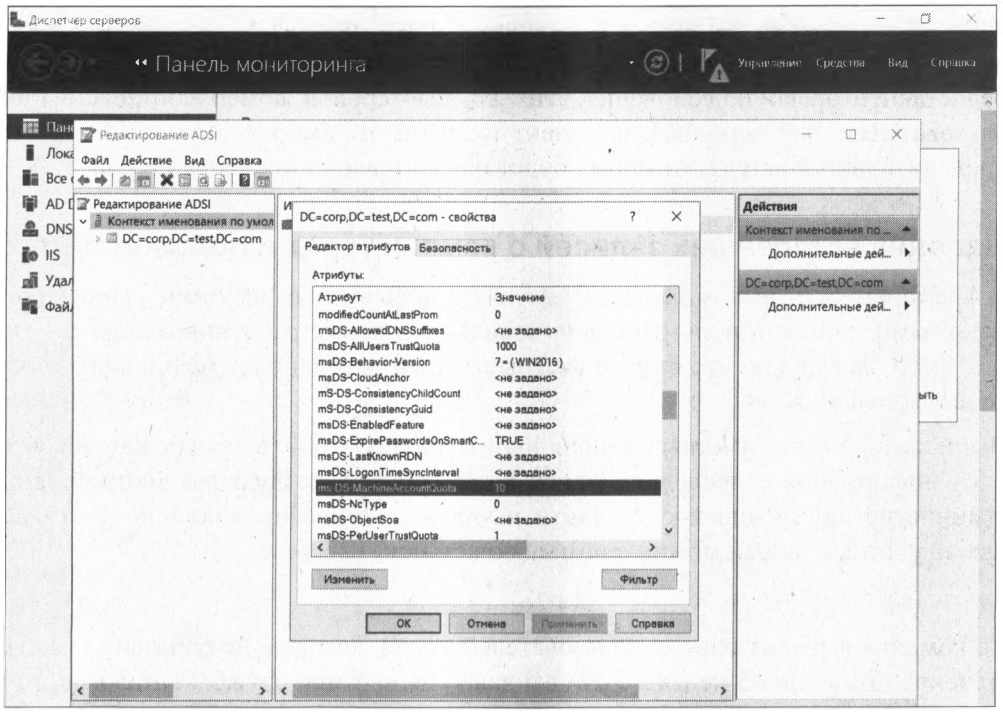


Рис. 4.1. Изменение квоты на добавление компьютеров в домен (Windows Server 2022)

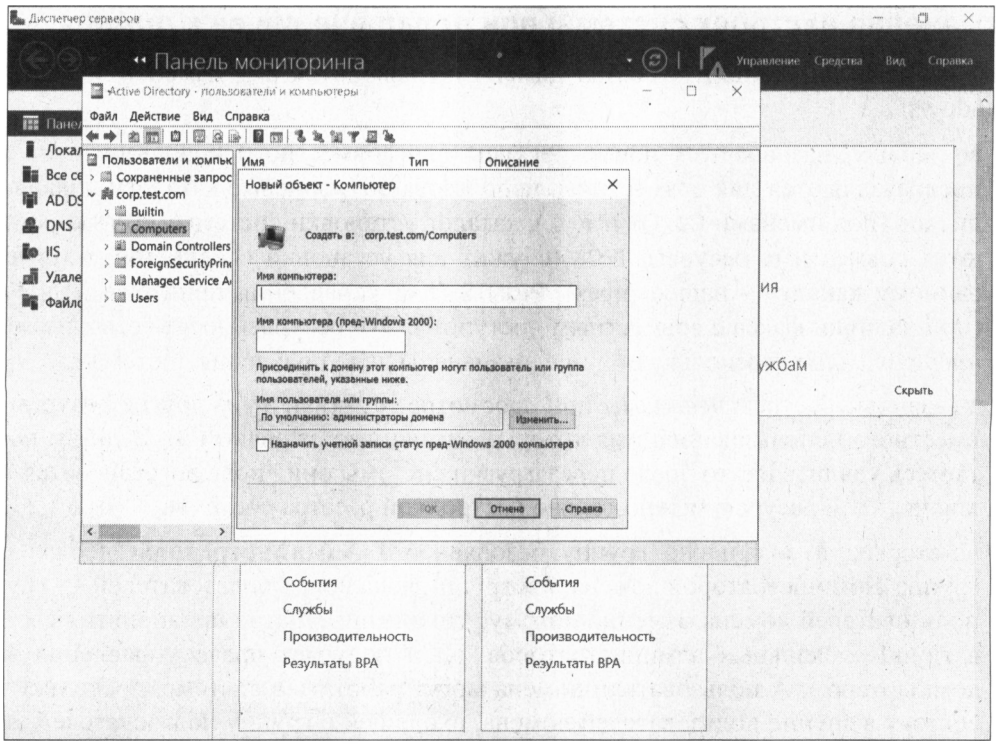


Рис. 4.2. Создание объекта **компьютер** с делегированием его подключения к домену

Более целесообразно не пускать создание новых систем в домене на самотек. Администратору следует создать объекты типа **компьютер** в службе каталогов и предоставить право подключения этих компьютеров в домен соответствующим пользователям, для чего надо в момент их создания выбрать опцию **Изменить** и определить пользователя, которому будет предоставлено такое право (рис. 4.2).

Удаление устаревших записей о компьютерах и пользователях

Со временем старые компьютеры заменяют новыми. То же самое происходит и с учетными записями пользователей: появляются новые работники, старые — уходят. Часто бывает так, что старые учетные записи сотрудников не блокируются после их увольнения.

«Вычислить» старые учетные записи достаточно просто — в службе каталогов хранится информация о последнем входе в домен соответствующей учетной записи. Администратору нужно просто найти и удалить устаревшие записи. Найти неактивные учетные записи можно с помощью команды `dsquery`:

```
dsquery user -inactive 5
```

Эта команда выводит список пользователей (`user`), которые не работали (`inactive`) в течение последних 5 недель. Если вы давно не чистили службы каталогов, то вывод будет весьма длинным.

Изменение настроек системы при подключении ее к домену

При добавлении станции в состав домена производится ряд изменений настроек Windows:

- во-первых, назначаются новые ресурсы для совместного использования. Так, предоставляются для совместного использования корневые каталоги локальных дисков (под именами C$, D$ и т. д.), каталог установки системы (ADMIN$), создаются совместные ресурсы: IPC$ (служит 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.

  Указанные ресурсы *невидимы* при просмотре сети (как и все другие ресурсы совместного использования, имя которых заканчивается знаком $). Если вы попытаетесь удалить их, то после перезагрузки системы они вновь восстановятся. Отключить эти ресурсы можно только настройкой реестра системы;

- 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 кеширование 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.

Локальный администратор против доменного

У некоторых пользователей централизованное управление вызывает негативную реакцию. 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 восстановления 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 и 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 этого 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
```

Следует учитывать, что отключение этих ресурсов может нарушить работу имеющейся в домене системы управления.

Для восстановления опции этот параметр необходимо будет удалить.

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. Существует возможность регулировать членство в группах с помощью групповых политик. Хотя практика контроля состава групп локальных администраторов вызывает крайнее недовольство у рядовых пользователей, администратор предприятия может самостоятельно определить список членов этой группы.

Блокировать такой вариант можно, только приняв меры по недопущению применения групповой политики для конкретной системы, блокировав порты на транспортном уровне, но работа полученной системы будет существенно затруднена.

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***
>
> Эта рекомендация может быть использована также при поступлении на работу нового администратора. Поскольку в системе нет штатных средств ограничения локального входа администратора, то это, по сути, единственный способ защиты наиболее ответственных ее участков от непрофессиональных действий нового, непроверенного работника.

Конечно, такое ограничение нельзя рассматривать всерьез, поскольку, например, групповой политикой (если не заблокировать и 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 явиться изменение ограничений, налагаемых групповой политикой, или полная ее блокировка.

> ***Примечание***
>
> 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. Эта проблема имеет только одно принципиальное решение — организационные выводы, когда подобные действия локального администратора навлекут на него «воспитательные меры» со стороны руководителя подразделения.

Проблема аудитора

Наличие у администратора (как локального, так и администратора домена) полных прав над управляемой им системой создает серьезные проблемы безопасности. Ведь он может выполнить в системе любые операции, а потом попытаться это скрыть. Такие возможности создают в системе безопасности огромные потенциальные дыры. Именно поэтому в некоторых системах вводится понятие *аудитора* — пользователя, у которого нет прав администратора, но который может протоколировать любые его действия. Причем даже администратор не имеет прав изменить протоколы аудитора. Другими словами, администратор не может скрыть от аудитора свои действия.

В Windows-системах такого пользователя, к сожалению, нет. Единственным вариантом может быть сбор данных протоколов работы компьютеров в реальном времени на отдельную изолированную рабочую станцию. В этом случае можно будет сравнить протоколы, находящиеся на этой станции, с возможно измененными протоколами домена. Для решения поставленной задачи есть много программ, с которыми вы можете ознакомиться в Интернете.

Методы управления локальной системой

После добавления рабочей станции в домен администратор домена получает над ней фактически неограниченную власть. Существуют три основных способа управления локальной системой:

- первый подразумевает использование оснастки **Управление компьютером** (рис. 4.3), с помощью которой можно подключиться к любой системе и управлять ею. Конечно, для подключения к системе нужны соответствующие права. Подключившись к системе, администратор может останавливать и запускать службы, просматривать протоколы работы системы, создавать удаленных локальных пользователей, менять их членство в группах и т. п.

  На практике этот метод управления используется редко, поскольку он подходит лишь для индивидуальных настроек, и если нужно применить одну и ту же настройку к нескольким компьютерам, прибегать к такому методу неудобно;

- второй метод настройки заключается в использовании *сценария* входа в систему. Тогда при регистрации в домене на компьютере запускается выполнение такого сценария. 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.

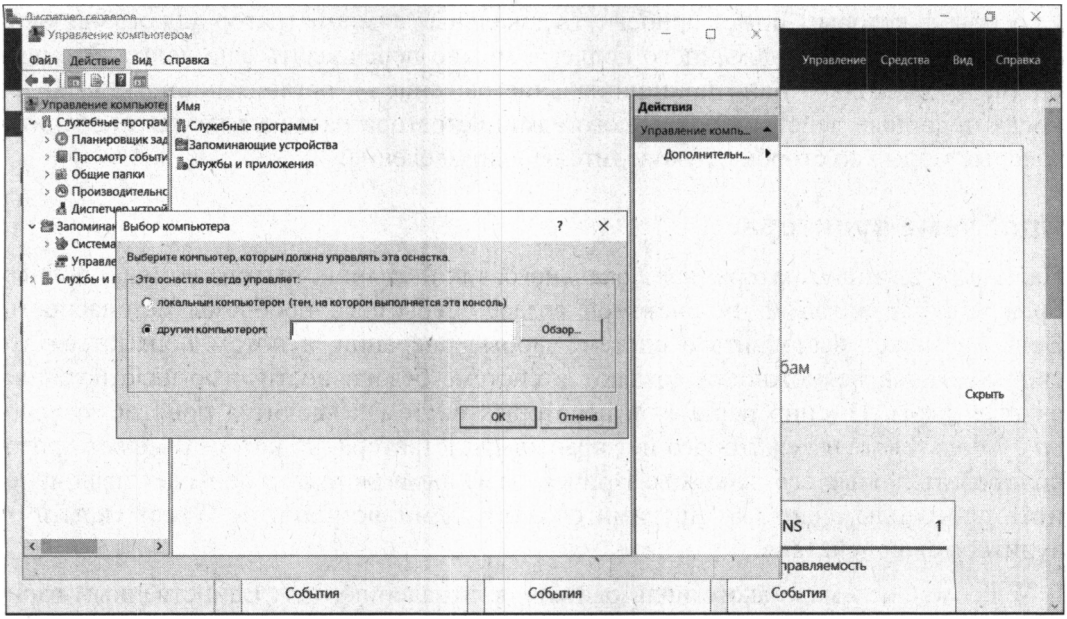


Рис. 4.3. Подключение оснастки управления к удаленному компьютеру

Преимущество этого способа управления — выполнение сценария при каждом входе в систему и максимальная простота настройки (например, создали один сценарий и настроили его выполнение для всех пользователей). Недостаток — сценарии выполняются от имени учетной записи пользователя. Если пользователь не имеет административных прав, то в сценарии не будут выполняться команды, требующие наличия прав на управление системой;

- самым распространенным является третий метод — использование *групповых политик*. С помощью групповых политик можно управлять тысячами самых разных настроек. При этом вы можете устанавливать не только параметры операционной системы, но и приложений. Поэтому сейчас этот метод считается оптимальным.

Есть и другие методы, но они используются очень редко. Например, администратор может написать собственные программы (на Visual Basic, WMI и PowerShell). Однако для этого ему нужно обладать навыками программирования. К тому же для запуска таких программ на целевом компьютере должны быть установлены соответствующие интерпретаторы, что не всегда бывает по умолчанию (использование групповых политик и основы написания сценариев рассмотрены в *главе 6*).

Служба каталогов

Информационные системы создаются не просто так. Скорее всего, структура информационных систем тесно связана с бизнес-процессами, протекающими на предприятии. Исходя из бизнес-действий, определяются права пользователей, их подчиненность и т. д. Структура компьютерной информационной системы обычно создается по образу и подобию организационной структуры предприятия.

Основное средство описания структуры информационной системы — *каталог*. По сути, каталог — это база данных, содержащая объекты, описывающие пользователей, компьютеры, производственные подразделения и т. д. У каждого объекта есть свой набор характеристик — свойства.

Работа с объектами осуществляется с учетом прав доступа, а набор операций специфичен для каждого объекта. Набор объектов, их атрибутов (свойств) и методов (допустимых операций) принято называть *схемой каталога*.

Служба каталогов Windows (Active Directory)

Начиная с Windows 2000, в Windows появился каталог, известный как *служба каталогов* (Active Directory, AD).

Служба каталогов Windows имеет в своей структуре следующие единицы:

- **организационное подразделение** (Organization Unit, OU) — подгруппа доменов, зеркально отображающая бизнес-структуру или функциональную структуру предприятия;
- **домен** — группа компьютеров, совместно использующих общую базу данных каталога;
- **дерево домена** — один или более доменов, которые разделяют непрерывное пространство имен;
- **лес** — одно или более деревьев, которые обмениваются общей информацией каталога;
- **подсеть** — сетевая группа с одной маской сети и определенным диапазоном IP-адресов;
- **сайт** — одна или более подсетей, использующихся для настройки доступа к каталогу и репликации.

Большинство методов управления сетью в Windows основаны на службе каталогов (например, групповые политики). Однако есть часть операций, унаследованная исторически. Например, группы безопасности существуют отдельно от подразделений. Если вы поменяете членство пользователя в OU, то для последующей коррекции его прав доступа необходимо будет дополнительно вручную изменить группу безопасности, в которую входит пользователь.

Служба каталогов хранит много информации, которая может быть полезной администратору, но не доступна явно в графических средствах управления. Оснастка **Active Directory** (AD) включает возможность поиска по службе каталогов. Например, можно найти рабочие станции, установленные средствами разворачивания образов, или пользователей, для которых установлен неограниченный срок действия пароля, и т. п. Каждый раз составлять заново строку поиска[1] неудобно — проще

[1] Например, даже простой поиск сотрудников, которым разрешен удаленный доступ в сеть, требует ввода запроса: `(&(&(objectclass=person)(msNPAllowDialin=TRUE)))`.

сохранить часто используемые запросы в самой оснастке и вызывать их по названию. На рис. 4.4 показан пример оснастки с сохраненными запросами (в примере — запрос по системам, развернутым средствами централизованной установки). Для создания сохраненного запроса нужно щелкнуть правой кнопкой мыши на узле **Сохраненные запросы** и выбрать команду **Создать | Запрос**. В открывшемся окне введите название запроса и, собственно, сам запрос или сконструируйте его, нажав кнопку **Запрос**.

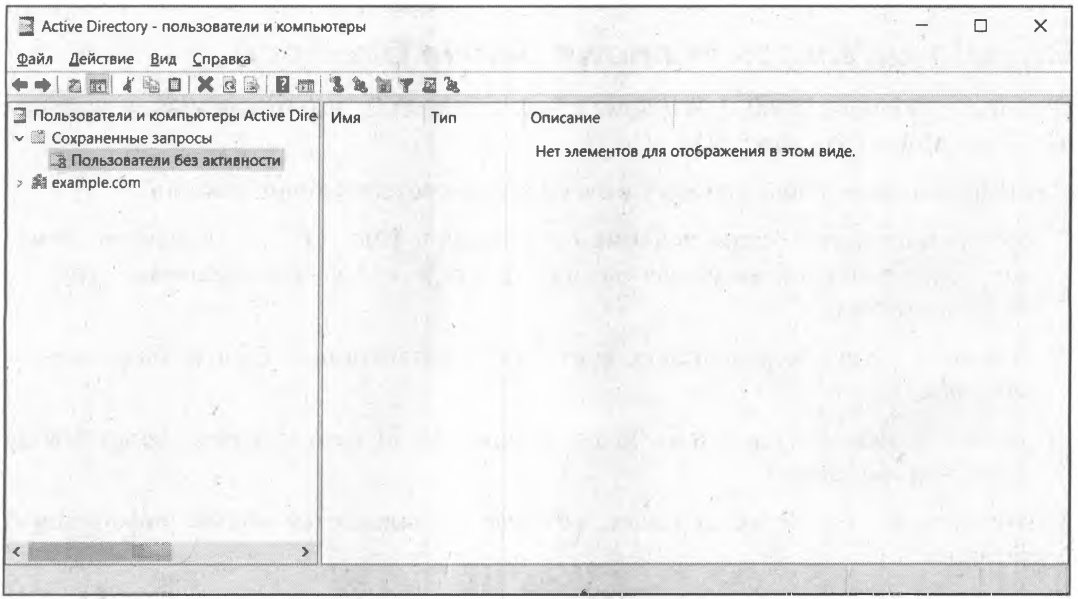


Рис. 4.4. Сохраненные поисковые запросы оснастки службы каталогов

Домены Windows

Исторически иерархические сети на основе Windows создавались на базе *доменов*. В локальных сетях на базе Windows понятие «домен» служит 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.

На одном предприятии 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 том или ином пространстве имен по конкретному имени однозначно может быть определен соответствующий ему объект. Типичный пример — структура DNS (Domain Name System, система доменных имен). 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 одном предприятии доменов с отличающимися именами характерно для транснациональных корпораций. 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 для доменов Windows Server 2003 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. В Windows Server 2012/2016/2019/2022 свойства паролей стали полностью управляться групповой политикой. Все другие настройки могут быть выполнены политиками подразделений.

Подразделение

Домены Windows (начиная с версии Windows 2000) могут содержать *организационные подразделения* (Organization Unit, OU). Организационное подразделение — это своеобразный контейнер, в который можно помещать как компьютеры, так и пользователей (очевидно, что речь идет о соответствующих логических объектах).

Основная причина создания OU для администраторов системы — это возможность применения к объектам OU *групповых политик* (подробнее о них см. *главу 6*). Повторимся: 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 — тогда компьютеры уже не будут членами домена).

Лес

На одном предприятии может существовать несколько доменов с различными пространствами имен — например: example.com и example.ru. В этом случае представленная структура будет напоминать *лес*. Лес — это коллекция (одного или более) доменов Windows 20*xx*, объединенных общей схемой, конфигурацией и двусторонними транзитивными доверительными отношениями.

Нужно понимать, что деревья в лесу не самостоятельны. Все эти деревья создаются *внутри одного предприятия*, а администраторы централизованно управляют ими. Если оперировать терминами логической организации сети, между любыми доменами внутри предприятия существуют *доверительные двусторонние отношения*.

На практике это означает, что администратор предприятия является «начальником» администратора любого домена, а пользователь, прошедший аутентификацию в одном домене, уже «известен» в другом домене предприятия.

При работе с сетями с централизованным управлением необходимо полностью доверять администраторам, которым принадлежат корневые права, поскольку они имеют возможность получить доступ к любым объектам и назначать любые права.

Сайты

Active Directory объединяет логическую и физическую структуру сети. Логическая структура Active Directory состоит из организационного подразделения, домена, дерева доменов и леса доменов. А к физической структуре относятся такие элементы, как подсеть и сайт.

Сайты 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. Именно поэтому между сайтами создаются специальные механизмы репликации данных — можно задать график репликации, выбрать используемый протокол (по электронной почте или посредством протокола IP) и т. д.

Соотношение территориальной и логической структуры выбирается исходя из конкретной конфигурации предприятия. Например, можно создать несколько сайтов в одном домене или сформировать в каждом сайте свой домен и т. п.

Сайты обычно используются для настройки доступа к каталогу и репликации. Также создание дополнительных сайтов может быть способом балансировки нагрузки между контроллерами домена, потому что алгоритм выбора контроллера домена рабочей станции использует структуру сайтов.

DN и RDN

Для успешной работы с каталогами необходимо ориентироваться в терминах DN (Distinguished Name, отличительное имя) и RDN (Relative Distinguished Name, относительное отличительное имя).

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 каталоги. В этой аналогии термин 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, на предприятии может быть заведен пользователь Иванов. Если на этом предприятии в разных отделах работают два Иванова, то только по фамилии невозможно определить конкретного работника. Но если использовать многоатрибутный RDN, состоящий, например, из фамилии и названия отдела, то работник будет обозначен точно:

```
cn = Петров + ou = IT
```

Управление структурой домена предприятия

Проектировщик логической структуры компьютерной сети предприятия должен учитывать различные факторы, например: бизнес-процессы, требования безопасности, количество и расположение офисов и т. д.

Создание разветвленной структуры сети имеет смысл только в крупной компании. В небольших компаниях в такой структуре нет смысла, поскольку внутри компании будет применяться всего несколько групповых политик. Однако по мере увеличения количества компьютеров в сети она будет становиться все более сложной.

Логическая структура домена, как правило, повторяет организационную структуру компании. В небольших компаниях обычно не стоит вопрос организации и размещения контроллеров домена (в *главе 5* мы рассмотрим ситуацию с удаленным офисом) — в большинстве случаев производительности одного сервера хватит на обслуживание нескольких сотен рабочих станций. Однако рекомендуется иметь не менее двух контроллеров — на случай неисправности одного из них.

Active Directory — сердце доменов на базе Microsoft Windows. Практически все задачи администрирования затрагивают технологию Active Directory, которая была создана, чтобы помочь вам определить четкую структуру сети вашего предприятия.

Создание нового домена

Active Directory тесно связана с системой доменных имен (DNS). Домены DNS организованы в иерархическую структуру, которая определена на основе всего Интернета. Благодаря DNS структура иерархии вашего домена Active Directory может стать частью доменной иерархии Интернета или, наоборот, может быть отделена от него.

Система доменных имен так глубоко интегрируется в технологию Active Directory, что сначала нужно настроить DNS в своей сети, а затем уже устанавливать Active Directory.

Ранее для настройки домена использовался файл dcpromo.exe, однако, начиная с Windows Server 2012, мастер установки доменных служб Active Directory перемещен в Диспетчер серверов.

В Windows Server 2016/2019/2022 установка Active Directory состоит из двух частей. Процесс установки начинается в Диспетчере серверов выбором команды **Добавить роли и компоненты**, которая запустит мастер добавления ролей и компонентов. В качестве устанавливаемой роли нужно выбрать **Доменные службы Active Directory** (AD DS). Установить AD DS можно и в командной строке, например, так:

```
install-windowsfeature -name AD-Domain-Services -includemanagementtools
```

Для удаления компонента из командной строки служит параметр `-Remove` команды `Uninstall-WindowsFeature`.

Однако полагаем, большинству администраторов будет привычнее использовать графический интерфейс Диспетчера серверов.

После завершения установки нужно запустить мастер настройки доменных служб Active Directory (Active Directory Domain Services Configuration Wizard), щелкнув на странице **Ход установки** по ссылке **Повысить роль этого сервера до уровня**

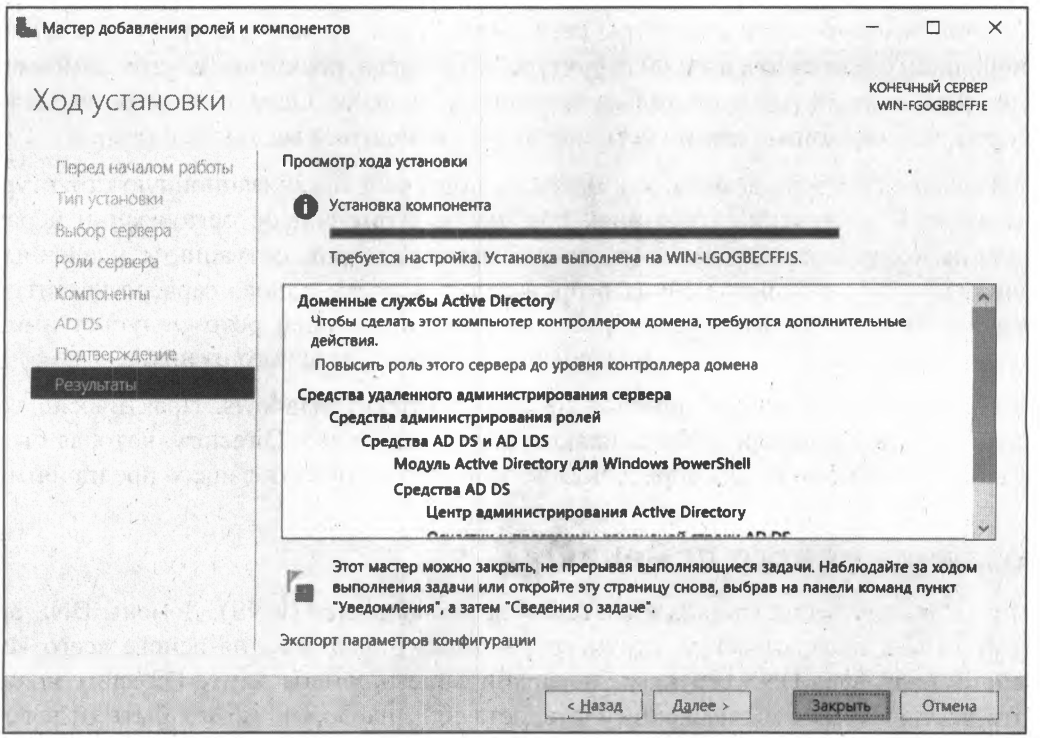


Рис. 4.5. Запуск мастера настройки доменных служб Active Directory

контроллера домена (рис. 4.5). Этот мастер служит для настройки контроллера домена и заменяет файл dcpromo.exe, который ранее использовался для этой цели.

Мастер также запустит программу Adprep.exe для подготовки надлежащей схемы. Впрочем, запустить ее раньше, чем в существующем домене/лесу будет установлен первый контроллер домена на базе Windows Server 2016/2019/2022, нельзя. Поэтому мастер попросит вас ввести соответствующие учетные данные, необходимые для запуска этой программы.

Для подготовки леса нужно предоставить учетные данные члена одной из следующих групп: **Администраторы предприятия** (Enterprise Admins), **Администраторы схемы** (Schema Admins) или **Администраторы домена** (Domain Admins). Для подготовки домена необходимо предоставить учетные данные члена группы **Администраторы домена**.

Если сервер DNS еще не установлен, вам будет предложено установить и его. Если домен еще не создан, мастер поможет создать домен и настроить Active Directory в созданном домене.

Дополнительную информацию вы можете получить на веб-странице:
https://technet.microsoft.com/ru-ru/library/hh472162.aspx.

Функциональный уровень домена

Функции домена ограниченны и регулируются выбранным функциональным уровнем или режимом работы домена:

- **Windows Server 2003** — поддерживаются контроллеры домена, которые работают под управлением Windows 2003 и более старых версий;
- **Windows Server 2008** — поддерживаются контроллеры домена, работающие под управлением Windows 2008 и более старых версий;
- **Windows Server 2008 R2** — поддерживаются контроллеры домена, работающие под управлением Windows 2008 R2 и Windows Server 2012;
- **Windows Server 2012** — поддерживаются контроллеры домена, работающие только под управлением ОС Windows Server 2012;
- **Windows Server 2012 R2** — поддерживаются контроллеры домена под управлением Windows Server 2012 R2 и Windows Server 2016;
- **Windows Server 2016** — поддерживаются контроллеры домена, работающие под управлением только Windows Server 2016 и Windows Server 2019.

> ***Примечание***
>
> Функционального уровня Windows Server 2019/2022 не существует. ОС Windows Server 2019/2022 использует функциональный уровень Windows Server 2016. Подробнее см. **https://learn.microsoft.com/en-us/windows-server/iMarktity/ad-ds/active-directory-functional-levels#windows-server-2016-functional-levels**.

Повысить функциональный уровень домена можно из командной строки PowerShell. Для этого служит команда:

```
Set-ADDomainMode -iMarktity <DNS имя домена> -DomainMode  <режим>
```

где:

- `iMarktity` — DNS имя домена;
- `DomainMode` — целевое значение функционального уровня домена. Этот параметр может принимать следующие значения:
  - Windows Server 2000: `0` или `Windows2000Domain`;
  - Windows Server 2003 Interim Domain: `1` или `Windows2003InterimDomain`;
  - Windows Server 2003: `2` или `Windows2003Domain`;
  - Windows Server 2008: `3` или `Windows2008Domain`;
  - Windows Server 2008 R2: `4` или `Windows2008R2Domain`;
  - Windows Server 2012: `5` или `Windows2012Domain`;
  - Windows Server 2012 R2: `6` или `Windows2012R2Domain`;
  - Windows Server 2016: `7` или `Windows2016Domain`.

Для повышения функционального уровня леса из командной строки PowerShell PowerShell необходимо выполнить команду:

```
Set-ADForestMode -IMarktity <DNS имя домена> -ForestMode <режим>
```

где:

- `iMarktity` — DNS имя леса (в примере имя леса `lab.lan`);
- `ForestMode` — целевое значение функционального уровня леса. Этот параметр может принимать следующие значения:
  - Windows Server 2000: `Windows2000Forest` или `0`;
  - Windows Server 2003: `Windows2003InterimForest` или `1`;
  - Windows Server 2003: `Windows2003Forest` или `2`;
  - Windows Server 2008: `Windows2008Forest` или `3`;
  - Windows Server 2008 R2: `Windows2008R2Forest` или `4`;
  - Windows Server 2012: `Windows2012Forest` или `5`;
  - Windows Server 2012 R2: `Windows2012R2Forest` или `6`;
  - Windows Server 2016: `Windows2016Forest` или `7`.

Дополнительную информацию можно найти по ссылке **https://learn.microsoft.com/en-us/powershell/module/activedirectory/set-adforestmode?view=windowsserver2022-ps**.

Компоненты Active Directory

Доменные службы Active Directory имеют множество компонентов:

- для функционального уровня Windows Server 2008 R2 характерны следующие компоненты:

- **Корзина Active Directory** — позволяет восстанавливать ошибочно удаленные объекты Active Directory, подобно тому, как файлы восстанавливаются из обычной Корзины. Далее в этой главе будет показано, как использовать Корзину AD;
- **Управляемые учетные записи служб** — специальный тип доменной учетной записи пользователя для управляемых служб, которые сокращают приостановки обслуживания и устраняют другие проблемы путем автоматического управления паролями учетной записи;
- **Управляемые виртуальные учетные записи** — специальный тип локальной учетной записи компьютера для управляемых служб, обеспечивающих доступ к сети с идентификацией компьютера в домене;
- **Обеспечение механизма аутентификации** — улучшает процесс аутентификации, позволяя администраторам управлять доступом к ресурсам на основе входа пользователя в систему с применением сертификата.

❒ Для функционального уровня Windows Server 2012 характерны следующие дополнительные компоненты:

- **Активация с помощью Active Directory** — позволяет использовать Active Directory для автоматической активации клиентов. Клиенты должны работать под управлением ОС Windows 8/10/11 или Windows Server 2012/2016;
- **Создание индекса с задержкой** — позволяет задержать создание индекса в каталоге до перезагрузки контроллера домена;
- **Средства управления политикой на основе заявок** — предоставляют более гибкие политики аудита;
- **Расширенная Корзина** — расширенная версия Корзины AD, позволяющая администраторам восстанавливать удаленные объекты с использованием Центра администрирования Active Directory;
- **Ограниченное делегирование Kerberos по доменам** — разрешает учетным записям службы работать от имени пользователей в доменах и лесах;
- **Расширенная детальная политика паролей** — позволяет управлять объектами настроек пароля (с помощью Центра управления Active Directory);
- **Групповые управляемые учетные записи службы** — позволяют нескольким службам использовать одну и ту же учетную запись службы;
- **Защита Kerberos** — позволяет клиенту и контроллеру домена связываться по защищенному каналу;
- **Интеграция диспетчеров серверов** — теперь все задачи, связанные с разворачиванием локальных и удаленных серверов, можно выполнить через Диспетчер серверов;
- **Клонирование виртуального контроллера домена** — название этого компонента говорит само за себя, с его помощью вы можете создать виртуальные копии контроллеров домена;

- **Внешнее подключение к домену** — позволяет подключение компьютера к домену через Интернет (необходимо включить DirectAccess).

Что же касается уровня Windows Server 2016, то здесь доступны все функции, доступные в режиме работы Windows Server 2012 R2, а также некоторые новые возможности — в частности, управление привилегированным доступом с помощью MS IMarktity Manager (MIM), а также некоторые изменения, связанные с Kerberos-аутентификацией. По сравнению с предыдущими выпусками (с той же Windows Server 2012) изменений не так уж и много. Дополнительная информация доступна на официальном сайте: **https://docs.microsoft.com/en-us/windows-server/iMarktity/adds/active-directory-functional-levels**.

Создание контроллеров домена «только для чтения»

В удаленных филиалах принято разворачивать *контроллеры домена «только для чтения»* (RODC, Read Only Domain Controller). Если злоумышленник получит доступ к контроллеру домена филиала (который часто менее хорошо охраняется, чем главный офис), то это снижает риск дискредитации данных всего домена.

Любой контроллер домена под управлением Windows Server 2008 R2 или более поздней версии может быть настроен как RODC. После установки службы DNS-сервера на RODC последний может работать так же, как и DNS-сервер только для чтения (read-only DNS, RODNS).

RODC тиражирует разделы каталога приложения, которые использует DNS, — в том числе разделы **ForestDNSZones** и **DomainDNSZones**. Клиенты могут использовать RODNS-сервер для разрешения имен. Но вы должны понимать, что RODNS-сервер не поддерживает прямые клиентские обновления, поскольку RODNS не регистрирует записи ресурсов (подробнее о создании RODC мы поговорим в *главе 5*).

Удаление контроллера домена

В некоторых случаях может понадобиться удалить контроллер домена. Для выполнения этой задачи можно использовать или Диспетчер серверов, или утилиту ntdsutil.

В первом случае нужно из меню **Управление Диспетчера серверов** выбрать опцию **Удалить роли и компоненты**, затем выбрать ваш сервер, после чего выключить переключатель **Доменные службы Active Directory**. Если это ваш основной контроллер домена, тогда сначала нужно понизить его роль, а потом выполнять удаление доменных служб Active Directory.

Весь процесс удаления контроллера домена не очень сложен — достаточно просто следовать дальнейшим инструкциям мастера удаления ролей и компонентов. Если этот процесс вызвал у вас затруднения, воспользуйтесь ссылкой на страницу со множеством иллюстраций: **https://winitpro.ru/index.php/2022/01/13/udalenie-kontrollera-domena-active-directory**.

Совсем другое дело, когда контроллер домена вышел из строя и штатными средствами его удалить не получается. Вот здесь и приходит на помощь утилита ntdsutil (рис. 4.6).

Использовать ее нужно так: введите команду `ntdsutil`, и все последующие команды вводите в приглашении утилиты ntdsutil, а не в командной строке Windows:

```
metadata cleanup
connections
```

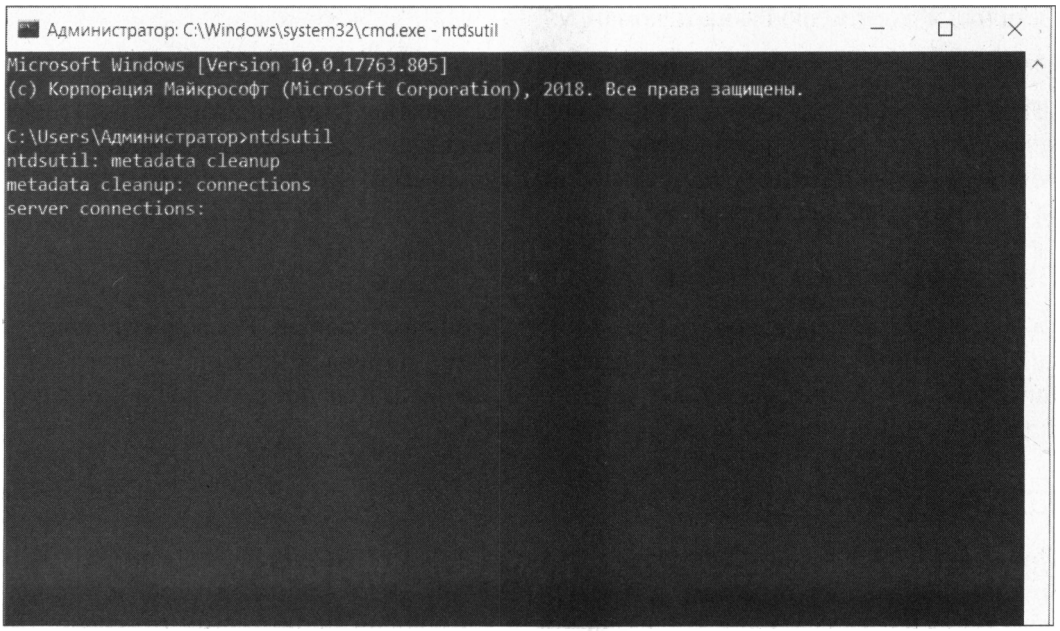


Рис. 4.6. Использование утилиты ntdsutil

Совсем не обязательно вводить всю команду целиком. Достаточно ввести строку, позволяющую идентифицировать команду, — например, `met` для команды `metadata cleanup`.

Теперь нужно подключиться к работающему контроллеру домена, на котором мы будем выполнять операцию удаления метаданных:

```
connections | connect to server <имя>
```

После подключения к контроллеру снова возвращаемся в режим `metadata cleanup`. На этом шаге необходимо выбрать тот контроллер, данные о котором предполагается удалить, для чего выполните команду:

```
Select operation target
```

После перехода в этот режим мы последовательно подключаемся к ресурсам предприятия. Например, чтобы указать на конкретный сервер, сначала нужно 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`.

Осталось в этом меню выбрать команду:

```
Remove selected server
```

Шпаргалка только с командами ntdsutil (без описания, что означает та или иная команда) доступна по адресу: **https://learn.microsoft.com/en-us/troubleshoot/windows-server/iMarktity/use-ntdsutil-manage-ad-files**. Можете ее себе распечатать — на случай нештатной ситуации.

Переименование домена

Операция переименования требует тщательной подготовки. Последовательность действий администратора для переименования домена изложена в документе Introduction to Administering Active Directory Domain Rename технической библиотеки Microsoft по адресу: **https://bit.ly/34BknKV**[1].

LDAP и Active Directory

Протокол LDAP (Lightweight Directory Access Protocol) является стандартным коммуникационным протоколом для сетей TCP/IP. Этот протокол разработан для получения доступа к службам каталогов с наименьшими затратами ресурсов. Он также определяет операции запроса и изменения информации в каталоге.

Поскольку служба каталогов поддерживает протокол LDAP, ставший стандартом для доступа к подобным службам, то для управления структурой домена удобно применять утилиты, реализующие подключение по этому протоколу.

Подключаемся к каталогу по протоколу LDAP

Существует несколько способов подключения к каталогу по протоколу LDAP. Первый способ заключается в использовании оснастки **Редактирование ADSI** (рис. 4.7). Используя эту оснастку, вы можете подключиться к любому узлу структуры службы каталогов, увидеть его атрибуты, отредактировать их и установить желаемые права доступа. Оснастка также позволяет создавать новые объекты в структуре каталогов, удалять существующие и т. д.

Второй способ заключается в использовании утилиты ldp.exe, которая позволяет подключиться к службам каталога по протоколу LDAP. Она также позволяет до-

---

[1] Полный адрес: **https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc816848(v=ws.10)?redirectedfrom=MSDN**.

бавлять, удалять объекты, редактировать их и выполнять поиск по каталогу. Утилита ldp.exe появляется в системе после добавления Support Tools.

Кроме этих двух способов в Интернете доступно много средств, в которых реализованы возможности подключения и управления системой по протоколу LDAP. Вполне вероятно, что они окажутся даже более удобными, чем только что упомянутые варианты.

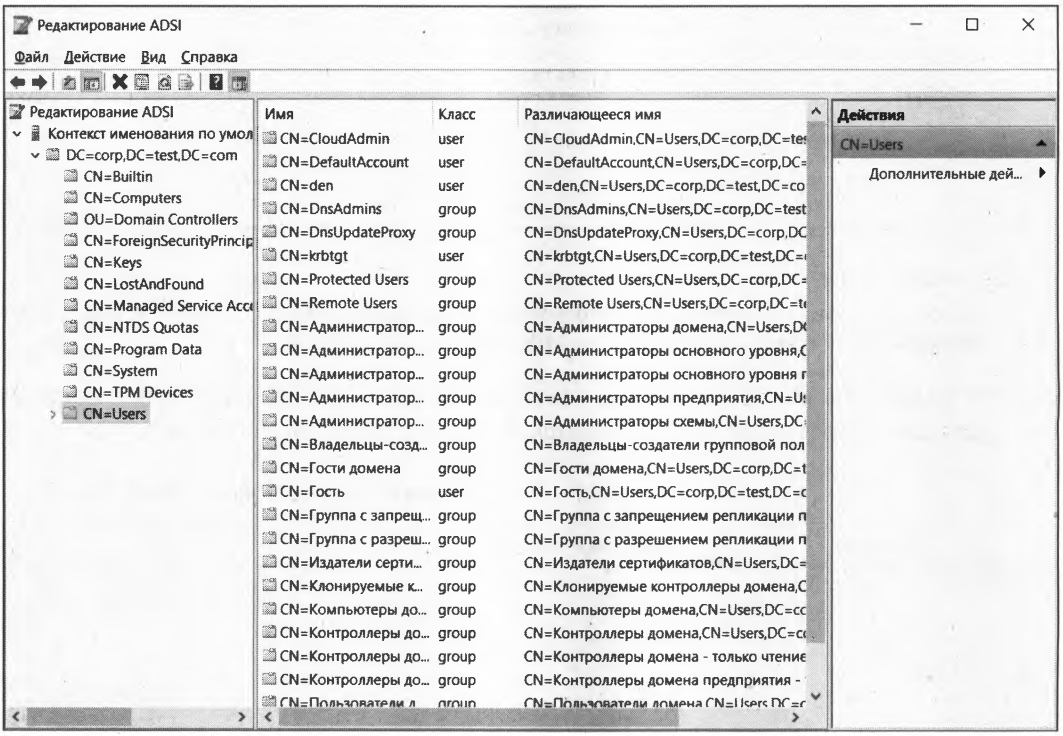


Рис. 4.7. Утилита ADSI Edit

Синтаксис поисковых запросов LDAP

Чтобы правильно составить запрос к службе каталогов, необходимо изучить основы LDAP-синтаксиса.

В службе каталогов информация хранится в виде объектов. Для обозначения *свойств* объектов (по терминологии Microsoft) в стандартах LDAP применяется термин *атрибуты*.

Чтобы выбрать нужные данные из службы каталогов, необходимо составить *фильтр*. 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 здесь требованием И, которое записано *до* условий.

В фильтрах допустимы операторы, приведенные в табл. 4.1.

***Таблица 4.1.** 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 (*), но 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 показано в табл. 4.2.

***Таблица 4.2.** 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 того 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 нужной строке указать (через точку с запятой) названия тех атрибутов, которые должны отображаться на экране по результатам поиска.

Покажем на небольшом примере, как можно быстро найти в домене пользователя по второму почтовому адресу.

Дополнительные адреса электронной почты, которые присвоены пользователю, приводятся 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*

Большинство системных администраторов предпочитают использовать для конфигурирования серверов текстовые файлы, поскольку с ними удобнее работать, чем с двоичной информацией. Для каталогов существует стандарт LDIF (LDAP Interchange Format, определен в документе RFC 2849), который устанавливает правила представления данных каталога в текстовом файле.

LDIF-файл состоит из текстовых строк, в которых приведены атрибуты объектов, их значения и директивы, описывающие способы обработки этой информации. В Windows имеется утилита ldifde (запускаемая одноименной командой), которая выполняет 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. Так, с помощью LDIF-файлов выполняется модификация схемы каталога при установке новых приложений.

Предположим также, 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. А с помощью утилиты ldifde можно выполнить экспорт в текстовый файл параметров учетных записей пользователей *только* для заданного подразделения (установив фильтр по конкретному 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

Подобная операция также весьма просто выполняется с помощью сценария Visual Basic. Необходимо лишь подключиться к нужному контейнеру, установить фильтр для выборки только объектов типа «пользователь» и запустить цикл для каждого элемента такого типа в этом контейнере. Однако приведенная схема работы с помощью утилиты ldifde не требует от администратора знания сценариев и может быть выполнена буквально в течение нескольких минут.

Ранее мы рассматривали пример, как с помощью команды `dsquery` получить список компьютеров, длительное время не работавших в составе сети. Приведем второй способ, дающий возможность 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. Необходимо учитывать, что компьютеры, которые не перезагружались в течение этого периода, также будут иметь «старые» значения времени входа в систему. Фильтр выводит и имена компьютеров, для которых отсутствует значение параметра времени входа в систему.

Представленный пример несколько искусственен, поскольку результат может быть получен более простым способом. Но он приведен именно для того, чтобы проиллюстрировать существование различных возможных вариантов действий администраторов.

Делегирование прав

На небольших предприятиях системный администратор выполняет все функции, касающиеся управления доменом. Он создает и удаляет пользователей, добавляет компьютеры в домен и т. д. Но в крупных компаниях у системного администратора слишком много работы, и некоторые функции администратор может переложить на других сотрудников. Например, поручить создание новых учетных записей можно сотруднику отдела кадров, а создавать учетные записи компьютеров — техническому специалисту. При этом у администратора сохраняется право выполнять все эти функции самостоятельно (т. е. у системного администратора остается возможность вмешаться — в экстренном случае), но у него высвободится некоторое время, поскольку часть его работы станут выполнять те сотрудники, кому он это доверит.

Такая передача прав называется *делегированием*. И принято говорить: не «передать право», а «делегировать» его. Перечень возможных прав доступа для контейнера является настолько подробным, что администратор может легко настроить объем

делегирования — например, делегировать право создания учетных записей пользователей, но запретить их редактирование и/или удаление.

Большинство утилит графического управления объектами службы каталогов содержит в контекстном меню команду **Делегирование управления**, которая вызывает **Мастер делегирования управления** (рис. 4.8). Этот мастер является самым простым способом делегирования прав на объекты.

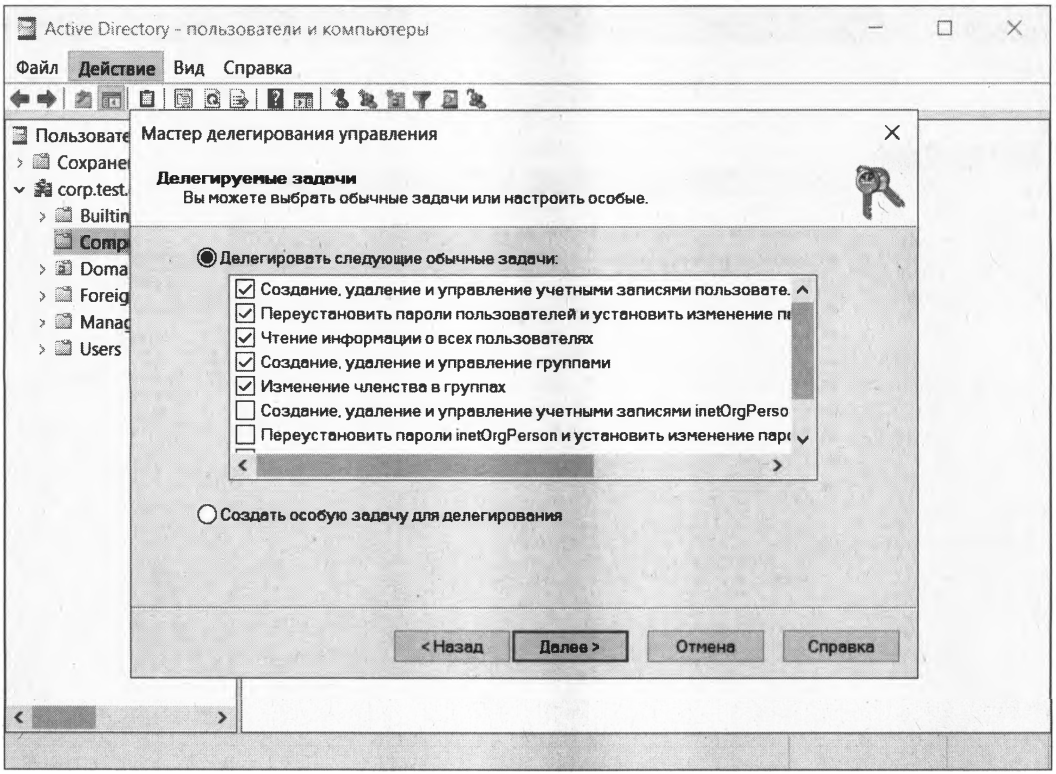


Рис. 4.8. Мастер делегирования управления

Обратите внимание, что какого-либо мастера *отзыва* делегирования не существует. Другими словами, если нужно у кого-то забрать делегированное ранее право, вам придется вручную редактировать права доступа контейнера.

Корзина Active Directory: просмотр и восстановление удаленных объектов каталога

Начиная с Windows Server 2008 R2, можно использовать корзину Active Directory (далее просто «корзина»). Корзина представляет собой легкое средство восстановления удаленных объектов Active Directory. Все атрибуты удаленного объекта сохраняются, и администратор может с легкостью восстановить нечаянно удаленный объект в то состояние, в котором он был до удаления.

Чтобы начать использовать корзину, ее нужно включить. Для этого надо воспользоваться ссылкой **Включить корзину** в центре администрирования Active Directory (рис. 4.9). Включенная корзина будет содержать сведения обо всех удаленных (с момента ее включения) объектах (рис. 4.10). Учтите, что, включив корзину, вы уже не сможете ее выключить.

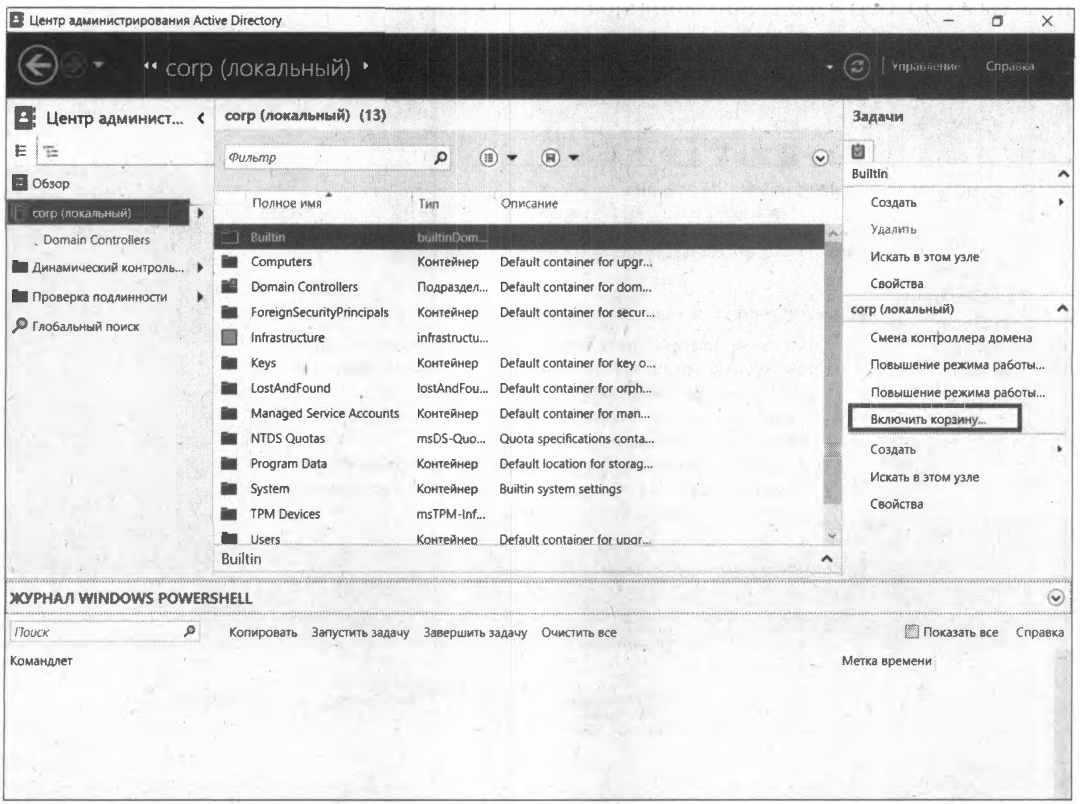


Рис. 4.9. Включение корзины Active Directory (Windows Server 2022)

Впрочем, если корзина и не включена, восстановить удаленные объекты можно из контейнера **Deleted Objects** с использованием *метода авторитетного восстановления*. Процедура такого восстановления осталась неизменной со времен самых первых версий Windows Server, поэтому, скорее всего, вы с ней знакомы (а если нет, то соответствующую информацию можно без особых проблем найти в Интернете).

Примечание

На рис. 4.10 показано, что удаленный объект находится в контейнере **Deleted Objects**, что может несколько сбивать с толку, — а как же корзина? Однако все правильно. Если корзина AD выключена, то при удалении объекта он помечается как удаленный (атрибут `isDeleted` объекта устанавливается в `true`) и из него удаляются лишние атрибуты. Затем объект переименовывается и помещается в контейнер **Deleted Objects**, в котором он хранится в течение срока жизни удаленного объекта. По истечении этого срока он удаляется окончательно. Когда же корзина AD включена, то объект помеча-

ется как *логически удаленный* (это новое состояние, появившееся в Windows Server 2008 R2). При этом объект помещается во все тот же контейнер **Deleted Objects**, в котором он тоже хранится в течение срока жизни удаленного объекта. По окончании этого срока объект переводится в состояние *утилизированный* (атрибут `isRecycled`). А окончательно объект будет удален сборщиком мусора по истечении времени жизни утилизированного объекта.

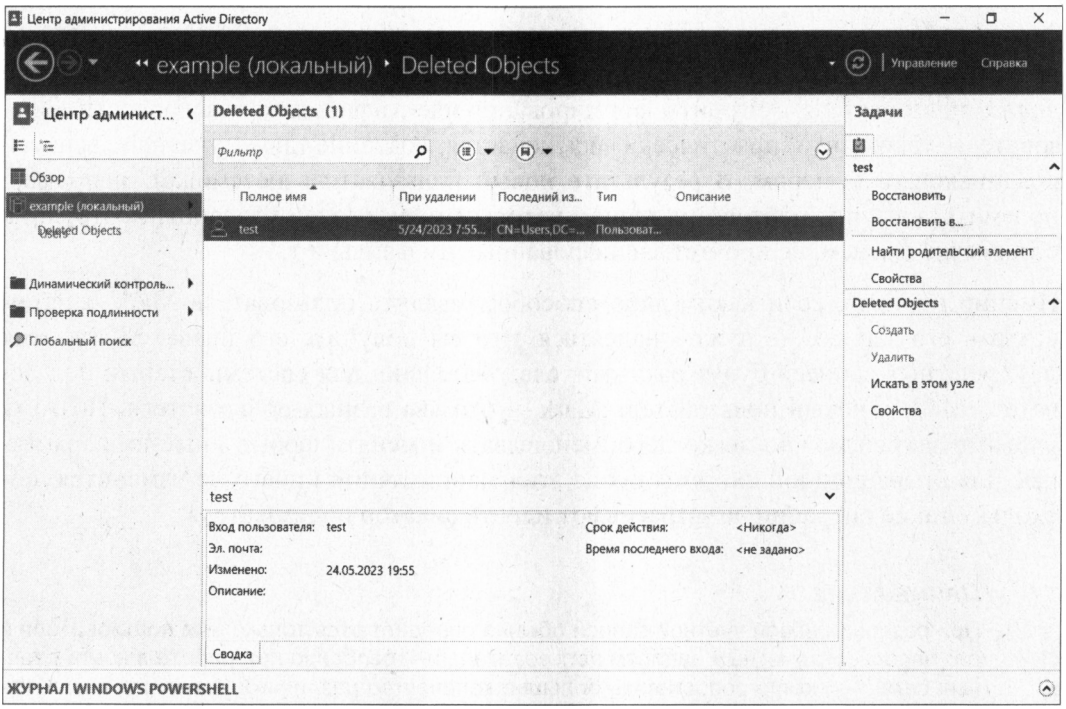


Рис. 4.10. Просмотр удаленных объектов

Учетные записи и права

Безопасность в операционных системах базируется на понятиях *учетной записи* и предоставляемых ей *прав*.

Понятие учетной записи

Любая программа, запущенная на компьютере с любой современной операционной системой, всегда выполняется от имени какого-либо пользователя и обладает данными ему правами. Например, вы работаете под пользователем Mark, запустили текстовый процессор и пытаетесь открыть какой-то файл. Если у пользователя Mark есть право доступа к этому файлу, текстовый процессор сможет его открыть.

Опять-таки, права доступа бывают разными. Есть право чтения документа, есть право изменения документа (записи). Если у пользователя Mark нет права записи

открытого документа, сохранить изменения он не сможет. Однако вы можете выбрать команду **Сохранить как** и сохранить документ в своем домашнем каталоге.

Операционная система «различает» пользователей не по их имени (полному или сокращенному), а по специальному уникальному номеру (идентификатору безопасности — Security Identifier, SID), который формируется в момент создания новой учетной записи.

Операцию удаления учетной записи и последующего создания пользователя с точно 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 пользователь не сможет, например, получить доступ к почтовому ящику, которым пользовался удаленный сотрудник с таким же именем, не прочтет зашифрованные им файлы и т. п.

Именно поэтому, если каким-либо способом удалить пользователя Mark, а затем создать его заново, не нужно надеяться, что вы получите его права. SID'ы этих двух учетных записей будут разными, следовательно, для системы старый пользователь Mark и новый пользователь Mark — это два разных пользователя. Поэтому учетные записи можно легко переименовывать и 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, право удаленного подключения к системе и т. п. Такие параметры являются дополнительными, их определение и использование на практике зависят от особенностей построения конкретной компьютерной сети. Дополнительные параметры могут быть использованы программным обеспечением — например, для поиска определенных групп пользователей (см., например, *группы по запросу*).

Каждый SID состоит из ID безопасности домена и уникального относительного ID (relative ID, RID), который выделяется хозяином относительных идентификаторов.

Стандартные учетные записи имеют идентичные SID (перечень Well Known Security Identifiers приведен, например, в документе KB243330). Так, `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
```

Примечание

Существует множество утилит, которые позволяют по имени входа пользователя определить его SID и наоборот. Например, утилита 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 пакета Account Lockout and Management Tools, которые добавляют к оснастке управления пользователями в домене еще одну вкладку свойств, на которой в том числе отображается и SID пользователя.

Локальные и доменные учетные записи

При работе в компьютерной сети существуют два типа учетных записей:

- *локальные учетные записи*, создаются на конкретном компьютере. Информация о них хранится локально (в локальной базе безопасности компьютера) и локально же выполняется аутентификация такой учетной записи (пользователя). Создать и изменить локальные учетные записи можно с помощью утилиты **Локальные пользователи и группы**;
- *доменные учетные записи*, создаются на контроллерах домена. И именно контроллеры домена проверяют параметры входа такого пользователя в систему. Учетные записи пользователей домена создаются и изменяются с помощью оснастки **Active Directory | Пользователи и компьютеры**.

В современных версиях Windows существует новый тип учетных записей — *учетные записи Microsoft*. ОС Windows Server 2012/2016/2019/2022 не управляет такими учетными записями, и их нельзя использовать в составе Active Directory. Их удел — домашние компьютеры. Собственно, для этого они и создавались, а в корпоративной среде их заменяют доменные учетные записи. Однако пользователи Windows 10/11 все же могут использовать их для получения доступа к Магазину Windows, чтобы загружать оттуда необходимые им приложения (например, приложение WiFi Analyzer, которое мы упоминали в *главе 3*, доступно к загрузке только через Магазин Windows).

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.

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 (**Bad Password Count**). Эту информацию можно получить, выполнив непосредственный 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.

Группы пользователей

Разные пользователи должны иметь разные права по отношению к компьютерной системе. Если на предприятии всего несколько сотрудников, то для администратора не составляет 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 ему были даны ранее, «снять» их и назначить новые, но принципиальной необходимости какого-либо объединения пользователей в группы не возникает.

Иная ситуация на среднем предприятии. 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, — например, при изменении должности пользователя достаточно переместить его в другую группу. А при создании новых проектов права доступа к ним будут назначаться на основе существующих групп и т. п. 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.

Операционная система Windows Server поддерживает группы трех типов:

- **Локальные группы** (Local groups) — группы, которые были определены на локальном компьютере. Создать такие группы можно с помощью утилиты **Локальные пользователи и группы** (Local Users And Groups);
- **Группы безопасности** (Security groups) — группы, имеющие связанные с ними дескрипторы безопасности (SID). Такие группы существуют в доменах и создаются с помощью оснастки **Active Directory | Пользователи и компьютеры**;

- **Группы рассылки** (Distribution group) — группы, использующиеся в списках рассылки электронной почты. Они не имеют SID. Создаются эти группы оснасткой **Active Directory | Пользователи и компьютеры**.

По области действия можно выделить следующие типы групп:

- *локальные группы домена* — обычно создаются для назначения разрешений доступа к ресурсам в пределах одного домена. Такие группы могут содержать членов из любого домена в лесу или из доверяемых доменов в других лесах. Обычно глобальные и универсальные группы являются членами локальных групп домена;
- *встроенные локальные группы* — имеют разрешения локального домена и часто относятся к *локальным группам домена*. Разница между ними и другими группами в том, что администратор не может создавать или удалять встроенные локальные группы. Их можно только модифицировать;
- *глобальные группы* — обычно создаются в одном и том же домене для определения прав пользователей и компьютеров, разделяющих подобную роль или функцию. Члены глобальных групп — только учетные записи и группы из домена, в котором они были определены;
- *универсальные группы* — обычно создаются для определения наборов пользователей или компьютеров, которые должны иметь широкие разрешения по всему домену или лесу. Членами таких групп являются учетные записи пользователей, глобальные группы и другие универсальные группы из любого домена в дереве доменов или лесу.

> ***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`).

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. 4.3).

Таблица 4.3. *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

В режиме native mode администраторы могут изменять типы групп, а именно — преобразовывать группу безопасности (Security group) в группу рассылки (Distribution group) и наоборот. Возможна также смена области действия группы с универсальной на доменную.

Обратите только внимание, что наличие вложенных групп в некоторых случаях может препятствовать преобразованию типа родительской группы.

Ролевое управление

Современные прикладные программы предусматривают работу с данными пользователей, имеющих различающиеся функциональные обязанности. 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.

Прикладные программы могут создавать роли как для группы безопасности в домене, так и для локальных групп на том компьютере, где работает программа. Администратору остается только включить необходимых пользователей (или группу пользователей, если таковая уже создана) в состав соответствующей роли.

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 той или иной 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 станет 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 принципа преимущества запрета перед разрешением, известное авторам. Это определение итогового разрешения на основе

наследуемых и *явно указанных* прав, которое описано в *разд. «Наследуемые разрешения: будьте внимательны» далее в этой главе.*

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 того или иного 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 работе в файловой системе 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 диск с ресурсами имеет формат файловой системы 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 разрешения общего доступа и разрешения безопасности 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 разных 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 с 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 по 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 этот объект *наследуются* от родительского. Для того чтобы изменить их, необходимо такую связь разорвать. Эта операция выполняется через кнопку **Дополнительно** — достаточно снять флажок **Заменить все записи разрешений дочернего объекта наследуемыми от этого объекта** (рис. 4.11).

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.

В свойствах файла отмечены как запреты (унаследованы от родительской папки и 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 отображаются самой системой — показано полное отсутствие прав, несмотря на наличие разрешения полного доступа.

> ***Примечание***
>
> Администратору следует внимательно отнестись к таким ситуациям, поскольку это может привести к неучитываемым возможностям доступа к данным. Так, на компьютерах авторов окно отображения результирующих прав доступа неверно демонстрировало существующие разрешения — права доступа к файлу не были показаны, хотя они фактически имелись.

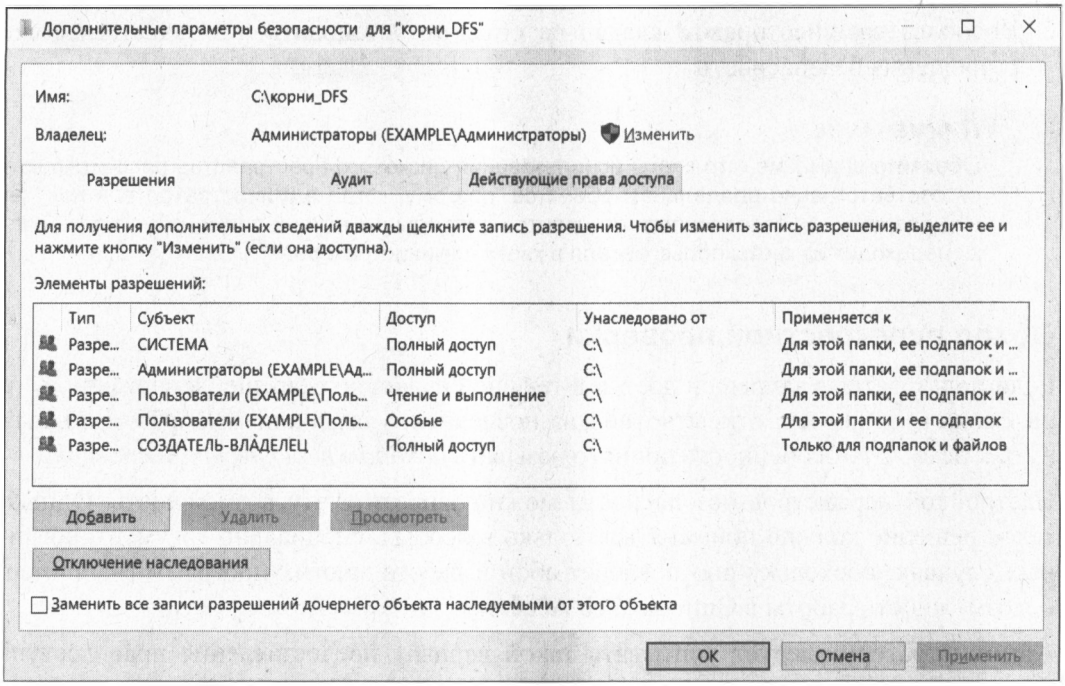


Рис. 4.11. Дополнительные параметры безопасности

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 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 таким 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 с помощью кнопки **Дополнительно** в настройках безопасности.

2. Воспользовавшись правом владельца объекта, установить для него желаемые разрешения безопасности.

> ***Примечание***
>
> Обратите внимание, что квоты использования дискового пространства рассчитываются соответственно владельцам объектов, поэтому, когда администратор для получения разрешения безопасности становится владельцем некоей папки, объем этой папки переходит 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 эту 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 такой вариант предоставления прав доступа и правильно настраивать соответствующие параметры.

Изменение атрибутов объектов при операциях копирования и перемещения

При операциях копирования/перемещения файлов могут меняться их атрибуты. Неточное понимание вариантов изменения разрешений может привести к незапланированному результату. Так, если при копировании файла он перестанет[1] быть зашифрованным, а вы по-прежнему считаете информацию, содержащуюся в нем, защищенной, то такой факт может привести к неприятным последствиям.

> ***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 флешку он перестанет быть 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. Соответственно если вы создаете новый файл в папке, которой

---

[1] Такое поведение было свойственно Windows XP — в последующих версиях система выдает предупреждение, что файл после копирования или перемещения будет уже незашифрованным.

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, 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 его удаления с прежнего места расположения. Поэтому атрибуты файлу будут присвоены по правилам операции копирования, и он будет иметь атрибут той папки, в которую 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. Таким образом, при перемещении незашифрованного файла в зашифрованную папку на том же диске информация в файле останется незашифрованной.

Результирующие права и утилиты

Как правило, на предприятии 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 тому или иному 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. 4.12).

> ***Примечание***
>
> Средствами групповой политики администратор имеет возможность отключения просмотра результирующих прав.

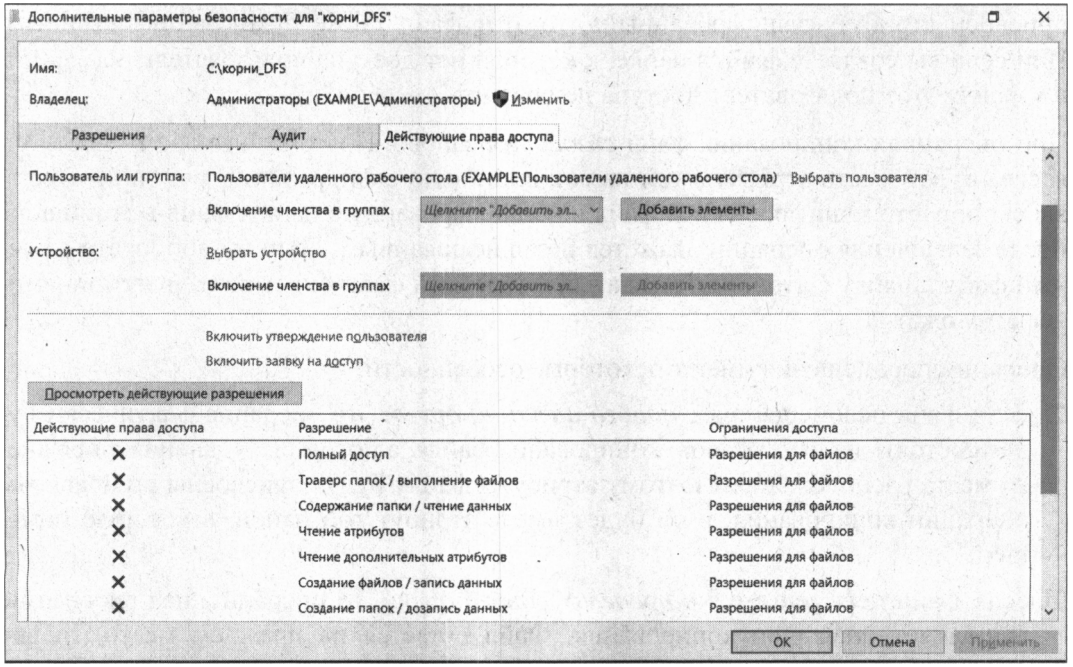


Рис. 4.12. Отображение действующих прав доступа к файлу для выбранного пользователя

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 и позволяет гораздо быстрее, проще и понятнее устанавливать разрешения.

Например, для локального компьютера можно создать несколько локальных групп, объединить в них как пользователей этой системы, так и доменные учетные записи, после чего уже с использованием созданных 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 своей операционной системе — используя права администратора можно создавать, модифицировать, удалять другие учетные записи, выполнять любые операции по настройке системы и т. п.

Настоятельно рекомендуется задать для этой учетной записи длинный и сложный пароль. Такой пароль должен состоять из цифр, букв и знаков подчеркивания. Слова не должны быть словарными. Если вы сами не можете придумать сложный пароль, воспользуйтесь генераторами паролей — таких в Интернете множество.

Для управления учетными записями используются специальные оснастки: управления компьютером в локальном случае и оснастка управления **Средства, Пользователи и компьютеры Active Directory** (рис. 4.13) при создании доменных пользователей.

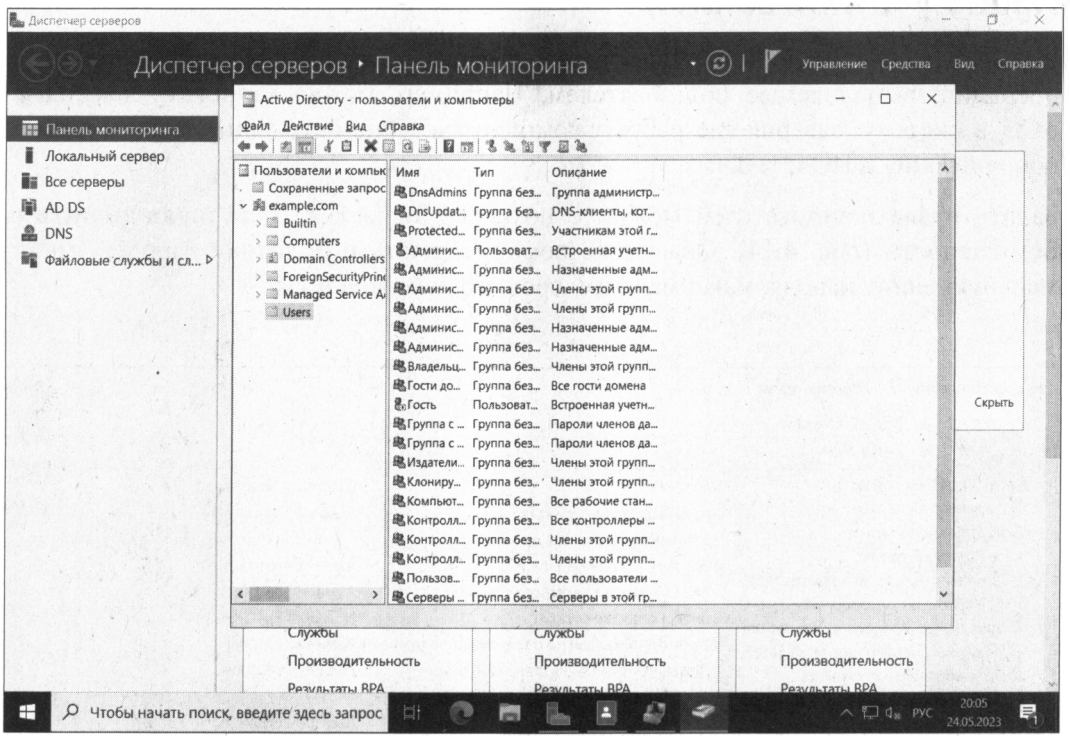


Рис. 4.13. Локальные пользователи

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
```

Если на предприятии 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 можно воспользоваться операцией *копирования учетной записи*. При копировании программа создает новую учетную запись, в настройки которой будут 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.

Права учетной записи

Кроме ограничения доступа пользователя к папкам и файлам, можно ограничить и операции, выполняемые пользователем. Например, можно запретить локальный вход в систему, завершение работы компьютера, установку или удаление нового оборудования и ПО и т. д.

Задать права пользователей можно с помощью оснастки **Локальная политика безопасности** (рис. 4.14). Она также поможет задать и политику паролей: минимальную длину пароля, максимальный срок его действия и т. п.

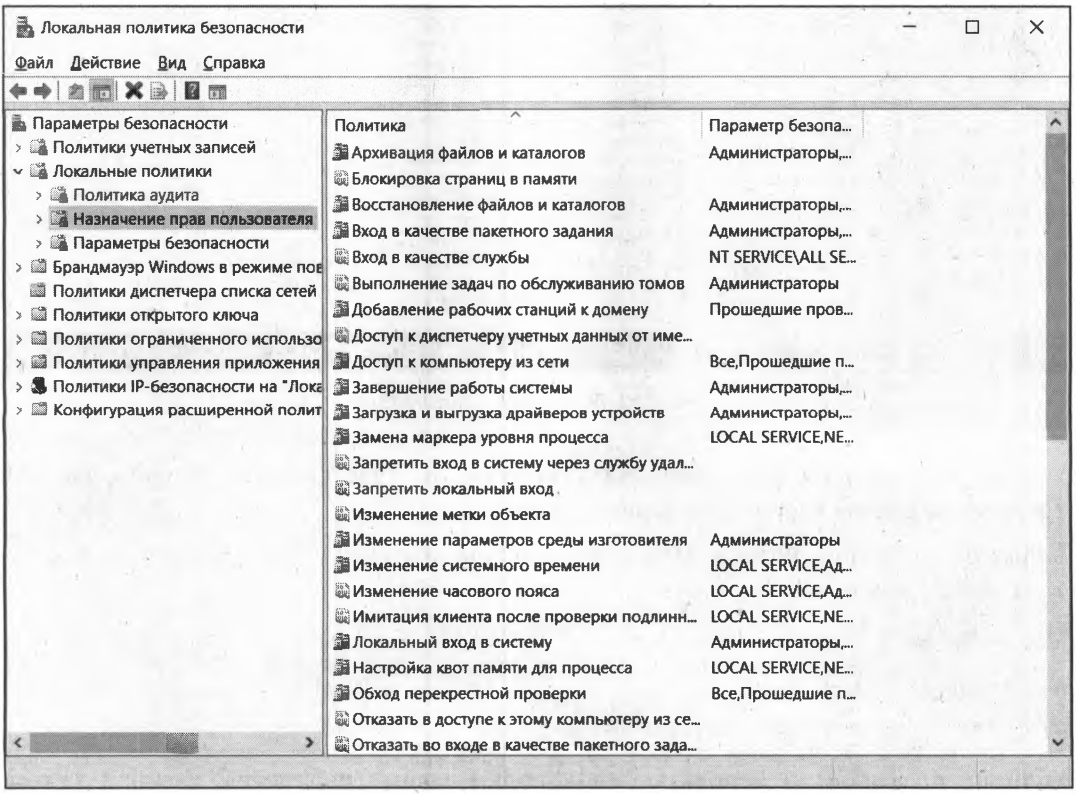


Рис. 4.14. Локальная политика безопасности

Восстановление параметров безопасности по умолчанию

В случае смены администраторов новому специалисту обычно не известны, например, те изменения прав доступа, которые выполнил прежний сотрудник. 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 в меню не включена, и чтобы начать с ней работу, следует открыть консоль управления (командой `mmc`) и выполнить процедуру добавления оснастки: в области **Доступные оснастки** окна **Добавление и удаление оснасток** выбрать строку **Анализ и настройка безопасности** (рис. 4.15), нажать кнопку **Добавить** и закрыть все последующие окна, нажимая на кнопки подтверждения операции.

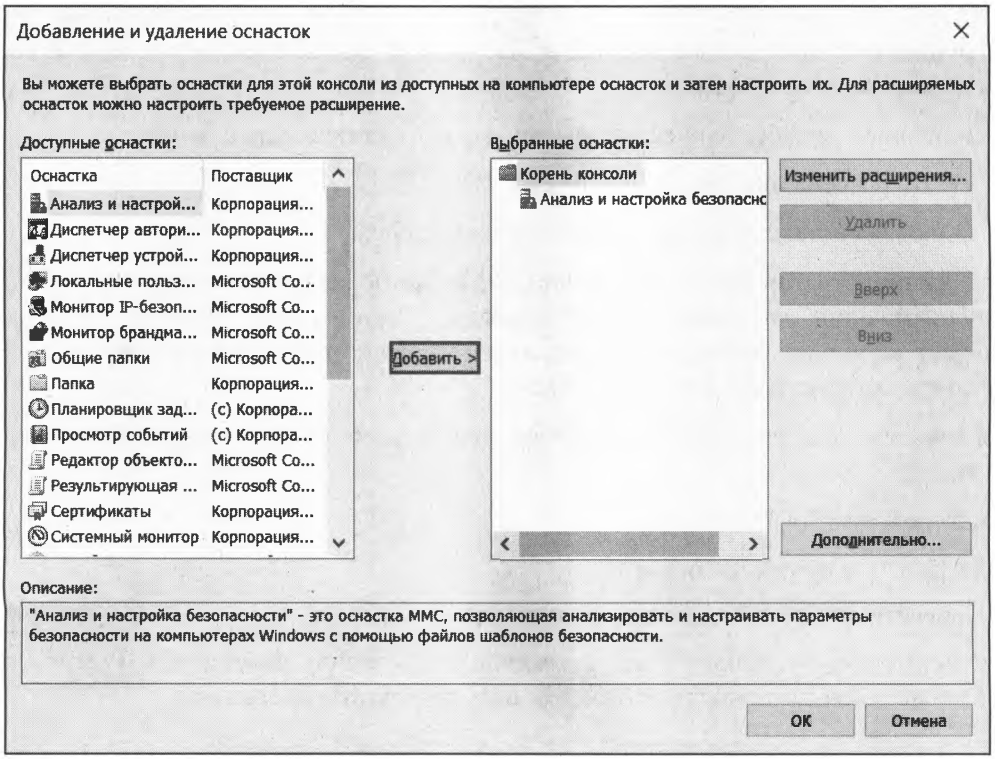


Рис. 4.15. Добавление оснастки **Анализ и настройка безопасности**

В операционной системе хранятся разработанные поставщиком шаблоны безопасности (по умолчанию они размещены в папке %windir%\Security\Templates) для нескольких типовых конфигураций компьютера. Это шаблон настроек безопасности, соответствующий установке системы, а также шаблоны безопасности для компьютеров (отдельно для рабочих станций, серверов и контроллеров домена), соответст-

вующие различным уровням защищенности и совместимые с программным обеспечением предыдущих версий, и т. д.

Оснастка **Анализ и настройка безопасности** 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 в отчете оснастки специально выделены.

Строго говоря, можно проанализировать следующие параметры:

- политики учетных записей: политика паролей, политика блокировки учетных записей и политика Kerberos;
- локальные политики: политика аудита, назначение прав пользователя и параметры безопасности;
- журнал событий: параметры журналов приложений, системы и событий безопасности;
- группы с ограниченным доступом: членство в чувствительных к безопасности группах пользователей;
- системные службы: запуск системных служб и разрешения для них;
- реестр: разрешения для разделов реестра;
- файловая система: разрешения для папок и файлов.

Если администратор сочтет необходимым, то он может с помощью этой оснастки применить один из шаблонов безопасности — применение шаблона фактически означает установку соответствующих параметров системы (разрешений, прав) в те значения, которые определены в шаблоне.

Для анализа или применения настроек необходимо выполнить следующие действия:

3. Создать пустую базу данных.
4. Загрузить в нее желаемый шаблон.
5. 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 предыдущей версией ОС. В этом режиме учетным записям пользователей даются дополнительные права на доступ к ресурсам системы. В результате появляется возможность запуска программ, не в полной мере совместимых с последними версиями операционной системы. Такая операция в новых ОС разрешена только администраторам, но после применения этого шаблона необходимые разрешения будут предоставлены.

Автоматически создаваемые учетные записи

При установке Windows Server 2016/2019/2022 создаются учетные записи групп и пользователей по умолчанию. Эти учетные записи разработаны для обеспечения базовой установки, необходимой для построения сети. Итак, по умолчанию создаются учетные записи трех типов:

- *встроенные* (Built-in) — учетные записи пользователя и группы, которые устанавливаются вместе с операционной системой, приложениями и службами;
- *предопределенные* (Predefined) — учетные записи пользователя и группы, которые устанавливаются вместе с операционной системой;
- *неявные* (Implicit) — специальные группы (специальные идентификаторы), создаваемые неявно, в момент доступа к сетевым ресурсам.

Встроенные учетные записи пользователей

Во всех системах Windows имеется несколько встроенных учетных записей пользователей:

- **LocalSystem** — псевдоучетная запись, которая используется для запуска системных процессов и управления задачами уровня системы. Эта учетная запись является частью группы **Администраторы** (Administrators) на сервере и имеет все права пользователя на сервере. При настройке приложений и служб на использование этой учетной записи все связанные процессы получат полный доступ к системе сервера. С помощью учетной записи **LocalSystem** запускаются многие службы. Но службы, которым нужны альтернативные привилегии или права входа, нужно запускать под учетными записями **LocalService** или **NetworkService** (см. далее);
- **LocalService** — псевдоучетная запись с ограниченными привилегиями, предоставляющая доступ только к локальной системе. Эта учетная запись является частью группы **Пользователи** (Users) на сервере и имеет те же права, что и учетная запись **NetworkService**, однако **LocalService** ограничена только локальным компьютером. От имени этой учетной записи должны работать процессы, которым не нужно получать доступ к другим серверам;
- **NetworkService** — псевдоучетная запись для запуска служб, которым нужны права входа в локальную систему и сеть. Является частью группы **Пользователи** на сервере и предоставляет меньше разрешений и привилегий по сравнению с учетной записью **LocalSystem** (но больше, чем **LocalService**).

Предопределенные учетные записи пользователя

Обычно вместе с Windows поставляется несколько предопределенных учетных записей, в том числе **Администратор** (Administrator) и **Гость** (Guest). Помните, что у предопределенных учетных записей есть дубликаты в каталоге Active Directory. Эти учетные записи распространяются на весь домен и отличаются от локальных учетных записей на локальных системах.

Учетная запись *Администратор*

Учетная запись **Администратор** является предопределенной учетной записью, предоставляющей полный доступ к файлам, каталогам, службам и другим объектам. В Active Directory у учетной записи **Администратор** есть полный доступ и полные полномочия, распространяющиеся на весь домен.

> ***Внимание!***
>
> Для предотвращения неавторизированного доступа к системе или домену убедитесь, что назначили учетной записи **Администратор** безопасный пароль. Кроме того, поскольку это всем известная учетная запись Windows, в качестве дополнительной меры предосторожности можно ее как-либо переименовать, а вместо нее создать фиктивную учетную запись с именем **Администратор** и минимальными правами. Такая учетная запись должна быть отключена, но в то же время для нее должен быть установлен сложный пароль. Пусть злоумышленники мучаются.

По умолчанию учетная запись **Администратор** для домена — член групп **Администраторы** (Administrators), **Администраторы домена** (Domain Admins), **Пользователи домена** (Domain Users), **Администраторы предприятий** (Enterprise Admins), **Владельцы-создатели групповой политики** (Group Policy Creator Owners) и **Администраторы схемы** (Schema Admins).

> ***Примечание***
>
> В Windows 7/10/11 учетная запись **Администратор** как бы разделилась на две: одна учетная запись соответствует той, с которой вы входите в систему, другая — используется, если вызывается команда **Запустить от имени администратора**. С этим связаны некоторые ошибки, когда пользователи не могут понять, почему не выполняется сценарий, исполняемый от имени пользователя **Администратор**. А все потому, что фактически этих учетных записей две и права у них различаются.

Учетная запись *Гость*

Учетная запись **Гость** предназначена для пользователей, которым необходим одноразовый или случайный доступ. Хотя у нее имеется лишь ограниченный доступ к системе, при ее использовании гарантированы потенциальные проблемы безопасности. Именно поэтому она по умолчанию отключена.

Учетная запись **Гость** по умолчанию является членом групп **Гости домена** (Domain Guests) и **Гости** (Guests). Учетная запись **Гость** одновременно является членом неявной группы **Все** (Everyone), которая обычно имеет доступ к файлам и папкам. У этой группы также есть набор прав пользователя по умолчанию.

Другие встроенные учетные записи пользователей

- Учетная запись **HelpAssisstant** применяется в случаях обращения к удаленному помощнику. Удаленный пользователь подключается к компьютеру с правами, предоставленными этой учетной записи.
- 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 учетные записи: **IUSR_имя_пользователя** и **IWAM_имя_пользователя**. Учетная запись **IUSR_имя_пользователя** применяется при предоставлении веб-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_пользователя**. Вы можете, например, запретить анонимный доступ к каким-либо ресурсам информационного сервера, если исключите чтение таких файлов этим пользователем. Пароль пользователя **IUSR_имя_пользователя** создается автоматически и синхронизируется между операционной системой и информационным сервером.

  Пароли учетных записей **IUSR_имя_пользователя** и **IWAM_имя_пользователя** легко можно узнать при помощи сценария, имеющегося на компьютере. Найдите файл Adsutil.vbs (обычно он расположен в папке административных сценариев IIS — например, в InetPub\AdminScripts), замените в текстовом редакторе строку сценария (иначе сценарий покажет пароль в виде звездочек):

  ```
  IsSecureProperty = True
  ```

  на

  ```
  IsSecureProperty = False
  ```

  и выполните для отображения пароля **IUSR_имя_пользователя** команду:

  ```
  cscript.exe adsutil.vbs get w3svc/anonymoususerpass
  ```

  или — для показа пароля **IWAM_имя_пользователя** команду:

  ```
  cscript.exe adsutil.vbs get w3svc/wamuserpass
  ```

- Учетная запись **IWAM_имя_компьютера** служит 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, синхронизировать с помощью специальных сценариев пароли учетных записей и т. п. Но гораздо эффективнее в этой ситуации будет просто удалить службу информационного сервера и вновь добавить этот компонент, предоставив программе установки выполнить все эти операции.

Кроме указанных учетных записей, новые пользователи системы часто создаются прикладными программами в процессе их установки. Обычно создаваемые таким образом учетные записи имеют необходимое описание в своих свойствах.

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;
- **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 файловой системы 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.

  Учетная запись с правами оператора резервного копирования является весьма серьезной брешью в системе безопасности предприятия. 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 станет бессмысленно. Но есть и более простые способы копирования информации, право доступа к которой запрещено на уровне файловой системы. В Windows имеется утилита Robocopy (robocopy.exe) для массового копирования файлов. 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;

Примечание

Программа 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 этой утилиты.

- **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** — члены этой группы могут осуществлять удаленное подключение к рабочему столу компьютера. 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** и **WINS Users** — группы создаются только при установке соответствующих служб. Пользователи групп имеют право лишь 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.

К специальным группам относятся:

- **Все** (Everyone);
- **Интерактивные пользователи** (Local Users);

- **Сетевые пользователи** (Network Users);
- **Пакетные файлы** (Batch);
- **Прошедшие проверку** (Authenticated).

Предназначение групп ясно уже по их названиям. Так, в группу **Интерактивные пользователи** автоматически включаются все пользователи, осуществившие вход в систему с консоли (клавиатуры). **Сетевые пользователи** — это те пользователи, которые используют ресурсы компьютера через сетевое подключение, и т. п.

Эти 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 конкретном компьютере. Иными словами, если вы предоставили ресурс компьютера в общий доступ с правами чтения для группы **Все**, то использовать его могут только те, кто на этом компьютере «прописан». 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 этой группы в каждом конкретном случае.

Рекомендации по использованию операции *Запуск от имени Администратора*

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. Понятно, что, несмотря на все рекомендации, большинство пользователей для удобства работают с правами учетной записи администратора.

В операционных системах Windows 7 и выше по умолчанию максимальные права не предоставлены и администратору. Чтобы выполнить действия, меняющие сис-

темные настройки, предусмотрен специальный механизм для быстрого запуска программ с использованием административных прав. Это операция **Запуск от имени Администратора**.

Такая команда доступна в контекстном меню соответствующего ярлыка. Кроме того, если при запуске программы система обнаружила попытку выполнения действий, для которых требуется подобная эскалация прав, то пользователь увидит на экране запрос на продолжение, который он должен подтвердить (или отказаться, если подобная операция не планировалась). Конечно, такой запрос пользователь получит только в том случае, если включен контроль учетных записей пользователей (UAC). Для его включения/выключения в апплете панели управления **Учетные записи пользователей** нужно перейти по ссылке **Изменение параметров контроля учетных записей** и выбрать соответствующее значение с помощью ползунка.

> ***Примечание***
>
> Обратите еще раз внимание, что учетная запись **Администратор** и учетная запись, которая используется при запуске от имени администратора, — это различные учетные записи. Если не учитывать такой нюанс, то это может привести к неожиданным результатам, например, при выполнении сценариев входа в домен.

Включение сетевого обнаружения в Windows Server 2016/2019/2022

По умолчанию сетевое обнаружение в Windows Server 2016/2019/2022 выключено, и одного включения соответствующего параметра в Центре управления сетями и общим доступом (рис. 4.16) недостаточно. Вы увидите, что значение параметра на самом деле не изменилось.

Причина в выключенных по умолчанию службах, необходимых для работы сетевого обнаружения. Итак, нужно включить следующие службы:

- Function Discovery Provider Host, FDPHost (хост поставщика функции обнаружения) — отвечает за обнаружение в сети других компьютеров;
- Function Discovery Resource Publication, FDResPub (публикация ресурсов обнаружения функции) — отвечает за то, чтобы другие компьютеры могли обнаружить в сети ваш компьютер;
- DNS Client, dnscache (DNS-клиент);
- SSDP Discovery, SSDPSrv (обнаружение SSDP);
- UPnP Device Host, upnphost (узел универсальных PNP-устройств).

Убедитесь, что они работают, а тип запуска для каждой из них установлен в значение **Автоматически**. После этого перезагрузите компьютер, и вы сможете увидеть содержимое сети (рис. 4.17).

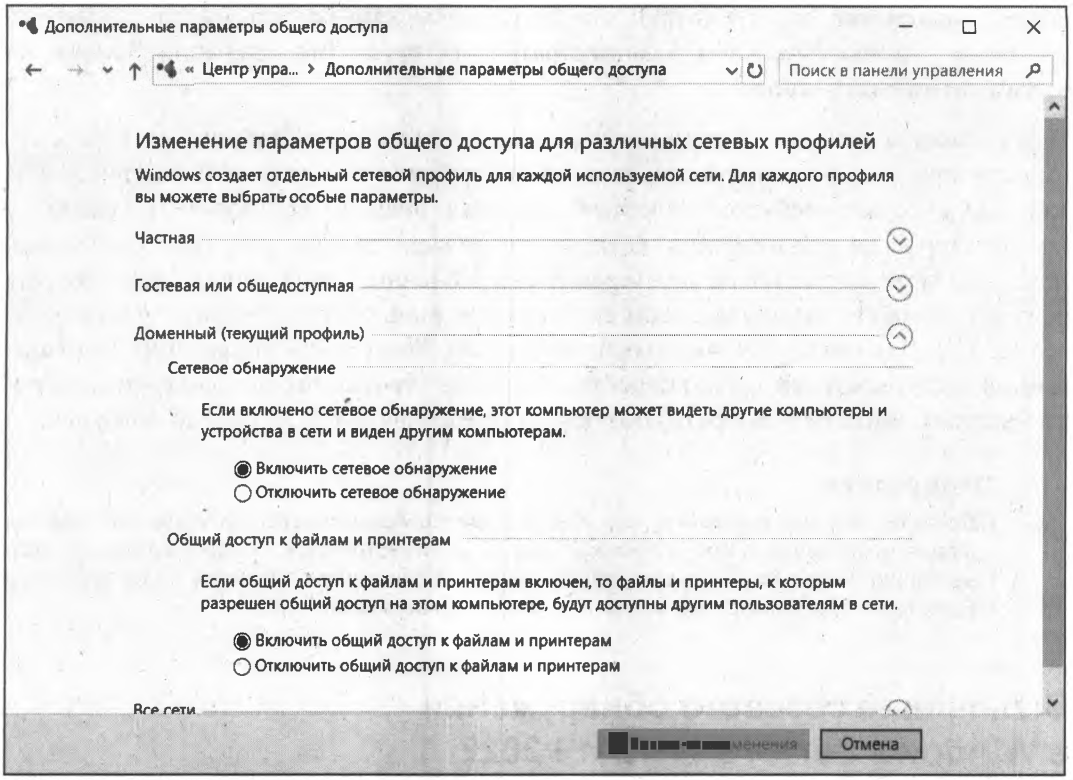


Рис. 4.16. Центр управления сетями и общим доступом

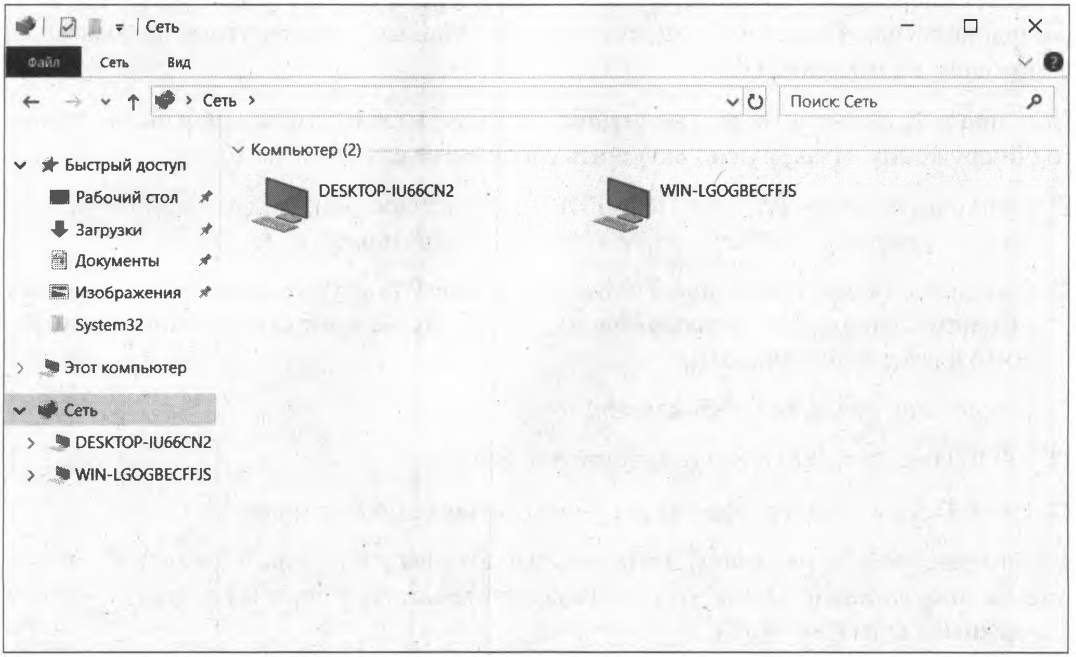


Рис. 4.17. Обозреватель сети

ГЛАВА 5

Работа в глобальной сети

В этой главе мы рассмотрим несколько типичных задач, с которыми сталкивается каждый администратор, а именно: предоставление доступа к Интернету, защита внутренних ресурсов предприятия от внешних угроз, организация связи между центральным офисом и филиалами, предоставление доступа мобильным сотрудникам к ресурсам предприятия. Первые две задачи решаются правильной настройкой брандмауэра, последние две — путем организации виртуальных частных сетей (VPN).

Организация доступа к ресурсам Интернета

Сетевая адресация

Для идентификации узлов Интернета используются IP-адреса. IP-адрес представляет собой четыре числа, разделенные точками (или одно 32-разрядное число, которое записывается в виде четырех восьмиразрядных чисел, разделенных точками, — как кому больше нравится). Нужно сразу отметить, что такая идентификация неоднозначная, поскольку IP-адреса могут быть статическими (постоянными) и динамическими. *Постоянные* (статические) IP-адреса обычно назначаются серверам, а *динамические* — обычным пользователям. Так что сегодня определенный динамический IP-адрес может быть назначен одному пользователю, а завтра — другому. Поэтому если в случае с аппаратными MAC-адресами еще можно говорить о какой-то однозначности (и то существуют способы подмены MAC-адресов), то IP-адреса по определению однозначными не являются.

Вот примеры IP-адресов: 127.0.0.1, 192.168.1.79, 111.33.12.99. Как было сказано ранее, IP-адрес — это одно 32-разрядное число или четыре 8-разрядных. Возведем 2 в восьмую степень и получим максимальное значение для каждого из четырех восьмиразрядных чисел — 256. Таким образом, учитывая, что некоторые IP-адреса зарезервированы для служебного использования, протокол IP может адресовать примерно 4,3 млрд узлов. Однако с каждым годом количество узлов во Всемирной паутине увеличивается, поэтому была разработана шестая версия про-

токола IP — IPv6 (если упоминается просто протокол IP, то, как правило, имеется в виду четвертая версия протокола — IPv4). Новый протокол использует 128-битные адреса (вместо 32-битных), что позволяет увеличить число узлов до 10^{12} и количество сетей до 10^9 (чуть далее о протоколе IPv6 рассказано более подробно).

IP-адреса выделяются *сетевым информационным центром* (NIC, Network Information Center). Чтобы получить набор IP-адресов для своей сети, вам надо обратиться в этот центр. Но, оказывается, это приходится делать далеко не всем. Существуют специальные IP-адреса, зарезервированные для использования в локальных сетях. Ни один узел глобальной сети (Интернета) не может обладать таким «локальным» адресом. Вот пример локального IP-адреса: 192.168.1.1. В своей локальной сети вы можете использовать любые локальные IP-адреса без согласования с кем бы то ни было. Когда же вы надумаете подключить свою локальную сеть к Интернету, вам понадобится всего один «реальный» IP-адрес — он будет использоваться на маршрутизаторе (шлюзе) доступа к Интернету. Чтобы узлы локальной сети (которым назначены локальные IP-адреса) смогли «общаться» с узлами Интернета, используется NAT (Network Address Translation) — специальная технология *трансляции сетевого адреса* (о NAT подробно рассказано чуть далее).

Наверное, вам не терпится узнать, какие IP-адреса можно использовать без согласования с NIC? Об этом говорить пока рано — ведь мы еще ничего не знаем о *классах* сетей. IP-адреса служат для адресации не только отдельных компьютеров, но и целых сетей. Вот, например, IP-адрес сети: 192.168.1.0. Отличительная черта адреса сети — 0 в последнем октете.

Сети поделены на классы в зависимости от их размеров:

- класс A — огромные сети, которые могут содержать 16 777 216 адресов, IP-адреса таких сетей лежат в пределах 1.0.0.0–126.0.0.0;
- класс B — средние сети, они содержат до 65 536 адресов. Диапазон адресов — от 128.0.0.0 до 191.255.0.0;
- класс C — маленькие сети, каждая сеть содержит до 256 адресов.

Существуют еще и классы D и E, но класс E не используется, а зарезервирован на будущее (хотя будущее — это IPv6), а класс D зарезервирован для служебного использования (широковещательных рассылок).

Представим ситуацию. Вы хотите стать интернет-провайдером. Тогда вам нужно обратиться в NIC для выделения диапазона IP-адресов под вашу сеть. Скажем, вы планируете сеть в 1000 адресов. Понятно, что сети класса C вам будет недостаточно. Поэтому можно или арендовать четыре сети класса C, или одну класса B. Но, с другой стороны, 65 536 адресов для вас — много, и если выделить вам всю сеть класса B, то это приведет к нерациональному использованию адресов. Так что самое время поговорить о *маске сети*. Маска сети определяет, сколько адресов будет использоваться сетью, фактически маска задает размер сети. Маски полноразмерных сетей классов A, B и C представлены в табл. 5.1.

Маска 255.255.255.0 вмещает 256 адресов (в последнем октете IP-адреса могут быть цифры от 0 до 255). Например, если адрес сети 192.168.1.0, а маска 255.255.255.0,

то в сети могут быть IP-адреса от 192.168.1.0 до 192.158.1.255. Первый адрес (192.168.1.0) называется IP-адресом сети, последний — зарезервирован для широковещательных рассылок. Следовательно, для узлов сети остаются 254 адреса: от 192.168.1.1 до 192.168.1.254.

Таблица 5.1. *Маски сетей классов A, B и C*

Класс сети	Маска сети
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

А вот пример маски сети на 32 адреса — 255.255.255.224:

255 – 224 = 31 + «нулевой» IP-адрес, итого 32.

Предположим, у нас есть IP-адрес произвольной сети — например: 192.168.1.0. Как узнать, к какому классу она принадлежит? Для этого нужно преобразовать первый октет адреса в двоичное представление. Число 192 в двоичной системе будет выглядеть так: **11**000000. Проанализируем первые биты первого октета. Если они содержат двоичные цифры 110, то перед нами сеть класса C. Теперь проделаем то же самое с сетью 10.0.0.0. Первый октет равен 10, и в двоичной системе он будет выглядеть так: **0**0001010. Здесь первый бит — 0, поэтому сеть относится к классу A. Опознать класс сети по первым битам первого октета поможет табл. 5.2.

Таблица 5.2. *Опознание класса сети*

Класс сети	Первые биты
A	0
B	10
C	110
D	1110
E	11110

Теперь вспомним о специальных зарезервированных адресах. Адрес 255.255.255.255 является *широковещательным*. Если пакет отправляется по этому адресу, то он будет доставлен всем компьютерам, находящимся с отправителем в одной сети. Можно уточнить сеть, компьютеры которой должны получить широковещательную рассылку, например, таким образом: 192.168.5.255. Этот адрес означает, что пакет получат все компьютеры сети 192.168.5.0.

Вам также следует знать адрес 127.0.0.1. Этот адрес зарезервирован для обозначения локального компьютера и называется *адресом обратной петли*. Если отправить пакет по этому адресу, то его получит ваш же компьютер, т. е. получатель является отправителем, и наоборот. Этот адрес обычно используется для тестиро-

вания поддержки сети. Более того, к локальному компьютеру относится любой адрес из сети класса A с адресом 127.0.0.0. Поэтому при реальной настройке сети нельзя использовать IP-адреса, начинающиеся со 127.

А теперь можно рассмотреть IP-адреса сетей, зарезервированные для локального использования. В локальных сетях вы можете задействовать следующие адреса сетей:

- 192.168.0.0–192.168.255.0 — сети класса C (всего 256 сетей, маска 255.255.255.0);
- 172.16.0.0–172.31.0.0 — сети класса B (всего 16 сетей, маска 255.255.0.0);
- 10.0.0.0 — сеть класса A (одна сеть, маска 255.0.0.0).

Обычно в небольших домашних и офисных сетях используются IP-адреса из сети класса C, т. е. из диапазона 192.168.0.0–192.168.255.0. Но поскольку назначение адресов контролируется только вами, вы можете назначить в своей локальной сети любые адреса — например, адреса из сети 10.0.0.0, даже если у вас в сети всего 5 компьютеров. Так что выбор сети — это дело вкуса. Можете себя почувствовать администратором огромной сети и использовать адреса 10.0.0.0.

Введение в IPv6

IPv6 (Internet Protocol version 6) — новая версия протокола IP, созданная для решения проблем, с которыми столкнулась предыдущая версия (IPv4) при ее использовании в Интернете, — адресов просто стало не хватать. У нового протокола длина адреса составляет 128 битов вместо 32.

В настоящее время протокол IPv6 используется в нескольких десятках тысяч сетей, и только Китай планирует в скором времени полностью перейти на IPv6.

Преимущества IPv6 (кроме большего адресного пространства) по сравнению с IPv4 выглядят так:

- возможна пересылка огромных пакетов — до 4 Гбайт;
- появились метки потоков и классы трафика;
- имеется поддержка многоадресного вещания;
- убраны функции, усложняющие работу маршрутизаторов (из IP-заголовка исключена контрольная сумма, и маршрутизаторы не должны фрагментировать пакет — вместо этого пакет отбрасывается с ICMP-уведомлением о превышении MTU).

В IPv6 существуют три типа адресов: одноадресные (Unicast), групповые (Anycast) и многоадресные (Multicast):

- адреса Unicast работают как обычно — пакет, отправленный на такой адрес, достигнет интерфейса с этим адресом;
- адреса Anycast синтаксически неотличимы от адресов Unicast, но они адресуют сразу группу интерфейсов. Пакет, который был отправлен на такой адрес, попа-

дет в ближайший (согласно метрике) интерфейс. Адреса Anycast используются только маршрутизаторами;

- адреса Multicast идентифицируют группу интерфейсов — пакет, отправленный по такому адресу, достигнет всех интерфейсов, привязанных к группе многоадресного вещания.

IP-адреса по протоколу IPv6 отображаются в виде восьми групп шестнадцатеричных цифр, разделенных двоеточиями. Вот пример адреса нового поколения: 1628:0d48:12a3:19d7:1f35:5a61:17a0:765d. Если в IPv6-адресе имеется большое количество нулевых групп (например, fe50:0:0:0:300:f4ff:fe31:57cf), оно может быть пропущено с помощью двойного двоеточия (fe50::300:f4ff:fe31:57cf). Однако такой пропуск допускается в адресе только один раз.

NAT — трансляция сетевого адреса

Как уже отмечалось ранее, чтобы узлы локальной сети смогли «общаться» с узлами Интернета, используется специальная технология *трансляции сетевого адреса* (NAT, Network Address Translation). Маршрутизатор получает от локального узла пакет, адресованный интернет-узлу, и преобразует IP-адрес отправителя, заменяя его своим IP-адресом. При получении ответа от интернет-узла маршрутизатор выполняет обратное преобразование, поэтому нашему локальному узлу «кажется», что он общается непосредственно с интернет-узлом. Если бы маршрутизатор отправил пакет как есть, т. е. без преобразования, то его отверг бы любой маршрутизатор Интернета и пакет так и не был бы доставлен получателю.

Реализация NAT средствами службы маршрутизации Windows Server

Реализовать NAT можно самыми разными способами. Например, обзавестись маршрутизатором Wi-Fi, который и будет выполнять функцию NAT. Это самое простое решение, но оно подойдет только для относительно небольших сетей (конечно, все относительно, и во многом размер обслуживаемой сети зависит от характеристик самого маршрутизатора). Далее мы рассмотрим популярные способы реализации NAT, а именно настройку NAT в Windows Server 2022, в Linux, а также аппаратное решение задачи. Теоретически NAT можно настроить и в клиентских ОС вроде Windows 10/11, но особого смысла мы в этом не видим. Такое решение могут себе позволить лишь очень небольшие фирмы, у которых нет выделенного сервера. А они, как правило, пойдут по пути минимального сопротивления и воспользуются аппаратным решением — маршрутизатором Wi-Fi, — дешево и сердито, а самое главное — проще и надежнее, чем создавать маршрутизатор из рабочей станции на базе Windows.

Итак, для настройки NAT в Windows Server 2022 первым делом нужно установить роль **Удаленный доступ** (рис. 5.1).

При установке этой роли вам будет предложено выбрать службы ролей (рис. 5.2). В нашем случае нужна только **Маршрутизация**, но если вы планируете установить связь между филиалами (складами) или предоставить мобильным пользователям

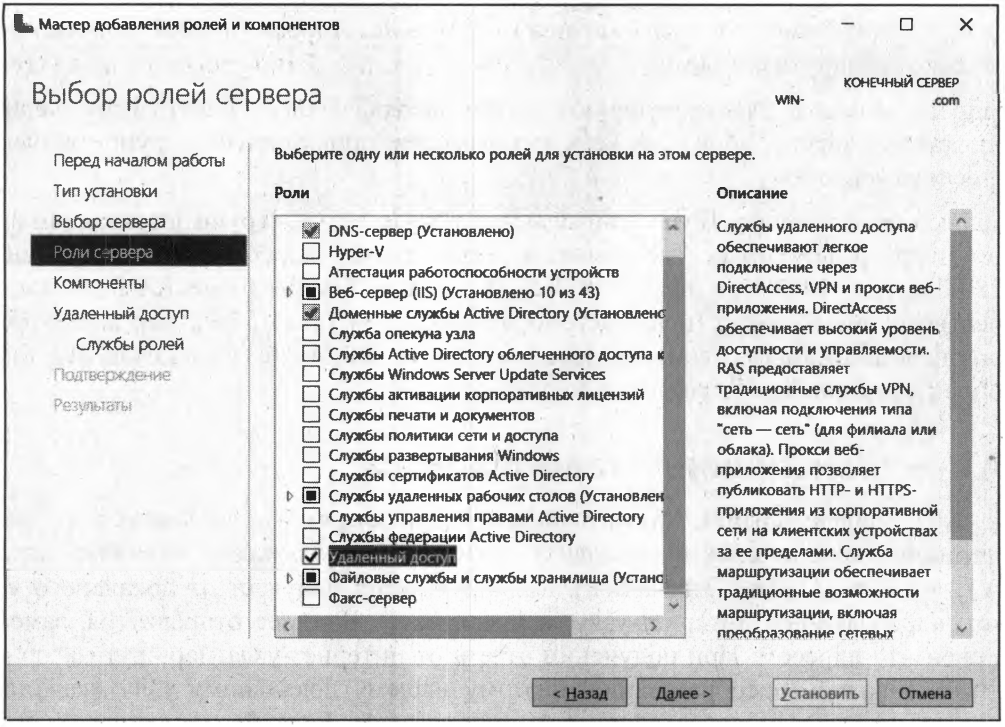


Рис. 5.1. Установка роли **Удаленный доступ** в Windows Server 2022

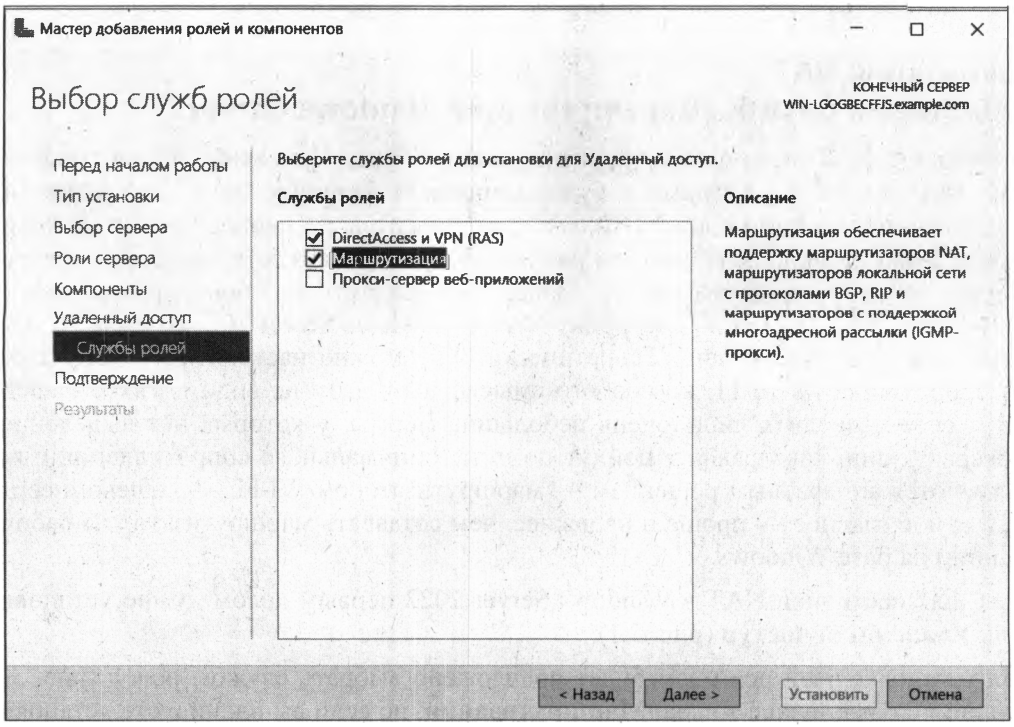


Рис. 5.2. Установка службы ролей

доступ к ресурсам локальной сети, то вам может пригодиться служба роли **DirectAccess и VPN (RAS)**. Служба **Прокси-сервер веб-приложений** нужна, если вы хотите организовать прокси-сервер с целью кеширования веб-трафика.

> ***Примечание***
>
> По сути, установка роли **Удаленный доступ** и службы роли **DirectAccess и VPN (RAS)** превращает ваш сервер в VPN-сервер, предоставляющий доступ к ресурсам корпоративной сети. Подробнее об этом можно прочитать в руководстве: **https://efsol.ru/manuals/vpn-ws2016.html**.

После установки ролей и служб из меню **Средства** оснастки **Диспетчер серверов** выберите команду **Маршрутизация и удаленный доступ** (рис. 5.3), а в открывшемся окне **Маршрутизация и удаленный доступ** — команду **Действие | Настроить и включить маршрутизацию и удаленный доступ**. Затем определитесь с требуемой конфигурацией (рис. 5.4) — в самом простом случае достаточно выбрать **Преобразование сетевых адресов (NAT)**.

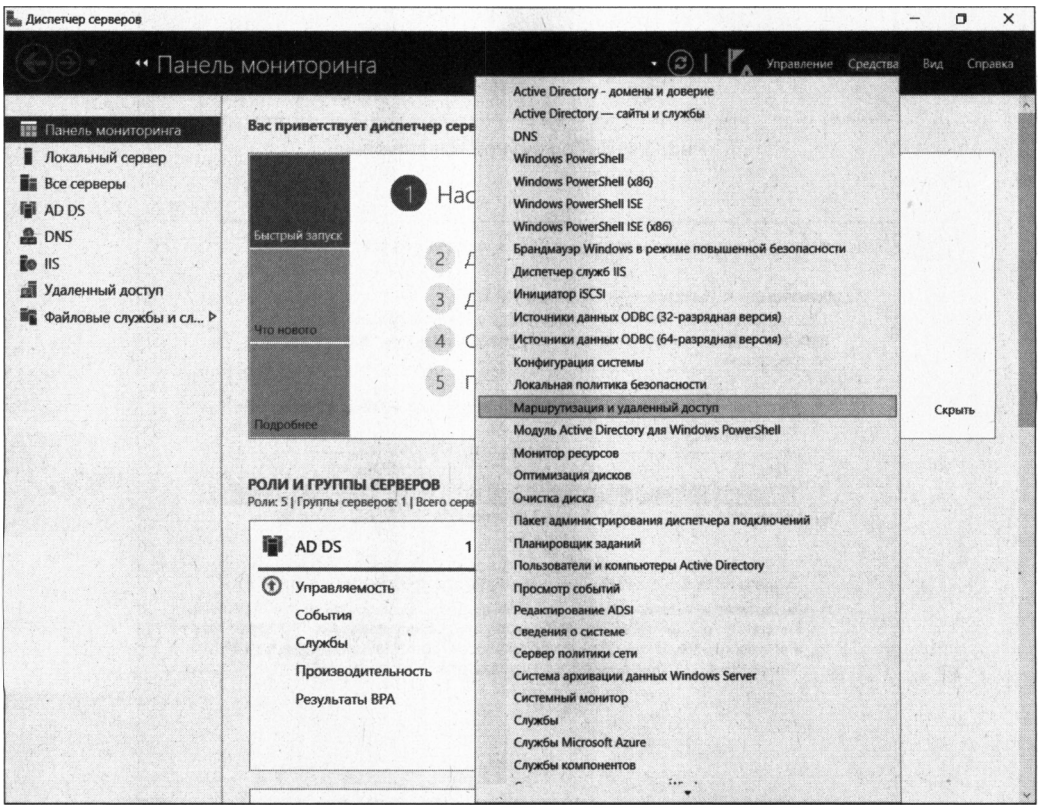


Рис. 5.3. Диспетчер серверов

Далее нужно выбрать интерфейс, который будет использоваться для доступа к Интернету. У вас должно быть как минимум два сетевых интерфейса (рис. 5.5): один будет использоваться для подключения к Сети, а второй — «смотреть» в локальную сеть.

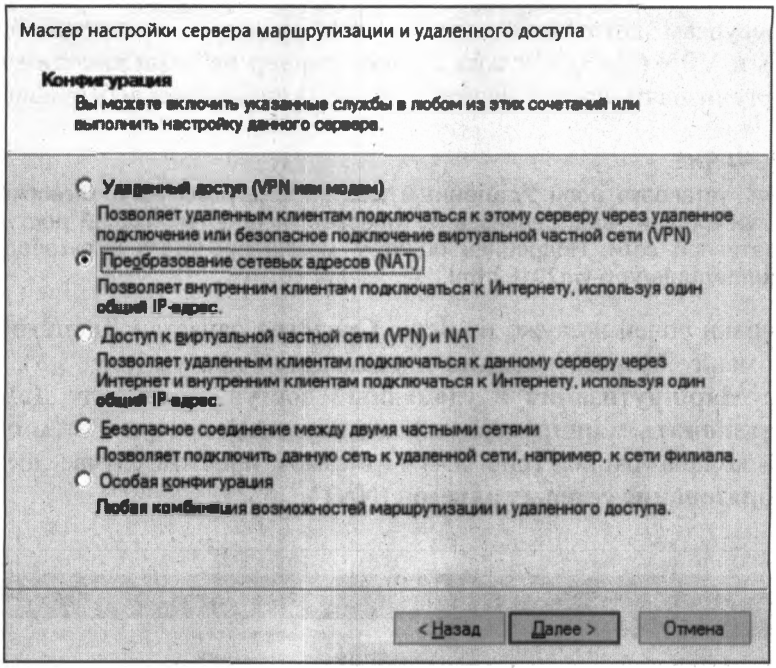


Рис. 5.4. Выбор нужной конфигурации

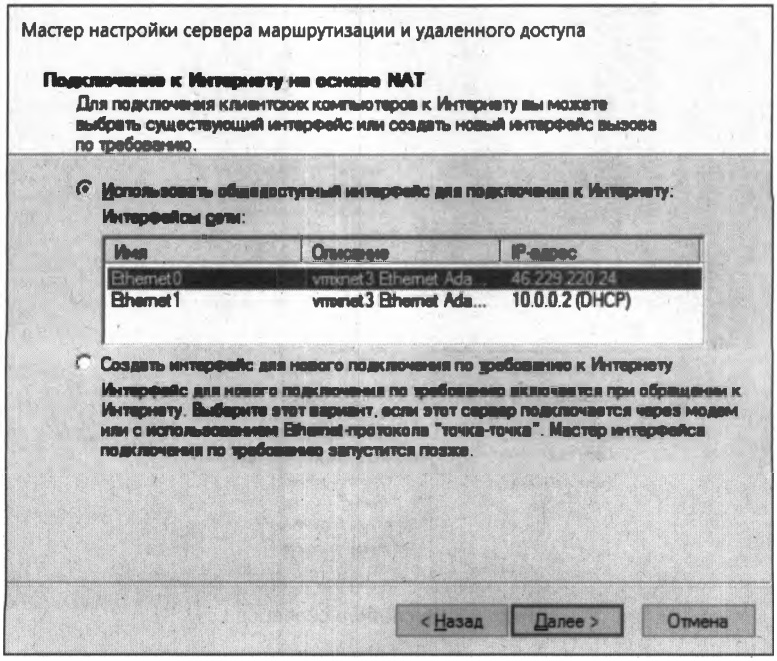


Рис. 5.5. Выбор интерфейса для соединения с Интернетом

Все — осталось лишь нажать кнопку **Готово** в следующем окне (рис. 5.6). Вы думали, что будет сложнее? Конечно, желательно еще настроить DHCP-сервер, чтобы он раздавал всем остальным рабочим станциям сетевые параметры, в которых бы указывался в качестве адреса шлюза по умолчанию адрес сервера Windows Server 2022, на котором вы включили NAT. Также хорошо бы настроить и брандмауэр, чтобы запретить доступ извне к ресурсам локальной сети (или, наоборот, разрешить, например, доступ к веб-серверу компании).

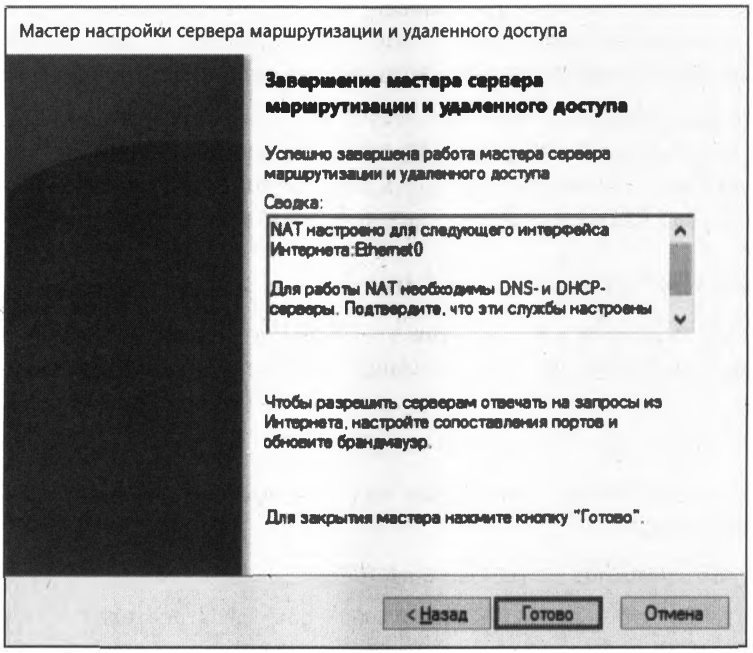


Рис. 5.6. Нажмите кнопку **Готово**

Аппаратный NAT

Как уже отмечалось, этот способ для небольшого предприятия является самым удобным. Вполне приличные маршрутизаторы Wi-Fi можно приобрести за 1500–2000 рублей. Как правило, маршрутизаторы Wi-Fi несут «на борту» и несколько (обычно — четыре) портов Ethernet (LAN), но можно поискать модель и с бóльшим их количеством — например, MikroTik RB2011UiAS-2HnD-IN или MikroTik CRS112-8G-4S-IN (без Wi-Fi). Надо отметить, что в 2023 году сложно найти недорогое (в пределах 5000 рублей) устройство на 8 портов и более. Эти же модели обладают 8 портами, 3 из которых — гигабитные. Позиционируются они как недорогие (порядка 20 тыс. рублей) модели для предприятия. Если же это выходит за рамки вашего бюджета, можно поискать устаревшие модели вроде D-Link DIR-632 или TP-Link TL-R860. Имеются в продаже и так называемые имиджевые модели вроде TP-Link Archer AX6000, но за дизайн нужно платить — цены на них колеблются в диапазоне 25–30 тыс. рублей.

К LAN-портам следует подключать в первую очередь устройства, которым нужно обеспечить стабильное соединение, — например, сервер каталогов (Active Directory),

сетевое хранилище, веб-сервер и т. п., а потом уже думать о подключении к LAN-портам компьютеров, у которых нет адаптеров Wi-Fi. Поскольку стабильность соединений по Wi-Fi иногда оставляет желать лучшего, особенно если рядом много точек доступа ваших соседей, вполне логично подключить по Ethernet серверы, а уже потом (если останутся свободные порты) — рабочие станции. Конечно, если есть такая необходимость, можно приобрести и подключить к маршрутизатору Wi-Fi дополнительный коммутатор.

Рекомендуется также приобретать маршрутизатор с несколькими (тремя-четырьмя) съемными антеннами. Именно съемными — так при необходимости можно весьма недорого «модернизировать» маршрутизатор, заменив антенны на более мощные.

Все имеющиеся маршрутизаторы построены на базе Linux и имеют несложный веб-интерфейс. Настраиваются они тоже достаточно просто — подключить кабель, ведущий к провайдеру, возможно, выбрать тип соединения, указать имя пользователя/пароль (в случае PPPoE[1]) и задать пароль и SSID вашей точки доступа.

Реализация NAT средствами Linux

Настроить NAT можно и в Linux. Для этого нужно первым делом включить IPv4-переадресацию (собственно, эта команда и превращает обычный компьютер в шлюз):

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

Эту команду надо добавить в сценарии загрузки системы, чтобы не вводить ее при каждом перезапуске.

Затем настроить брандмауэр iptables командой:

```
# iptables --table nat --append POSTROUTING --out-interface eth0 -j MASQUERADE
```

> ***Пояснение***
>
> Здесь `eth0` — это интерфейс к провайдеру.

Конечно, кроме этой команды нужно еще создать правила фильтрации пакетов. Не забывайте о них!

Фильтрация трафика

Очень важно не просто предоставить локальным компьютерам доступ к Интернету, но еще и защитить их от злоумышленников, находящихся вовне. Каждая информационная система (ИС) должна быть защищена межсетевым экраном (брандмауэром). При обработке особо важных данных — например, конфиденциальных или относящихся к государственной тайне, межсетевыми экранами должна защищаться каждая система в составе ИС. Другими словами, брандмауэр должен быть установлен не только на шлюзе, но и на каждом компьютере сети.

---

[1] PPPoE (от *англ.* Point-to-point protocol over Ethernet) — сетевой протокол канального уровня передачи кадров PPP через Ethernet. В основном используется *x*DSL-сервисами. Предоставляет дополнительные возможности: аутентификацию, сжатие данных, шифрование.

Демилитаризованная зона

Если вы когда-либо настраивали брандмауэр, особенно по некоторым устаревшим руководствам, то сталкивались с понятием *демилитаризованной зоны* (Demilitarized zone, DMZ). В DMZ следует помещать компьютеры, ресурсы которых могут быть опубликованы в Интернете. Остальные компьютеры, которые не предоставляют пользователям Интернета свои ресурсы, должны находиться за пределами DMZ.

DMZ — это специально организованная подсеть локальной сети, которая отделена как от Интернета, так и от локальной сети (рис. 5.7). Даже если злоумышленник взломает компьютер из DMZ, он не сможет, используя его, обратиться к локальным ресурсам предприятия, что очень важно.

Создать DMZ можно путем использования двух межсетевых экранов (рис. 5.7, *слева*) или одного, но имеющего три сетевых адаптера (рис. 5.7, *справа*). Второй вариант несколько дешевле, но реализовать его сложнее.

Впрочем, сегодня понятие DMZ осталось в прошлом, поскольку считается, что защищать межсетевыми экранами нужно не отдельные сегменты локальной сети, а все серверы и рабочие станции.

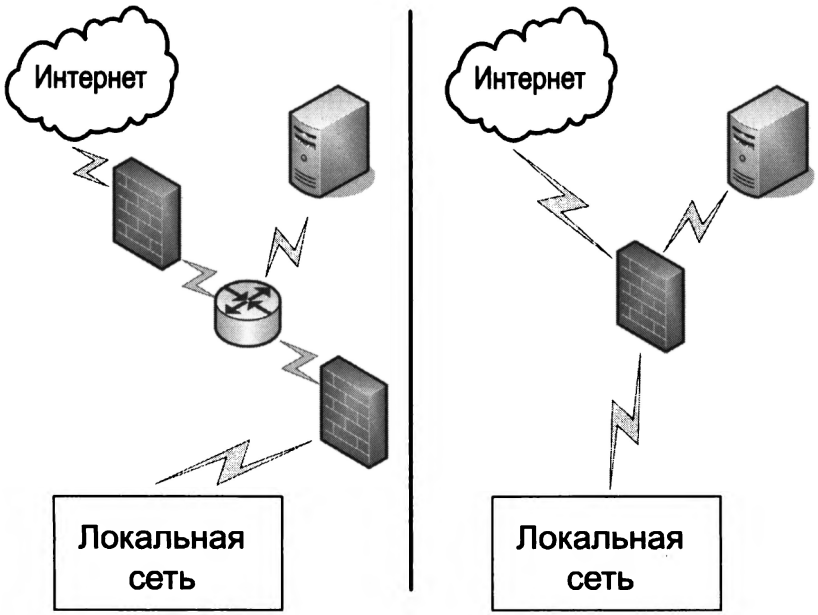


Рис. 5.7. Варианты создания демилитаризованной зоны:
слева — с использованием двух межсетевых экранов;
справа — с использованием одного межсетевого экрана

Межсетевой экран (брандмауэр)

Межсетевой экран (МЭ), или *брандмауэр* (firewall) — это комплекс технических, программных и организационных мер по безопасному подключению одной сети к другой.

Что собой представляет МЭ? Это программа-фильтр пакетов. Межсетевой экран обладает набором правил, который просматривается при прохождении через него различных пакетов. МЭ анализирует каждый проходящий пакет на основании набора правил и решает, что с этим пакетом делать: разрешить, запретить, перенаправить и т. д.

Многое зависит от того, где запущен МЭ: на том самом маршрутизаторе Wi-Fi, на сервере удаленного доступа и, конечно же, на всех остальных компьютерах вашей сети. Но брандмауэры везде разные. На маршрутизаторе Wi-Fi, скорее всего, это будет программа iptables, поскольку такие маршрутизаторы построены на базе Linux. На Windows-системах, если нет особых требований к защите данных, в качестве маршрутизатора может использоваться встроенный брандмауэр Windows.

Выбор межсетевого экрана

В «раньшие» времена хороших межсетевых экранов было относительно немного. Из программ, ставших классикой, можно вспомнить Outpost Firewall и Kerio WinRoute Firewall. Сейчас эти программы канули в Лету, а на их место пришли интегрированные продукты (Internet Security или Security Suite), сочетающие в себе функции как брандмауэра, так и антивируса. Примеров можно привести множество: тот же Kaspersky Internet Security, Avast Premium Security, ESET NOD32 Smart Security, Comodo Internet Security, Outpost Security Suite и Symantec Endpoint Protection. И это далеко не все программные продукты, содержащие в себе функции межсетевого экрана, а только лишь те, которые мы вспомнили, не прибегая к помощи всезнающего Google.

Все эти решения предоставляют примерно одинаковую функциональность (кроме разве что Symantec Endpoint Protection — его развертывание лучше применять только в крупных предприятиях), поэтому вы можете выбрать подходящий вам продукт, основываясь на тестах независимых экспертов и, конечно же, на их стоимости.

Если ваше предприятие не обрабатывает конфиденциальные (персональные) данные, можно остановить выбор на любом лицензионном программном продукте. При желании сэкономить можно выбрать также и бесплатный программный продукт наподобие Comodo Internet Security или вообще установить в качестве антивируса бесплатные Avast или Avira (решения уровня Internet Security у них, как правило, коммерческие) и использовать встроенный брандмауэр Windows, который тоже неплох. Тратиться есть смысл только на решения для защиты сервера.

Но совсем другое дело, если ваше предприятие обрабатывает конфиденциальные (персональные) данные. В этом случае следует ориентироваться только на сертифицированное ФСТЭК программное обеспечение. Вопросам сертификации можно посвятить отдельную книгу, поэтому есть два способа решения вопроса сертификации: или обратиться к специалистам, или перелопатить несколько нормативных актов и самостоятельно определить, какое программное обеспечение вам необходимо.

Вкратце поясним, что в зависимости от типа обрабатываемых данных и от их количества вам нужно будет определить требуемый уровень защищенности этих дан-

ных и наметить программное обеспечение соответствующего класса. Так, в самом простом случае вам потребуется межсетевой экран 5-го класса.

Пояснение

Защищенность нарастает по уровням по нисходящей — так, 4-й класс обеспечивает лучшую защищенность, чем 5-й, 3-й — лучшую, чем 4-й, и т. д.

Определив класс требуемого ПО, нужно посетить реестр ФСТЭК (находится на сайте **http://fstec.ru/**) и найти в нем ПО, которое вы планировали установить. Если это ПО присутствует в реестре и его класс соответствует вашему уровню защищенности, ПО можно устанавливать. Если нет, тогда придется искать другой программный продукт. Другими словами, даже если вам нравится какой-то продукт, но он не сертифицирован или его сертификат не соответствует необходимому уровню защищенности, устанавливать такой продукт нельзя.

Обращайте также внимание на то, как именно сертифицирован тот или иной продукт. Например, некоторые продукты «Лаборатории Касперского» сертифицированы как средство антивирусной защиты, а не как средство межсетевого экранирования, хотя межсетевой экран и входит в состав продукта.

Что выбрать? Как уже отмечалось, для самого простого случая подойдет межсетевой экран 5-го или 4-го уровня — например, Security Studio Endpoint Protection Personal Firewall.

Нужен ли прокси-сервер?

Понятно, что межсетевой экран просто необходим в качестве средства защиты сети от вторжений извне. Но нужен ли прокси-сервер? Это зависит от ряда обстоятельств. Если у вас есть лишний компьютер, который можно выделить под прокси-сервер, и размер сети довольно большой (скажем, от 50 компьютеров), или же сеть поменьше, но пользователи работают с одними и теми же интернет-ресурсами, тогда прокси нужен. С его помощью вы сможете обеспечить кеширование получаемой из Интернета информации (а это не только HTML-код, но еще и картинки, сценарии, файлы стилей и т. п.), что повысит скорость открытия страниц, сэкономит трафик и нагрузку на сеть. Прокси-сервер может также запретить доступ к определенным узлам Интернета, но с этой функцией с легкостью справится и межсетевой экран, поэтому основная функция прокси-сервера — все же кеширование информации.

Системы обнаружения вторжений

Межсетевой экран сам по себе является весьма простым решением — он сопоставляет проходящий через него пакет списку правил и выполняет заданные правилами действия над этим пакетом. Например, вы запретили отправку пакетов на IP-адрес 111.111.111.079. Если через межсетевой экран попытается пройти исходящий пакет с таким IP-адресом в качестве получателя, пакет будет блокирован. Брандмауэр ничего больше не делает с пакетом: или разрешает, или запрещает его (есть и другие действия, но в основном все сводится к этим двум). Остальные пакеты, которые не

соответствуют ни одному из правил, либо по умолчанию пропускаются, либо блокируются (все зависит от настроек брандмауэра).

Но вредоносные программы могут «замаскироваться» и отправлять пакеты, которые с точки зрения брандмауэра выглядят полностью нормальными. Брандмауэр, скорее всего, пропустит такие пакеты, что может повлечь за собой многомиллионные убытки. Для обнаружения таких «вторжений» используются *системы обнаружения вторжений* (СОВ), в англоязычной литературе называемые Intrusion Detection Systems (IDS).

Существуют и *системы предотвращения вторжений* (СПВ) — Intrusion Prevention Systems (IPS) — выполняющие активную функцию. Они не только обнаруживают вторжение, но и блокируют подозрительный трафик. СПВ могут обнаружить подготовку DoS-атаки (атаки на отказ), выявить сетевые черви, активность эксплойтов и т. п.

Принцип действия СПВ основывается на сравнении передаваемой по сети информации с заранее подготовленной базой данных сигнатур, которые присутствуют во вредоносных программах. Способны СПВ обнаруживать и аномальные изменения трафика — например, резкое увеличение пакетов определенного типа, и сохранять пропускную способность канала для полезных данных.

Понятно, что база данных сигнатур вредоносных программ растет с каждым днем, и защита всего сетевого трафика без снижения производительности просто невозможна. Производители этого не скрывают, и та же Cisco в своих аппаратных решениях заявляет, что включение функции Cisco Intrusion Detection Systems на коммутаторах Cisco приведет к снижению производительности.

Программных решений IDS/IPS также достаточно много. Как и в случае с брандмауэрами, многие поставщики предоставляют IDS/IPS в качестве одного комплекса, содержащего также антивирус и брандмауэр. В качестве примера можно привести Security Studio Endpoint Protection — кроме того, что в состав этого комплекта входят брандмауэр, СОВ и антивирус, продукт является сертифицированным, что позволяет использовать его при обработке конфиденциальной информации.

Варианты межсетевых экранов

Как уже отмечалось, межсетевые экраны бывают как аппаратными, так и программными. Разница между ними весьма условна. Ведь так называемое *аппаратное решение* представляет собой компьютер с ограниченной функциональностью, на котором запущена та же самая программа-фильтр. Как правило, такие компьютеры работают или под управлением Linux (бюджетные решения), или под управлением ОС проприетарной разработки (например, Cisco IOS).

Программное решение

Программное решение — это установка программы-фильтрации на персональный компьютер. Какая именно программа будет заниматься фильтрацией трафика, зависит от операционной системы. Как уже отмечалось, в Linux — это iptables, а для

Windows существует множество программ (в том числе и встроенный брандмауэр Windows).

Аппаратные решения

Самое дешевое аппаратное решение — это маршрутизатор Wi-Fi, в состав ПО которого уже, как правило, входит программа-брандмауэр. Даже самые дешевые модели поддерживают статическую фильтрацию пакетов, обеспечивают наличие DMZ-портов, возможность создания VPN-подключений, NAT-трансляцию с сервером DHCP, средства предупреждения администратора (отправка ему e-mail и т. п.).

Однако не все так просто, если вы обрабатываете конфиденциальную информацию. В этом случае нужно выбирать сертифицированное аппаратное решение, а таковых не так уж и много. Сейчас можно выбрать его из числа следующих устройств: ViPNet Coordinator HW, «АПКШ Континент», ALTELL NEO, а также из бесчисленных вариантов от Cisco, в том числе:

- Cisco PIX-501 (кл. 3, кл. 4);
- Cisco PIX-506 (кл. 3, кл. 4);
- Cisco PIX-515E (кл. 3, кл. 4);
- Cisco PIX-520 (кл. 3, кл. 4);
- Cisco PIX-525 (кл. 3, кл. 4);
- Cisco PIX-535 (кл. 3, кл. 4) ;
- Cisco FWSM (кл. 3, кл. 4);
- Cisco WS-SVC-FWM-1 (кл. 4).

Полный список сертифицированного ФСТЭК оборудования от Cisco можно найти по адресу: **https://www.slideshare.net/CiscoRu/cisco-90483415**. Список не самый актуальный (октябрь 2017 года), но более точную информацию вы всегда сможете получить у партнеров Cisco.

Настройка параметров межсетевого экрана при помощи групповой политики

В последних версиях Windows брандмауэр по умолчанию включен. Однако его параметры, установленные по умолчанию, удобны не для всех: защита активна, но задействованы исключения, обеспечивающие работу компьютера в локальной сети. В сетях с развернутыми системами управления брандмауэр будет блокировать доступ таких программ. Не будет обеспечиваться и должный уровень защиты в публичных сетях. Именно поэтому брандмауэры Windows нуждаются в централизованной настройке с помощью групповых политик.

Параметры настройки групповой политики брандмауэра Windows можно найти по следующему пути: **Конфигурация компьютера | Административные шаблоны | Сеть | Сетевые подключения | Брандмауэр Защитника Windows** (рис. 5.8).

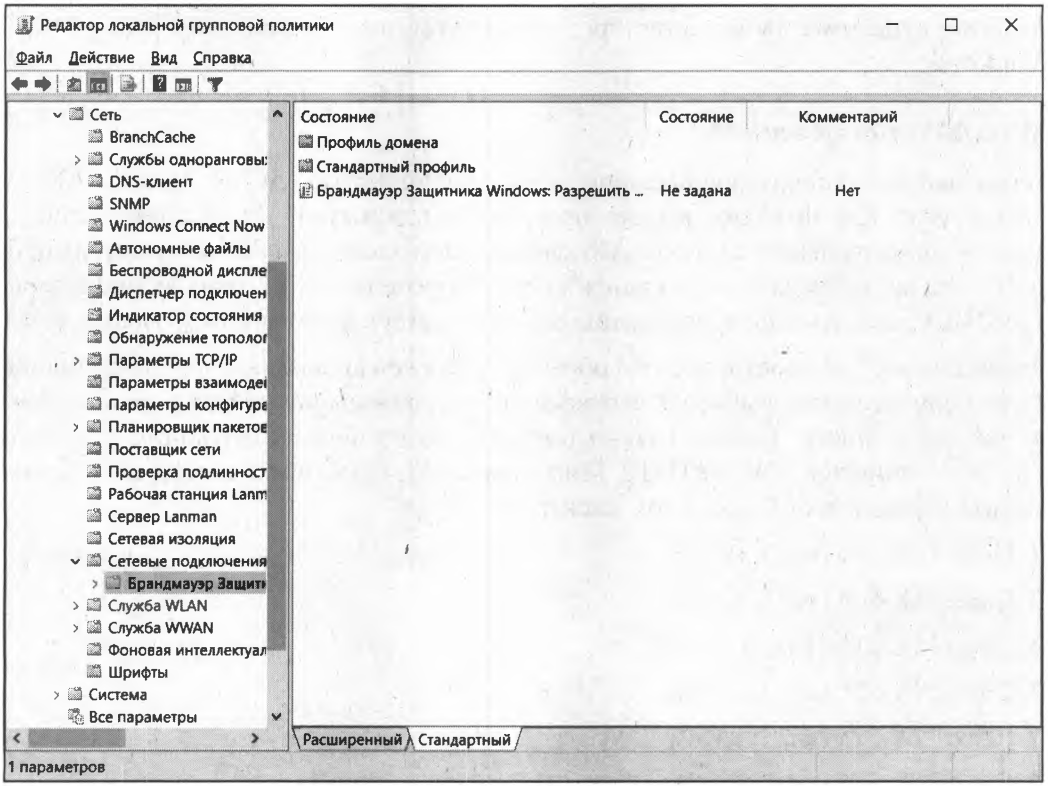


Рис. 5.8. Настройка параметров брандмауэра Windows при помощи групповых политик

В политике **Брандмауэр Защитника Windows** вы найдете контейнеры **Профиль домена** и **Стандартный профиль**. Первый используется при работе компьютера в домене, а второй — когда компьютер подключен к сети, где нет домена Windows.

Если на предприятии внедрена система удаленного мониторинга, то нужно открыть для этой программы все порты и включить опцию **Разрешать исключения для удаленного управления** — что даст возможность управления через удаленную консоль.

Для стандартного профиля нужно запретить использование всех исключений брандмауэра, потому что такой вариант является самым безопасным для публичной сети, а мы организуем сеть предприятия.

Рекомендуемые настройки параметров групповой политики для брандмауэра Windows приведены в табл. 5.3.

Таблица 5.3. *Рекомендуемые параметры настройки брандмауэра Windows*

Параметр	Профиль домена	Стандартный профиль
Защитить все сетевые подключения	Включен	Включен
Не разрешать исключения	Не задан	Включен, и настроены исключения для используемых программ

Таблица 5.3 (окончание)

Параметр	Профиль домена	Стандартный профиль
Задать исключения для программ	Включен, и настроены исключения для используемых программ	Включен, и настроены исключения для используемых программ
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

Межсетевой экран Linux

В состав практически всех современных дистрибутивов Linux входит весьма мощный брандмауэр (межсетевой экран) — iptables. Как правило, в случае с Linux никто не прибегает к установке сторонних продуктов фильтрации пакетов, а все так называемые брандмауэры для Linux (вроде Firestarter) являются лишь оболочками для того же iptables.

Настройки запуска

Обычно при установке Linux задается вопрос, хотите ли вы активировать сетевой экран по умолчанию или нет. Предположим, что администратор, производивший установку Linux, ответил на этот вопрос утвердительно.

Запустить iptables можно командой:

```
service iptables start
```

А остановить командой:

```
service iptables stop
```

Для перезапуска iptables служит параметр `restart`. Настроить автоматический запуск iptables в Red Hat-совместимых системах можно с помощью команды `chkconfig`:

```
/sbin/chkconfig --level 345 iptables on
```

Более точная команда настройки автоматического запуска iptables зависит от используемой системы инициализации. Вполне вероятно, что в вашем дистрибутиве используется другая система инициализации и команда будет иной.

Цепочки и правила

Основная задача брандмауэра — это фильтрация пакетов, которые проходят через сетевой интерфейс. При поступлении пакета брандмауэр анализирует его и затем принимает решение: принять пакет (`ACCEPT`) или избавиться от него (`DROP`). Брандмауэр может выполнять и более сложные действия, но часто ограничивается именно этими двумя.

Прежде чем брандмауэр примет решение относительно пакета, пакет должен пройти по цепочке правил. Каждое правило состоит из условия и действия (цели). Если пакет соответствует условию правила, то выполняется указанное в правиле действие. Если пакет не соответствует условию правила, он передается следующему правилу. Если же пакет не соответствует ни одному из правил цепочки, выполняется действие по умолчанию.

Вроде бы все понятно, но, чтобы лучше закрепить знания, рассмотрим пример, приведенный в табл. 5.4 и демонстрирующий принцип работы цепочки правил.

***Таблица 5.4.** Цепочка правил*

Номер правила	Условие	Действие (цель)
1	Пакет от 192.168.1.0	ACCEPT
2	Пакет от 192.168.0.0	DROP
3	Пакет для 192.168.2.0	ACCEPT
DEFAULT	*	DROP

Предположим, что пакет пришел из сети 192.168.4.0 для узла нашей сети 192.168.1.7. Пакет не соответствует первому правилу (отправитель не из сети 192.168.1.0), поэтому он передается правилу 2. Пакет не соответствует и этому правилу. Пакет адресован компьютеру 192.168.1.7, а не компьютеру из сети 192.168.2.0, поэтому он не соответствует третьему правилу. Брандмауэру остается применить правило по умолчанию — пакет будет отброшен (действие `DROP`).

Цепочки правил собираются в три основные таблицы:

- filter — таблица фильтрации, основная таблица;
- nat — таблица NAT, используется пакетом при создании нового соединения;

- mangle — используется, когда нужно произвести специальные действия над пакетом.

> ***Примечание***
>
> Ранее брандмауэр в Linux поддерживал только цепочки правил и назывался ipchains, сейчас брандмауэр поддерживает и цепочки правил, и таблицы цепочек и называется iptables. Это примечание сделано, чтобы вы понимали разницу между старым брандмауэром ipchains (ядра 2.2 и ниже) и новым — iptables (ядра 2.4 и выше).

Если необходимо, вы можете создать собственные таблицы. В состав таблицы входят три цепочки:

- `INPUT` — для входящих пакетов;
- `OUTPUT` — для исходящих пакетов;
- `FORWARD` — для пересылаемых (транзитных) пакетов.

Над пакетом можно выполнить следующие действия:

- `<имя цепочки>` — пакет будет отправлен для обработки в цепочку с указанным именем;
- `ACCEPT` — пакет будет принят;
- `DROP` — пакет будет отброшен. После этого пакет удаляется и больше над ним не выполняется каких-либо действий;
- `MASQUERADE` — IP-адрес пакета будет скрыт.

Это не все действия, но пока нам больше знать и не нужно. На рис. 5.9 представлена схема обработки пакета. Входящий пакет (на схеме **ПАКЕТ IN**) поступает в цепочку **PREROUTING** таблицы **mangle**. После чего (если он не был отброшен правилами таблицы **mangle**) пакет обрабатывается правилами цепочки **PREROUTING**, но таблицы **nat**. На этом этапе проверяется, нужно ли модифицировать назначение пакета (этот вид NAT называется Destination NAT, DNAT).

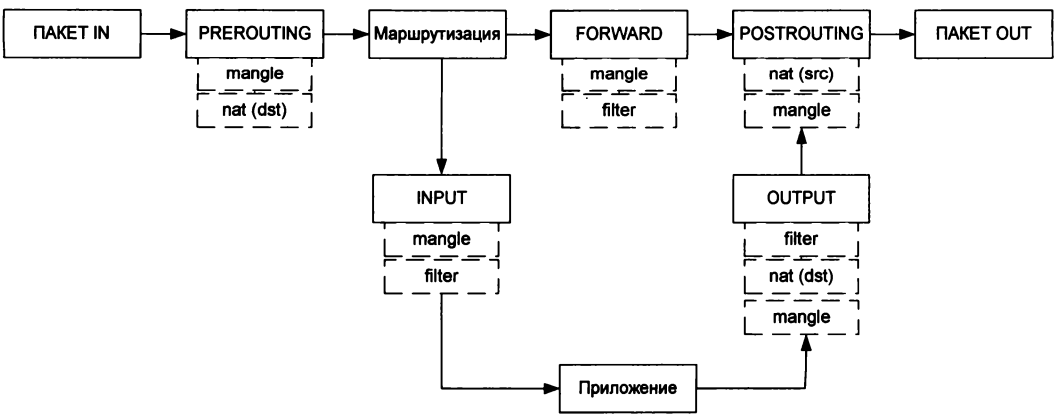


Рис. 5.9. Схема обработки пакета

Затем пакет может быть направлен либо в цепочку **INPUT** (если получателем пакета является этот компьютер), либо в цепочку **FORWARD** (если пакет нужно передать другому компьютеру).

Если получатель компьютера — сам шлюз (на нем может быть запущен, например, почтовый или веб-сервер), то пакет сначала обрабатывается правилами цепочки **INPUT** таблиц **mangle** и **filter**. Если пакет не был отброшен, он передается приложению (например, почтовому серверу). Приложение получило пакет, обработало его и отправляет ответный пакет. Этот пакет обрабатывается цепочкой **OUTPUT** таблиц **mangle**, **nat** и **filter**. Далее пакет отправляется на цепочку **POSTROUTING** и обрабатывается правилами таблиц **mangle** и **nat**.

Если пакет нужно передать другому компьютеру, то он обрабатывается правилами цепочки **FORWARD** таблиц **mangle** и **filter**, а после этого к нему применяются правила цепочки **POSTROUTING**. На этом этапе используется подмена источника пакета (этот вид NAT называется Source NAT, SNAT).

После всех правил пакет «выжил»? Тогда он становится исходящим пакетом (на схеме **ПАКЕТ OUT**) и отправляется в сеть.

Задание правил брандмауэра

Теперь, когда мы разобрались с правилами и цепочками, самое время научиться использовать брандмауэр iptables. Для себя сразу определитесь, что вы настраиваете. Можно настраивать просто брандмауэр, защищающий локальный компьютер от всевозможных атак. А можно настраивать шлюз сети, предоставляющий всем остальным компьютерам сети доступ к Интернету. В последнем случае нужно включить IP-переадресацию (IPv4-forwarding). О том, как это сделать, было сказано ранее. В большинстве случаев хватит вот такой команды:

```
sudo sysctl -w net.ipv4.ip_forward=«1»
sudo echo 1 > /proc/sys/net/ipv4/ip_forward
```

Для изменения правил брандмауэра нужны полномочия root, поэтому все команды iptables следует вводить или через команду `sudo` (для этого ваш пользователь должен иметь право использовать `sudo`), или с предварительно полученными полномочиями root (команда `su`).

Для добавления правила в цепочку служит команда:

```
sudo iptables -A цепочка правило
```

Например:

```
sudo iptables -A INPUT правило
```

Такая команда добавит правило в цепочку **INPUT** таблицы **filter** — это таблица по умолчанию (см. рис. 5.9). Если вы желаете добавить правило в другую таблицу, нужно указать ее в параметре `-t`:

```
sudo iptables -t таблица -A цепочка правило
```

Например:

```
sudo iptables -t nat -A INPUT правило
```

Действие по умолчанию задается ключом `-P`:

```
sudo iptables -P INPUT DROP
```

Обычно устанавливаются вот такие действия по умолчанию:

```
sudo iptables -P INPUT DROP
sudo iptables -P FORWARD ACCEPT
sudo iptables -P OUTPUT DROP
```

Обратимся к данным табл. 5.4, но предварительно рассмотрим фазы установки TCP-соединения. Соединение устанавливается в три этапа (фазы). Сначала первый компьютер отправляет второму компьютеру SYN-пакет, запрашивая открытие соединения. Второй компьютер отправляет ему подтверждение SYN-пакета — ACK-пакет. После этого соединение считается установленным (ESTABLISHED). Открытое, но не установленное соединение (когда компьютеры обмениваются пакетами SYN-ACK), называется новым (NEW). Уточнения, приведенные здесь в скобках, помогут разобраться с материалом табл. 5.5, где при описании параметров указываются не полные команды iptables, а только их фрагменты, имеющие отношения к тому или иному параметру.

Таблица 5.5. *Параметры фильтрации пакетов*

Параметр	Описание
`--source`	Позволяет указать источник пакета. Можно указывать как доменное имя компьютера (например, `den.dkws.org.ua`), так и его IP-адрес (`192.156.1.1`) и даже набор адресов (`192.168.1.0/255.255.255.0`). Пример: `iptables -A FORWARD --source 192.168.1.11 ...`
`--destination`	Задает назначение (адрес получателя) пакета. Синтаксис такой же, как и у `--source`

`--protocol`(или `-p`)	Задает протокол. Чаще всего работают с tcp, icmp или udp, но можно указать любой протокол, определенный в файле */etc/protocols*. Также можно указать `all`, что означает все протоколы.
	Примеры:
	`iptables -A FORWARD --protocol tcp ...`
	`iptables -A FORWARD -p tcp ...`

`--source-port` (или `--sport`)	Определяет порт отправителя. Эта опция может использоваться только вместе с параметром `-p`. Например: `iptables -A FORWARD -p tcp -source-port 23 ...`
`--destination-port`(или `--dport`)	Задает порт назначения. Опция возможна только с параметром `-p`. Синтаксис такой же, как и в случае с `-source-port`

Таблица 5.5 (окончание)

Параметр	Описание
-state	Позволяет отфильтровать пакеты по состоянию. Параметр -state доступен только при загрузке модуля state с помощью другого параметра: -m state. Состояния пакета: • NEW — новое соединение (еще неустановленное); • ESTABLISHED — установленное соединение; • RELATED — пакеты, которые не принадлежат соединению, но связаны с ним; • INVALID — неопознанные пакеты. Пример: iptables -A FORWARD -m state -state RELATED,INVALID
-in-interface(или -i)	Определяет интерфейс, по которому прибыл пакет. Пример: iptables -A FORWARD -i eth1
-out-interface(или -o)	Определяет интерфейс, по которому будет отправлен пакет: iptables -A FORWARD -o ppp0
-tcp-flags	Производит фильтрацию по TCP-флагам (см.: man iptables)

Ранее мы познакомились с основными действиями iptables. В табл. 5.6 представлены все действия iptables (цели iptables). Действие задается параметром -j.

Таблица 5.6. Цели iptables

Действие	Описание
ACCEPT	Принять пакет. При этом пакет уходит из этой цепочки и передается дальше
DROP	Уничтожить пакет
REJECT	Уничтожает пакет и сообщает об этом отправителю с помощью ICMP-сообщения. Параметр -reject-with позволяет уточнить тип ICMP-сообщения: • icmp-host-unreachable — узел недоступен; • icmp-net-unreachable — сеть недоступна; • icmp-port-unreachable — порт недоступен; • icmp-proto-unreachable — протокол недоступен. По умолчанию отправляет сообщение о недоступности порта. Но, используя сообщение icmp-host-unreachable, можно сбить злоумышленника с толку. Предположим, что вы просто решили отбрасывать неугодные вам пакеты (действие DROP). Но злоумышленник будет посылать и посылать вам эти пакеты, чтобы брандмауэр только бы и делал, что занимался фильтрацией и удалением этих пакетов (один из видов атаки на отказ). А если вы ответите сообщением icmp-host-unreachable, то злоумышленник будет думать, что узел недоступен, т. е. компьютер выключен, либо он уже достиг своей цели —

Таблица 5.6 (окончание)

Действие	Описание
	добился отказа компьютера. С другой стороны, помните, что это действие порождает ответный ICMP-пакет, нагружающий исходящий канал, который в некоторых случаях (например, одностороннее спутниковое соединение) очень «узкий». Если злоумышленник пришлет вам 1 миллион пакетов, то вы должны будете отправить 1 миллион сообщений в ответ. Подумайте, готовы ли вы к такой нагрузке на исходящий канал
LOG	Заносит информацию о пакете в протокол. Полезно использовать для протоколирования возможных атак — если вы подозреваете, что ваш узел кем-то атакуется. Также полезно при отладке настроек брандмауэра
RETURN	Возвращает пакет в цепочку, откуда он прибыл. Действие возможно, но лучше его не использовать, т. к. легко ошибиться и создать непрерывный цикл: вы отправляете пакет обратно, а он опять следует на правило, содержащее цель RETURN
SNAT	Выполняет подмену IP-адреса отправителя (Source NAT). Используется в цепочках **POSTROUTING** и **OUTPUT** таблицы **nat** (см. рис. 5.10)
DNAT	Выполняет подмену адреса получателя (Destination NAT). Используется только в цепочке **POSTROUTING** таблицы **nat**
MASQUERADE	Похож на SNAT, но «забывает» про все активные соединения при потере интерфейса. Используется при работе с динамическими IP-адресами, когда происходит потеря интерфейса при изменении IP-адреса. Применяется в цепочке **POSTROUTING** таблицы **nat**

Пример настройки брандмауэра

Создать шлюз в Linux очень просто, и сейчас вы сами в этом убедитесь. Гораздо сложнее правильно его настроить — чтобы шлюз не только выполнял свою непосредственную функцию (т. е. передачу пакетов из локальной сети в Интернет и обратно), но и защищал сеть.

В последнее время очень популярны DSL-соединения, поэтому будем считать, что для подключения к Интернету используется именно оно. Хотя вся разница только в названии интерфейса — ppp0. Вполне может быть, что у вас иная конфигурация. Например, у вас могут быть два сетевых интерфейса: eth0 и eth1. Первый «смотрит» в локальную сеть, а второй — подключен к Интернету. Тогда и правила вы будете формировать исходя из того, что соединение с Интернетом происходит по интерфейсу eth1.

При DSL-соединении у нас тоже будет два сетевых адаптера: первый (eth0) соединен с локальной сетью, а ко второму (eth1) подключен DSL-модем. Перед настройкой шлюза проверьте, действительно ли это так. Вполне может оказаться, что сетевая плата, к которой подключен DSL-модем, — это интерфейс eth0, а не eth1. Тогда вам придется или изменить названия интерфейсов при формировании правил, или просто подключить модем к другому сетевому адаптеру.

IP-адрес DSL-соединения будет динамическим (обычно так оно и есть), а вот IP-адрес сетевого адаптера, обращенного к локальной сети, назначим такой:

192.168.1.1. Вы можете использовать и другой адрес (адрес должен быть локальным, если только у вас нет подсети с реальными IP-адресами).

Итак, мы настроили локальную сеть, узнали имена сетевых адаптеров, включили IP-переадресацию. Осталось только ввести команду:

```
sudo iptables -t nat -A POSTROUTING -o ppp0 -j MASQUERADE
```

Установите на всех компьютерах вашей сети IP-адрес 192.168.1.1 в качестве шлюза по умолчанию (можно настроить DHCP-сервер, чтобы не настраивать все компьютеры вручную) и попробуйте пропинговать с любого узла какой-нибудь сайт.

Оказывается, вы прочитали весь предшествующий материал этой главы ради одной строчки. Так и есть. Но, сами понимаете, на этом настройка шлюза не заканчивается. Надо еще защитить вашу сеть. Как минимум требуется установить следующие действия по умолчанию:

```
sudo iptables -P INPUT DROP
sudo iptables -P FORWARD ACCEPT
sudo iptables -P OUTPUT DROP
```

Разрешим входящие соединения на шлюз только от узлов нашей внутренней сети 192.168.1.0:

```
sudo iptables -A INPUT -i eth0 --source 192.168.1.0/24 --match state --state
NEW,ESTABLISHED -j ACCEPT
```

Надо также установить правило для цепочки `OUTPUT` — оно разрешает шлюзу отвечать компьютерам нашей локальной сети:

```
sudo iptables -A OUTPUT -o eth0 --destination 192.168.1.0/24 --match state
--state NEW,ESTABLISHED -j ACCEPT
```

Будьте внимательны при указании имен интерфейсов и IP-адресов. Очень легко запутаться, а потом полчаса разбираться, почему шлюз не работает.

Нам осталось только запретить соединения из Интернета (компьютеры нашей сети смогут устанавливать соединения с серверами Интернета, зато внешние интернет-пользователи не смогут установить соединения с компьютерами нашей сети):

```
sudo iptables -A FORWARD -i eth0 --destination 192.168.1.0/24 --match state
--state ESTABLISHED -j ACCEPT
```

У нас получилась вполне приличная конфигурация: компьютеры нашей сети могут выступать инициаторами соединения, а интернет-узлы могут передавать данные в нашу сеть только в том случае, если инициатором соединения выступил локальный компьютер.

Но и это еще не все. Как вы уже догадались, поскольку мы не сохранили правила брандмауэра, при перезагрузке компьютера его придется настраивать заново. Нам нет резона описывать настройку брандмауэра (сохранение и восстановление правил) в каждом дистрибутиве (пусть это будет вашим домашним заданием), так что рассмотрим универсальный способ. Он заключается в создании bash-сценария, вызывающего необходимые нам команды настройки iptables. Такой сценарий вам

останется только вызывать при загрузке системы. А для этого придется изучить строение системы инициализации в вашем дистрибутиве.

Вместо того чтобы объяснять вам, как вызвать сценарий, загружающий правила брандмауэра (с этим вы и сами разберетесь), мы лучше приведем здесь сценарий (понятно, с комментариями), реализующий более сложную конфигурацию iptables. Этот сценарий (листинг 5.1) будет не только выполнять все функции шлюза, но и защищать сеть от разного рода атак. Сценарий лучше сразу поместить в каталог /etc/init.d (это наша вам подсказка) и сделать исполняемым:

```
# touch /etc/init.d/firewall_start
# chmod +x /etc/init.d/firewall_start
```

Листинг 5.1. Сценарий firewall_start

```
# Путь к iptables
IPT="/sbin/iptables"

# Сетевой интерфейс, подключенный к Интернету
INET="ppp0"

# Номера непривилегированных портов
UPORTS="1024:65535"

# Включаем IPv4-forwarding (чтобы не думать, почему шлюз не работает)
echo 1 > /proc/sys/net/ipv4/ip_forward

# Удаляем все цепочки и правила
$IPT -F
$IPT -X

# Действия по умолчанию.
$IPT -P INPUT DROP
$IPT -P FORWARD ACCEPT
$IPT -P OUTPUT DROP

# Разрешаем все пакеты по интерфейсу lo (обратная петля)
$IPT -A INPUT -i lo -j ACCEPT
$IPT -A OUTPUT -o lo -j ACCEPT

# Запрещаем любые новые соединения с любых интерфейсов, кроме lo,
# с нашим компьютером
$IPT -A INPUT -m state ! -i lo --state NEW -j DROP
$IPT -A INPUT -s 127.0.0.1/255.0.0.0 ! -i lo -j DROP

# Отбрасываем все пакеты со статусом INVALID
$IPT -A INPUT -m state --state INVALID -j DROP
$IPT -A FORWARD -m state --state INVALID -j DROP
```

```
# Принимаем все пакеты из уже установленного соединения
# Состояние ESTABLISHED
$IPT -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
$IPT -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT

# Наш провайдер использует IP-адреса из сети 10.0.0.0 для
# доступа к своим локальным ресурсам. Ничего не поделаешь,
# нужно разрешить эти адреса, иначе мы даже не сможем войти
# в билинговую систему. В вашем случае, может, и не нужно будет
# добавлять следующее правило, а может, у вас будет такая же
# ситуация, но адрес подсети будет другим
$IPT -t nat -I PREROUTING -i $INET -s 10.0.0.1/32 -j ACCEPT

# Защищаемся от SYN-наводнения (довольно популярный вид атаки)
$IPT -A INPUT -p tcp ! --syn -m state --state NEW -j DROP
$IPT -A OUTPUT -p tcp ! --syn -m state --state NEW -j DROP

# Защищаемся от UDP-наводнения
$IPT -A INPUT -p UDP -s 0/0 --dport 138 -j DROP
$IPT -A INPUT -p UDP -s 0/0 --dport 113 -j REJECT
$IPT -A INPUT -p UDP -s 0/0 --sport 67 --dport 68 -j ACCEPT
$IPT -A INPUT -p UDP -j RETURN
$IPT -A OUTPUT -p UDP -s 0/0 -j ACCEPT

# Защищаемся от ICMP-перенаправления
# Этот вид атаки может использоваться злоумышленником для
# перенаправления своего трафика через вашу машину
$IPT -A INPUT --fragment -p ICMP -j DROP
$IPT -A OUTPUT --fragment -p ICMP -j DROP

# Но обычные ICMP-сообщения мы разрешаем
$IPT -A INPUT -p icmp -m icmp -i $INET --icmp-type source-quench -j ACCEPT
$IPT -A OUTPUT -p icmp -m icmp -o $INET --icmp-type source-quench -j ACCEPT

# Разрешаем себе пинговать интернет-узлы
$IPT -A INPUT -p icmp -m icmp -i $INET --icmp-type echo-reply -j ACCEPT
$IPT -A OUTPUT -p icmp -m icmp -o $INET --icmp-type echo-request -j ACCEPT

# Разрешаем передачу ICMP-сообщения "неверный параметр"
$IPT -A INPUT -p icmp -m icmp -i $INET --icmp-type parameter-problem -j ACCEPT
$IPT -A OUTPUT -p icmp -m icmp -o $INET --icmp-type parameter-problem -j ACCEPT

# Запрещаем подключение к X.Org через сетевые интерфейсы
$IPT -A INPUT -p tcp -m tcp -i $INET --dport 6000:6063 -j DROP --syn

# Указываем порты, открытые в системе, но которые должны быть
# закрыты на сетевых интерфейсах. Мы пропишем только порт 5501:
$IPT -A INPUT -p tcp -m tcp -m multiport -i $INET -j DROP --dports 5501
```

```
# Разрешаем DNS
$IPT -A OUTPUT -p udp -m udp -o $INET --dport 53 --sport $UPORTS -j ACCEPT
$IPT -A OUTPUT -p tcp -m tcp -o $INET --dport 53 --sport $UPORTS -j ACCEPT
$IPT -A INPUT -p udp -m udp -i $INET --dport $UPORTS --sport 53 -j ACCEPT
$IPT -A INPUT -p tcp -m tcp -i $INET --dport $UPORTS --sport 53 -j ACCEPT

# Разрешаем AUTH-запросы к удаленным серверам, но запрещаем такие
# запросы к своему компьютеру
$IPT -A OUTPUT -p tcp -m tcp -o $INET --dport 113 --sport $UPORTS -j ACCEPT
$IPT -A INPUT -p tcp -m tcp -i $INET --dport $UPORTS --sport 113 -j ACCEPT
                                                                    ! --syn
$IPT -A INPUT -p tcp -m tcp -i $INET --dport 113 -j DROP

# Далее мы открываем некоторые порты, необходимые
# для функционирования сетевых служб.

# FTP-клиент (порт 21)
$IPT -A OUTPUT -p tcp -m tcp -o $INET --dport 21 --sport $UPORTS -j ACCEPT
$IPT -A INPUT -p tcp -m tcp -i $INET --dport $UPORTS --sport 21 -j ACCEPT ! --syn

# SSH-клиент (порт 22)
$IPT -A OUTPUT -p tcp -m tcp -o $INET --dport 22 --sport $UPORTS -j ACCEPT
$IPT -A INPUT -p tcp -m tcp -i $INET --dport $UPORTS --sport 22 -j ACCEPT ! --syn
$IPT -A OUTPUT -p tcp -m tcp -o $INET --dport 22 --sport 1020:1023 -j ACCEPT
$IPT -A INPUT -p tcp -m tcp -i $INET --dport 1020:1023 --sport 22 -j ACCEPT
                                                                    ! --syn

# SMTP-клиент (порт 25)
$IPT -A OUTPUT -p tcp -m tcp -o $INET --dport 25 --sport $UPORTS -j ACCEPT
$IPT -A INPUT -p tcp -m tcp -i $INET --dport $UPORTS --sport 25 -j ACCEPT ! --syn

# HTTP/HTTPS-клиент (порты 80, 443)
$IPT -A OUTPUT -p tcp -m tcp -m multiport -o $INET --sport $UPORTS -j ACCEPT
                                                        --dports 80,443
$IPT -A INPUT -p tcp -m tcp -m multiport -i $INET --dport $UPORTS -j ACCEPT
                                                    --sports 80,443 ! --syn

# POP-клиент (порт 110)
$IPT -A OUTPUT -p tcp -m tcp -o $INET --dport 110 --sport $UPORTS -j ACCEPT
$IPT -A INPUT -p tcp -m tcp -i $INET --dport $UPORTS --sport 110 -j ACCEPT
                                                                    ! --syn

# Разрешаем прохождение DCHP-запросов через iptables
# Необходимо, если IP-адрес динамический
$IPT -A OUTPUT -p udp -m udp -o $INET --dport 67 --sport 68 -j ACCEPT
$IPT -A INPUT -p udp -m udp -i $INET --dport 68 --sport 67 -j ACCEPT
```

Вот практически и все... Конечно, приведенное здесь описание iptables нельзя назвать исчерпывающим. Для полного описания iptables пришлось бы создавать отдельную книгу под названием «Брандмауэр в Linux».

> ***Примечание***
>
> В Интернете мы нашли одно из наиболее полных руководств по iptables на русском языке. Так вот, если его распечатать, оно займет 121 страницу формата A4. Учитывая размер полосы набора страницы книжного формата, которая обычно меньше A4, смело можно говорить, что объем такой книги составил бы около 200 страниц. Адрес указанного руководства: **http://www.opennet.ru/docs/RUS/iptables/**.
>
> Вот еще одна очень хорошая статья по iptables: **http://ru.wikipedia.org/wiki/Iptables**.
>
> А для пользователей Debian и Ubuntu будет полезным следующее руководство: **http://www.linux.by/wiki/Index.php/Debian_Firewall**.

Брандмауэр UFW

Традиционно в качестве брандмауэра (фильтра пакетов) в Ubuntu и других дистрибутивах используется iptables, но поскольку Ubuntu позиционируется как простой дистрибутив, то и оболочка iptables была для него разработана соответствующая — UFW (Uncomplicated Firewall), т. е., дословно, несложный Firewall.

Установка и базовая настройка

Первым делом нужно убедиться, что пакет ufw вообще установлен или установить его, если это не так:

```
sudo apt install ufw
```

Теперь посмотрим состояние брандмауэра:

```
sudo ufw status verbose
```

По умолчанию фильтр пакетов выключен, поэтому вы получите сообщение:

```
Status: inactive
```

Не нужно спешить включать брандмауэр — сначала его нужно настроить. Ведь если порт 22 окажется по умолчанию недоступен, то вы потеряете доступ к своему VDS. Конечно, в службе поддержки вам помогут, но все это — потеря времени.

По умолчанию брандмауэр запрещает все входящие соединения и разрешает все исходящие. Такая политика идеальна с точки зрения безопасности (дальше вы поймете почему) — ведь если кто-то (и вы в том числе) захочет подключиться к защищенному брандмауэром серверу, у него это не получится. В то же время приложения на сервере смогут создавать исходящие соединения.

Рассмотрим две команды:

```
ufw default deny incoming
ufw default allow outgoing
```

Эти два правила как раз и задают политику по умолчанию: запрещаются все входящие соединения и разрешаются все исходящие.

Итак, все входящие соединения запрещены. Чтобы до сервера можно было «достучаться» по определенному порту, его нужно сначала открыть. UFW хорош тем, что вам даже не надо помнить номер порта — нужно знать только название сервиса. Например, вот как можно разрешить подключение по SSH:

```
ufw allow ssh
```

При этом UFW сам создаст правило для порта 22 — именно этот порт используется для SSH. Брандмауэр знает порты и имена всех распространенных служб (HTTP, SSH, FTP, SFTP и т. д.).

Однако если вы перенастроили SSH на нестандартный порт из соображений той же безопасности, нужно явно указать номер порта:

```
ufw allow 3333
```

После разрешения SSH (это главное, чтобы сейчас брандмауэр нам не разорвал соединение) можно включить UFW командой:

```
ufw enable
```

Необходимо подтвердить запуск, ответив «y»:

```
Command may disrupt existing ssh connections. Proceed with operation (y|n)?
```

Разберемся, что произошло. Сначала мы разрешили SSH, на что получили ответ, что правила обновлены:

```
Rules updated
```

Затем включаем брандмауэр и получаем сообщение, что он активен и будет запускаться при загрузке системы.

На этом базовая настройка выполнена: SSH успешно работает, и мы можем приступить к дальнейшей настройке фильтра пакетов.

Создание правил для сетевых сервисов

Теперь нужно разрешить работу других приложений. Как правило, надо разрешить службу HTTP (веб-сервер), FTP (если этот сервис вам нужен) и постараться не забыть о HTTPS (что очень важно в последнее время):

```
ufw allow http
ufw allow https
ufw allow ftp
```

Сделать то же самое можно было бы и по номерам портов:

```
ufw allow 80
ufw allow 443
ufw allow 21
```

При желании можно разрешить целый диапазон портов, указав при этом транспортный протокол (UDP или TCP):

```
sudo ufw allow 2000:2200/tcp
sudo ufw allow 4000:4400/udp
```

Разрешаем IP-адреса

UFW позволяет разрешить определенному IP-адресу доступ ко всем портам сервера — например:

```
ufw allow from 12.345.67.89
```

Если нужно разрешить доступ конкретному IP-адресу только к определенному порту, то делается это так:

```
ufw allow from 12.345.67.89 to any port 22
```

Здесь мы разрешаем не все подключения к SSH, а только подключения с IP-адреса 12.345.67.89.

Разрешить доступ целого диапазона IP-адресов (например, когда у админа динамический IP) можно так:

```
1ufw allow from 123.45.67.89/24 to any port 22
```

Запрещаем IP-адреса и службы

Запретить доступ с определенного IP-адреса можно аналогично:

```
ufw deny from 123.45.67.89
```

При желании можно запретить все подключения к определенной службе:

```
ufw deny ftp
```

Сброс правил

Сбросить все правила можно командой:

```
ufw reset
```

Но убедитесь, что на момент ввода этой команды вы отключили брандмауэр, иначе вы потеряете доступ по SSH.

Удалить конкретное правило можно по номеру — сначала введите следующую команду, чтобы узнать номер правила:

```
ufw status numbered
```

Затем удалите правило:

```
ufw delete <номер правила>
```

Оптимизация доступа в Интернет

Основные мероприятия оптимизации

Сейчас большинство пользователей Интернета (как предприятия, так и частные лица) пользуются выделенным безлимитным (без учета количества передаваемого трафика) каналом доступа в Интернет. Ранее трафик был платным (т. е. платилась не фиксированная сумма в месяц, а оплачивалось количество принятой/переданной информации), поэтому вопрос оптимизации доступа к Интернету стоял особенно

остро. Оптимизация не только ускоряла доступ, но и экономила деньги. В настоящее время оптимизация уже не так важна: интернет-каналы быстрые, плата за безлимитное соединение с Интернетом, как правило, фиксированная. Но все же есть еще предприятия, пользующиеся по тем или иным причинам медленными (5–10 Мбит/с на все компьютеры) соединениями. Оптимизация в их случае не помешала бы.

Оптимизация доступа к Интернету сводится к следующим мероприятиям:

- **установке кеширующего прокси-сервера и увеличению дискового объема для кеширования файлов** — как правило, кеширующий прокси-сервер работает на стороне провайдера, но там он общий, а здесь будет ваш личный. Выполняя свои обязанности, пользователи одного предприятия часто заходят на одни и те же ресурсы. Как показывает практика, изображения, сценарии, файлы стилей меняются там крайне редко. Выходит, что если один пользователь зашел на некий сайт **example.com** в первый раз, и в кеш прокси-сервера были загружены оттуда все вспомогательные файлы, то все остальные пользователи получат доступ к этим файлам (картинки, CSS и т. д.) уже не со скоростью 5 Мбит/с, а со скоростью 100 Мбит/с, — поскольку получать они будут их не из Интернета, а с нашего локального прокси-сервера;
- **ограничению и распределению полосы пропускания** — если какой-либо пользователь запустит Torrent-клиент и начнет закачку фильма, то все остальные (учитывая ширину канала) не смогут открыть даже простые веб-странички. Именно поэтому можно ограничить и распределить полосу пропускания, сохранив возможность быстрого открытия веб-страниц. В результате остальные сотрудники не почувствуют разницы, а закачка фильма будет осуществляться чуть медленнее. Можно вообще запретить загрузку фильмов, музыки и Torrent-файлов, и тогда нагрузка на канал станет минимальной. Решайте сами;
- **ограничению количества клиентов** — представьте современный офис, в котором трудятся 20–30 человек. Как правило, количество клиентов будет в 2 раза больше (как минимум): 20–30 компьютеров/ноутбуков и столько же личных смартфонов. Чем больше количество клиентов, тем ниже производительность Wi-Fi. Можно задать белый список MAC-адресов, которым разрешено подключаться к внутренней сети Wi-Fi, — это будут MAC-адреса сетевых адаптеров стационарных компьютеров/ноутбуков, а личные устройства пусть подключаются через сеть мобильного оператора;
- **блокированию рекламы** — чем меньше информации на страничке, тем быстрее она загружается. К сожалению, объем рекламы на интернет-страницах часто превышает объем содержащейся в них полезной информации. Если блокировать рекламу, то странички будут загружаться быстрее.

Прокси-сервер

С помощью прокси-сервера можно очень эффективно управлять ресурсами своей сети — например: кешировать трафик (HTTP), «обрезать» рекламные баннеры, указывать, какие файлы можно скачивать пользователям, а какие — нет, допуска-

ется также задать максимальный объем передаваемого объекта и даже ограничить пропускную способность пользователей определенного класса.

Однако основная функция прокси-сервера — это кеширование трафика. Если в сети используется прокси-сервер, можно сократить кеш браузеров клиентов практически до нуля — он уже не будет нужен, поскольку кеширование станет выполнять прокси-сервер. Тем более что он выполняет кеширование всех клиентов сети, и уже запрошенные кем-то ранее страницы оказываются доступны другим пользователям. Это означает, что если кто-то зашел на сайт **firma.ru**, то у всех остальных пользователей сети этот сайт будет открываться практически мгновенно, потому что его уже кешировали.

Даже если у вас всего один компьютер, все равно есть смысл использовать прокси-сервер, хотя бы для того, чтобы «обрезать» рекламные баннеры, — так можно сэкономить на трафике, да и страницы начнут открываться быстрее, потому что многочисленные баннеры загружаться перестанут.

В среднем, если судить по статистике использования прокси-серверов, при правильной его настройке можно добиться снижения интернет-трафика в два раза. То есть если раньше вы загружали из Интернета 10 Гбайт в день, то после установки прокси-сервера вы будете загружать 5 Гбайт. Если трафик платный, экономия — налицо. Если трафик безлимитный, налицо прирост скорости, поскольку примерно 5 Гбайт информации вы будете загружать не со скоростью относительно медленного интернет-соединения, а со скоростью локальной сети (100 Мбит/с).

Впрочем, прокси-сервер нужен не всем (если рассматривать его в разрезе оптимизации скорости доступа к Интернету). Возьмем, например, небольшой офис: три ноутбука, один стационарный компьютер (как бы сервер), несколько смартфонов/планшетов. Подключается все это добро к Интернету через маршрутизатор Wi-Fi, скорость доступа к Интернету согласно тарифному плану — 70 Мбит/с. Маршрутизатор Wi-Fi в силу особенностей технологии Wi-Fi скорость немного «режет». Если судить не по тестам вроде **speedtest.net**, которые не всегда показывают объективные результаты, а по торрентам, то реальная скорость не превышает 8 Мбайт/с, т. е. примерно 64 Мбит/с. Учитывая, что речь идет о Wi-Fi, это очень хороший показатель. Однако если измерить скорость передачи данных между двумя узлами этой сети Wi-Fi, то окажется, что из-за отсутствия полного дуплекса и поочередности передачи кадров в лучшем случае удается достигнуть 2–2,2 Мбайт/с.

Следовательно, если в такой сети развернуть прокси-сервер, то кешированные страницы будут открываться со скоростью 2,2 Мбайт/с, а загружаться из Интернета — со скоростью 8 Мбайт/с. Как видите, вместо прироста производительности мы получим «тормоза». Именно поэтому, прежде чем принимать решение о развертывании прокси-сервера, нужно тщательно все спланировать с учетом имеющейся инфраструктуры сети.

Конечно, прокси-сервер, как это и отмечалось ранее, может выполнять и другие полезные функции: блокировку рекламы, ограничение скорости и т. п. Однако блокировать рекламу можно и с помощью современных клиентских брандмауэров

в составе систем Internet Security — практически во все такие системы встроена возможность блокировки нежелательного контента.

Прозрачный прокси

С прокси-сервером часто связаны две проблемы. Первая заключается в том, что для работы через прокси-сервер нужно настраивать все клиенты. Если сеть большая — скажем, 100 компьютеров, — можете себе представить, сколько это займет времени, — ведь нужно будет подойти к каждому компьютеру. Даже если на настройку одного компьютера потребуется 5 минут, то на настройку всей сети уйдет уже 500 — целый рабочий день. Но настройкой браузера может дело и не обойтись. Ведь у пользователей могут быть и другие интернет-программы, работающие с WWW/FTP, которые также нужно будет настроить.

Проблема настройки — не самая страшная. Понятно, что если в сети предприятия 100 или более компьютеров, то и администратор на этом предприятии будет не один. А вдвоем-втроем можно настроить все 100 компьютеров за 2–3 часа.

Вторая проблема — более серьезная. Представим, что в сети есть «продвинутые» пользователи (а они-таки есть), которые знают, для чего служит прокси-сервер. Они могут просто изменить его настройки и вместо работы через прокси использовать прямое соединение с Интернетом, т. е. работать в обход прокси-сервера. Вы так старались, создавая список «черных» интернет-адресов (преимущественно это сайты для взрослых и всевозможные чаты/форумы), а они с помощью пары щелчков мышью свели все ваши старания к нулю.

Обе проблемы можно решить, если настроить *прозрачный* прокси-сервер, — пользователи даже не будут подозревать, что он есть. Во-первых, это решит проблемы с настройкой — вам не придется настраивать браузеры пользователей, потому что все HTTP-запросы станут автоматически поступать на прокси-сервер. Во-вторых, прозрачный прокси обеспечит принудительное кеширование информации и соответственно принудительный контроль за страницами, которые посещают пользователи.

Конечно, в домене Windows можно использовать групповые политики, но не всегда все рабочие станции работают под управлением Windows, — есть еще Linux, macOS, Android и т. п. Соответственно, групповые политики можно применять только в случае, если абсолютно все клиенты сети работают под управлением Windows. Именно поэтому настройка прозрачного прокси-сервера нам кажется лучшей затеей, чем автоматическая настройка через групповые политики.

Для настройки прозрачного прокси вам нужно изменить как конфигурационный файл самого прокси-сервера, так и правила брандмауэра iptables. Вот правила iptables:

```
iptables -t nat --new-chain TransProxy
# только порт 80 (HTTP) и 443 (SSL, https) — остальные обрабатывать не будем
iptables -t nat -A PREROUTING -p tcp --dport 80 -j TransProxy
iptables -t nat -A PREROUTING -p tcp --dport 443 -j TransProxy
iptables -t nat -A TransProxy -d 127.0.0.1/8 -j ACCEPT
```

```
# укажите IP-адрес своей сети
iptables -t nat -A TransProxy -d 192.168.1.0/24 -j ACCEPT
# все запросы перенаправляются на прокси-сервер 192.168.1.1, порт 3128
iptables -t nat -A TransProxy -p TCP -j DNAT --to 192.168.1.1:3128
```

А для работы с весьма популярным прокси-сервером Squid потребуется небольшая его донастройка. Так, в конфигурационный файл squid.conf добавьте следующие директивы:

```
# серверу назначается реальный IP-адрес, его и нужно указать
tcp_outgoing_address ваш_реальный_IP
httpd_accel_host virtual
httpd_accel_with_proxy on
httpd_accel_uses_host_header on
```

Напомним, что iptables обычно устанавливается на шлюзе — компьютере, который предоставляет доступ к Интернету другим компьютерам сети. На этом же компьютере должен быть установлен и прокси-сервер Squid.

Настройка использования полосы пропускания

Прокси-сервер Squid позволяет регулировать полосу пропускания, и использовать его для этой задачи наиболее рационально, учитывая, что существуют версии Squid как для Linux, так и для Windows.

Распределять полосу пропускания можно разными способами. Например — разделить пользователей на группы и указать лимит для каждой группы. Пусть у вас есть четыре категории пользователей: IT-отдел, юристы, бухгалтеры, администрация. Можно разделить полосу пропускания поровну — для всех по 25%. Можно установить и другие лимиты — например, по 30% для IT-отдела и администрации и по 20% для остальных отделов. В результате пользователи из одного отдела не смогут «узурпировать» всю пропускную полосу.

Можно также установить различную скорость загрузки файлов в зависимости от типа файла или его размера. Например, вы можете установить, что файлы размером более 100 Мбайт должны загружаться со скоростью 2 Мбит/с. При этом объем до ограничения (первые 100 Мбайт) будет загружаться на максимальной скорости, а оставшаяся часть файла — на скорости 2 Мбит/с. И волки сыты, и овцы целы: есть возможность загрузки больших файлов, и эта загрузка не мешает остальным пользователям работать.

Управление пропускной полосой в Squid реализовано через пулы задержек (delay pools). *Пул задержек* — это набор параметров, определяющих использование интернет-канала. Каждый пул задержек может быть одного из пяти *классов*:

- **класс 1** — ограничивает общую скорость для всех хостов, входящих в определенную группу;
- **класс 2** — ограничена общая скорость загрузки и скорость загрузки отдельного хоста;
- **класс 3** — ограничивается общая скорость загрузки, скорость загрузки для подсети и для отдельного хоста;

- **класс 4** — то же, что и класс 3, но еще и накладывает ограничение на каждого отдельного пользователя (не хоста, а пользователя — у вас должна быть включена аутентификация);
- **класс 5** — ограничивает скорость для запросов, сгруппированных по их тегу.

Обычно реализуются пулы первых трех классов. Иногда, если есть время заниматься настройкой аутентификации, можно настроить класс 4. Класс 5 используется крайне редко.

По умолчанию число пулов задержки равно 0. Определить количество пулов можно так:

```
delay_pools 4
```

В этом случае мы определили четыре пула. Далее нужно определить сами пулы. Адресация пула осуществляется по номеру, например:

```
delay_class 1 1
delay_class 2 1
delay_class 3 1
delay_class 4 1
```

Первый параметр задает номер пула, второй — его класс. Здесь мы определили, что все пулы будут класса 1 (если для каждого отдела организована своя подсеть, тогда нужно использовать пулы второго класса).

После определения пулов нужно задать их параметры ограничения пропускной способности. Для этого служит команда `delay_parameters`, которой нужно передать номер пула и лимиты. Для класса 1 лимит всегда один — общий. Для классов 2 и 3 сначала указывают лимит сети (или для сетей, если класс 3), а потом — индивидуальные значения. Цифры указываются в байтах, а не в битах — это нужно учитывать.

Пример:

```
delay_parameters 1 64000/128000
```

Здесь мы задаем максимальный размер файла: 128 000 байтов (почти 128 Кбайт). Файлы меньшего размера (HTML-страницы, сценарии, CSS-файлы, картинки — это тоже файлы) будут загружаться с максимальной скоростью. А вот если размер файла превышает 128 Кбайт, то первые 128 Кбайт будут загружены на максимальной скорости, а все, что осталось, — со скоростью около 512 Кбит/с (что равно 64 Кбайт/с).

Если какой-то пул ограничивать не нужно, тогда установите значение `-1/-1`:

```
delay_parameters 2 -1/-1
```

Хотя мы объявили все пулы как пулы первого класса, рассмотрим пример ограничения для пула второго класса:

```
delay_parameters 2 -1/-1 64000/128000
```

Здесь для сети нет ограничений, но есть ограничение для отдельного хоста.

Аналогично задаются ограничения для пула третьего класса:

```
delay_parameters 2 -1/-1 64000/128000 5000/20000
```

Здесь общая скорость не ограничена, для сетей, описанных в ACL[1], скорость ограничена так: `64000/128000`, для отдельных пользователей (хостов): `5000/20000`.

Задать, кого мы будем ограничивать, можно с помощью того же ACL. Вот пример:

```
acl office src 192.168.1.1/24
delay_access 1 allow office
delay_access 1 deny all
```

Здесь мы определили `acl office` для компьютеров, принадлежащих сети 192.168.1.1/24. Через пул с номером 1 разрешена передача данных этих компьютеров и запрещена всем остальным.

Чтобы вы не запутались, держите описание отдельных пулов вместе, например:

```
delay_class 1 2
acl office src 192.168.1.1/24
delay_access 1 allow office
delay_access 1 deny all
delay_parameters 1 -1/-1 64000/128000
```

Так все будет под рукой, и вы уже не запутаетесь в настройках.

Блокировка рекламы, сайтов «для взрослых» и т. п.

Как можно заблокировать нежелательные сайты с помощью прокси-сервера Squid? Очень просто — путем создания черного списка таких сайтов:

```
acl blacklist url_regex adult
http_access deny blaklist
http_access allow all
```

Этот черный список не пропускает интернет-адреса (URL), содержащие слово `adult`. По аналогии можно было бы создать отдельный файл и записать в него все «плохие» URL. Например, вот так (впрочем, это довольно накладно — проще использовать *регулярные выражения*):

```
acl banners urlpath_regex "/etc/squid/banners.txt"
http_access deny banners
```

В файл banners.txt нужно внести URL баннерных сетей, например:

```
^http://www.clickhere.ru
^http://banner.kiev.ua
...
```

Эти способы приемлемы, но требуют от администратора рутинной работы — ведь с каждым днем различных сайтов с нежелательным контентом становится все больше и больше. Именно поэтому есть другие, более совершенные решения.

---

[1] ACL (Access Control List) — список контроля доступа.

Для эффективной защиты вашего трафика (точнее, для его экономии) лучше использовать систему squidGuard, обладающую базой данных запрещенного контента. Вам не придется самому заполнять эту базу — она уже разработана за вас. Все, что вам нужно, — это установить squidGuard. Стандартная база squidGuard охватывает сайты, посвященные наркотикам, порно, насилию, азартным играм, а также рекламу. Закрыв доступ ко всему этому, можно сэкономить немало трафика. squidGuard — это не отдельный сетевой сервис, а дополнение к прокси-серверу Squid, поэтому squidGuard не может работать без Squid.

Итак, squidGuard — штука нужная, поэтому сразу приступим к его установке и настройке. После установки пакета squidGuard вам нужно скопировать файл /etc/squid/squidGuard.conf.sample в файл /etc/squid/squidGuard.conf:

```
# cp /etc/squid/squidGuard.conf.sample /etc/squid/squidGuard.conf
```

Теперь откройте файл /etc/squid/squidGuard.conf — в листинге 5.2 приведен пример этого файла, вам нужно только изменить его «под себя».

Листинг 5.2. Пример файла /etc/squid/squidGuard.conf

```
# Путь к базе данных, x.x.x — номер версии squidGuard
dbhome /usr/share/squidGuard-x.x.x/db
logdir /var/log/squidGuard

# Дни и время работы
# s = Вс, m = Пн, t =Вт, w = Ср, h = Чт, f = Пт, a = Сб

time workhours {
    weekly s 10:00-13:00
    weekly m 08:00-13:00 14:00-18:00
    weekly t 08:00-13:00 14:00-18:00
    weekly w 08:00-13:00 14:00-18:00
    weekly h 08:00-13:00 14:00-18:00
    weekly f 08:00-13:00 14:00-18:00
    weekly a 09:20-13:00
}

# Наша сеть

# пользователи сети
src users {
ip 10.0.0.1-10.0.0.100
}

# демилитаризованная зона (внутренние серверы сети)
src dmz {
ip 10.0.1.1-10.0.1.10
}
```

```
# далее описываются базы запрещенного контента
...
# файл конфигурации мы сократили, ведь у вас все равно есть полная
# версия, мы только рассмотрим пример описания одной базы –
# базы рекламы
dest advertising {
        domainlist      advertising/domains
        urllist         advertising/urls

# вместо рекламы будет отображен файл nulbanner.png,
# размещенный на локальном веб-сервере 0x0
        redirect http://127.0.0.1/cgi-bin/nulbanner.png
}
...

# Списки доступа, т. е. кто и что может делать в нашей сети
acl {
# компьютерам из зоны DMZ разрешим любой контент, кроме рекламы
 dmz {

# управлять контентом можно с помощью директивы pass
# в качестве значений можно передать название базы,
# например, advertising – реклама, porn – порно и т. д.
# (базы описаны выше)
# значение all означает весь контент, а none – обратно all, т. е.
# будет запрещен любой контент. Значение none используется редко.
# Чаще используется выражение !база, например, !porn запрещает
# порнографию

        pass !advertising all

# Все запрещенные запросы будут передаваться
# на сценарий http://127.0.0.1/cgi-bin/squidGuard.cgi
        redirect http://127.0.0.1/cgi-bin/squidGuard.cgi?clientaddr=%a&srcclass=
                                                        %s&targetclass=%t&url=%u
        }

# Обычные пользователи сети
        users {
         # запрещаем весь ненужный контент
               pass !adult !audio-video !forums !hacking !redirector !warez
                 !ads !aggressive !drugs !gambling !publicite !violence
                 !banneddestination !advertising all
               redirect http://127.0.0.1/cgi-bin/squidGuard.cgi?clientaddr=
                                        %a&srcclass=%s&targetclass=%t&url=%u
        }

# Значение по умолчанию. Все запрещено, запросы перенаправляются
# на сценарий squidGuard.cgi
```

```
        default {
                pass none
                redirect http://127.0.0.1/cgi-bin/squidGuard.cgi?clientaddr=
                                        %a&srcclass=%s&targetclass=%t&url=%u

        }
}
```

В файле конфигурации squidGuard нет ничего сложного. Вам нужно изменить только IP-адреса вашей сети, а также время работы.

Наверное, вы обратили внимание, что вместо просмотра запрещенного контента браузер перенаправляется на сценарий squidGuard.cgi, установленный на локальном веб-сервере. Получается, что для работы squidGuard нужен веб-сервер Apache. Если Apache вам необходим только для squidGuard, тогда просто установите его — настраивать его не придется, хватит конфигурации по умолчанию. Также не нужно самостоятельно копировать файл /usr/share/squidGuard-1.x.x/sample/squidGuard.cgi в каталог /var/www/cgi-bin — это происходит автоматически при установке squidGuard.

Практически все готово. Нам нужно только указать, что Squid должен использовать squidGuard. Сделать это очень просто — достаточно добавить в файл /etc/squid/squid.conf строки:

```
redirector_bypass on
redirect_program /usr/local/squidGuard/bin/squidGuard

redirect_children 1
```

Все, что вам осталось сделать, — это перезапустить Squid:

```
# /etc/init.d/squid restart
```

После этого откройте журнал squidGuard — файл /var/log/squidGuard/squidGuard.log. В нем вы должны увидеть строку:

```
squidGuard ready for requests
```

Если она есть, значит, вы все сделали правильно и squidGuard работает.

> ***Примечание***
>
> Фильтрация HTTPS-ресурсов требует дополнительной настройки Squid. Подробнее об этом можно прочитать в статье: **https://habr.com/post/267851/**.

Поддержка SSL

По умолчанию Squid выполняет кеширование только сайтов, загружаемых по протоколу HTTP. Однако сегодня большая часть сайтов перешла на безопасный протокол HTTPS, и Squid в этой части требует дополнительной настройки.

Трафик HTTPS использует для шифрования информации протокол SSL (Secure Socket Layer). С одной стороны, это хорошо, с другой — зашифрованный трафик может представлять угрозу безопасности и скрывать вредоносный контент. Кроме

того, зашифрованный трафик будет не полностью отображаться в журналах Squid, что так же не есть хорошо. Исправить эту проблему можно с помощью функции Squid SSL bump, которая позволяет осуществлять расшифровку и запись в журнал запросов, передаваемых по протоколу HTTPS.

Первым делом для работы Squid SSL bump нужно создать корневой сертификат:

```
openssl req -new -newkey rsa:2048 -sha256 -days 365 -nodes -x509 -extensions
v3_ca -keyout proxyCA.pem  -out proxyCA.pem
```

Созданный сертификат надо поместить в каталог /etc/squid/ssl_cert. Этот сертификат должен быть установлен как корневой в браузерах всех пользователей, для чего его необходимо конвертировать в формат DER:

```
openssl x509 -in proxyCA.pem -outform DER -out proxyCA.der
```

Затем этот сертификат требуется установить на всех компьютерах. Установка сертификата достаточно проста: щелкните двойным щелчком на DER-файле, в открывшемся окне нажмите кнопку **Установить сертификат**, а далее следуйте инструкциям мастера. Обратите внимание, что сертификат нужно устанавливать не для текущего пользователя, а для всей машины (Local Machine). Если не установить сертификат в браузеры пользователей, то при каждом запросе страницы через Squid HTTPS прокси-пользователю будет выдаваться предупреждение безопасности, что очень неудобно.

Если вам повезет, то в вашем дистрибутиве уже установлена поддержка SSL. Как правило, в современных дистрибутивах так и есть, но серверы не всегда работают под управлением современных версий, поскольку серверное ПО не так часто переустанавливается, как клиентское. В таком случае нужно скачать исходники squid и откомпилировать их со следующими опциями:

```
./configure \
--with-openssl \
--enable-ssl-crtd
```

Если вы никогда не компилировали ПО из исходных кодов, можете найти соответствующую инструкцию в Сети — вот, например, одна из них: **http://jakondo.ru/ustanovka-squid-3-5-19-na-ubuntu-14-04-5-lts-s-podderzhkoj-https-protokola/**. Эту статью мы упомянули здесь не просто так и не ради ее рекламы. Обратите внимание: загрузка исходников в этой статье подразумевается с сайта автора статьи. Никогда так не делайте! Есть официальные репозитории (для Squid это: **https://github.com/squid-cache/squid**) — оттуда и нужно загружать исходные коды. Может, автор статьи и не планировал ничего ужасного, а выложил исходники на своем сайте удобства ради, а может, и внес в них изменения. Можно, конечно, сравнить их с эталоном той же версии, но, думаю, вам не захочется тратить на это свое время.

Далее нужно отредактировать конфигурационный файл squid.conf:

```
http_port 3128 ssl-bump \
  cert=/etc/squid/ssl_cert/proxyCA.pem \
  generate-host-certificates=on dynamic_cert_mem_cache_size=4MB
```

```
acl step1 at_step SslBump1

ssl_bump peek step1
ssl_bump bump all

sslproxy_cafile /usr/local/openssl/cabundle.file
```

Здесь /etc/squid/ssl_cert/proxyCA.pem — ранее созданный сертификат.

После выполнения указанных настроек информация обо всех запросах, выполненных по протоколу HTTPS через прокси, будет записываться в лог-файл access.log, так же как и запросы, выполненные по HTTP.

Дополнительную информацию о настройке SSL bump вы без особых проблем найдете в Интернете.

Удаленная работа

Виртуальные частные сети

Предположим, что пользователям нашего предприятия нужно обращаться к ресурсам корпоративной сети, когда они находятся за ее пределами — например, в другом городе. Первое, что приходит в голову, — это настроить сервер удаленного доступа (Remote Access Server, RAS или dial-in-сервер). Пользователь с помощью модема «дозванивается» до сервера удаленного доступа, сервер идентифицирует пользователя, после чего последний подключается к сети предприятия и работает в ней как ни в чем не бывало (разве что скорость передачи данных будет значительно ниже, чем обычно).

Но использование RAS — затея весьма дорогая и неудобная. Во-первых, нужно организовать модемный пул, а это недешево и накладно: чтобы обеспечить одновременную работу нескольких пользователей, понадобится или многоканальная линия, или же несколько телефонных линий. Во-вторых, надо будет оплачивать междугородние и даже международные звонки пользователей (для удобства самих пользователей желательно при этом организовать callback-режим). В-третьих, далеко не всегда у пользователя есть возможность подключиться к телефонной сети. В-четвертых, RAS не может обеспечить связь нескольких филиалов компании.

Выходом из сложившейся ситуации является использование *виртуальной частной сети* (Virtual Private Network, VPN). В случае с VPN данные передаются по каналам Интернета. Это существенно упрощает и удешевляет нашу задачу. Доступ к Интернету есть везде, пользователи сами смогут выбирать провайдера и способ (соответственно и скорость) подключения к Интернету. Понятно, чтобы оградить данные от перехвата, информация при передаче через VPN шифруется. Вот основные преимущества VPN:

- не требуется никакого дополнительного оборудования (модемного пула) и каких-либо дополнительных ресурсов (например, многоканальной телефонной линии). Все, что нужно, — это подключение к Интернету, а поскольку нет такого частного предприятия, которое не было бы подключено к Интернету, будем считать, что все необходимое для организации VPN уже есть;

- безопасность передачи данных по сравнению с обычной передачей данных по Интернету;
- возможность как соединения филиалов компании, так и подключения отдельных пользователей к корпоративной сети. При этом отдельные пользователи могут подключаться к Интернету с использованием возможностей мобильной связи, что делает их подключение к VPN максимально гибким — им не придется искать свободную телефонную розетку.

Настройка VPN-сервера — задача непростая и требует особого подхода. К сожалению, описание конфигурации такого сервера выходит за рамки этой книги. Если вы заинтересовались, то можете обратиться к книге Д. Колисниченко «Серверное применение Linux» (3-е изд). издательства «БХВ-Петербург»[1].

Удаленное подключение к Linux

Администратору очень важна возможность удаленного доступа к серверу. Ведь не всегда есть возможность получить к нему физический доступ — вы можете находиться на другом конце города или даже в другой стране, а сервер предприятия вдруг потребует вашего оперативного вмешательства.

Для организации удаленного доступа мы применим два совершенно разных способа: протокол SSH и X-терминалы. В первом случае мы получим доступ к консоли сервера. Именно это нам и нужно, если мы подключаемся по относительно медленному каналу (модем, смартфон) — ведь для передачи текста большая скорость не нужна.

Второй способ подходит для более скоростного канала — выделенной линии или же локальной сети. Но зато X-терминалы позволяют работать с удаленным компьютером как с локальным, т. е. с полным эффектом присутствия. В отдельном окне вы будете видеть графический интерфейс удаленного компьютера. А если активизировать полноэкранный режим, тогда вообще нельзя будет даже и предположить, что работаешь за удаленным компьютером, — разницы вы просто не заметите. Впрочем, все будет выполняться немного медленнее — ведь данные нужно передать по сети, а не по внутренней шине компьютера. Но тут все зависит от конфигурации самих компьютеров и, конечно же, непосредственно от сети.

Протокол SSH

Раньше для организации удаленного доступа к консоли сервера использовался протокол Telnet. В каждой сетевой операционной системе, будь то FreeBSD или Windows, есть telnet-клиент. Эта программа так и называется — telnet (в Windows — файл telnet.exe).

Но технологии не стоят на месте и протокол Telnet устарел. Сейчас им практически никто не пользуется. Ему на смену пришел протокол SSH (Secure Shell), который,

[1] См. **https://bhv.ru/product/servernoe-primenenie-linux-3-e-izd/**.

как видно из названия, представляет собой безопасную оболочку. Главное его отличие от Telnet состоит в том, что все данные (включая пароли доступа к удаленному компьютеру и файлы, пересылаемые по SSH) передаются в зашифрованном виде. Во времена Telnet нередки были случаи перехвата паролей и другой важной информации, что и стало причиной создания SSH.

Протокол SSH использует следующие алгоритмы для шифрования передаваемых данных: BlowFish, 3DES (Triple Data Encryption Standard), IDEA (International Data Encryption Algorithm) и RSA (Rivest-Shamir-Adelman algorithm). Самыми надежными являются алгоритмы IDEA и RSA. Поэтому, если вы передаете действительно конфиденциальные данные, лучше использовать один из этих алгоритмов.

В состав любого дистрибутива Linux входит ssh-сервер (программа, которая и обеспечивает удаленный доступ к компьютеру, на котором она установлена) и ssh-клиент (программа, позволяющая подключаться к ssh-серверу). Для установки ssh-сервера нужно установить пакет openssh (это разновидность ssh-сервера), а для установки ssh-клиента — пакет openssh-clients.

Если у вас на рабочей станции установлена система Windows и вам нужно подключиться к ssh-серверу, запущенному на Linux-машине, то мы рекомендуем бесплатное приложение Bitvise SSH Client. Приятная особенность — приложение может хранить неограниченное число профилей с настройками для подключения к разным ssh-серверам, что очень удобно, если вы администрируете несколько серверов. Оно также позволяет открывать несколько сеансов в разных окнах. Один сеанс, например, вы можете использовать для редактирования файлов конфигурации, а на втором запустить программу htop для мониторинга использования ресурсов сервера.

Имеются ssh-клиенты и для Android, и для iOS, что очень удобно, если вы находитесь не на рабочем месте, а ситуация требует вашего срочного вмешательства. Для iOS неплохим (и, главное, бесплатным!) является приложение WebSSH, которое вы сможете загрузить из App Store.

Работать с ssh-клиентом очень просто. Для подключения к удаленному компьютеру введите команду:

```
ssh [опции] <адрес_удаленного_компьютера>
```

В качестве адреса можно указать как IP-адрес, так и доменное имя компьютера. В табл. 5.7 приведены часто используемые опции программы ssh.

***Таблица 5.7.** Опции программы ssh*

Опция	Описание
`-c blowfish|3des|des`	Выбор алгоритма шифрования — при условии, что используется первая версия протокола SSH (об этом позже). Можно указать `blowfish`, `des` или `3des`
`-c` *шифр*	Задает список шифров, разделенных запятыми в порядке предпочтения. Опция используется для второй версии SSH. Можно указать `blowfish`, `twofish`, `arcfour`, `cast`, `des` и `3des`

Таблица 5.7 (окончание)

Опция	Описание
`-f`	Переводит ssh в фоновый режим после аутентификации пользователя. Рекомендуется использовать для запуска программы X11. Например: `ssh -f server xterm`
`-l` *имя_пользователя*	Указывает имя пользователя, от имени которого нужно зарегистрироваться на удаленном компьютере. Опцию использовать не обязательно, поскольку удаленный компьютер и так запросит имя пользователя и пароль
`-p` *порт*	Определяет порт ssh-сервера (по умолчанию используется порт 22)
`-q`	«Тихий режим». Будут отображаться только сообщения о фатальных ошибках. Все прочие предупреждающие сообщения в стандартный выходной поток выводиться не будут
`-x`	Отключает перенаправление X11
`-X`	Задействовать перенаправление X11. Полезна при запуске X11-программ
`-1`	Использовать только первую версию протокола SSH
`-2`	Использовать только вторую версию протокола SSH. Вторая версия протокола более безопасна, поэтому при настройке ssh-сервера нужно использовать именно ее

Теперь можно приступить к конфигурированию ssh-сервера. Обычно в качестве ssh-сервера используется OpenSSH-сервер. Как правило, он запускается автоматически и не нуждается в настройках. Его конфигурационный файл называется /etc/ssh/sshd_config — и, главное, убедиться, что ssh-сервер запущен.

Настройки программы-клиента хранятся в файле /etc/ssh/ssh_config, и они также приемлемы по умолчанию. На всякий случай вы можете заглянуть в этот файл — его формат, как и назначение опций (большая часть из них закомментирована), вы поймете и без наших подсказок.

«Тонкие» клиенты

В последние годы все чаще говорят о «тонких» клиентах. Суть «тонкого» клиента заключается в том, что рабочая станция подключается к серверу терминалов, и после регистрации пользователя в системе он может работать с графическим интерфейсом сервера так, как если бы он непосредственно находился за клавиатурой и монитором сервера терминала. Особую прелесть этому решению придает то, что в качестве рабочей станции могут выступать компьютеры самой минимальной конфигурации. Главное, чтобы на таком компьютере можно было запустить операционную систему, способную подключиться к серверу терминалов. Не нужны большие объемы ни оперативной памяти, ни дисковой. Нужна только сетевая карта — через нее действия пользователя будут передаваться на сервер терминалов, через нее же будет возвращаться «картинка» с сервера — результат выполнения этих команд.

Все программы, запускаемые пользователем, будут выполняться на сервере терминалов, а компьютер пользователя станет только отображать результат их выполнения, ну и, разумеется, будет передавать серверу терминалов нажатия клавиш и перемещения мыши (см. также далее *разд. «Терминальный доступ»*).

Удобно? С одной стороны, да, с другой — нет. В первую очередь приходит мысль о том, что можно сэкономить на рабочих станциях. Но сервер терминалов должен быть очень мощным компьютером. Очень! Тут все зависит от поставленной задачи. Иногда бывает дешевле или проще приобрести несколько относительно дешевых рабочих станций, чем мощный сервер. Тем более что скорость выполнения задач все равно окажется не столь высокой, как ожидается. Во-первых, данные передаются по сети, на что требуется дополнительное время. Во-вторых, к серверу терминалов при этом одновременно подключается (и нагружает его) множество рабочих станций — иначе зачем он нам нужен?

Использование графических утилит для подключения к Linux

Если в вашей ОС Linux установлена графическая оболочка, то существуют программы, позволяющие работать в ней удаленно. Одним из наиболее частых решений является бесплатный пакет VNC, который позволяет использовать в качестве сервера и клиента системы Windows и Linux в любом сочетании. Другими словами, из Linux вы можете подключаться к Windows-клиентам и наоборот.

Подключение филиалов

У многих предприятий есть удаленные филиалы. Такие филиалы могут находиться в пределах одного города, одной страны или вообще за пределами страны. Очень часто бывает необходимо, чтобы все компьютеры филиалов работали в составе единой сети. Для этого локальные сети филиалов должны быть объединены *туннелем*.

Создать туннель можно с помощью VPN. Здесь возможны два решения: либо программное, либо аппаратное. Первое заключается в настройке VPN-серверов, и оно описано в уже упомянутой ранее книге «Серверное применение Linux» (3-е изд.). Второе подразумевает использование уже готовых VPN-маршрутизаторов. Между этими маршрутизаторами создается туннель, по которому осуществляется обмен данными двух локальных сетей. Преимущество такого решения — надежность (решения, заложенные в маршрутизаторы, хорошо отработаны), стабильность работы (в маршрутизаторах используются UNIX-подобные операционные системы), быстрота восстановления канала в случае обрыва связи и т. д.

Если в качестве пограничных компьютеров используются Linux-системы, то создать безопасное объединение локальных сетей очень просто. Сначала организуется безопасное соединение сетей, а после этого настраивается туннель и правила фильтрации.

Информацию о настройке самого туннеля между двумя Linux-системами вы без проблем найдете или в Интернете, или в книге «Серверное применение Linux» (3-е изд.), поэтому сейчас на этом мы подробно останавливаться не будем.

Контроллер домена «только для чтения»

Сейчас наличием филиалов или территориально удаленных подразделений (например, складов) никого не удивишь. Филиалы могут находиться как в пределах города, так и по всей стране.

К сожалению, центральный офис не всегда бывает достижим. Случается всякое — от выхода из строя сетевого оборудования до банального отключения в центральном офисе электричества. Что делать в этом случае?

Тут поможет размещение в филиале дополнительного контроллера домена. Однако в филиале гораздо сложнее обеспечить необходимый уровень безопасности сервера, а при наличии физического доступа к системе злоумышленнику не составит особого труда скомпрометировать ее. Впрочем, начиная с Windows Server 2008, появилась возможность установки контроллера домена «только для чтения» — RODC (Read-Only Domain Controller). RODC в некоторой мере похож на Backup Domain Controller — контроллер в домене Windows NT 4.0, в который также нельзя было вносить изменения.

Вот чем отличается RODC от обычного контроллера домена:

- **односторонняя репликация** — данные копируются на RODC с других контроллеров. Если программа пытается внести изменения в базу, хранящуюся на RODC, то операция записи будет транслироваться на «обычные» контроллеры и выполняться там;
- **ограниченный набор атрибутов** — на RODC кешируется только часть атрибутов каталога. Настройками на контроллере — хозяине схемы администратор может изменить состав этих атрибутов, но часть их помечена как критические и не подлежит репликации на RODC. На RODC также можно установить сервер DNS в режиме «только для чтения»;
- **возможность хранения данных аутентификации** — администратор может настроить список учетных записей, для которых данные аутентификации будут храниться (кешироваться) на RODC. Эти пользователи смогут входить в домен и т. п. даже в случае отсутствия соединения с центральным офисом. В случае же компрометации RODC администратор будет знать, к каким учетным записям злоумышленник мог получить доступ, и сможет принять необходимые меры;
- **делегирование прав локального администратора** — на «обычных» контроллерах домена локальный администратор является администратором домена. Для выполнения задач обслуживания RODC (установка драйверов и аналогичные операции, требующие наличия прав администратора) предусмотрено, что любая учетная запись, включенная в группу локальных администраторов, будет обладать правами локального администратора, но не получит никаких прав по управлению доменом.

> ***Примечание***
>
> В случае взлома RODC злоумышленник может настроить репликацию на него дополнительных атрибутов службы каталогов, которые не копируются в филиал в нормальных условиях по соображениям безопасности. При взаимодействии с контроллером на

> Windows Server 2008 последний откажет в операции копирования. Если же связь будет установлена с контроллером на основе Windows Server 2003, то *данные будут скопированы*. Поэтому в целях безопасности необходимо устанавливать RODC в домене, режим которого переведен на уровень Windows Server версий с 2008 по 2022.

Установка RODC не представляет никакой сложности. Администратору необходимо начать установку контроллера домена (командой `dcpromo` или из консоли управления). Далее на соответствующем шаге мастера указать, что необходимо установить контроллер в режим «только для чтения», а затем выбрать политику репликации паролей учетных записей. Обычно достаточно согласиться с предложением мастера операций — настройки по умолчанию подходят в большинстве случаев.

Подробно об установке RODC вы можете прочитать в книге У. Станека «Microsoft Windows Server 2012 R2: хранение, безопасность, сетевые компоненты. Справочник администратора» издательства «БХВ-Петербург»[1].

Решение DirectAccess

В операционных системах Windows 10/11 и Windows Server версий с 2008 R2 по 2022 появилась возможность подключения извне к ресурсам внутренней сети предприятия без операций создания VPN — с использованием возможностей системы безопасности протокола IPv6 (технология DirectAccess).

Преимущества решения DirectAccess — в отсутствии каких-либо пользовательских операций для подключения к локальной сети. Например, ноутбук из локальной сети переносится в глобальную сеть и по-прежнему продолжает работать с внутренним ресурсом. Можно сказать, что при работе в Интернете автоматически создается туннель к ресурсам локальной сети.

Настройка DirectAccess предполагает выполнение ряда операций. Подробно об этом можно прочесть в руководстве по адресу: **https://technet.microsoft.com/ru-ru/library/dd630627%28WS.10%29.aspx** (главная страница технологии доступна по адресу: **https://www.microsoft.com/en-us/server-cloud/windows-server/directaccess.aspx**).

Особенностью технологии DirectAccess является постоянный контроль над клиентской системой со стороны IT-служб предприятия. Поскольку компьютер-клиент DirectAccess должен быть членом домена, а туннель подключения к домену всегда работает при наличии доступа в Интернет, то к компьютеру постоянно применяются действующие на предприятии технологии управления: выполняются групповые политики, обновляются антивирусные базы данных и т. п.

Сегодня технология DirectAccess пока не нашла широкого распространения в нашей стране. Причина в том, что DirectAccess основана на возможностях протокола IPv6, а этот протокол у нас пока практически не используется.

---

[1] См. **https://bhv.ru/product/microsoft-windows-server-2012-r2-hranenie-bezopasnost-setevye-komponenty-spravochnik-administratora/**.

Терминальный доступ

При удаленном подключении к офису пользователи хотят воспользоваться всеми сервисами, которые реализованы в его локальной сети. Однако недостаточное качество каналов связи зачастую не позволяет эффективно работать во многих приложениях. Одним из вариантов решения этой 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 при этом играет роль «удаленной консоли». Данные и команды, которые пользователь вводит с клавиатуры или 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 и мышь.

В результате при работе в типовой офисной программе терминальный клиент в среднем передает по сети около 500 байтов данных в секунду, что позволяет полноценно работать с удаленным компьютером, используя модемные соединения или медленные каналы связи.

> ***Примечание***
>
> Подробно настройка терминального сервера описана в *главе 8*. Там мы настроим виртуальный сервер терминалов для доступа к популярной бухгалтерской программе «1С:Предприятие» и другим приложениям. Процесс настройки для физического сервера ничем не отличается.

Терминальные серверы от Microsoft

В 1995 году компания Citrix выпустила продукт под названием Winframe, который стал первым терминальным сервером на базе Windows NT. В 1998 году, после заключения между Microsoft и Citrix договора о кросс-лицензировании, вышли версии Windows NT Terminal Server Edition (TSE) и Citrix MetaFrame (продукт Citrix расширял возможности терминального сервера Windows NT TSE). В «поколении W2K» терминальные службы включены в поставку всей линейки серверов Windows Server 20*xx*.

Терминальные клиенты

В качестве клиентов терминала могут служить практически любые компьютеры, причем сами терминалы *не нуждаются в модернизации*. Поскольку все вычисления выполняются 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 из одного места». Терминальные системы более безопасны, поскольку устранение уязвимости

на сервере ведет к аналогичному результату для всех его клиентов и практически не оставляет никаких «вольностей» пользователю — ведь контролю администратора поддается практически все.

Кроме того, стоимость терминальных устройств существенно ниже стоимости полнофункциональных компьютеров. Терминалы могут быть выполнены как на бездисковой основе (Linux-терминалы, например, можно загрузить по сети с сервера), так и на основе загрузки с тех или иных аналогов жесткого диска (например, с Disk On Module[1] и т. п. — объем ядра Linux вместе с программой подключения к RDP-серверу составляет менее 8 Мбайт).

> ***Примечание***
>
> «Тонкие» клиенты на базе Linux обычно содержат возможности подключения к различным терминальным службам (по протоколам Citrix ICA, RDP, Tarantella, X, Telnet, tn5250 и т. п.). Пользователи могут бесплатно загрузить как исходные коды, так и готовые образы программ для любого варианта загрузки: с флешки, с CD, по сети и т. п. (см., например: **http://thinstation.sourceforge.net/**).

Если в качестве клиента терминального сервера используется компьютер на Windows 7, то необходимое программное обеспечение для подключения к серверу на нем уже установлено и программа подключения к удаленному рабочему столу вызывается командой меню **Пуск | Стандартные | Связь**. Однако желательно обновить ее до последней версии. Имеющиеся версии можно продолжать использовать, но все же лучше бесплатно загрузить обновления с сайта вендора. В случае с Windows 10/11 ситуация аналогичная — приложение **Подключение к удаленному рабочему столу** находится в программной группе **Стандартные**.

Обратите внимание, что для подключения к терминалу необходимо быть на нем либо администратором, либо членом группы **Пользователи удаленного рабочего стола**. Поскольку эта группа первоначально пуста, то в нее нужно добавить соответствующих пользователей.

Еще одно 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.

Режимы терминальных служб

Существуют два варианта подключения к рабочему столу удаленного компьютера:

- **Подключение к рабочему столу** (ранее — *административный режим*) используется *только* для удаленного управления сервером или рабочей станцией. При

[1] Disk on Module (DOM) — устройство, выполняющее функции жесткого диска, но реализованное на модуле памяти (как правило, энергонезависимой — флеш-памяти). Наиболее распространенной реализацией DOM является карта CompactFlash с адаптером CF для интерфейса IDE, SATA или USB. От обычного SSD устройство отличается тем, что устанавливается непосредственно на материнскую плату.

подключении к рабочему столу сервера одновременно могут работать не более двух человек, причем обладающих на этом сервере административными правами[1]. В таком режиме не требуется дополнительных лицензий;

- в **терминальном режиме** (ранее назывался *режимом приложений*) для подключения необходимы дополнительные специальные лицензии, но количество одновременных подключений не ограничено, причем работать на сервере могут и пользователи с обычными, не административными правами.

Лицензирование терминальных служб

Для использования *терминальных служб* необходимы специальные лицензии, которые приобретаются отдельно от сервера. Существуют различные схемы лицензирования, на которых мы не будем останавливаться. Лицензии достаточно дорогие, и это обстоятельство вполне способно обеспечить благожелательное отношение к вам продавца при обращении за консультациями.

Лицензии специфичны для каждого выпуска — иными словами, лицензии от сервера Windows 2008 не подойдут для Windows Server 2016/2022. Приобретаться они должны для каждого подключения — независимо от того, подключается ли рабочая станция Windows 10/11 или бездисковая Linux-система.

Необходимость приобретения 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 (с использованием службы каталогов) в любом домене леса, но только в пределах сайта.

Сервер лицензий обязательно должен быть активирован через сайт изготовителя. Так же активируются и клиентские лицензии. В случае необходимости администраторы легко найдут в Сети любые рекомендации по выполнению такой операции. Без активации лицензий сервер создает временные лицензии, которые можно использовать в течение 120 дней. Но и постоянные лицензии также не выдаются клиентам на неограниченный срок — они периодически обновляются, чтобы восстановить лицензии, «отданные» компьютерам, которые уже больше не работают в сети (например, вышли из строя).

> ***Совет***
>
> После установки лицензий имеет смысл выполнить резервное копирование сервера, чтобы можно было восстановить лицензии.

---

[1] К рабочей станции можно удаленно подключиться только администратору, при этом текущий пользователь от рабочего стола отключается. Ограничение это, скорее, лицензионное, поскольку в Интернете можно найти решения, снимающие ограничения на количество удаленных сессий и фактически превращающие рабочую станцию в терминальный сервер.

Особенности использования приложений на терминальном сервере

Режим терминального сервера не предназначен для работы программ, вызывающих интенсивную нагрузку на процессор. Соответственно, 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 (или когда установка производится файлом setup или install).

После установки приложения имеет смысл проанализировать внесенные в автозагрузку изменения. Например, многие программы выводят в системной области панели задач некие индикаторы. Так, антивирусная программа показывает наличие и состояние защиты на компьютере и т. п. В большинстве случаев такие индикаторы только отнимают лишние ресурсы системы и могут быть отключены в целях повышения производительности.

Для корректной работы приложений в режиме терминального сервера должен выполняться ряд условий: отсутствие записи данных в каталоги самой программы и т. п. Эти требования стали предъявляться и к программам, предназначенным для установки в Windows 7/8/10/11, а также в Windows Server 2012/2019/2022, поэтому такие условия обычно выполняются. Но на практике можно встретить любую ситуацию. Исправить ее можно включением специальных сценариев (подробности можно уточнить в сопроводительной документации).

Безопасность 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 предвидеть 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.

Поскольку терминальный сервер предоставляется многим пользователям, то администратору крайне важно сохранить его работоспособность, не давая пользователям устанавливать лишнее программное обеспечение, менять настройки и т. п. Мы не будем останавливаться на описании возможных административных настроек, отметим только, что для терминального сервера очень развиты опции тюнинга через политики безопасности — в политиках безопасности можно установить практически любые ограничения, и администратору нужно найти лишь золотую середину.

В частности, пользователей надо ограничить применением только заданного перечня программ. Следует запретить им доступ к локальным ресурсам сервера, не разрешать выполнение ресурсоемких операций, лишить права устанавливать новые программы и т. п. Приведем далее небольшой список возможных ограничений.

> ***Примечание***
>
> Желательно создать в службе каталогов (OU, Organization Unit) специальное подразделение, в которое и переместить терминальный сервер. Для этого OU следует назначить собственную групповую политику, где и определить необходимые ограничения.

- Ограничить список программ, которые разрешено запускать пользователям терминала.
- Ограничить перечень устройств, к которым предоставляется доступ пользователю терминала. Например, исключить доступ к CD-ROM, сменным дискам и т. д.
- Без необходимости не стоит разрешать пользователю подключать как диски своего компьютера, так и любых других систем (для исключения запуска программ с этих носителей).
- Желательно отключить возможность установки пользователем программ с использованием Windows Installer.
- Рекомендуется запретить просмотр и поиск *любых* ресурсов (например, просмотр сети, поиск принтеров, поиск файлов и т. п.).
- Желательно настроить административные шаблоны для таких задач, как Проводник, меню **Пуск**, панель управления и т. п., ограничив состав возможностей только необходимыми функциями.

> ***Примечание***
>
> Как известно, операцию поиска в Проводнике можно вызвать быстрыми клавишами <Ctrl>+<E>. Чтобы заблокировать такую возможность, создайте файл с некоторым поясняющим текстом (например, текстовый или в формате HTML) и установите для строки реестра системы: `HKLM\SOFTWARE\Microsoft\Internet Explorer\Search` следующие параметры: `SearchAssistant=REG_SZ: <путь к этому файлу>` и `CustomizeSearch=REG_SZ: <путь к этому файлу>`. Теперь при попытке выполнить операцию поиска пользователь увидит только содержание этого 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.

Подключение к консоли терминального сервера

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 — со своим экраном, а не с тем, который вы оставили. Это не всегда удобно для администраторов — иногда им необходимо увидеть со-

общения, которые отображаются после старта системы (например, сообщения от системы контроля серверной платформы или предупреждения о неудачном запуске службы), осуществлять задачи управления, доступ к которым сохранен на локальном столе, или просто продолжить работу с документом, который остался открытым, когда вам неожиданно пришлось уйти с рабочего места.

Для работы с экраном консоли нужно запустить клиент подключения к удаленному рабочему столу с ключом `/console`:

```
MSTSC /console
```

Этот ключ можно указать в параметрах (свойствах) ярлыка подключения. 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`, эта команда не сможет подключить к консоли, если с последней предварительно не был выполнен вход в систему.

Подключение администратора к сессии пользователя

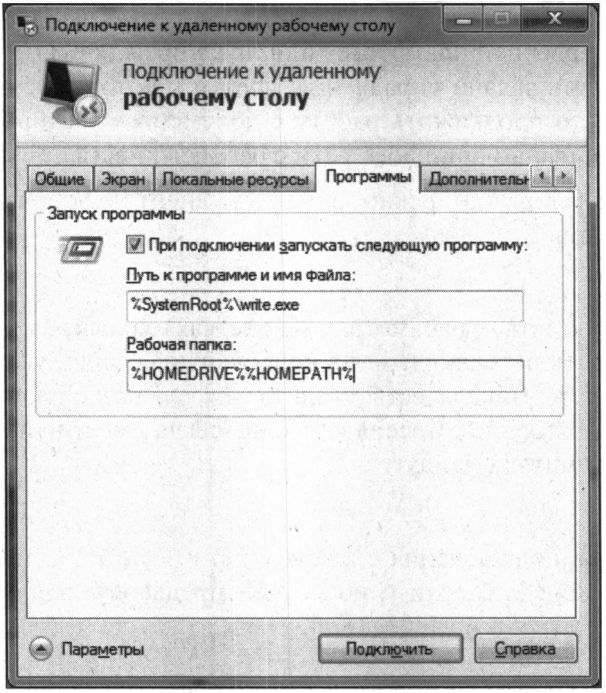
Администратор терминального сервера (точнее, тот пользователь, которому такое право дано протоколом RDP. По умолчанию это только администраторы терминального сервера, но при необходимости такое положение можно изменить, воспользовавшись оснасткой управления параметрами RDP-протокола) имеет возможность подключиться к пользовательской сессии. Этот режим обычно служит для оказания помощи пользователям терминального сервера — администратор получает возможность наблюдать за чужим экраном и демонстрировать пользователю выполнение операций, вызвавших у него затруднение.

Подключение осуществляется через задачу управления терминальными сессиями исполнением соответствующей команды меню свойств. По умолчанию на такое подключение система запрашивает подтверждение у пользователя. Однако можно легко установить настройки, позволяющие подключиться и без такого согласия. Иными словами, администратор может подсмотреть этим способом за пользователем, причем последний не будет и подозревать о наличии такого контроля.

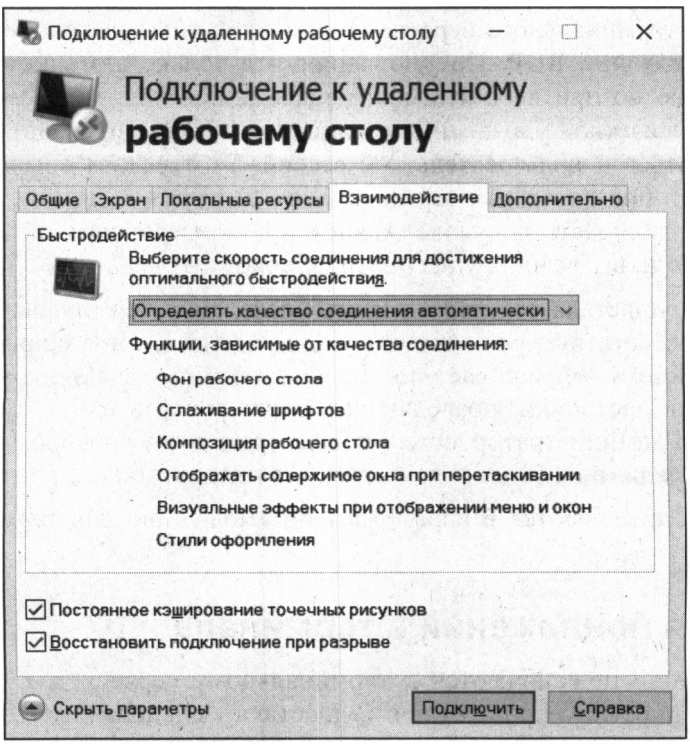
Эти настройки определяются в параметрах по умолчанию для терминальной сессии.

Публикация приложений в терминале

Часто пользователи подключаются к терминальному серверу для работы только в каком-либо конкретном приложении. Существуют специальные технологии публикации одного приложения, лидером таких решений являются продукты Citrix. Публикация приложения позволяет работать в нужной программе без ее установки на локальную систему.



а



б

Рис. 5.10. Подключение к удаленному рабочему столу:
а — настройка запуска в терминальной сессии заданного приложения в Windows 7;
б — настройка подключения к удаленному рабочему столу в Windows 10

Для терминалов Microsoft можно реализовать такие настройки подключения, которые внешне соответствуют подключению к одной задаче. В версии терминальных серверов Windows достаточно в свойствах подключения на вкладке **Программы** указать параметры вызываемой задачи (рис. 5.10, *а*). После этого при подключении пользователя к терминальному серверу автоматически запускается указанное приложение. Если пользователь завершает работу в приложении, то вслед за его закрытием прерывается и подключение к терминальному серверу.

Настройку запускаемого приложения администраторы обычно используют для таких пользователей, как бухгалтеры, — чтобы подключение к терминальному серверу для них воспринималось просто как запуск бухгалтерской программы «1С:Предприятие».

> ***Примечание***
>
> Запуск программы при подключении не сработает в Windows Server 2016/2022. О том, как реализовать подобное поведение, будет рассказано в *главе 8*. Кроме того, в современных версиях RDP-клиента вкладка **Программы** удалена (см. рис. 5.10, *б*). О том, как запускать программы в терминальной сессии в новых версиях Windows, также будет сказано в *главе 8*.

С появлением новой версии протокола подключения к терминальному серверу (начиная с Windows Server 2012) возможность указания запускаемого приложения появилась не только на клиентской стороне, но и на сервере. При этом технология подключения не изменилась. При подключении пользователя также полностью формируется терминальная сессия, и только после этого осуществляется запуск программы. Причем для клиентов, использующих предыдущую версию протокола (предыдущую версию программного обеспечения терминального клиента), просто

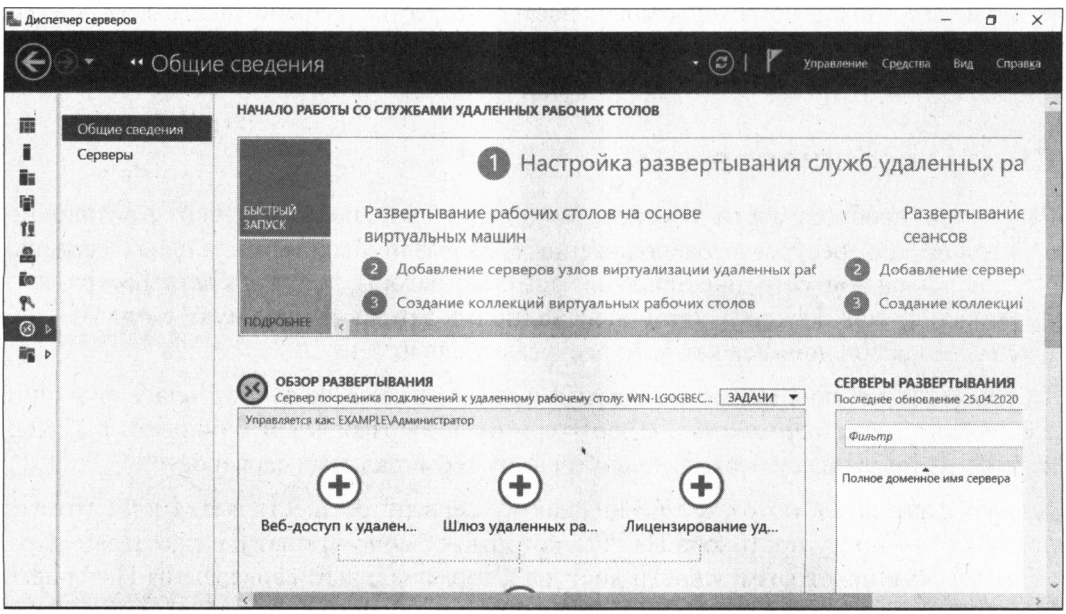


Рис. 5.11. Диспетчер серверов Windows Server 2022

открывается рабочий стол терминального сервера — параметры настройки подключаемого приложения игнорируются.

Настройка удаленных приложений (RemoteApp) в Windows Server 2019/2022 осуществляется через **Диспетчер серверов** (рис. 5.11).

Подробно о развертывании удаленных приложений вы можете прочитать замечательную статью «Настройка RemoteApp на платформе Windows Server 2012 R2»: **https://it-community.in.ua/2012/11/nastroyka-remoteapp-na-platforme-windows-server-2012.html**.

Веб-доступ к терминальному серверу

Веб-доступ к терминальному серверу появился в тот момент, когда программное обеспечение терминальных клиентов по умолчанию на рабочих станциях Windows не устанавливалось. Фактически это решение представляет собой модуль ActiveX, автоматически устанавливаемый на локальный компьютер при обращении из обозревателя к терминальному серверу. Соответственно, использовать для работы можно только Internet Explorer и необходимо иметь права и разрешающие настройки обозревателя для установки ActiveX. Реальное подключение к терминальной сессии осуществляется по протоколу RDP (Remote Display Protocol, протокол для удаленных дисплеев), что требует и открытого порта 3389.

По умолчанию веб-интерфейс доступен по пути: **http://<*имя_сервера*>/ts**.

Веб-интерфейс удобно использовать для разового доступа к необходимому приложению с компьютеров, не принадлежащих локальной сети. При постоянном использовании рациональнее ссылку на такое приложение сохранить на локальном компьютере. Администраторы могут настроить веб-интерфейс таким образом, что на нем будут опубликованы приложения с различных терминальных серверов внутри предприятия. Но это, конечно, решение уже для крупных предприятий.

Шлюз терминалов

Ранее при необходимости обеспечить подключение пользователей, работающих в Интернете, к ресурсам, расположенным на различных терминальных серверах внутри локальной сети предприятия, администраторы должны были настраивать публикацию для каждого терминала, а пользователи — вручную создавать несколько подключений для каждого ресурса отдельно.

Так было до тех пор, пока с выходом Windows Server 2008 не появилась функциональность *шлюза терминалов*. Шлюз терминалов позволяет публиковать в Интернете по одному адресу несколько внутренних терминальных серверов.

Доступ к шлюзу, а потом к терминальному серверу осуществляется клиентом по порту 443 — порту протокола HTTPS, который обычно открыт в межсетевых экранах. Это расширяет возможности доступа к терминальным серверам из Интернета. Регулируется доступ к внутренним терминалам обычным способом, с помощью политик.

Настройка шлюза терминалов не представляет особой сложности, и мы специально останавливаться на ней не будем.

Создание локальных копий данных

Пользователю, удаленно работающему с ресурсами предприятия, хочется выполнять работу так же быстро, как если бы он находился в офисе, и иметь возможность продолжить работу независимо от наличия удаленного доступа к офису. Выходом в такой ситуации является создание копий данных на мобильном устройстве с последующей их синхронизацией с сервером. Такое решение позволяет пользователю продолжать работу полностью в автономном режиме.

> ***Примечание***
>
> Первым средством Windows, предназначенным для синхронизации данных двух источников, была программа Портфель. Эта 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 Портфеле легко разобраться, воспользовавшись интерактивной справочной системой.

История файлов

В Windows 8/10/11 и Windows Server 2012/2016/2019/2022 появился аналог *машины времени* (Time Machine) из Mac OS X — функция **История файлов** (ранее History Vault). В Windows 7 уже имелась функция теневого копирования файлов, позволяющая восстановить содержимое файла, скажем, по состоянию на вчера или позавчера, что весьма удобно, ведь ошибочное удаление файла — явление достаточно редкое, а вот внесение некорректных изменений в файл встречается гораздо чаще.

В Windows 8/10/11 эта функция усовершенствована. Теперь вы можете выбрать, из каких каталогов файлы не требуется резервировать, где следует хранить резервные копии (предполагается, что их надо хранить на внешнем жестком диске или хотя бы на сетевом диске), как часто делать резервные копии.

Перед настройкой функции **История файлов** подключите внешний жесткий диск (можно и не внешний, но чтобы он был физически отдельным, — нет смысла хранить резервную копию на другом разделе того же жесткого диска — в случае сбоя диска все данные, в том числе и резервная копия, будут утеряны). Затем откройте панель управления и перейдите в раздел **Система и безопасность | История файлов**.

По умолчанию история файлов выключена (рис. 5.12). Для ее включения нажмите кнопку **Включить**. Если же у вас не будет подходящего для копирования жесткого диска, вы увидите соответствующее сообщение.

Как использовать историю файлов, показано в видеоролике от Microsoft: **https://windows.microsoft.com/ru-ru/windows-8/how-use-file-history**.

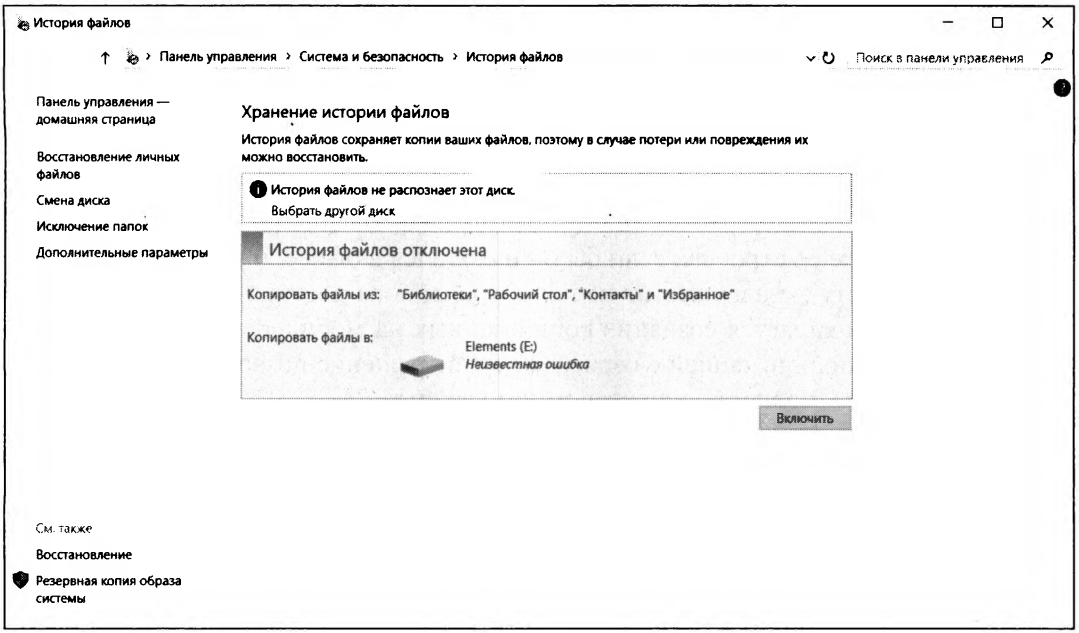


Рис. 5.12. История файлов выключена

Технология BranchCache

Технология BranchCache предназначена для ускорения работы с документами в филиалах за счет их кеширования. Технология эта появилась только в Windows 7 SP1 и Windows Server 2008 R2 соответственно и доступна она лишь пользователям домена, работающим в этих операционных системах или более новых (Windows 8/10/11, Windows Server 2012/2016/2019/2022). Информация о поддерживаемых версиях Windows доступна по ссылке: **https://docs.microsoft.com/en-us/sccm/core/plan-design/configs/support-for-windows-features-and-networks**.

Технология BranchCache позволяет кешировать в филиале информацию из основного офиса, предоставляемого с серверов Windows Server 2008 R2 или более поздних версий как по протоколу SMB (Server Message Block, блок сообщений сервера) — для обычных сетевых папок общего доступа, так и по протоколу HTTP/HTTPS — для веб-сервера IIS.

Существуют два варианта настройки технологии. Вариант *выделенного кеша* предполагает наличие в филиале сервера Windows 2008 R2/2012/2016/2019/2022, на котором хранится и обновляется кеш. В варианте *распределенного кеша* данные хранятся на пользовательских системах (Windows 7 SP1, 8, 10, 11). Выбор варианта осуществляется при настройке технологии (определяется в групповой политике), каждый из них имеет сильные и слабые стороны и должен быть выбран в зависимости от конфигурации филиала.

Если в общих чертах описать технологию BranchCache, то процесс происходит следующим образом. При запросе данных клиент сначала обращается на сервер

основного офиса (соответственно если этот сервер недоступен, то и воспользоваться кешированными данными, хранящимися в офисе, не удастся). Сервер предоставляет метаданные файла, т. е. его хеш-функцию (строго говоря, файл разбивается на блоки и контролируется именно хеш-функция блока). В силу особенностей работы IIS хеш-функция клиентом будет сформирована только при втором обращении к файлу по протоколу HTTP, и соответственно данные из кеша можно будет получить только при *третьем* обращении к этому файлу. При работе по протоколу SMB данные в кеше будут доступны при втором обращении к файлу. Клиент, получив хеш-функцию, проверяет наличие файла в филиале (широковещательным[1] запросом — в случае распределенного кеша и уникастовым — при хранении кеша на сервере). Если файл в кеше имеется, он передается с компьютеров филиала, если нет (или, например, обновлен на сервере, и хеш-функции не совпадают), то копируется по каналу связи «центральный офис — филиал». Естественно, что на каждом этапе проверяются права доступа к файлу.

В результате того, что хеш-функция примерно в две тысячи раз меньше размера файла, операции с ней по каналу связи между офисами выполняются существенно быстрее, чем копирование собственно данных. Но эффект от включения функции BranchCache будет лишь в том случае, если сами данные меняются редко, а обращения к ним с компьютеров филиала достаточно часты.

Для того чтобы включить BranchCache, следует добавить компонент **BranchCache** (**BranchCache для удаленных файлов** в случае файлового сервера) в настройках сервера и настроить групповую политику как для сервера, так и для клиентов. Дополнительно желательно — для повышения уровня защищенности данных — настроить для серверов использование сертификатов (описание доступно в документации по технологии).

Доступ из-за межсетевого экрана

Заблуждением является мнение, что межсетевой экран препятствует любой попытке подключения к персональному компьютеру извне. Если компьютеру разрешен доступ в глобальную сеть, то нельзя исключить и обратную возможность — подключение к нему из внешнего мира.

Мы не станем рассматривать возможности, использующие уязвимости межсетевых экранов. Они есть и будут. Но чтобы воспользоваться ими, нужно иметь серьезный опыт. Однако есть способы, доступные любому пользователю. На рис. 5.13 (из руководства LogMeIn) обычному пользователю доходчиво объясняются возможности его подключения к данным локальной системы из любой точки Сети.

Идея доступа к локальному компьютеру извне заключается в следующем. На этот локальный компьютер устанавливается программа, которая инициирует подключение к заданному серверу в глобальной сети. Поскольку такое подключение осу-

[1] Поэтому компьютеры должны находиться в пределах локального сегмента сети.

ществляется *изнутри* сети по разрешенным протоколам, то оно пропускается межсетевым экраном. Компьютер, с которого требуется подключиться к системе, защищенной межсетевым экраном, получает доступ к ней через сервер соответствующей программы. Обычно в этих целях применяется обозреватель Интернета (поскольку эта программа доступна в любых интернет-кафе и других публичных точках).

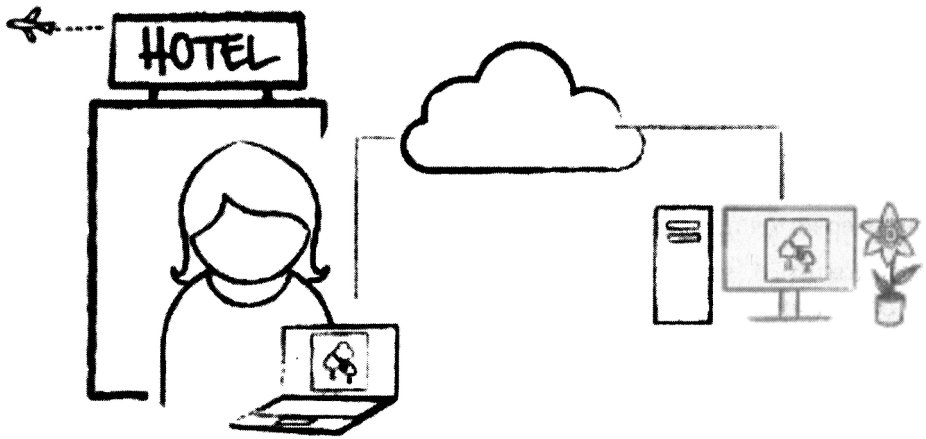
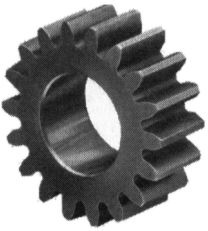


Рис. 5.13. Подключение к данным компьютера возможно из любой точки Интернета

Подобных решений существует много. Можно упомянуть бесплатное решение LogMeIn (**https://secure.logmein.com/solutions/personal/**), решение Anyplace Control (**http://www.anyplace-control.com/solutions.shtml**) и др. Поэтому блокирование на межсетевом экране списка таких серверов не решает кардинально проблему безопасности — не исключена возможность появления нового сервера или перехода на иное программное решение.

Предотвратить описанный способ нарушения безопасности информационной системы можно, если полностью исключить возможность установки пользователем приложений (тотальным контролем запускаемого программного обеспечения).



ГЛАВА 6

Управление информационной системой

Управление компьютерной информационной системой невозможно без инструментов, помогающих администратору выполнять различные рутинные операции. Обычно администратору нужно знать состав информационной системы, контролировать функционирование ее компонентов, а также централизованно управлять ими.

Состав информационной системы

К сожалению, документированию информационной системы редко уделяется должное внимание. Многие думают: мол, мне это не нужно, а те, кто будет после меня, — пусть разбираются сами. Поэтому новому администратору приходится тратить много усилий на инвентаризацию. Это в корне неправильно, поскольку, когда вы сами придете на новое место работы, вам тоже придется разбираться самостоятельно.

Что такое инвентаризация информационной системы? Это построение схемы сети, составление списка компьютеров, списка используемого программного обеспечения и прочего оборудования (принтеры, маршрутизаторы, коммутаторы и т. д.).

Построение топологии существующей СКС

Чтобы эффективно устранять неисправности, администратору нужно знать, к какому порту подключен тот или иной компьютер, как соединено между собой активное оборудование и т. п. Соответственно, администратор должен иметь документацию, содержащую описание линий связи, а также журналы кроссировок, журналы со сведениями о ремонтных работах и пр.

Если ваша структурированная кабельная сеть (СКС) построена на *управляемых* коммутаторах, то сведения о реальной топологии можно получить автоматически (вместе с информацией о портах и подключенном к ним оборудовании). Программ для построения топологии сети предостаточно. В предыдущем издании книги мы рекомендовали программу «10-Страйк: Схема Сети» в противовес программе LAN Flow, аргументируя тем, что она дешевле. Так, на момент подготовки предыдущего издания «10-Страйк: Схема Сети» стоила 3990 рублей, а программа LAN Flow —

$99. Сейчас же лучше рассмотреть именно LAN Flow. Во-первых, «10-Страйк: Схема Сети» подорожала, и теперь лицензия для одного компьютера стоит 7990 рублей (те же $99 по сути). Во-вторых, новую версию разработчики испортили «обновленным» интерфейсом, который не совсем корректно отображается (рис. 6.1). Впрочем, «10-Страйк: Схема Сети» позволяет построить схему сети по протоколу SNMP[1], чем не может похвастаться LAN Flow. В общем, теперь выбор программы не столь однозначен.

Рис. 6.1. Построение схемы сети в программе «10-Страйк: Схема Сети»

Инвентаризация физических каналов связи

Самая сложная задача — это инвентаризация кабельной инфраструктуры, особенно если сеть предприятия разветвлена. В идеальном случае у администратора должны быть кабельные журналы, содержащие перечни кабелей и списки соединений на коммутационных панелях. Однако часто такие журналы уже устарели, а реальные подключения администратор либо просто помнит, либо хранит информацию о них на различного рода записках.

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 значительное время, в течение которого

[1] Стандартный интернет-протокол для управления устройствами в IP-сетях на основе архитектур TCP/UDP.

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.

Существуют специальные программы, ведущие учет рабочих мест, соединительных кабелей и другого оборудования, позволяющие в случае необходимости быстро вывести всю информацию о пути соединения точки А и точки Б, а именно: номер розетки, кабель, номера коммутационных панелей и портов, на которые разведены кабели, и др. Первоначальный ввод в такие программы данных о размещении на чертежах рабочих мест и коммутационного оборудования, а также занесение данных о соединении портов и пр. выполняются 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 коммутационные шнуры. Коммутационные панели оснащаются дополнительными контактными площадками, специальные модули осуществляют сбор сведений о фактических подключениях и передают их в отдельную систему контроля. Примерами таких систем могут послужить решения PatchView компании RiT Technologies, технология Itracks, система iPatch Real Time Infrastructure Management от компании SYSTIMAX Solutions и др.

Подобные системы позволяют настроить схему подключений в автоматическом режиме и отслеживать ее изменения в режиме реального времени. Единственный их недостаток — стоимость. Прокладка дополнительных проводников стоит недорого, а вот программное обеспечение, сервер контроля, модули анализаторов стоят столько, что часто даже средние компании не могут себе их позволить.

Учет компьютеров и программ

Автоматическая инвентаризация программного обеспечения и оборудования для функционирующих систем не представляет большой сложности. Современные операционные системы позволяют собрать такие данные различными способами: через объекты операционной системы, через командный интерпретатор специального назначения WMIC (Windows Management Instrumentation Command-line) — см. о нем далее в этой главе — и т. п.

Данные о параметрах оборудования и программного обеспечения можно легко получить, используя, например, Центр администрирования Active Directory (рис. 6.2). Обратите внимание — он сообщает не только о состоянии компьютера сети, но даже и определяет версию установленной на нем операционной системы.

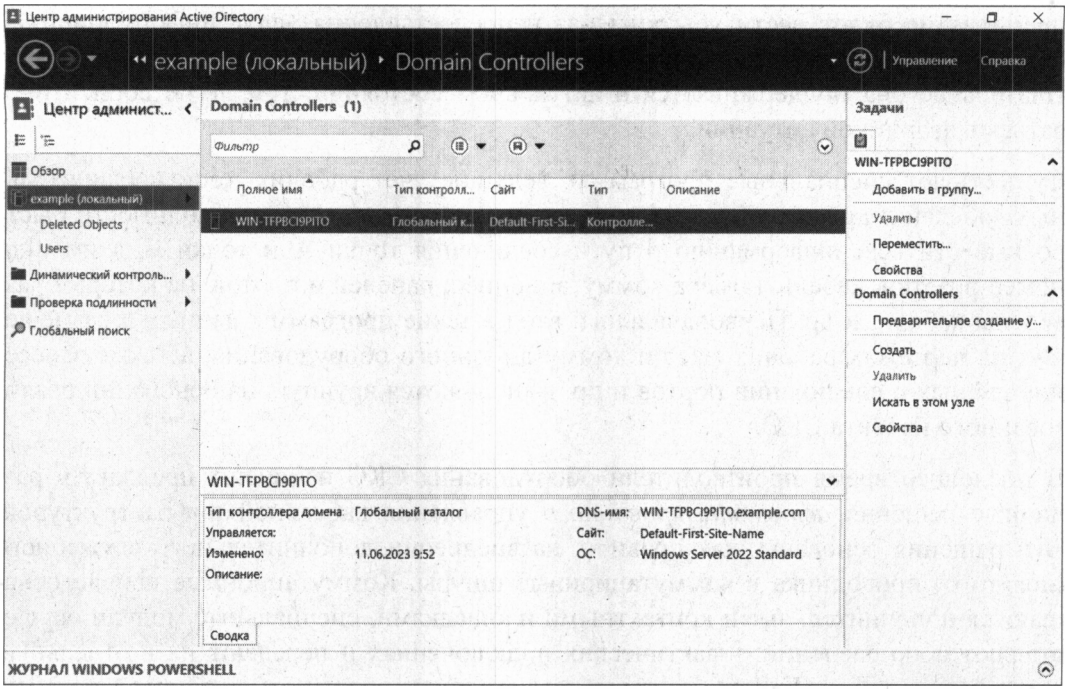


Рис. 6.2. Центр администрирования Active Directory Windows Server 2022: список контроллеров домена

Мониторинг функционирования ПО

Для администратора очень важно вовремя получить информацию о том или ином сбое в информационной системе. Для этого используются специальные системы мониторинга и информирования администратора о событиях в информационной системе. Такие системы описаны в *главе 7*.

Управление с помощью групповых политик

Самый эффективный способ управления компьютерной сетью, построенной на базе Windows-сетей, — это использование *групповых политик*. Групповые политики упрощают администрирование, предоставляя администраторам централизованное управление привилегиями, правами и возможностями как пользователей, так и компьютеров.

При помощи политики возможно:

- контролировать доступ к Windows-компонентам, системным ресурсам, сетевым ресурсам, утилитам панели управления, рабочему столу и экрану **Пуск**;
- автоматически устанавливать (разворачивать) программное обеспечение на компьютеры сети;
- создавать централизованно управляемые каталоги для специальных папок;

- настраивать права доступа к файлам и папкам (при использовании файловой системы NTFS);
- определять сценарии пользователя и сценарии компьютера, которые будут запускаться в конкретное время;
- ограничивать членство пользователей в группах безопасности;
- устанавливать параметры использования прикладного программного обеспечения;
- настраивать блокировку учетных записей, параметры паролей, аудита, назначения прав пользователей и безопасности.

О групповой политике можно думать как о ряде правил, которые помогают управлять пользователями и компьютерами. Групповые политики можно применить к нескольким доменам сразу, к отдельным доменам, к подгруппам в домене или к отдельным системам.

Политики, применяемые к отдельным системам, называются *локальными групповыми политиками*. Такие политики хранятся только на локальном компьютере. Остальные групповые политики соединены в объекты и хранятся в хранилище данных Active Directory.

Порядок применения множественных политик

Порядок применения множественных групповых политик следующий:

1. Локальные групповые политики.
2. Групповые политики сайта.
3. Групповые политики домена.
4. Групповые политики организационного подразделения.
5. Групповые политики дочернего организационного подразделения.

Если настройки политик конфликтуют, приоритет имеют настройки политики, которые применялись позже, — они перезаписывают более ранние настройки. Например, политики организационного подразделения имеют приоритет над политиками сайта.

Совместимость версий групповых политик

Поддержка групповых политик имеется только в профессиональных и серверных версиях Windows. Другими словами, если кто-то сэкономил и приобрел для предприятия домашние версии Windows, управлять ими с помощью групповых политик не получится.

Каждая новая версия Windows вносила свои изменения в групповую политику. Поэтому в некоторых случаях эти изменения делают бессмысленными старые политики на более новых версиях Windows. Одна и та же политика может корректно совместно работать только в определенных версиях Windows — например, в Windows XP Professional и Windows Server 2003.

Обычно большинство политик прямо совместимы. Это означает, что, как правило, политики, представленные в Windows Server 2003, могут использоваться на Windows 7 и более поздних, а также на Windows Server 2008 и более поздних. Однако политики для Windows 10/11 и Windows Server 2016/2019/2022 обычно неприменимы к более ранним версиям Windows.

Если политика неприменима к определенной версии Windows, то ее нельзя использовать на компьютерах, работающих под этими версиями операционной системы. Чтобы узнать, поддерживается политика на определенной версии Windows или нет, откройте окно ее свойств — там вы увидите поле **Поддерживается** или **Требования к версии** (рис. 6.3). В нем указаны версии ОС, на которых эта политика будет работать.

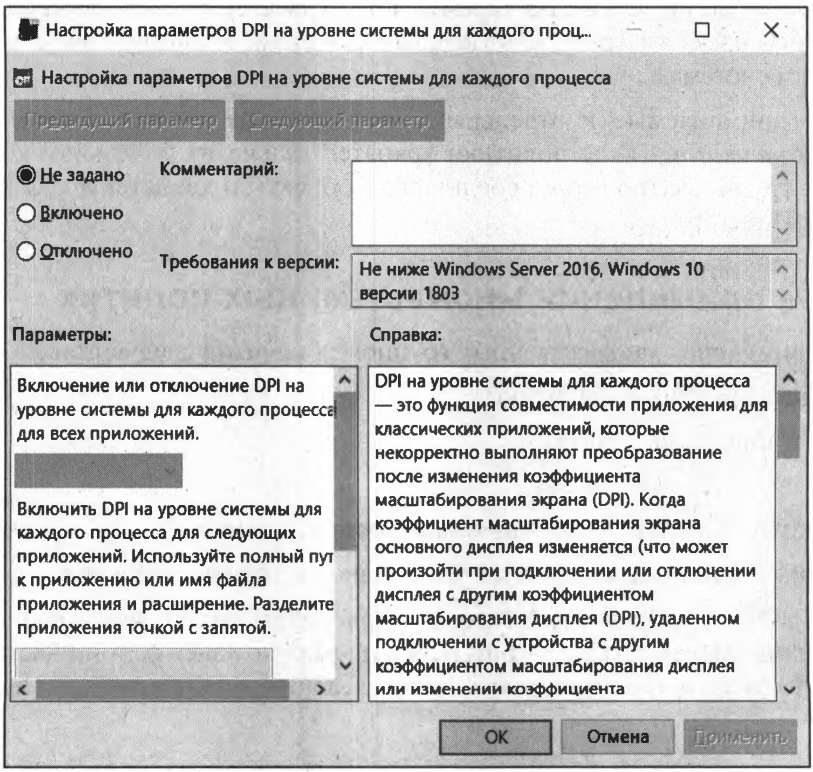


Рис. 6.3. Информация о версиях Windows, которые поддерживают ту или иную политику

Места хранения и условия применения групповых политик

Групповые политики хранятся в специальных файлах на контроллере домена. Каждая политика соответствует папке Policies с GUID-именем, содержащейся в каталоге Sysvol контроллера домена.

Внутри этой папки находятся две папки, соответствующие настройкам компьютера и пользователя. В каждой из них имеется файл Registry.pol, в котором и записаны

настройки политик (в сущности, политики — это параметры соответствующих ключей реестра системы). В структуре папки Machine содержится файл gpttmpl.inf. Этот файл включает в себя параметры опций безопасности раздела компьютера.

Там же хранятся и административные шаблоны — ADMX-файлы, представляющие собой XML-файлы конфигураций. Ранее вместо ADMX-файлов использовался старый формат — ADM-файлы. При желании можно преобразовать файлы старого образца в ADMX-формат. Заинтересовавшимся рекомендуем прочитать статью: **https://technet.microsoft.com/ru-ru/magazine/2008.01.layout.aspx**.

Настройки групповых политик, как уже было отмечено ранее, разделены на две категории:

- политики, применяемые к компьютерам;
- политики, применяемые к пользователям.

Политики компьютера обычно применяются во время запуска системы, а политики пользователя — во время входа в систему. Точная последовательность событий часто важна при поиске и устранении неисправностей поведения системы.

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, — это так называемое *фоновое изменение*. Если изменений не обнаружено, никаких действий не производится. Чтобы не создавать пиковую нагрузку на контроллеры домена, момент проверки наличия изменений случайным образом смещается на величину до получаса в ту или иную сторону. Если контроллер домена в момент проверки недоступен по причинам отсутствия связи с ним, то обновление политики будет проведено сразу после восстановления связи.

Политику можно обновить и вручную. Для этого следует выполнить команду:

```
gpupdate /force
```

В системах на базе Windows 8/10/11 необходимо использовать команду `secedit`:

```
secedit /refreshpolicy {machine_policy user_policy} /enforce
```

Для ускорения процесса возможно задать дополнительный ключ: `target`, сужающий область применяемой политики (компьютер или пользователь).

Некоторые настройки пользователя, например перенаправление папок, не могут быть обновлены, пока пользователь зарегистрирован в системе. Чтобы эти настройки вступили в силу, пользователь должен выйти из системы и снова в нее войти. Для автоматического выхода пользователя из системы после обновления можно ввести команду:

```
gpupdate /lofogg
```

Некоторые настройки компьютера могут быть определены только при его запуске. Для применения этих настроек компьютер должен быть перезагружен, что осуществляется командой:

```
gpupdate /boot
```

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. Иными словами, отключение политики осуществится безболезненно.

Вторая группа параметров задает значения *существующих* ключей реестра или создает такие ключи при первом применении. Суть в том, что такие параметры не будут удалены при снятии политики. В первую очередь это свойственно настройкам, импортируемым из файлов *административных шаблонов*.

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 для таких параметров значения по умолчанию, 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) этой 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.

Редактирование групповых политик

Групповые политики домена Windows Server 2016/2019/2022 можно создавать и редактировать как на серверах Windows Server 2016/2019/2022, так и с рабочих станций Windows 10/11.

Консоль редактирования групповой политики входит в состав сервера, но ее необходимо установить в Диспетчере сервера как дополнительный компонент управления групповыми политиками. Воспользуйтесь для установки компонента **Управление групповой политикой** мастером добавления ролей и компонентов. После этого оснастку **Управление групповой политикой** можно вызвать через меню **Средства** Диспетчера серверов.

Если необходимо управлять групповыми политиками с рабочей станции, то на компьютер сначала следует установить средства удаленного администрирования сервера (RSAT, Remote Server Administration Tool), которые бесплатно доступны со страницы: **http://go.microsoft.com/fwlink/?LinkId=130862**. Средства удаленного администрирования сервера позволяют администраторам управлять ролями и компонентами, которые устанавливаются на компьютерах под управлением Windows Server с удаленного компьютера под управлением Windows 10/11.

После установки RSAT нужно через панель управления включить новые компоненты: выполнить команду **Программы и компоненты | Включение или отключение компонентов Windows** и установить флажок **Средства управления групповыми политиками** по пути **Средства удаленного администрирования сервера | Средства администрирования возможностей**.

После этих операций в составе программ меню **Администрирование** появляется задача **Управление групповыми политиками**.

В оснастке **Управление групповой политикой** (рис. 6.4) четко видна иерархическая структура политик, с помощью которой удобно назначать («привязывать», создавать *линк*) 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 без подобного инструментария определить, какие параметры будут применены из создаваемой политики, крайне затруднительно.

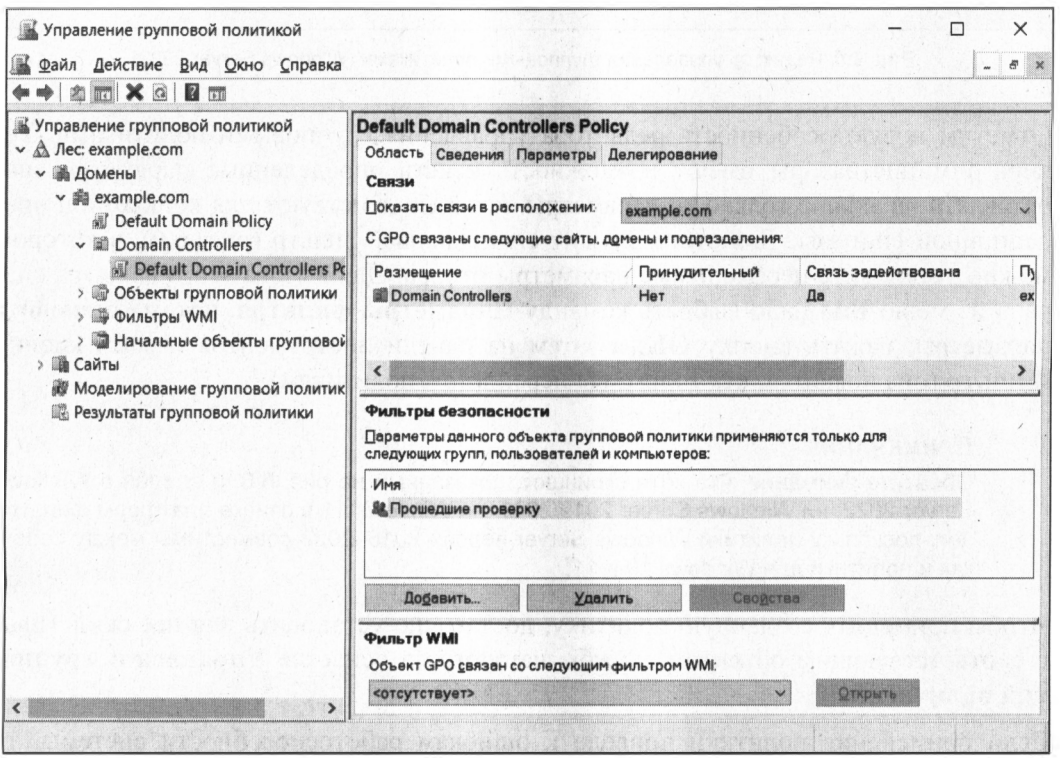


Рис. 6.4. Оснастка **Управление групповой политикой** (Windows Server 2022)

Групповая политика изменяется в редакторе управления групповыми политиками (рис. 6.5) — для этого достаточно выбрать команду **Изменить** в меню **Действия**. Новую групповую политику можно создать либо с нуля, либо скопировать в нее параметры уже существующей. Все зависит от конкретной ситуации.

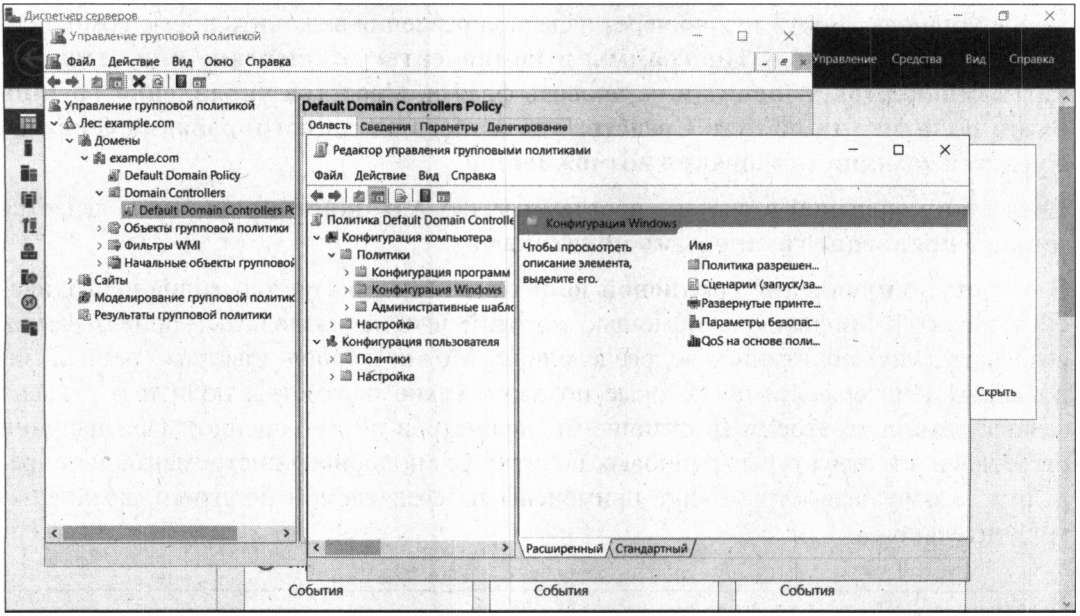


Рис. 6.5. Редактор управления групповыми политиками (Windows Server 2022)

Отметим новую особенность редактора управления групповыми политиками. Теперь администраторы имеют возможность искать определенные параметры или оставлять на экране только те параметры, которые действуют для конкретной операционной системы. Для этого служит специальный фильтр (рис. 6.6), в котором можно установить необходимые параметры отбора. Для вызова этого фильтра сначала из меню **Вид** надо выбрать команду **Параметры фильтра**, потом установить параметры, нажать кнопку **OK**, а затем на панели инструментов нажать кнопку **Фильтр** (она появится, как только вы перейдете к политикам).

> ***Примечание***
>
> Обратите внимание, что хотя скриншот, показанный на рис. 6.6, и сделан в Windows Server 2022, ни Windows Server 2019/2022, ни Windows 11 в списке платформ фильтра нет, поскольку политики Windows Server версий 2016–2022 совместимы между собой, как и политики для Windows 10 и 11.

Чтобы применить созданную политику, достаточно установить для нее связь (link) с соответствующим объектом службы каталогов в оснастке **Управление групповой политикой**.

Если применение политики привело к ошибкам работоспособности системы, то в некоторых ситуациях может помочь возвращение групповой политики к параметрам по умолчанию. На ПК с Windows Server 2008/2022 это можно сделать с помощью утилиты `dcgpofix`. Подробности ее работы можно получить, выполнив команду:

```
dcgpofix /?
```

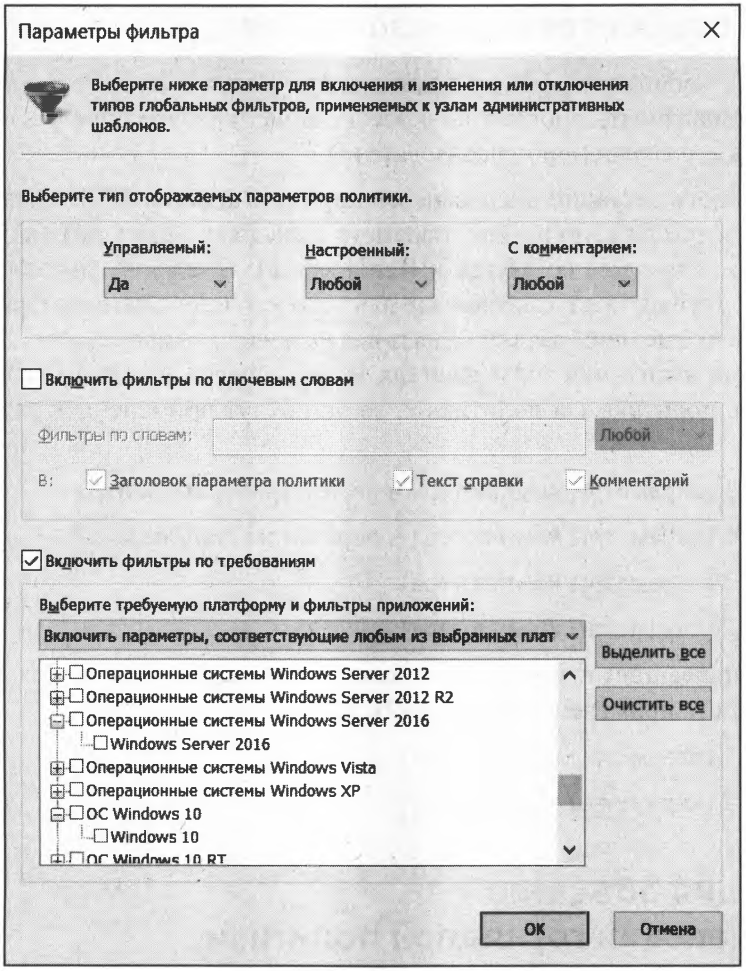


Рис. 6.6. Настройка параметров фильтра редактора групповой политики (Windows Server 2022)

Начальные объекты групповой политики

Начальные объекты групповой политики (GPO) — это наборы настроек, предоставленные вендором. Они предназначены для быстрой настройки рабочих станций под управлением Windows 10/11.

Начальные GPO включены в состав Windows Server 2008 R2 (и более новых версий) и Windows 7 (и более новых версий) с RSAT и предназначены для настройки компьютеров по конфигурациям Enterprise Client (Предприятие) и Specialized Security Limited Functionality (Специализированная безопасность с ограниченной функциональностью). Описание этих конфигураций доступно по ссылкам:

- **http://go.microsoft.com/fwlink/?LinkID=121852**;
- **http://go.microsoft.com/fwlink/?LinkID=121854**.

«Обход» параметров пользователя

Иногда нужно «обойти» политику пользователя. Например, на сервере терминалов не нужно устанавливать программное обеспечение, которое определено групповыми политиками для каких-либо пользователей.

Именно для таких ситуаций предназначен параметр **Loopback** (Замыкание на себя) свойств групповой политики. Этот параметр позволяет задать два варианта «обхода» политики пользователя: **Merge** и **Replacement**. В первом случае система применяет все политики, предусмотренные для того или иного компьютера и пользователя, после чего еще один раз применяет *все политики компьютеров*. Другими словами, если для каких-либо пользователя и компьютера должны быть применены две политики: политика 1 и политика 2, то они будут применены в следующем порядке:

1. Политика 1 (параметры компьютера и параметры пользователя).
2. Политика 2 (параметры компьютера и параметры пользователя).
3. Политика 1 (параметры компьютера).
4. Политика 2 (параметры компьютера).

В режиме **Replacement** используются только параметры компьютера, поэтому последовательность применения политики будет такова:

1. Политика 1 (параметры компьютера).
2. Политика 2 (параметры компьютера).

Фильтрация объектов при применении групповой политики

Групповые политики привязываются к контейнерам службы каталогов. Обычно в подразделение объединено много систем, и если необходимо выполнить настройку групповыми политиками только части систем, то приходится применять дополнительные настройки.

Самый простой способ состоит в создании дополнительной структуры службы каталогов (дополнительные подразделения) и привязке к ним соответствующих групповых политик. Но при большом числе задач такое решение неоправданно увеличит сложность структуры каталогов.

Выделить из всего состава часть систем для применения политики можно несколькими способами:

- настройкой WMI-фильтров;
- настройкой параметров безопасности для групповой политики;
- настройкой *нацеливания на элемент* для параметров **Настройки**.

Фильтрация при помощи WMI-запросов

Существует возможность уточнять область применения политики на основе WMI-фильтров. Администратор, знакомый с основами программирования и использования WMI (см. *разд. «Windows Management Interface» далее в этой главе*), может создать фильтры применения политики, учитывающие любые параметры конфигурации систем (как аппаратного, так и программного обеспечения).

При помощи фильтров можно выполнить сколь угодно точную фильтрацию, однако интерфейс назначения фильтров в групповой политике не содержит никаких средств проверки правильности запроса (это можно сделать уже при моделировании или проверке результирующих значений). Поэтому, чтобы исключить ошибки в настройках, WMI-запросы должны быть предварительно проверены другими средствами.

Настройка параметров безопасности групповых политик

Фильтровать доступ к групповой политике можно с помощью настройки ее параметров безопасности — достаточно соответствующим образом определить те группы (или пользователей), которые будут иметь или не иметь право доступа к настройкам и установке групповой политики.

Метод не требует дополнительных разъяснений. Но фактически при его использовании мы вместо усложнения структуры каталогов создаем соответствующую структуру групп безопасности.

Предпочтения групповых политик

В групповых политиках, начиная с Windows Server 2008, появился дополнительный раздел — **Предпочтения**. Параметры этого раздела позволяют управлять подключением дисков, параметрами реестра, локальными пользователями и группами, службами, файлами и папками.

Главное преимущество раздела **Предпочтения** — легкость назначения параметров без обращения к каким-либо сценариям, составлению сложных запросов и т. д. Это позволяет, с одной стороны, облегчить настройку групповой политики, с другой — упростить структуру службы каталогов, поскольку не понадобится создавать дополнительные контейнеры для выборки компьютеров.

Для работы в разделе **Предпочтения** не требуется знать языки программирования, правила составления запросов в них и т. п. — все операции проводятся при помощи графического интерфейса. При этом возможности отбора крайне велики.

На рис. 6.7 изображен **Редактор нацеливания**, облегчающий настройку предпочтений. Если вы этим заинтересовались, рекомендуем к прочтению статью: **http://habrahabr.ru/post/206744/**.

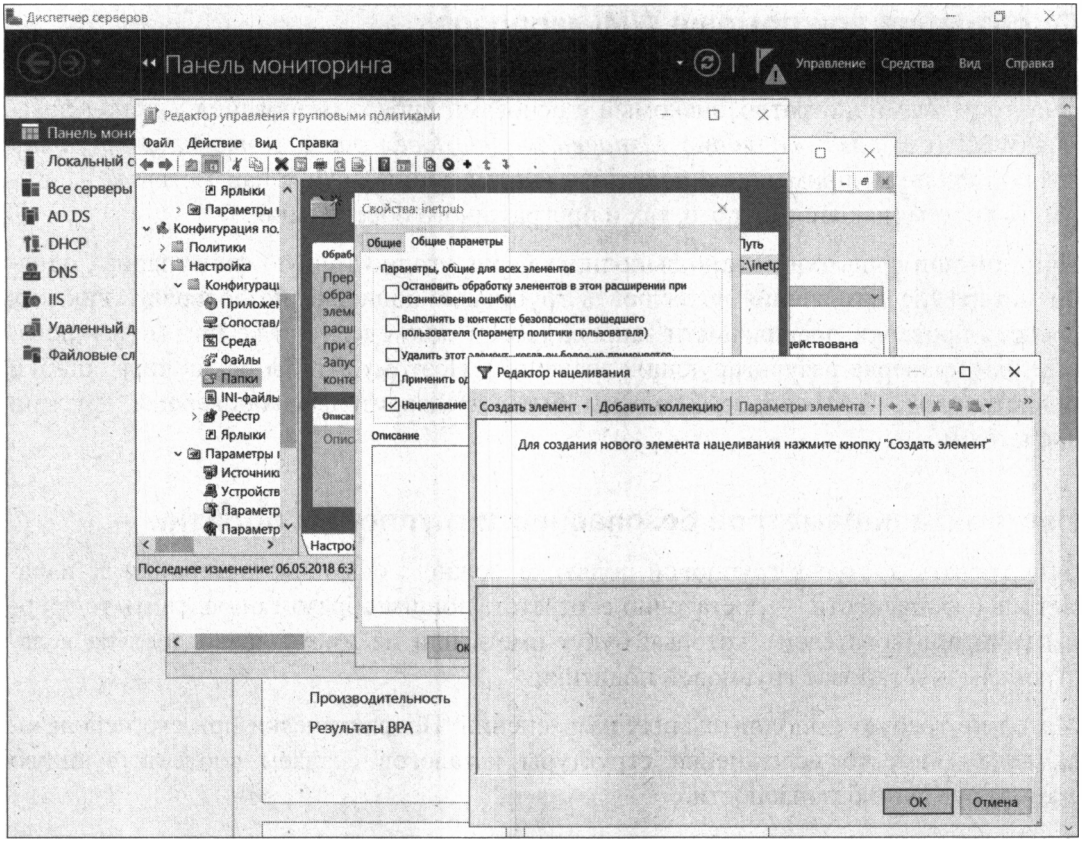


Рис. 6.7. Редактор нацеливания

Рекомендации по применению политик

Главная рекомендация состоит в том, чтобы *не изменять политику по умолчанию*. Если в политике возникнет какая-либо серьезная ошибка, то возврат к начальному состоянию приведет к удалению не только последних настроек, но и всех других параметров, тщательно настраиваемых в течение долгого времени.

Поэтому для основных административных действий по управлению системой создавайте *новые политики*. Тогда для изменения настроек вам будет достаточно только отключать/включать привязку политик к организационной структуре.

При настройке параметров политик ориентируйтесь на рекомендуемые значения для конфигураций предприятия (см. *разд. «Начальные объекты групповой политики» ранее в этой главе*).

Обработка одной политики с большим числом назначенных параметров практически не отличается по времени от обработки нескольких политик, в каждой из которых назначается только часть этих параметров. Поэтому удобнее создавать несколько политик, чем включать все изменения в одну.

Не удаляйте созданные ранее групповые политики — просто отключите привязку их от объектов службы каталогов. Они могут понадобиться для анализа ситуации в случае обнаружения каких-либо проблем в дальнейшем.

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.

Блокирование запуска нежелательных приложений с помощью компонента AppLocker

Начиная с Windows 7, для предотвращения запуска нежелательных программ применяется компонент AppLocker, а не политики ограниченного использования программ, как было ранее.

Запуск нестандартного или неутвержденного программного обеспечения может изменить желаемое состояние программной конфигурации обычного настольного компьютера. Пользователи могут загрузить новые программы из Интернета, принести их с собой на сменных носителях, получить программы через torrent-сети и/или по электронной почте. Все это приводит к росту числа обращений к администратору, а также к увеличению числа случаев заражения компьютера вирусами и вредоносными программами. Каждый простой, связанный с неправильной работой системы после установки стороннего программного обеспечения, снижает эффективность работы предприятия в целом. Именно поэтому многие предприятия стремятся тщательно контролировать рабочую среду компьютеров своих пользователей, используя различные схемы блокировки, в том числе ограничение использования учетных записей с правами администратора.

Если пользователь работает в системе с обычными правами, а не с правами администратора, то и внести изменения в программную конфигурацию у него не получится, поскольку он не имеет права устанавливать программы. Однако не нужно забывать, что пользователь может загрузить и запустить так называемые Portable-версии программ, которые иногда содержат вредоносный код.

В Windows XP и Windows Vista использовались политики ограниченного использования программ (SRP), которые предоставляли администраторам механизм для определения и обеспечения выполнения политик управления приложениями.

Однако в сложной динамичной среде, где установка и обновление приложений выполняются очень часто, управление SRP становится неудобным, поскольку политики управления приложениями интенсивно используют правила для хеша. Соответственно администратору приходится создавать правила хеша при каждом обновлении приложения.

Компонент AppLocker предоставляет простой и гибкий механизм, позволяющий администраторам точно определять приложения, которые разрешено запускать на компьютерах предприятия.

С помощью AppLocker администратор может:

- предотвращать выполнение уязвимых и заблокированных приложений, в том числе вредоносных программ;
- предотвращать запуск нелицензионного программного обеспечения, если таковое явно не внесено в список разрешенных;
- запретить запуск программ (тех же torrent-клиентов), оказывающих негативное влияние на все предприятие, — например, «узурпирующих» всю пропускную способность сети;
- запретить запуск программ, нарушающих стабильное функционирование настольной системы.

Компонент AppLocker предоставляет два действия: разрешение и запрет, а также позволяет определить исключения из этих действий, — вы можете создать список разрешенных и запрещенных программ.

Если ваше предприятие нуждается в подобном компоненте, рекомендуем ознакомиться со следующими статьями, в которых компонент AppLocker рассматривается более подробно:

- **https://technet.microsoft.com/ru-ru/library/dd548340(v=ws.10).aspx**;
- **http://www.oszone.net/11303/AppLocker**.

Некоторые особенности политики установки 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.

При работе с такими политиками администратору необходимо учесть следующее.

- 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 представляет собой текстовый файл с описанием особенностей предполагаемой установки. Формат файла описан в документе KB231747. Мы просто процитируем часть этой 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.
- В-третьих, установка программ может быть включена в политику как в раздел **Компьютер**, так и в раздел **Пользователь**. В первом случае установка программ будет проведена на систему, и 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 **Установ-**

ка/удаление программ в панели управления. В случае использования *назначенных программ* в меню **Пуск** системы появляется ярлык к ним, при первом вызове которого осуществляется установка соответствующего программного обеспечения.

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 администратору легко 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.

Обычно административные шаблоны копируются на локальный диск после установки соответствующего программного обеспечения. Поэтому администратору для добавления нового шаблона достаточно открыть для изменения групповую политику (с компьютера, на котором установлено приложение) и выполнить операцию добавления нового шаблона. Другой способ — загрузить административные шаблоны с сайта разработчика (если они там предоставлены) и импортировать их в политику.

В завершение следует настроить необходимые параметры и привязать групповую политику к соответствующему подразделению.

Утилиты группового управления

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.

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 предприятиях управление сетью строится на использовании отдельных, не интегрированных друг с другом комплектов.

Существует много средств, облегчающих выполнение административных задач. Часть из них мы упомянем в этой книге. Но, естественно, каждый системный администратор будет применять только продукты, оптимально подходящие для конфигурации его парка оборудования. Читатель должен понимать, что в объеме одной книги невозможно даже привести перечень всех таких продуктов. Авторы попытаются показать прежде всего спектр таких программ, основываясь на некотором опыте работы с ними.

Средства поддержки пользователей

Одной из задач администрирования информационной системы является оказание пользователям технической поддержки. Обычно в этих целях используются программы доступа к рабочему столу.

> ***Примечание***
>
> Технологии, описываемые в следующих разделах, могут быть использованы только на *работоспособной операционной системе*.

Удаленный помощник

Удаленный помощник (режим удаленного подключения к рабочему столу) предназначен для оказания помощи пользователю компьютера, чтобы в случае возникновения проблем в работе он имел возможность обратиться к специалисту, а тот, подключившись к его компьютеру, мог оперативно оказать ему посильную помощь. Параметры вызова помощника могут быть определены централизованно в групповой политике.

Чтобы перейти в этот режим, предусмотрен специальный механизм отправки приглашений на удаленное подключение. При подключении удаленного помощника рабочий стол виден одновременно обоим: самому пользователю и тому помощнику, который принял приглашение.

Первоначально 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.

Для запуска удаленного помощника (рис. 6.8) в Windows 7 нужно нажать кнопку **Пуск** и ввести команду `Удаленный помощник`. В Windows 10/11 после нажатия кнопки **Пуск** надо ввести команду `MsrA`.

В случае необходимости (этот вариант доступен в Windows 7/10/11) администратор может сам инициировать предложение помощи. Команда `msra` (ее можно запомнить как аббревиатуру от MS Remote Assistance):

```
msra /offerRA <имя удаленного компьютера>
```

позволяет запустить помощника и инициировать сессию на удаленной системе. Такой способ очень удобен при оказании поддержки неопытным пользователям, которым будет сложно объяснить по телефону процедуру запроса помощи. 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 через систему 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.

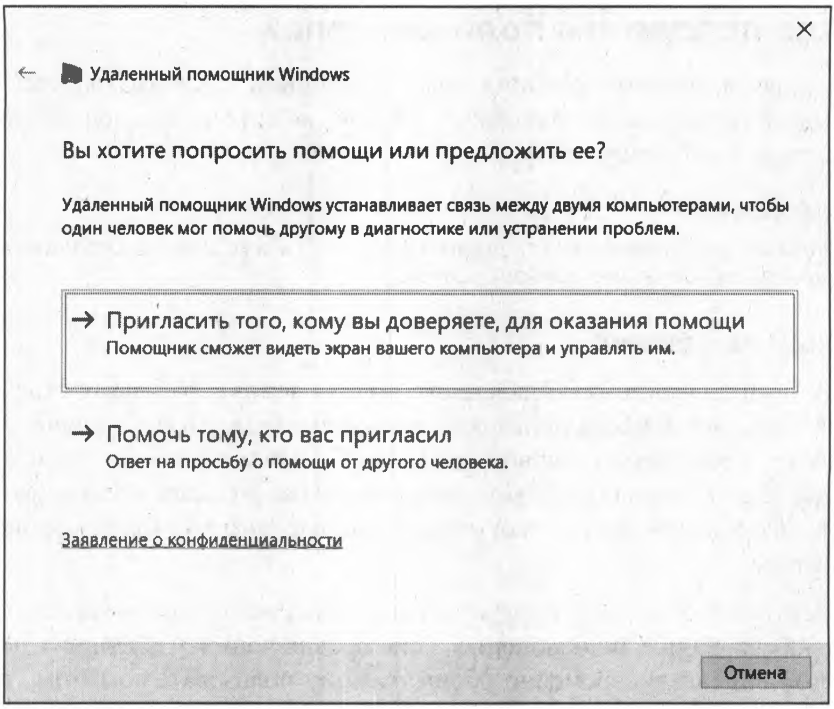


Рис. 6.8. Удаленный помощник

Утилиты подключения к рабочему столу

Хотя в рабочих станциях с ОС Windows присутствует возможность удаленного подключения к рабочему столу, на практике она редко используется администраторами. Во-первых, соответствующие опции должны быть предварительно включены в настройках клиентского компьютера (это, конечно, можно сделать и централизованно), во-вторых, при попытке удаленного подключения текущий пользователь отключается от экрана. Администратор может только посмотреть, но не показать пользователю, что и как нужно выполнить.

Поэтому администраторы применяют ту или иную программу, позволяющую увидеть удаленный рабочий стол на локальном компьютере и перехватить управление клавиатурой и мышью.

Существует большое количество таких программ: как бесплатные версии (UltraViewer, VNC), так и коммерческие (TeamViewer от TeamViewer GmbH, pcAnywhere[1] от компании Symantec, Remote Admin от Famatech Inc., NetOp Remote Control от DanWare Data и пр.). Выбор конкретной программы определяется возможностями администратора.

В любом случае для управления удаленным компьютером программой такого класса на него должна быть установлена ее клиентская часть. Эта операция может быть

[1] Последняя версия программы позволяет администратору удаленно управлять как системами на основе Windows, так и Linux-компьютерами.

проведена централизованно любым способом. Приведем описание возможностей некоторых программ управления удаленным компьютером[1].

- VNC (Virtual Network Computing, **www.realvnc.com**) — дает возможность удаленно просматривать любые платформы (UNIX, Win32, Mac, мобильные клиенты и т. п.). Это кросс-платформенное 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 (периодически обновляемый список наиболее успешных компаний).

- Hidden Administrator (**www.hidadmin.ru**) — 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 одна часто используемая программа удаленного управления для платформы Windows. 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.

- TeamViewer — программа чем-то похожа на RAdmin и является, наверное, самой популярной программой для удаленного доступа. Для некоммерческого использования программа бесплатна. Имеется поддержка Windows, macOS, Linux. Программа гораздо проще в использовании, чем RAdmin, что понравится начинающим пользователям, кроме того, она не требует установки. Поскольку программа работает через порт 80, то понравится и многим администраторам, поскольку это стандартный порт веб-сервера и он не блокируется брандмауэрами, — следовательно, для использования этой программы не придется вносить изменения в конфигурацию брандмауэра. Имеется возможность организации интерактивных конференций — вы можете собрать целый консилиум для обсуждения проблемы с компьютером (поддерживается до 25 участников).

- UltraViewer (**https://www.ultraviewer.net**) — эта программа работает по такому же принципу, что и TeamViewer: удаленный пользователь сообщает вам ID компьютера и сгенерированный программой пароль, вы вводите эти данные на своем компьютере и получаете удаленный доступ к компьютеру пользователя, которому нужна помощь. Для персонального использования (один пользователь и одно устройство) программа навсегда бесплатна, и для нашего личного использования она давно вытеснила TeamViewer, которая в коммерческом варианте стала, во-первых, очень дорогой, а во-вторых, сейчас не продается для российских пользователей.

---

[1] Следует учитывать, что часть антивирусных программ рассматривает утилиты удаленного управления в качестве вредоносного кода.

- Skype — при желании совместно с ним можно использовать режим демонстрации рабочего стола. В этом случае человек, оказывающий помощь по настройке компьютера, будет говорить, что делать, а выполнять операции придется самому пользователю. Но, учитывая, что Skype установлен очень у многих (а в Windows 10 он вообще присутствует по умолчанию) и бесплатен, то этот вариант не нужно сбрасывать со счетов.

Средства автоматизации — сценарии

Управление в режиме консоли, хотя и требует от администратора наличия опыта работы, привлекательно тем, что позволяет полностью автоматизировать процесс, например выполнять заданные операции по расписанию.

При изучении правил использования сценариев могут помочь следующие ресурсы:

- Script Center, **http;//technet.microsoft.com/en-us/scriptcenter/default**;
- центр технологий Windows PowerShell, **http://go.microsoft.com/fwlink/?LinkID=102372**;
- блог Windows PowerShell, **http://go.microsoft.com/fwlink/?LinkID=128557**;
- Windows PowerShell Script Repository, **http://go.microsoft.com/fwlink/?LinkId=169615**.

Использование командной строки

Несмотря на то что командная оболочка включает не так уж и много операций, с ее помощью опытный администратор может автоматизировать многие процессы. Чаще всего командные сценарии используются администраторами для настройки параметров входа в систему.

Обратите внимание, что командный интерпретатор может выполнять циклы, анализировать условия, «разбирать» текстовые файлы и т. д. Если среди команд нет тех, которые выполняют нужные операции, можно использовать внешние утилиты и обрабатывать код их завершения. Например, для анализа членства пользователя в группе службы каталогов можно применить утилиту ifmember (доступна с сайта Microsoft) и проанализировать ее результат. Приведем пример такого блока сценария командной строки:

```
:sales
ifmember "sales"
if not errorlevel 1 goto ops
net use q: \\server\share
GoTo NextSection
```

Примеры использования командных сценариев доступны в Интернете.

Сценарии Visual Basic

В Windows возможно выполнение сценариев, написанных на таких языках программирования, как VBScript, JScript и JScript.NET. Использование этих языков программирования оправдано в тех случаях, когда нужно проанализировать параметры приложений, членство в группах, создать файлы отчетов, создать интерфейс программы и т. п. Иными словами, с их помощью создается новая программа для компьютера.

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 — такие как Perl, TCL, REXX, Python и пр. Для этого необходимо установить соответствующие модули интерпретаторов разработки третьих фирм.

WSH поддерживается всеми современными версиями Windows. Каждая последующая версия WSH существенно функциональнее предыдущей, поэтому для систем, находящихся в эксплуатации, целесообразно обновить эту службу до последней версии.

Как правило, администраторы редко создают нужные сценарии с нуля. Обычно ищется подходящий пример, который лишь незначительно модифицируется. По-

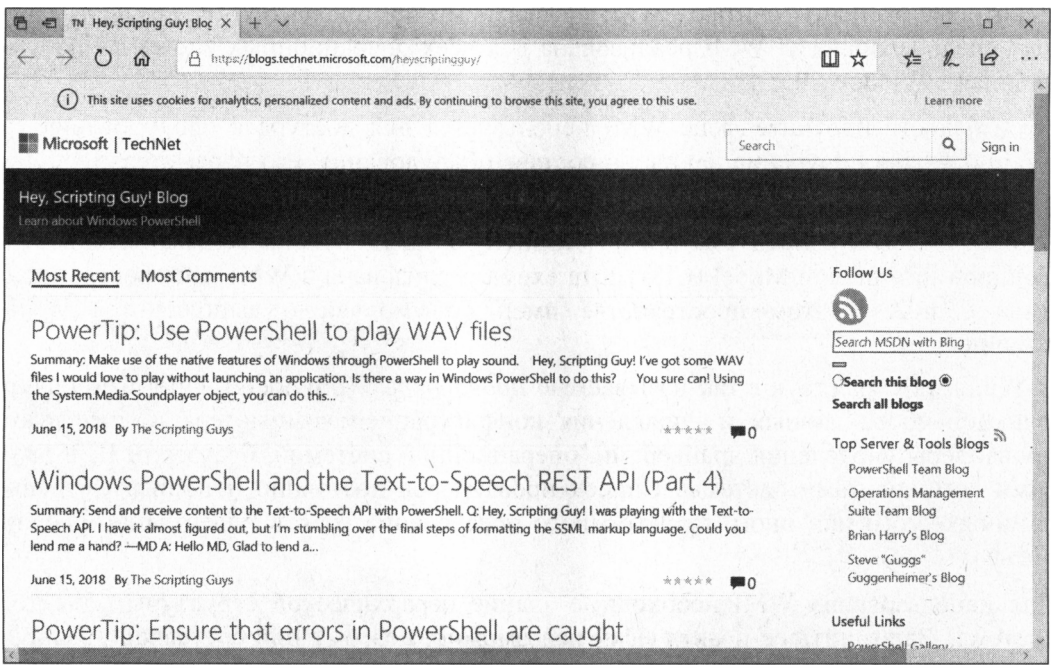


Рис. 6.9. Блог **Hey, Scripting Guy! Blog**

добные коды достаточно широко представлены в Сети, а на сайте разработчика Windows можно воспользоваться ресурсами блога **Hey, Scripting Guy! Blog** (рис. 6.9) по адресу: **http://technet.microsoft.com/ru-ru/scriptcenter/default.aspx**.

Интерфейс IPMI

Стандарт IPMI (Intelligent Platform Management Interface) разработан для описания требований по управлению компьютерными платформами, а точнее — серверами. Серверы, поддерживающие IPMI, могут управляться удаленно с консоли.

Администратор может удаленно включать, выключать и перезагружать такой сервер, независимо от состояния операционной системы, а также удаленно производить обновление BIOS и контролировать основные рабочие параметры сервера (температуру процессора, уровни напряжения и пр.).

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.

Интерфейс WMI

Интерфейс WMI (Windows Management Interface) — это технология управления Windows-компьютерами, реализующая стандарты веб-управления предприятием (WBEM, Web-based Enterprise Management), разработанные компанией Distributed Management Task Force (**http://www.dmtf.org/**).

Некоторые эксперты считают WMI «развитием» протокола SNMP для программных сред. Технология WMI реализована для всех операционных систем Windows, начиная с Windows 95.

Преимущественно интерфейс WMI используется для доступа к оборудованию, а именно — для получения данных о составе оборудования, его параметрах, состоянии и пр.

Стандарт WBEM предусматривает типичную схему управляемых объектов — Common Information Model (CIM). Эта схема реализована в WMI как пространство имен Cimv2. В этом пространстве имен по умолчанию выполняются WMI-команды.

В Windows существуют так называемые *провайдеры* (providers). Они выполняют функции сбора данных и управления конфигурацией компьютера. Существуют провайдеры управления драйверами, операционной системой, браузером IE и другими компонентами системы. Список провайдеров постоянно пополняется и при установке того или иного программного обеспечения может существенно расшириться.

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, или другие продукты просмотра WMI (WMI Command-line Tool, WBEMTest.exe и др). С помощью такой

программы администратор имеет возможность подключиться к любому пространству имен, зарегистрированному в системе, отобразить существующие классы объектов, увидеть свойства класса (те характеристики, которые можно получить при исполнении запроса) и методы (те параметры, которые можно установить в команде), выявить существующие экземпляры. Здесь же можно открыть окно, в котором попробовать создать собственный WMI-запрос и сразу увидеть его результаты. Средства среды разработки WMI Administrative Tools удобны тем, что наряду с просмотром существующих на компьютере классов WMI-администратор может получить значения реальных объектов, составить и отладить WQL-запросы.

Язык запросов WMI Query Language

Практическое использование интерфейса WMI для получения данных о состоянии оборудования или программной среды во многом напоминает работу с базой данных — вам необходимо указать, какие параметры должны быть получены от какого объекта и при каких ограничениях (фильтрах). Язык запросов для WMI так и называют — WMI Query Language (WQL). Даже команды WQL принято называть *запросами*. Запросы WMI обрабатываются в специальном интерпретаторе — wmic (WMI Command-line tool). Объекты WMI доступны и для использования в Visual Basic, что позволяет составлять любые сценарии.

После запуска интерпретатора 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 таком режиме необходимо четко представлять, в каком классе находится объект, характеристики которого вы хотите получить, или в настройки которого предполагается внести изменения.

Язык 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 этого элемента методы управления, провести желаемые изменения.

Варианты применения WMI

Существуют различные методы использования возможностей интерфейса WMI.

Для автоматизации управления компьютерными системами доступ к WMI может быть реализован через Windows Scripting Host. Это позволяет администратору создавать сценарии управления системами. Вы можете запросить характеристики какого-либо объекта с помощью языка WQL и изменить значения некоторых из них, присвоив новые величины параметрам выбранного объекта.

Определенную помощь в представлении о структуре классов WMI может оказать программа **WBEMTest.exe**, имеющаяся на каждом компьютере с установленным WMI. Используя эту программу, можно просмотреть 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 уже упомянутая ранее программа CIM Studio, которая может быть свободно загружена с сайта Microsoft.

> ***Примечание***
>
> Те, кто использует в своей работе Microsoft Visual Studio.NET, могут применять входящие в ее состав утилиты. Если ни одна из упомянутых программ по каким-либо причинам вас не устраивает, то в Интернете легко можно найти и другие утилиты.

Примеры WMI-сценариев

Большинство практических WMI-сценариев создаются на основе того или иного примера, который найден в Интернете. Приведем несколько возможных вариантов WMI-сценариев.

- **Вывод перечня 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 сценарий (третья его строчка) 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 этого сценария можно установить автоматический запуск через определенные промежутки времени, чтобы гарантировать работу всех служб компьютера. 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.

PowerShell

PowerShell представляет собой средство, разработанное Microsoft для автоматизации различных задач и состоящее из интерпретатора и языка высокого уровня. PowerShell входит в состав Windows 7/8/10/11 и Windows Server 2012/2016/2019/2022, но также может быть загружен и для предыдущих версий. Язык PowerShell реализован на Microsoft .NET Framework и интегрирует в себя доступ к WMI, COM и ADSI.

Сценарии PowerShell составляются из *командлетов* (cmdlet). Командлет объединяет в себе команду и объект, над которым она выполняется, и обычно называется по принципу глагол-объект. Например, командлет Get-Content возвратит (`get`) содержимое (`content`) того элемента, который будет указан в параметрах. Так, команда `Get-Content c:\test.txt` выведет на экран содержимое файла c:\test.txt.

PowerShell поддерживает перенаправление вывода, которое получило в его интерпретаторе название *конвейера*. Поддерживаются регулярные выражения, обработка условий — в общем, все те функции, которые присущи современным языкам программирования.

Например, следующий сценарий выведет на экран список созданных в течение последнего дня файлов:

```
get-childitem c:\ -R |? {$_.creationtime -gt $(get-date).adddays(-1)}
```

Первый командлет возвращает список всех файлов на диске C: (ключ `R` выполняет рекурсивный поиск), полученные данные передаются на обработку, сценарий выбирает параметр `creationtime` (дату создания) и сравнивает его с текущей датой минус 1 день. Этот сценарий можно модифицировать — например, изменить маску и выбирать файлы журналов (`-Filter*.log`), сменить условие (меньше — `lt`) и перенаправить вывод на команду удаления (`% {del $_}`). Таким образом можно автоматически удалять с компьютера устаревшие журналы, если эту команду настроить на автоматическое выполнение.

Помимо командной строки интерпретатора в последних версиях PowerShell появилась и графическая среда — интегрированная среда сценариев ISE (Integrated Script Environment) Windows PowerShell. Это приложение, в котором можно выполнять команды PowerShell, создавать, тестировать и отлаживать скрипты с использованием удобного графического интерфейса (рис. 6.10).

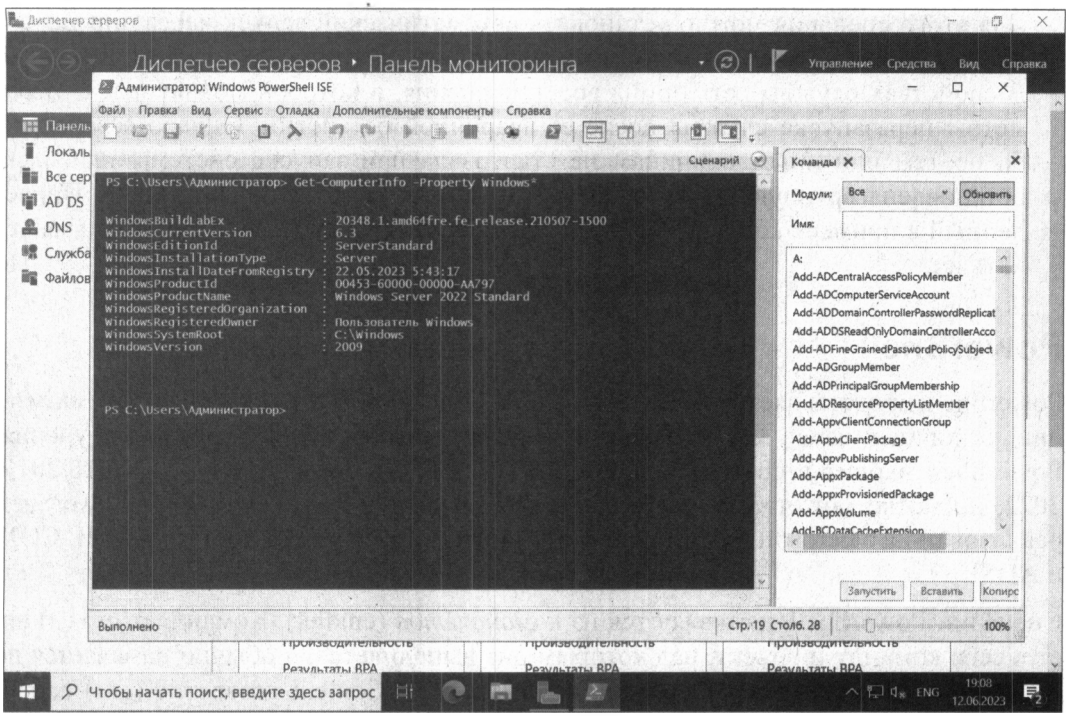


Рис. 6.10. Интегрированная среда сценариев PowerShell (Windows Server 2022)

Обратите внимание, что, начиная работать с PowerShell, желательно настроить личный профиль — сценарий, который исполняется при каждом открытии интерпретатора. В этом профиле можно определить такие настройки, как локальный путь, параметры безопасности, синонимы (сокращения для часто употребляемых команд) и т. п.

Утилиты администрирования третьих фирм

Администраторы весьма часто пополняют свой арсенал продуктами, выпущенными независимыми разработчиками программного обеспечения. Приведем несколько ссылок на подобные продукты.

Утилиты от компании Sysinternals

По адресу **http://www.sysinternals.com/** (компания вошла в состав Microsoft, и эти утилиты стали частью технической библиотеки: **http://technet.microsoft.com/ru-ru/sysinternals**) находится список нескольких бесплатных утилит, весьма необходимых администратору.

Наверное, многим администраторам знакомы программы Filemon и Regmon. Первая отслеживает все активные файловые операции, вторая — операции с реестром. Ранее это были две различные утилиты, сейчас они объединены в одну: Process Monitor (рис. 6.11).

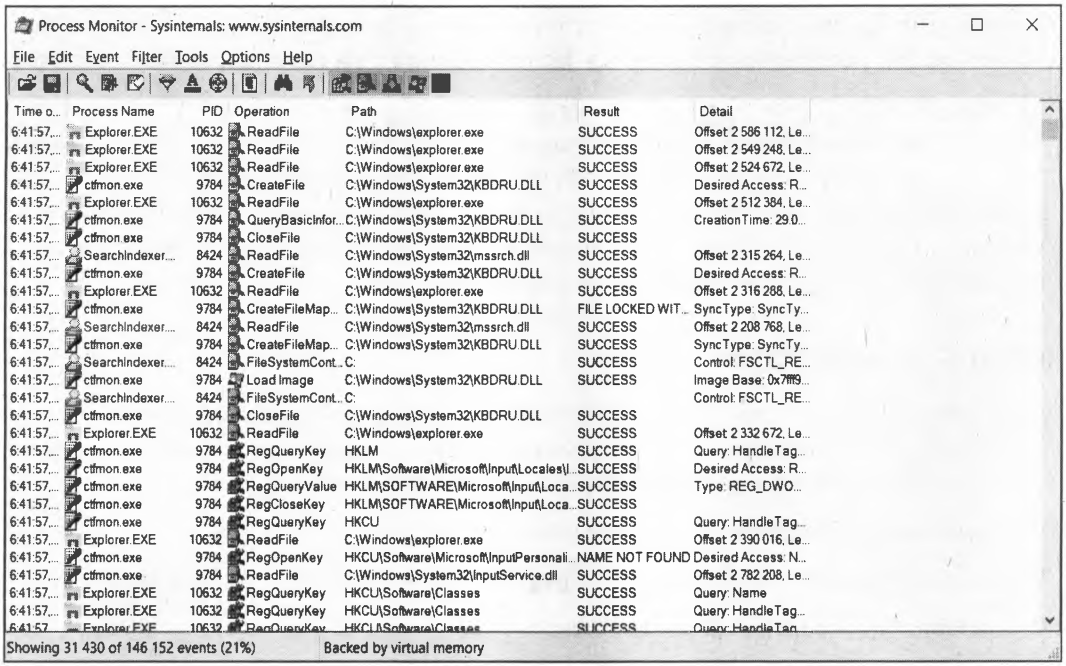


Рис. 6.11. Программа Process Monitor

В состав продуктов компании Sysinternals входят утилиты мониторинга системы, инструменты анализа безопасности ресурсов, программы настройки ресурсов компьютера и т. п. Список утилит достаточно велик, поэтому мы просто рекомендуем вам посетить упомянутый сайт и загрузить необходимые программы.

Снифферы

Хотя администратору и не нужно разбираться в тонкостях сетевых протоколов, он должен уметь на базовом уровне применить тот или иной вариант программы сетевого анализатора — *сниффера*. Сниффер (sniffer) может быть использован для оценки основных параметров функционирования сети: процента использования полосы пропускания, задействованных протоколов, количества пакетов с ошибками и т. п. Кроме того, сниффер позволяет обнаружить отклонения в работе устройств — например, избыточное количество пакетов того или иного типа, что может быть признаком заражения какой-либо системы вирусом или готовящейся атаки.

Сниффер незаменим и 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.

Мы советуем вам установить ту или иную программу анализа и мониторинга сетевого трафика и проанализировать трафик системы 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.

Одним из лучших сетевых анализаторов ранее считался EtherPeek от Wild Packets. Сейчас компания Wild Packets известна под новым названием — Savvius. На ее сайте **https://www.savvius.com** вы можете скачать два анализатора: OmniPeek Network Analysis и Only WLAN Analysis and Recorder Appliance. Первый подойдет для сетей любых типов, второй «заточен» под беспроводные сети.

Ideal Administrator

Ideal Administrator — еще один набор утилит, весьма любимых системными администраторами. Он включает множество функций и весьма прост в использовании. На сайте разработчика **www.pointdev.com** вы найдете продукты для:

- оптимизации и защиты серверов и клиентских ПК;
- централизованного администрирования доменов и рабочих групп Windows;
- удаленного развертывания программ;
- удаленного управления для Windows, macOS и Linux;
- мониторинга серверов и клиентских ПК.

Средняя цена одного продукта — от 200 евро, но есть и более дорогие. Весь набор утилит обойдется в 1705 евро (это начальная цена, поскольку есть и дополнительные модули). Но для всех продуктов предоставляется бесплатная 30-дневная версия, и вы можете попробовать их и решить, нужен ли вам тот или иной продукт.

Hyena

Вот еще один популярный пакет для каждодневного администрирования Windows-систем: **http://www.systemtools.com/hyena/index.html**. Не обращайте внимание на дизайн странички — она выглядит, как привет из начала 2000-х. Продукт поддерживает современные версии Windows, в том числе Windows 10/11 и Windows Server 2022. Продукт не бесплатный, но есть 30-дневная пробная версия.

Автоматизация установки программного обеспечения

Системному администратору постоянно приходится вводить в эксплуатацию новые рабочие места, а также модернизировать существующие. Для этого ему обычно необходимо либо полностью подготовить компьютер (начиная от установки операционной системы и прикладных программ и заканчивая всеми предлагаемыми обновлениями), либо только установить прикладные программы (если компьютер поставлен с OEM-версией Windows).

Для полной подготовки компьютера нужно использовать либо варианты разворачивания операционных систем, либо операции их дублирования. Если надо лишь установить на новую систему прикладное программное обеспечение, можно воспользоваться предназначенными для распространения программного обеспечения средствами группового управления (сценариями входа в систему или групповыми политиками). Но при этом установочные пакеты следует специально подготовить: в них должны быть включены настройки, принятые на вашем предприятии, и исключены запросы к пользователю (для полной автоматизации процесса).

Развертывание Windows 8

Для развертывания версий Windows 7 и более ранниих использовался Windows Automated Installation Kit (Windows AIK или WAIK) — набор инструментальных средств и технологий, созданных Microsoft с целью помочь в развертывании Windows. Так что выполнить развертывание Windows 8 с помощью WAIK у вас не получится. Для новых операционных систем существует новая версия WAIK, которая стала называться Windows ADK (Assessment and Deployment Kit). Название на русском звучит так: комплект средств для развертывания и оценки Windows. Скачать Windows ADK можно с официального сайта Microsoft: **https://www.microsoft.com/ru-ru/download/details.aspx?id=30652**.

Развертывание Windows 10/11

Как и в случае с Windows 8, для развертывания Windows 10/11 вы можете использовать Windows ADK. Но, кроме этого набора, есть и другие средства — например, DISM, USMIT, WDS и т. п.

Ознакомиться с различными средствами развертывания Windows 10 можно по ссылке: **https://docs.microsoft.com/ru-ru/windows/deployment/windows-10-deployment-tools-reference**. Мы также рекомендуем ознакомиться со списком статей на тему развертывания Windows 10: **https://docs.microsoft.com/ru-ru/windows/deployment/deploy**.

Материалы по развертыванию Windows 11 можно найти здесь:

https://learn.microsoft.com/ru-ru/windows-hardware/manufacture/desktop/oem-deployment-of-windows-desktop-editions?view=windows-11.

Клонирование Windows-систем

Самый быстрый способ подготовить новую систему к эксплуатации — сделать ее *копией* уже существующей, т. е. *клонировать*. Клонирование представляет собой процесс воспроизведения существующей системы на другом рабочем месте. Клонированная станция будет иметь аналогичную версию операционной системы, те же установленные (и соответствующим образом настроенные) прикладные программы пользователей и т. п.

К клонированию прибегают при обновлении аппаратной части рабочего места (новый системный блок), при создании новых рабочих мест и т. д.

Существуют различные способы клонирования. Новый образ можно скопировать на жесткий диск, загрузившись со сменного носителя и перенеся данные со сменного устройства, или по сети с сервера, если обеспечить удаленную загрузку новой рабочей станции. Первый вариант более прост в настройке и использовании, второй — более гибок, поскольку на сервере можно хранить образы для различных вариантов установки, но требует установки серверной части.

Администратор выбирает тот вариант, который оптимальным образом подходит для его системы.

Подводные камни процесса клонирования

При кажущейся простоте операции при дублировании системы на другой компьютер администратора ждет много проблем.

Первая группа трудностей связана с возможным различием оборудования на старой и новой системах. Для новой платформы могут понадобиться новые драйверы, и система не сможет работать с программным обеспечением тех устройств, на которые была настроена исходная система. Критичными для переноса являются два момента: HAL в операционной системе Windows и различия в устройствах хранения, с которых запускается операционная система.

> ***Пояснение***
>
> *HAL — hardware abstraction layer*, представляет собой программный код, позволяющий операционной системе без изменений работать с различным аппаратным обеспечением. Условно HAL можно представить себе как драйвер материнской платы компьютера.

В обоих случаях такого расхождения загрузка клонированной системы может завершиться так называемым голубым экраном смерти.

> ***Примечание***
>
> Существует способ добавить в систему драйверы основных устройств так, чтобы система смогла стартовать на новом оборудовании. Этот способ описан в *разд. «Снятие образа физического сервера» главы 8*.

Причиной второй части проблем является наличие в системе уникальных параметров, которые были созданы одной из установленных программ. Самый известный пример из этой области — уникальный идентификатор безопасности, который присваивается каждому компьютеру при включении его в домен. Поскольку в домене не может быть двух компьютеров с уникальным идентификатором безопасности, то простое дублирование диска приведет в таком случае к ошибке в работе.

Другие уникальные характеристики настройки компьютера — это его имя, параметры сетевой настройки (IP-адрес) и т. п. В зависимости от установленного программного обеспечения на компьютере могут присутствовать и иные уникальные идентификаторы (например, идентификатор для систем мониторинга или централизованного управления). Заранее предвидеть все такие ситуации практически невозможно. Поэтому администратору необходимо быть готовым к поиску решений возникающих проблем.

Еще одна сложность, которая может возникнуть при клонировании системы, — это наличие зашифрованных файлов (папок). Поскольку при шифровании данных применяется уникальный идентификатор безопасности, который заменяется программами дублирования диска (иными словами, на новой системе данные уже не прочесть), то для сохранности информации *все зашифрованные файлы необходимо перед клонированием расшифровать*.

Утилита sysprep

Рекомендуемый вендором вариант подготовки жесткого диска к дублированию и установке на другом компьютере состоит в использовании утилиты sysprep, поставляемой в составе дистрибутива системы. Версии утилиты отличаются для различных операционных систем. По возможности следует всегда использовать наиболее ее свежие версии. Например, начиная с версии 1.1, в утилиту добавлена возможность обнаружения при завершении установки новых драйверов IDE-дисков. Проверять наличие новых версий необходимо на сайте изготовителя.

В Windows Server 2008 утилита sysprep находится в папке Windows. В Windows Server 2012/2016/2019/2022 она размещена в папке C:\Windows\System32\Sysprep\. В других версиях ее нужно искать в архиве deploy.cab, содержащемся в папке Support\Tools\ установочного компакт-диска системы.

Утилита sysprep практически «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.

Особенностью использования программы является то, что установленные на исходном компьютере прикладные программы остаются работоспособными после операции клонирования. То есть вы можете полностью «укомплектовать» компьютер, установить все прикладные программы, а затем быстро создать новые компьютеры «по образцу».

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 желаемую версию операционной системы, последние обновления безопасности, все прикладное программное обеспечение (офис, антивирусное ПО, обозреватели Интернета третьих фирм и т. п.).
2. Создайте в корне диска, предназначенного для переноса на новый компьютер, папку SYSPREP, запишите в нее программы 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 дис-

петчера установки: Setupmgr.exe. После генерации файла ответов желательно просмотреть его и включить в него дополнительные параметры, если это необходимо.

4. Сохранив файл ответов, запустите программу Sysprep.exe. По завершении ее работы можно перенести жесткий диск в новую систему и включить компьютер. Обычно через несколько минут система завершит процесс установки и будет полностью работоспособна.

> ***Примечание***
>
> Если предполагается наличие устройств, не поддерживающих PnP (это обычно относится к установке системы на устаревшее оборудование), то при запуске программы *Sysprep.exe* используйте ключ `-pnp`. Это позволит обнаружить такие устройства на новом компьютере, но может существенно (до 20 минут) замедлить процесс установки.

Подготовка диска для существенно отличающейся системы

Если аппаратная платформа, на которую предполагается установить клонированный образ жесткого диска, содержит устройства, драйверы которых не включены в состав дистрибутива операционной системы, то нужно предпринять дополнительные шаги. В первую очередь это относится к платформам с аппаратными RAID-массивами.

В этом случае необходимо специальным образом подготовить жесткий диск *перед* операцией клонирования (можно воспользоваться утилитами редактирования файла образа диска, чтобы добавить в него необходимые папки и изменить соответствующим образом файлы настроек).

1. Чтобы команда `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 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***
>
> Можно разместить драйверы и в другом месте — например, в корневой папке жесткого диска, соответственно подправив путь к ним в файле ответов. Причина размещения драйверов именно в папке *SYSPREP* — это автоматическое ее удаление после завершения установки системы.

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, следует включить в секцию [Unattended] файла ответов строку: DriverSigningPolicy = Ignore.

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 указаны 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.

Дублирование жесткого диска

Сформированный с помощью утилиты sysprep жесткий диск можно использовать как образец для создания новых. Существует много средств, позволяющих сделать копию жесткого диска. Наиболее простой вариант создания копии диска заключается в дублировании его структуры. Для этого часто используют утилиты от фирмы Acronis (**http://www.acronis.ru/**). Можно также воспользоваться бесплатным приложением Clonezilla (**https://clonezilla.org/**), которое поддерживает не только файловые системы UNIX, но и NTFS.

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 через сеть. Можно сохранить образ диска в виде файла и использовать этот файл для последующего создания копий дисков. Особенно удобно использовать вариант сетевого развертывания образа диска при одновременной подготовке нескольких систем. В этом случае запись диска будет вестись одновременно на все компьютеры.

Развертывание по сети требует установки соответствующего сервера. Загрузка систем в этом случае будет происходить либо по сети (с использованием PXE-варианта загрузки), либо со специально подготовленного загрузочного диска (если сетевая карта не поддерживает режим PXE). Функция подготовки такого диска включается в корпоративные версии соответствующих программ.

> ***Пояснение***
>
> PXE (от *англ.* Preboot eXecution Environment) представляет собой среду для загрузки компьютеров с помощью сетевой карты без использования жестких дисков и других аналогичных устройств. PXE-код, находящийся в сетевой карте, загружает из сети исполняемый файл, которому и передает управление для дальнейшей работы системы.

Заметим, что корпоративные версии программ предлагают и иные специальные варианты выполнения такой операции.

Образы клонируемого диска и их модификация

Вместо дублирования подготовленного диска можно создать его *образ* и сохранить такой файл на сервере. Практически все программы клонирования дисков позволяют формировать новый диск из такого файла. Этот способ, во-первых, упрощает хранение образов, а во-вторых, позволяет добавлять в образы новые файлы, программы и т. п.

При запуске новой системы с диска, подготовленного утилитой sysprep, начинается просмотр специальных папок. В эти папки можно включить сценарии (и соответствующие файлы программ установки), которые при запуске системы будут выполнены автоматически. Таким образом можно легко добавлять в образы новые программы и возможности.

Описание правил добавления автозапускаемых сценариев можно найти в справке утилиты sysprep. А для редактирования файла образа легко найти соответствующую утилиту.

Клонирование компьютеров — членов домена

Утилита sysprep не позволяет клонировать системы, являющиеся членами домена. Необходимо сначала перевести компьютер в рабочую группу, после чего клонировать диски и добавить новые станции в домен.

Обратите внимание, что некоторые программы — например, Symantec Ghost Solution Suite, имеют специальные функции для клонирования дисков со станций, являющихся членами домена. 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 эта операция воспринимается как клонирование станции — члена домена.

Клонирование Linux-систем

Средства клонирования Linux

Самым мощным средством для клонирования систем на Linux является Clonezilla. Этот продукт может не только создать LiveCD, но и развернуть систему по сети. На сайте разработчиков (**http://clonezilla.org/**) имеется следующая информация: за 10 минут Clonezilla SE (Server Edition) развернула по сети образ объемом 5,6 Гбайт на 41 компьютер сети. Таким образом, все компьютеры были настроены всего за 10 минут. Правда, для подобной сетевой установки придется развернуть специальный сервер, но об этом позже. Может Clonezilla использоваться и для создания резервных копий компьютеров, работающих под управлением Windows и FreeBSD.

Любителям Slackware подойдет скрипт Linux Live (**http://www.linux-live.org/**). Этот сценарий позволяет создать как LiveCD, так и LiveUSB.

Подобные утилиты можно найти и для других дистрибутивов — например, утилита mklivecd (подобна Remastersys Backup) используется для создания LiveCD на базе

Mandriva. Обсуждать все такие утилиты нет смысла, так что мы рассмотрим одно универсальное средство — Clonezilla, которое устроит администратора в большинстве случаев.

Использование Clonezilla

Основные особенности Clonezilla:

- полностью бесплатна (распространяется по лицензии GPL);
- поддерживает файловые системы: ext2, ext3, ext4, ReiserFS, Reiser4, XFS, JFS, FAT, NTFS, HFS (macOS), UFS (FreeBSD, NetBSD, OpenBSD), VMFS (VMware ESX) — поэтому вы можете с ее помощью клонировать не только Linux, но и MS Windows, macOS (Intel), FreeBSD, NetBSD и OpenBSD;
- поддерживает LVM2 (LVM версии 1 не поддерживает);
- поддерживает GRUB версий 1 и 2;
- поддерживает Multicast для массового клонирования по сети (версия Clonezilla Server Edition при условии, что компьютеры поддерживают PXE и Wake-on-LAN);
- может сохранить не только отдельно взятый раздел, но и весь жесткий диск со всеми разделами.

Clonezilla — программа не простая, и здесь мы рассмотрим лишь один из примеров ее использования, а именно: создание LiveCD и восстановление системы с его помощью. Познакомиться же с остальными возможностями программы можно в документации к ней или на сайте ее разработчиков.

Итак, для создания/восстановления образа системы нужно выполнить следующие действия:

1. Скачать с сайта **http://clonezilla.org/download/sourceforge/** ISO-образ Clonezilla Live и развернуть его на болванку компакт-диска.
2. Загрузиться с компакт-диска Clonezilla Live (рис. 6.12), выбрав команду **Clonezilla live**. Вы увидите процесс загрузки Debian (рис. 6.13) — тут все как обычно, нужно просто подождать. Если возникнут проблемы (например, с видеокартой), можно в стартовом окне компакт-диска Clonezilla Live (см. рис. 6.12) выбрать команду **Other modes of Clonezilla live** и попробовать другой режим загрузки Clonezilla.
3. Далее (рис. 6.14) нужно выбрать язык (русский, к сожалению, пока не предвидится). Можно также выбрать и раскладку клавиатуры (рис. 6.15), но поскольку раскладку изменять нам ни к чему, выберите вариант **Don't touch keymap**.
4. Выбрать команду **Start Clonezilla** (рис. 6.16).
5. Выбрать режим **device-image** для создания файла образа диска или раздела (рис. 6.17). Другой режим, предлагаемый меню, — **device-device** служит для создания копии диска или раздела на другом диске (разделе) без создания файла образа.

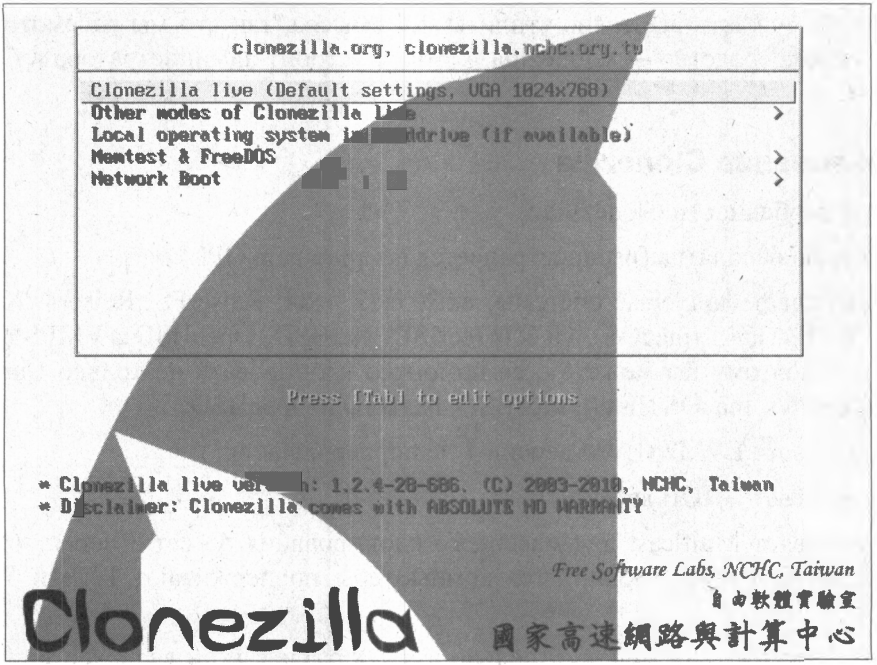


Рис. 6.12. Загрузочное меню Clonezilla Live

```
[    2.298874] scsi 1:0:1:0: Direct-Access     ATA      VMware Virtual I 0000 PQ: 0 ANSI: 5
[    2.340195] ata2.00: ATAPI: VMware Virtual IDE CDROM Drive, 00000001, max UDMA/33
[    2.341583] ata2.00: configured for UDMA/33
[    2.342129] scsi 2:0:0:0: CD-ROM            NECVMWar VMware IDE CDR10 1.00 PQ: 0 ANSI: 5
[    2.350556] sr0: scsi3-mmc drive: 1x/1x xa/form2 cdda tray
[    2.352065] Uniform CD-ROM driver Revision: 3.20
[    2.358812] sd 1:0:0:0: [sda] 16777216 512-byte logical blocks: (8.58 GB/8.00 GiB)
[    2.359612] sd 1:0:0:0: [sda] Write Protect is off
[    2.361466] sd 1:0:0:0: [sda] Write cache: disabled, read cache: enabled, doesn't support DPO or
FUA
[    2.362200]  sda: sda1 sda2 sda3 < sda5 >
[    2.363092] sd 1:0:1:0: [sdb] 31457280 512-byte logical blocks: (16.1 GB/15.0 GiB)
[    2.363185] sd 1:0:1:0: [sdb] Write Protect is off
[    2.363228] sd 1:0:1:0: [sdb] Write cache: disabled, read cache: enabled, doesn't support DPO or
FUA
[    2.380613]  sdb: sdb1
[    2.386360] sd 1:0:1:0: [sdb] Attached SCSI disk
[    2.387994] sd 1:0:0:0: [sda] Attached SCSI disk
[    2.391994] sd 1:0:0:0: Attached scsi generic sg0 type 0
[    2.393897] sd 1:0:1:0: Attached scsi generic sg1 type 0
[    2.400551] sr 2:0:0:0: Attached scsi generic sg2 type 5
Begin: Loading essential drivers ... [    2.593615] Atheros(R) L2 Ethernet Driver - version 2.2.3
[    2.593830] Copyright (c) 2007 Atheros Corporation.
[    2.612151] Broadcom NetXtreme II 5771x 10Gigabit Ethernet Driver bnx2x 1.52.1 (2009/08/12)
[    2.632202] device-mapper: uevent: version 1.0.3
[    2.634009] device-mapper: ioctl: 4.15.0-ioctl (2009-04-01) initialised: dm-devel@redhat.com
done.
Begin: Running /scripts/init-premount ... done.
Begin: Mounting root file system ... [    2.745155] Uniform Multi-Platform E-IDE driver
[    2.745836] ide_generic: please use "probe_mask=0x3f" module parameter for probing all legacy ISA
 IDE ports
[    2.882403] aufs: module is from the staging directory, the quality is unknown, you have been war
ned.
[    2.885440] aufs 2-standalone.tree-32-20100125
[    2.930106] loop: module loaded
[    3.041203] squashfs: version 4.0 (2009/01/31) Phillip Lougher
```

Рис. 6.13. Процесс загрузки Debian

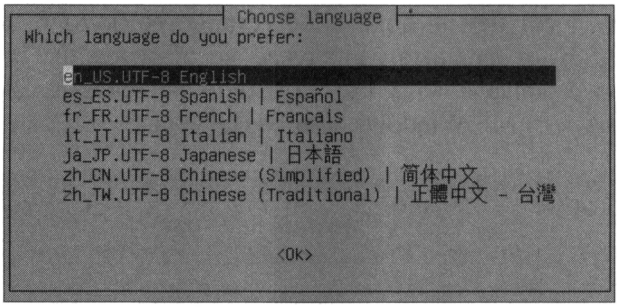


Рис. 6.14. Выбор языка Clonezilla

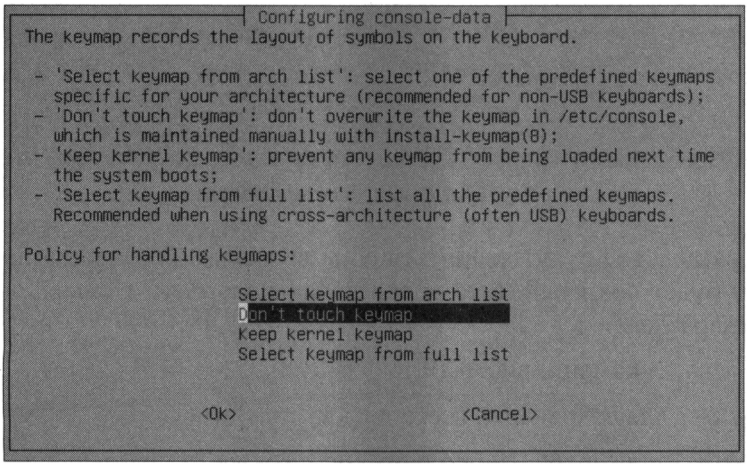


Рис. 6.15. Выбор раскладки

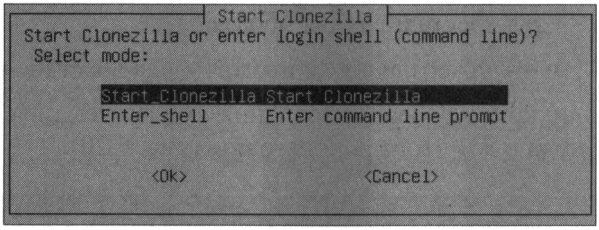


Рис. 6.16. Выбор команды **Start Clonezilla**

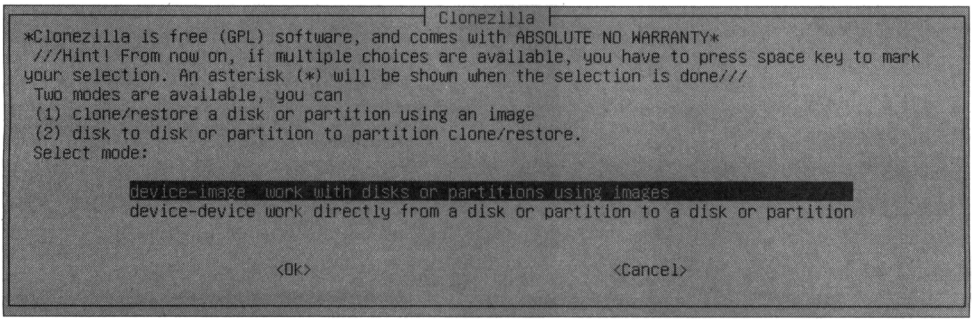


Рис. 6.17. Выбор режима **device-image**

6. Выбрать режим **local_dev** — локальное устройство, куда будет сохранен образ или откуда он будет прочитан в случае восстановления системы по образу (рис. 6.18). Также образ можно получить (или записать) по SSH, NFS (Network File System) и из сети MS Windows (**samba_server**).

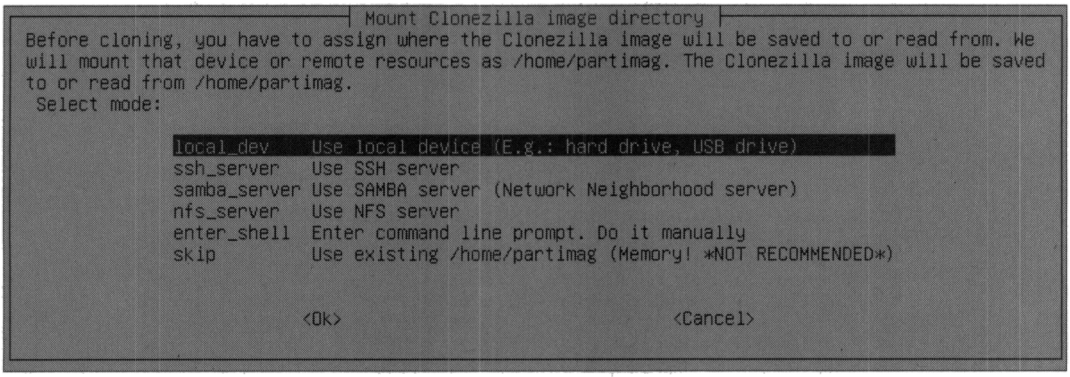


Рис. 6.18. Выбор носителя образа

7. Выбрать раздел, где будут храниться образы. Если вы создаете образ, то на этот раздел он будет сохранен, а если восстанавливаете, то Clonezilla будет искать его на этом разделе.
8. Выбрать одну из команд (рис. 6.19):
   - **savedisk** — для сохранения всего диска;
   - **saveparts** — для сохранения одного или нескольких разделов диска;
   - **restoredisk** — для восстановления образа диска на локальный диск;
   - **restoreparts** — для восстановления образа раздела;
   - **recovery-iso-zip** — для создания «живого» диска восстановления.
9. Если вы выбрали команду восстановления образа, то далее следует выбрать образ, который нужно для этого использовать (рис. 6.20).

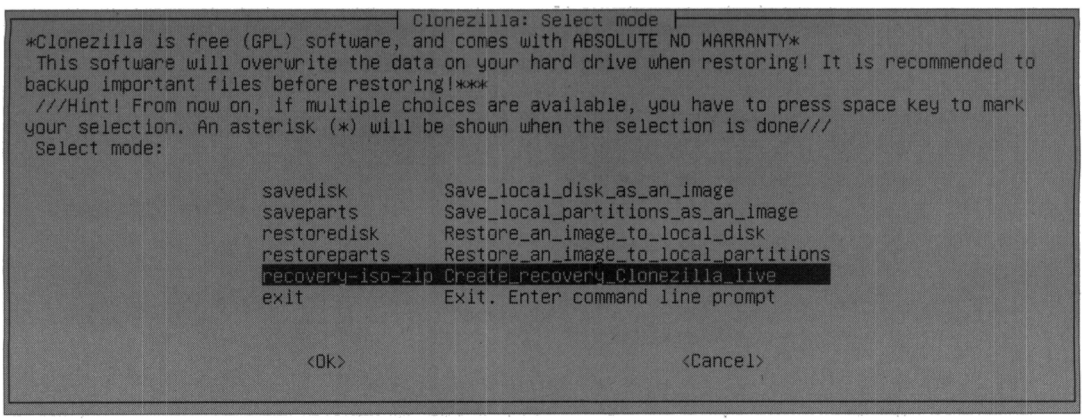


Рис. 6.19. Создать образ или восстановить?

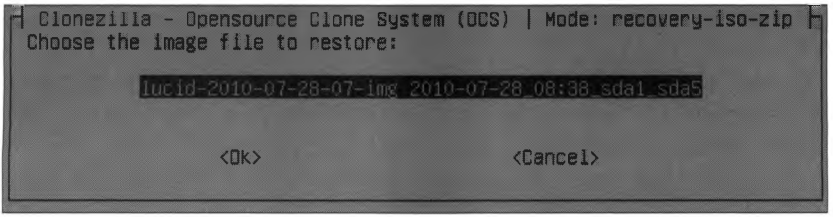


Рис. 6.20. Выбор образа для восстановления

10. Ввести устройство (имена устройств соответствуют именам устройств в Linux), на которое нужно развернуть образ (рис. 6.21). Будьте внимательны, чтобы не развернуть образ раздела на весь диск — потеряете остальные разделы!

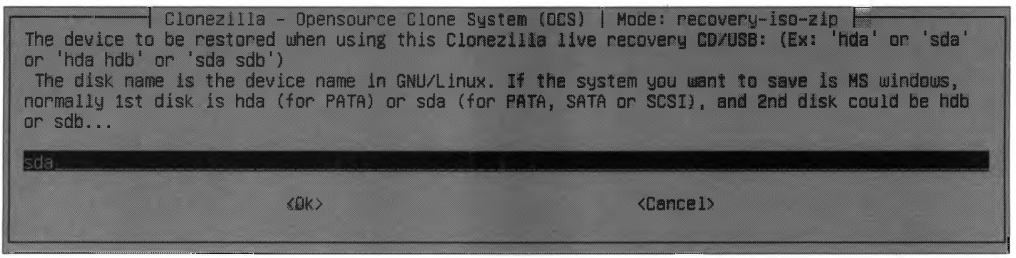


Рис. 6.21. На какое устройство «развернуть» образ?

11. Если вы выбрали команду **recovery-iso-zip** для создания LiveDVD/USB, то нужно также выбрать режим (рис. 6.22):
    - **iso** — будет создан образ для записи на DVD;
    - **zip** — будет создан образ для записи на LiveUSB;

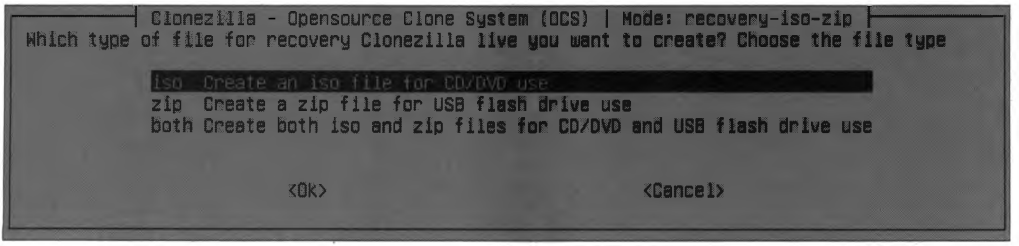


Рис. 6.22. Выбор режима команды **recovery-iso-zip**

    - **both** — будут созданы оба файла, которые можно использовать впоследствии как для создания LiveDVD, так и для создания LiveUSB. Созданный файл (файлы) будет сохранен в каталоге /home/partimag (рис. 6.23).

На рис. 6.24 показан процесс создания LiveCD, а из рис. 6.25 видно, что этот процесс удачно завершен.

Вот и все! Как видите, это весьма просто. Программа работает с устройствами (дисками, разделами) напрямую, поэтому при создании/восстановлении образа все равно, под какой операционной системой работает компьютер.

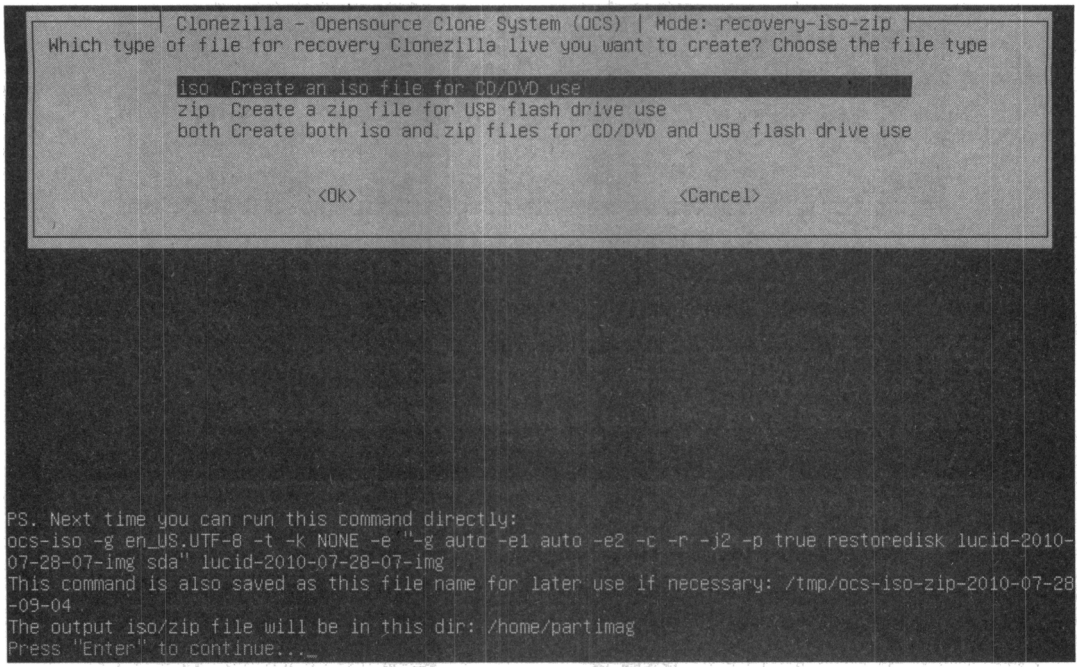


Рис. 6.23. Созданный файл будет сохранен в каталоге /home/partimag

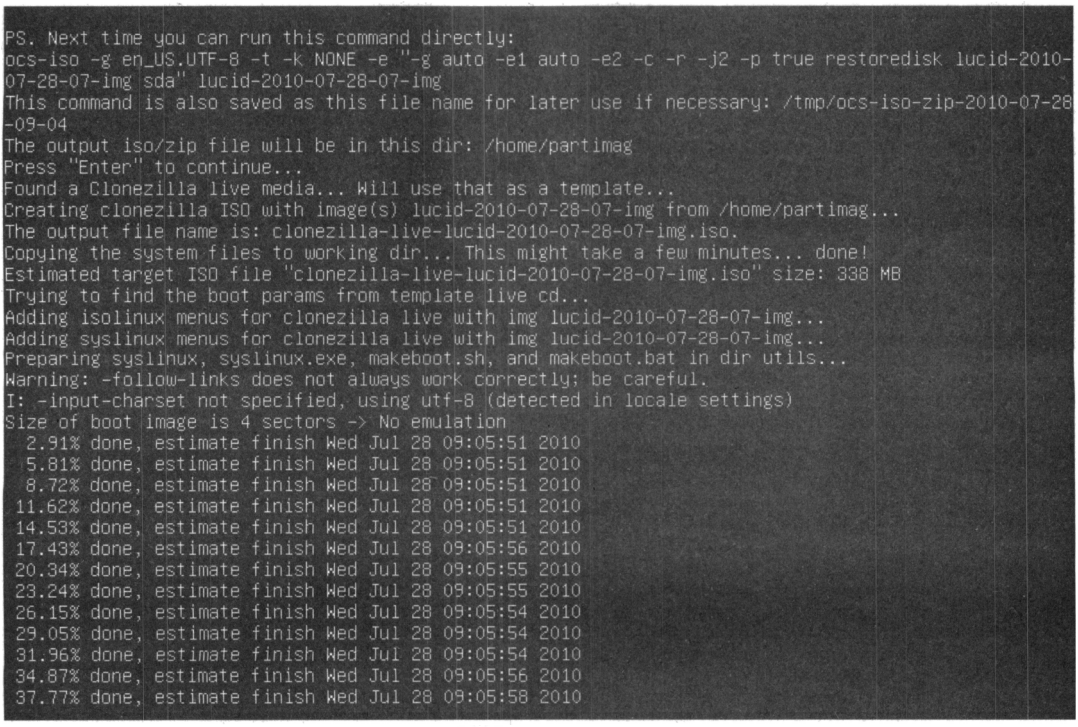


Рис. 6.24. Процесс создания LiveCD

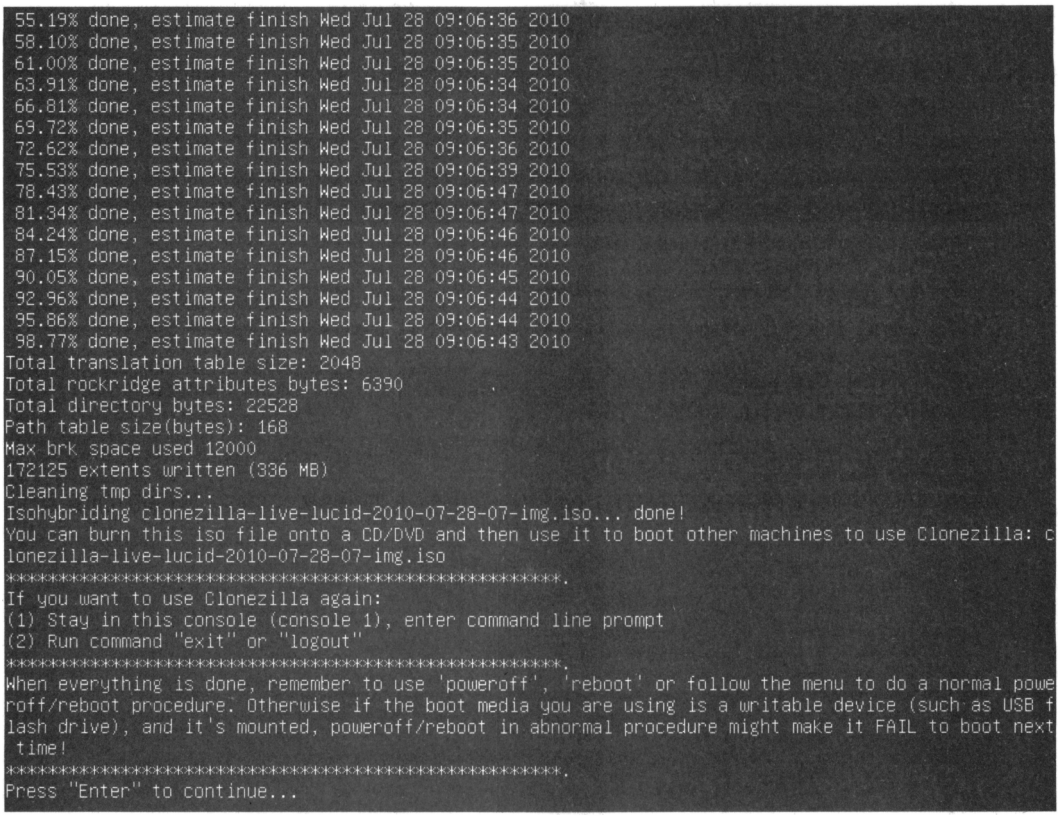


Рис. 6.25. LiveCD создан, нажмите клавишу <Enter> для продолжения

Если у вас есть необходимость в серверной версии (Clonezilla Server Edition), найти руководство по ее использованию вы можете по адресу: **http://clonezilla.org/clonezilla-server-edition/**.

Подготовка программ для «тихой» установки

При установке прикладных программ часто приходится вводить много ответов, указывая путь установки, состав выбранных функций и т. п. Необходимость таких операций, с одной стороны, снижает скорость установки программного обеспечения, а с другой — усложняет выполнение операций установки в автоматическом режиме.

> ***Примечание***
>
> Для «тихой» установки следует использовать корпоративные версии программ. Если программа требует, например, ввода индивидуального серийного номера, то такие действия крайне сложно автоматизировать.

Существуют разные способы подготовки программ к установке без запросов к пользователю.

Файлы ответов (трансформаций)

Программные пакеты часто включают возможности создания специальных файлов ответов, которые могут быть использованы при их установке. Например, это установка самой операционной системы (рис. 6.26), установка программ Microsoft Office и аналогичных. Загрузить пакет Windows ADK можно по адресу: **https://docs.microsoft.com/ru-ru/windows-hardware/get-started/adk-install**. На рис. 6.27 показана его установка в Windows 10.

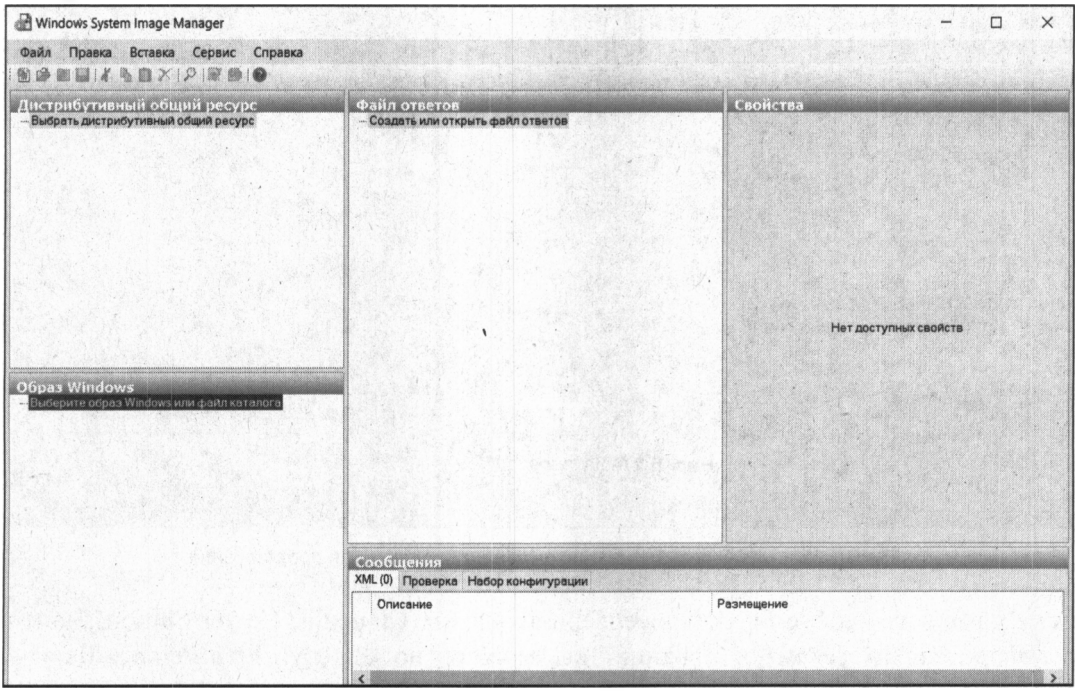


Рис. 6.26. Программа формирования файла ответов для автоматизированной установки операционной системы

Для прикладных программ наиболее корректным вариантом является формирование файлов ответов (или *трансформаций*, transform, MST-файлов). 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.

Для подготовки файлов трансформаций необходимо использовать специальные программы (см. рис. 6.26). Например, для Microsoft Office они должны быть загружены с сайта изготовителя (обычно включаются в состав Resource Kit). При их запуске администратору достаточно выбрать в графическом режиме желаемые параметры установки, чтобы создать файл трансформации.

К сожалению, большинство программ, с которыми приходится сталкиваться на практике, не имеют описаний файлов трансформаций или мастера создания ответов.

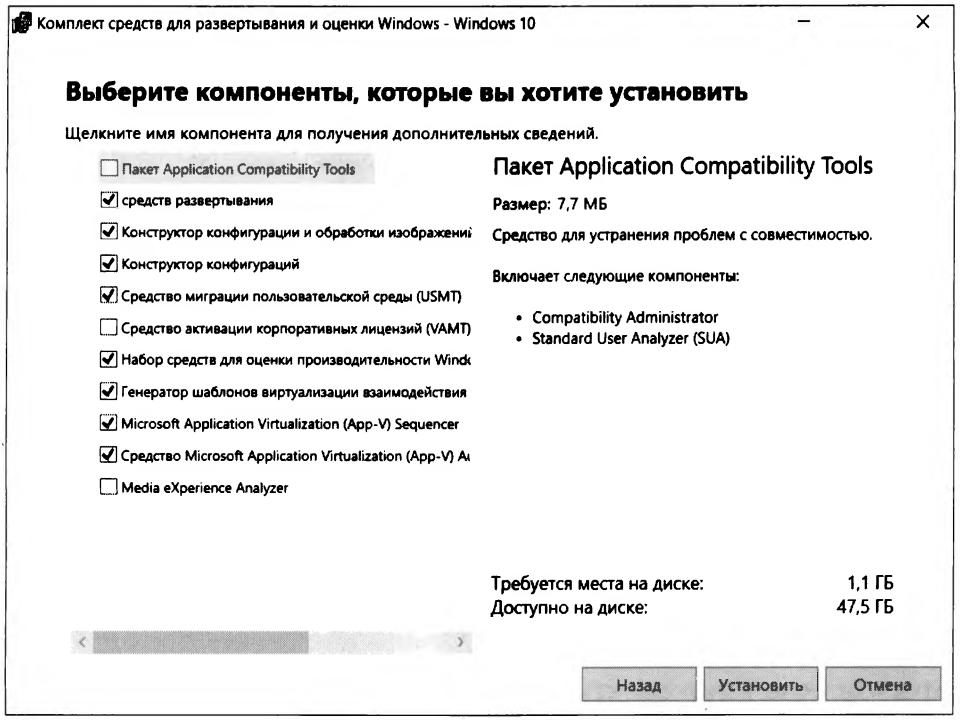


Рис. 6.27. Установка Windows ADK

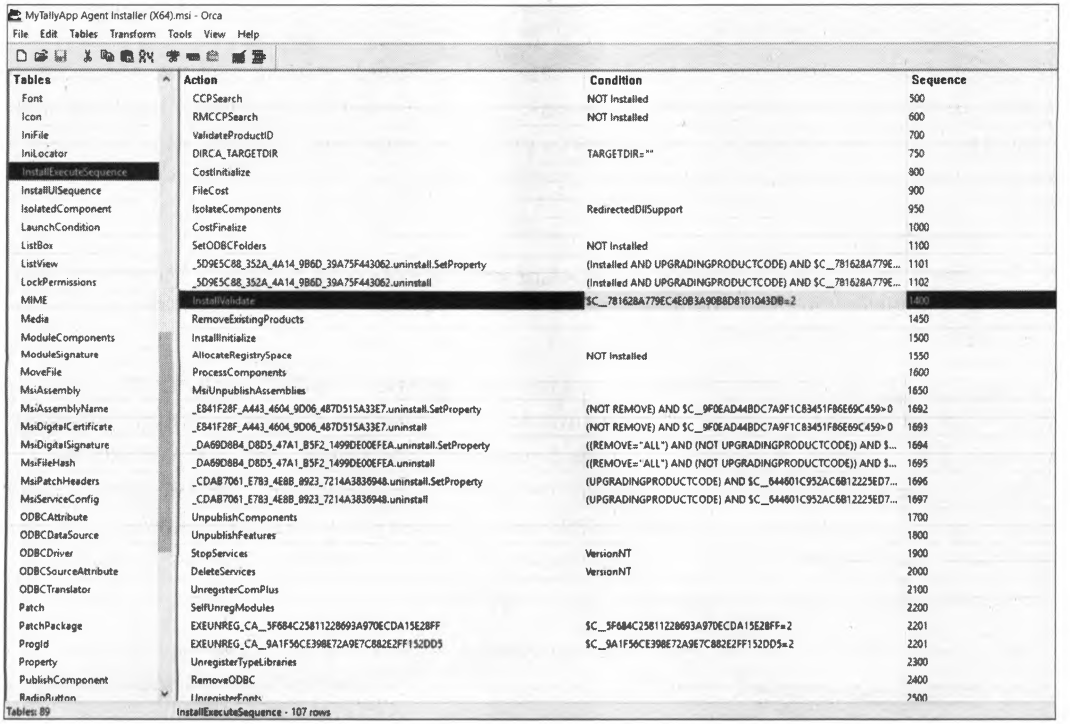


Рис. 6.28. Редактирование установочного файла с помощью специализированной программы Orca

Если не удается найти инструкции по составлению трансформаций у изготовителя продукта, то можно воспользоваться программами для редактирования установочных файлов, — не забывайте при этом, что есть программы, преобразующие исполняемые файлы установки setup.exe к виду *.msi. Как правило, эти программы либо записывают ответы пользователя во время тестовой установки, либо позволяют отобразить структуру MSI-файла, назначить необходимые параметры, скрыть диалоговые окна и т. п. Одна из таких программ — Orca (рис. 6.28), входящая в состав Microsoft Windows SDK (**https://developer.microsoft.com/ru-ru/windows/downloads/windows-10-sdk/**). К сожалению, отдельно приложение скачать не получится, нужно загружать и устанавливать весь SDK. Зато приложение бесплатное.

> ***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. Поэтому подготовленные к установке пакеты должны быть обязательно протестированы.

Использование ключей «тихой» установки

«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.

Установочные файлы для «тихой» установки обычно имеют ключи командной строки, позволяющие выполнить установку в таком именно режиме с настройками установки по умолчанию. К сожалению, синтаксис командных строк инсталляторов различных разработчиков отличается друг от друга.

> ***Примечание***
>
> Если в процессе установки с выбранным ключом возникла ситуация, требующая введения *пользователем* дополнительной информации, то программа покажет соответствующее диалоговое окно.

Стандартным для установочных файлов программ Windows является формат MSI — он подробно описан разработчиком и фактически является открытым стандартом. Для файлов в таком формате предусмотрен ключ «тихой» установки `/q`. При этом следует использовать следующий синтаксис запуска (в примере вы также видите ключ `/n`, наличие которого позволяет выполнить установку скрыто, без интерфейса пользователя):

```
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 наличия файла ответов.

По умолчанию файл ответов должен иметь имя setup.iss и располагаться в той же папке, что и setup.exe. Если вы не используете для файла ответов имя по умолчанию, то его имя при запуске «тихой» установки (с ключом /s) необходимо указать с ключом /f1.

Если файл ответов 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 с ключом /r:

```
setup.exe /r /f1
```

> ***Примечание***
>
> Ключ /f1 в командной строке можно не указывать. В этом случае файл ответов будет записан по умолчанию в папку Windows с именем *setup.iss*.

> ***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 дистрибутивы PackageForTheWeb (PFTW). Эти пакеты представляют собой один самораспаковывающийся файл, который после разархивирования автоматически запускает программу setup.exe, содержащуюся в этом архиве. Дистрибутивы 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.

> ***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**.

Переупаковка

Если в программе не предусмотрен вариант «тихой» установки, то администратор имеет все же возможность настроить продукт для установки без запросов. Для этого используется технология *переупаковки* (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 включается только в коммерческие версии программ.

Не все дистрибутивы допускают переупаковку. Во-первых, нельзя переупаковывать сервис-паки (service pack), «горячие заплатки» и другие продукты, вносящие изменения 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.

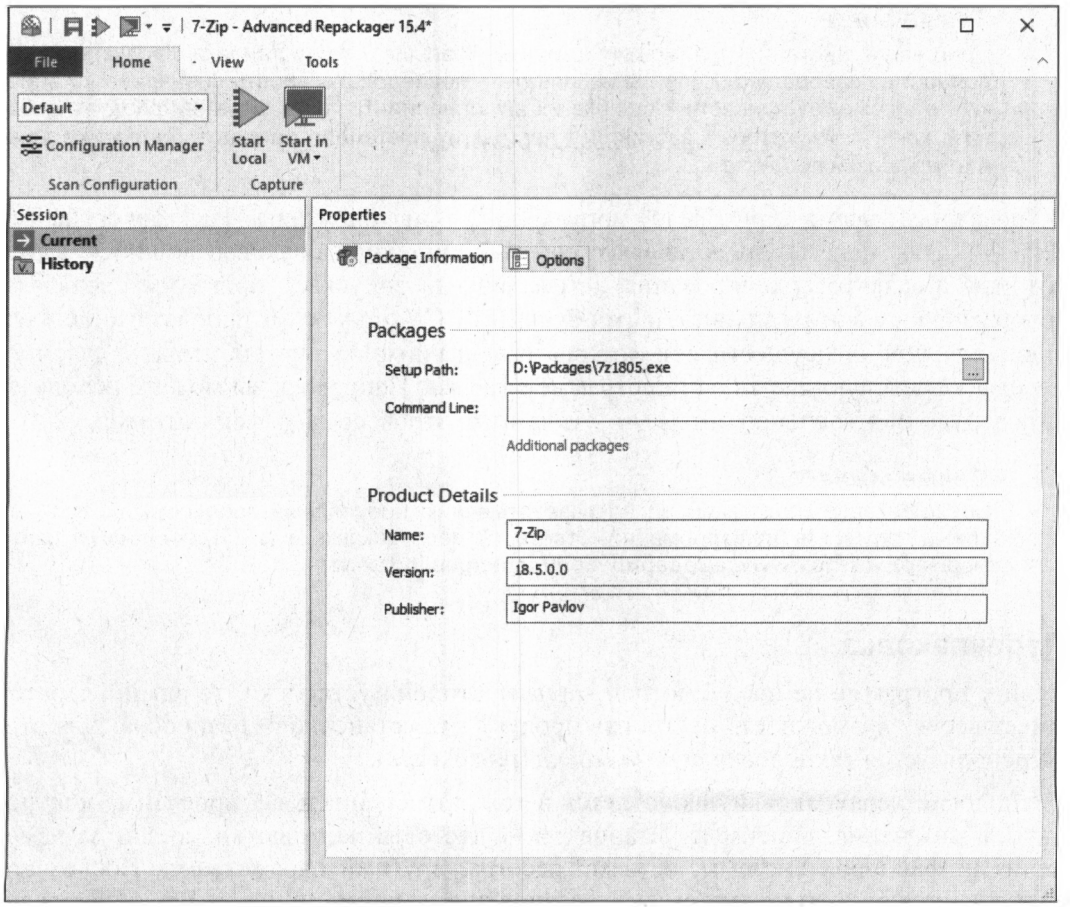


Рис. 6.29. Программа Advanced Repackager

Переупаковка весьма 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. На рис. 6.29 показано окно одной из таких программ — Advanced Repackager (**https://www.advancedinstaller.com/repackager.html**).

Переупаковка позволяет включить в один дистрибутив несколько последовательно устанавливаемых продуктов — достаточно запустить до второго сканирования системы необходимое число программ. Кроме того, с помощью переупаковки легко выполнить пользовательские настройки. Для этого нужно до начала анализа запустить на тестовом компьютере установленную программу, настроить ее и сохранить изменения. Все эти изменения войдут в переупакованный дистрибутив.

Административная установка

На предприятиях часто используют *административную установку*. Административная установка подразумевает перенос дистрибутивных файлов продукта в какую-либо сетевую папку с одновременным внесением настроек, специфичных для того или иного предприятия. 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.

Развертывание программы в Active Directory

Развертывание — это процесс централизованной установки программы на все компьютеры домена Active Directory или на какую-то часть этих компьютеров (например, на компьютеры определенного организационного подразделения).

Рассмотрим процесс развертывания программы с помощью Active Directory. Прежде всего нужно создать папку для развертывания программного обеспечения (теоретически папку можно создать на любом компьютере домена, но мы ее создадим на контроллере домена). Она будет содержать все MSI-пакеты, развертывания которых нужно выполнить, и соответствующие файлы трансформаций. Создавать отдельную папку для каждой устанавливаемой программы не требуется.

Пусть это будет папка C:\Install. В ней создайте подпапку с названием устанавливаемой программы. В нее нужно поместить установочный MSI-файл и MST-файл

трансформации (например, csfirewall.msi и csfirewall.mst), который вы создали, используя инструкции, приведенные ранее в *разд. «Файлы ответов (трансформаций)»*.

К папке C:\Install надо предоставить общий доступ. Для этого щелкните правой кнопкой мыши на папке и выберите команду **Свойства**. На вкладке **Доступ** нажмите кнопку **Общий доступ** и предоставьте доступ на чтение и запись администратору и доступ только на чтение всем остальным пользователям сети.

Затем запустите редактор групповой политики gpmc.msc. Мы предполагаем, что программу нужно установить на все компьютеры сети. Поэтому щелкните правой кнопкой мыши на домене и выберите команду **Создать объект групповой политики в этом домене и связать его** (рис. 6.30). Если ПО нужно установить только на контроллерах домена, вы можете щелкнуть правой кнопкой мыши на объекте групповой политики (GPO) **Default Domain Controller Policy**, — далее, как обычно.

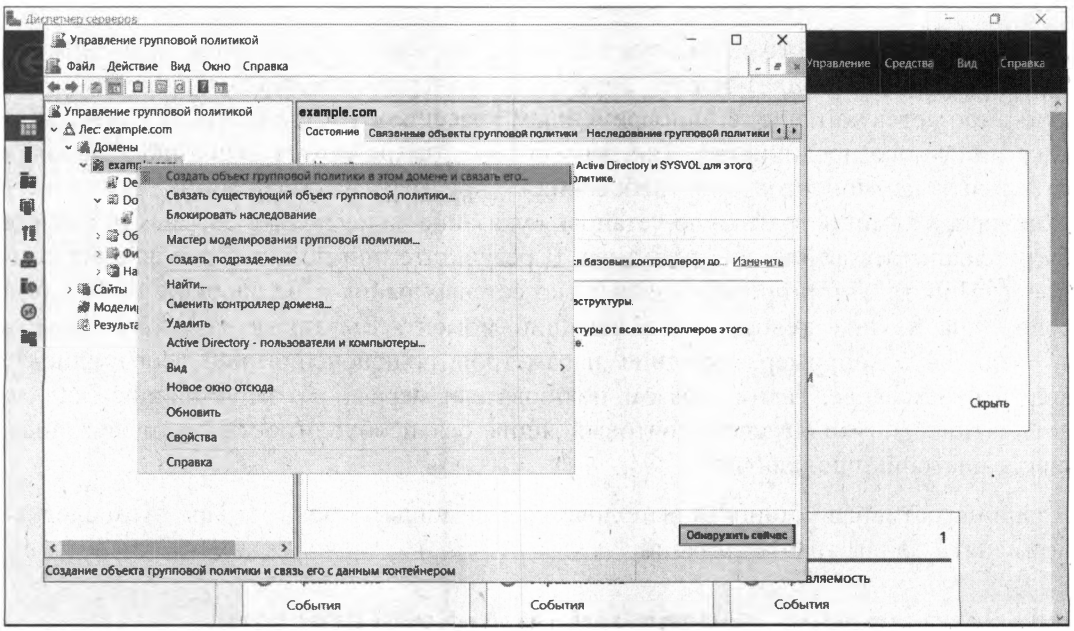


Рис. 6.30. Редактор групповой политики

> ***Примечание***
>
> Иллюстрации для этого раздела созданы в Microsoft Windows Server 2019, но все приведенные инструкции будут работать и в других версиях (Microsoft Windows Server 2012/2016/2022) — возможно, вы увидите незначительные отличия в иллюстрациях.

Дайте название новому объекту групповой политики — можно использовать название устанавливаемой программы (рис. 6.31).

В разделе **Фильтры безопасности** удалите группу **Прошедшие проверку** и добавьте компьютеры, группы и пользователей, к которым будут применены параметры созданного объекта групповой политики (рис. 6.32). Другими словами, добавьте компьютеры, на которые должна быть установлена программа.

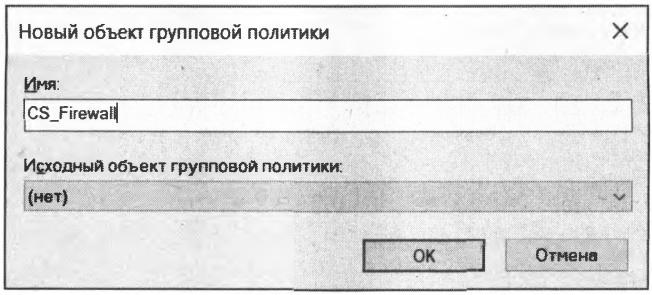


Рис. 6.31. Создание нового объекта GPO

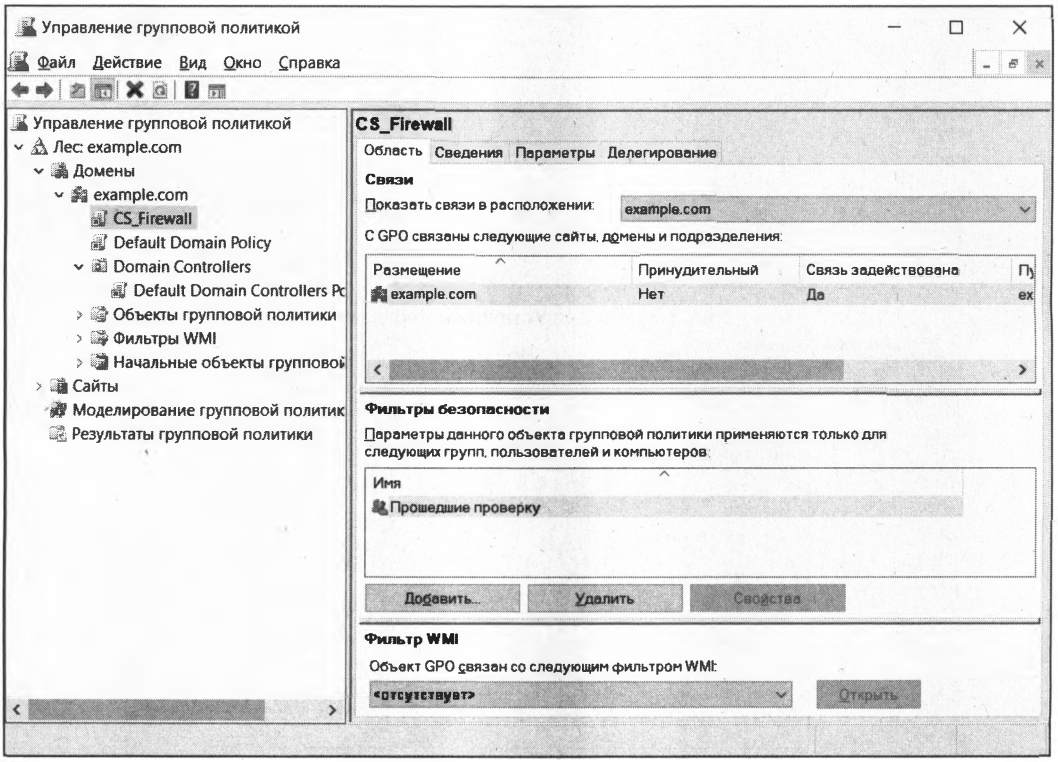


Рис. 6.32. Созданный объект GPO

Щелкните правой кнопкой мыши на только что созданном GPO и выберите команду **Изменить**. Перейдите в раздел **Конфигурация пользователя | Политики | Конфигурация программ | Установка программ** (рис. 6.33).

Щелкните правой кнопкой мыши на разделе **Установка программ** и выберите команду **Создать | Пакет**. В открывшемся окне выберите путь к MSI-файлу программы. Обратите внимание, что вводить нужно не локальный путь, а сетевой, поскольку пользователи будут получать доступ к пакету по сети.

Следующий шаг — выбор метода развертывания. Поскольку мы хотим предоставить файл трансформации (MST-файл, созданный ранее), то нужно выбрать **особый** метод развертывания (рис. 6.34). В результате откроется окно настройки пакета

Рис. 6.33. Раздел **Установка программ**

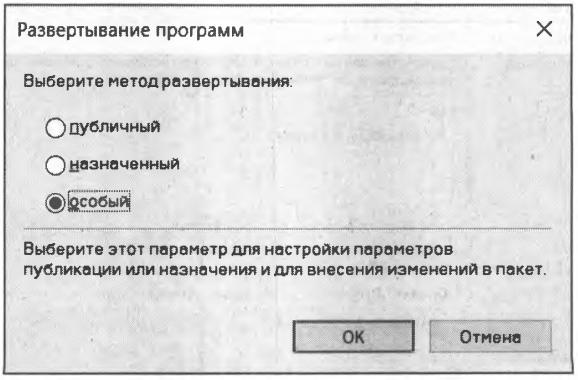


Рис. 6.34. Выбор метода развертывания

развертывания. Перейдите в нем на вкладку **Модификации**, нажмите кнопку **Добавить** и выберите MST-файл трансформации (рис. 6.35). Нажмите кнопку **OK**.

> ***Примечание***
>
> После нажатия кнопки **OK** пакет и файл трансформации (файлы **.msi* и **.mst* соответственно) будут прокешированы. Если вам понадобится изменить файл трансформации после создания пакета, то придется создавать пакет развертывания заново.

На этом работа с редактором групповой политики завершена. Закройте все окна, откройте командную строку (или хотя бы окно **Выполнить**, нажав комбинацию клавиш <Win>+<R>) и введите команду:

```
gpupdate /force
```

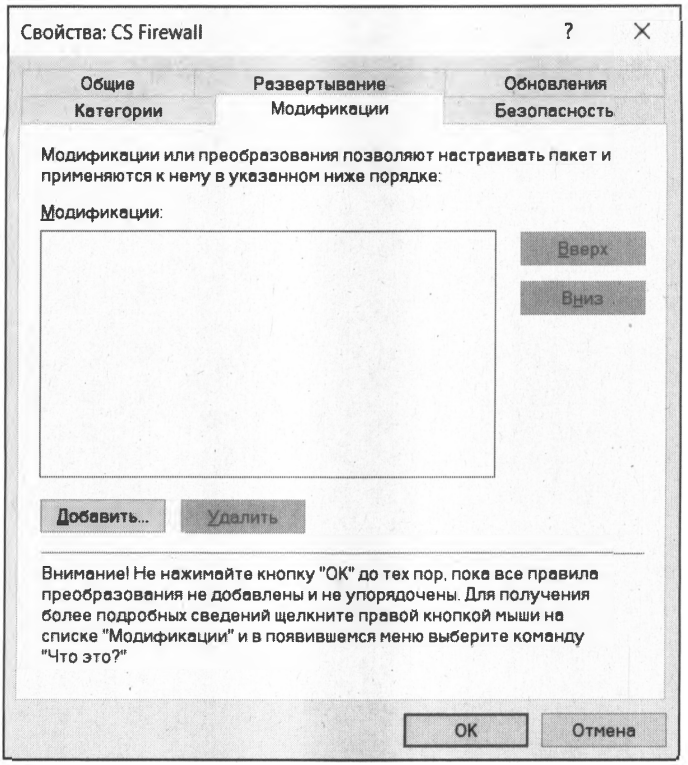
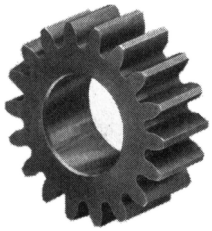


Рис. 6.35. Указываем файл трансформации

Программа будет автоматически установлена на компьютеры после их перезагрузки и до отображения окна входа в систему. Пользователь ни на что не сможет повлиять и ни в чем не сможет ошибиться.

Иногда программа не устанавливается автоматически. Чтобы все же выполнить ее установку, нужно еще раз вручную ввести команду `gpupdate /force`.

ГЛАВА 7



Мониторинг информационной системы

Для предотвращения возможных отказов информационной системы администратору нужно осуществлять регулярный ее мониторинг. Сама эта операция весьма рутинна, а вот анализ получаемой информации требует высокой квалификации. Ничего интересного в мониторинге нет, но, увы, производить его надо. В этой главе будут рассмотрены основные методы и средства мониторинга информационной системы.

Основные способы мониторинга

Существует несколько способов мониторинга информационной системы. На небольших предприятиях, насчитывающих совсем немного серверов, как правило, выполняется анализ сообщений в журналах системы.

На предприятиях среднего и крупного размера контроль активного оборудования производится на основе протокола SNMP (Simple Network Management Protocol). Конечно, протокол SNMP может применяться и на малых предприятиях, если будет куплено активное оборудование с поддержкой этого протокола. Вот только цена такого оборудования столь высока, что малые компании наверняка откажутся его приобретать, да и целесообразности для них в нем нет.

На предприятиях крупного размера задействуются, как правило, специальные программы-агенты, устанавливаемые на каждый сервер и на каждую рабочую станцию. Такие агенты собирают информацию о работе системы и передают ее на сервер.

В этом разделе мы приведем краткие характеристики основных способов мониторинга, а затем рассмотрим их более подробно.

Журналы системы и программ

Система и приложения записывают в журналы сведения об основных событиях. Можно сказать, что основной способ мониторинга работы системы и приложений — это анализ содержимого журналов.

В Windows — это журналы системы и безопасности, а также журналы приложений. В Linux все журналы находятся в каталоге /var/log. Системный журнал Linux создается или специальным демоном syslogd, или самой системой инициализации (в более современных дистрибутивах). Далее мы поговорим об этом подробнее.

Протокол SNMP

Протокол SNMP позволяет контролировать оборудование информационных систем. Конечно, далеко не все оборудование поддерживает SNMP. Бюджетные устройства, предназначенные для небольших компаний, оснащены только простейшими веб-интерфейсами управления, которые позволяют увидеть лишь общую информацию о состоянии системы. В самом лучшем случае можно настроить оповещение по электронной почте — это будет вершина функционала мониторинга таких устройств. А вот устройства с поддержкой SNMP, как уже отмечалось, стоят дорого, и для небольших компаний их приобретение себя не оправдает.

Опрос служб

Есть еще один способ, который не был упомянут ранее, — опрос служб. Он заключается в том, что администратор периодически отправляет запросы серверу или серверам и опрашивает работу необходимых ему служб. Например, можно telnet'ом «подцепиться» к 80-му порту — если ответ получен, значит, веб-сервер работает. Можно отправить тестовый SQL-запрос к базе данных — что-либо простое и безобидное, главное — получить ответ. Если ответ получен, значит, сервер баз данных работает.

Конечно, если серверов много, а контролировать их доступность нужно постоянно, лучше всего написать небольшой сценарий, — скажем, на PHP, и обеспечить его регулярное выполнение средствами демона-планировщика cron или аналогичного (в Windows можно создать так называемую *задачу*).

Основное преимущество этого способа — невмешательство в контролируемые системы. На них не придется устанавливать какое-либо программное обеспечение, а один запрос, скажем, в час не перегрузит ваши серверы. Основной недостаток — подобное решение придется реализовывать вручную, и потребуются некоторые навыки программирования. Гуру программирования для этого быть не нужно, но основы надо знать. Если вы заинтересовались именно таким решением, рекомендуем книгу Д. Колисниченко «PHP и MySQL. Разработка веб-приложений» (6-е изд.) издательства «БХВ-Петербург»[1]. В ней вы найдете все необходимые знания для реализации этого решения.

Конечно, необязательно подобное решение писать на PHP. Можно использовать и другие языки программирования — например, Python. Но одно из преимуществ PHP в случае, если на вашем предприятии эксплуатируется сервер баз данных, — наличие модулей поддержки различных СУБД: от MySQL до Oracle.

---

[1] См. **https://bhv.ru/product/php-i-mysql-razrabotka-veb-prilozhenij-6-izd/**.

Мониторинг с использованием агентов

Этот способ заключается в следующем: на каждую машину устанавливается программа-агент, которая выполняет проверки по заданному графику (график или задается вручную при настройке клиента, или поступает с сервера мониторинга). Результаты проверки передаются на сервер мониторинга. Далее администратор, используя панель управления системы мониторинга, контролирует состояние тех или иных узлов сети.

Преимущество такого способа контроля заключается в том, что наблюдению доступны практически любые параметры, как оборудования, так и программной среды. Недостатки — необходимость предварительной установки агентов и затраты производительности на их исполнение (эта производительность отнимается от основных задач, для которых и установлен сервер). В зависимости от числа проверок, их частоты, производительности контролируемой системы и т. п. накладные затраты могут достигать величины 3–5% и более.

Из бесплатных OpenSource-решений можно порекомендовать систему мониторинга Zabbix (**https://www.zabbix.com/ru/**). Ее сервер мониторинга работает под управлением Linux, а вот агенты имеются для всех платформ, кроме macOS: Windows, Linux, FreeBSD, OpenBSD, Solaris, HP-UX, AIX и др. На рис. 7.1 показана панель управления Zabbix.

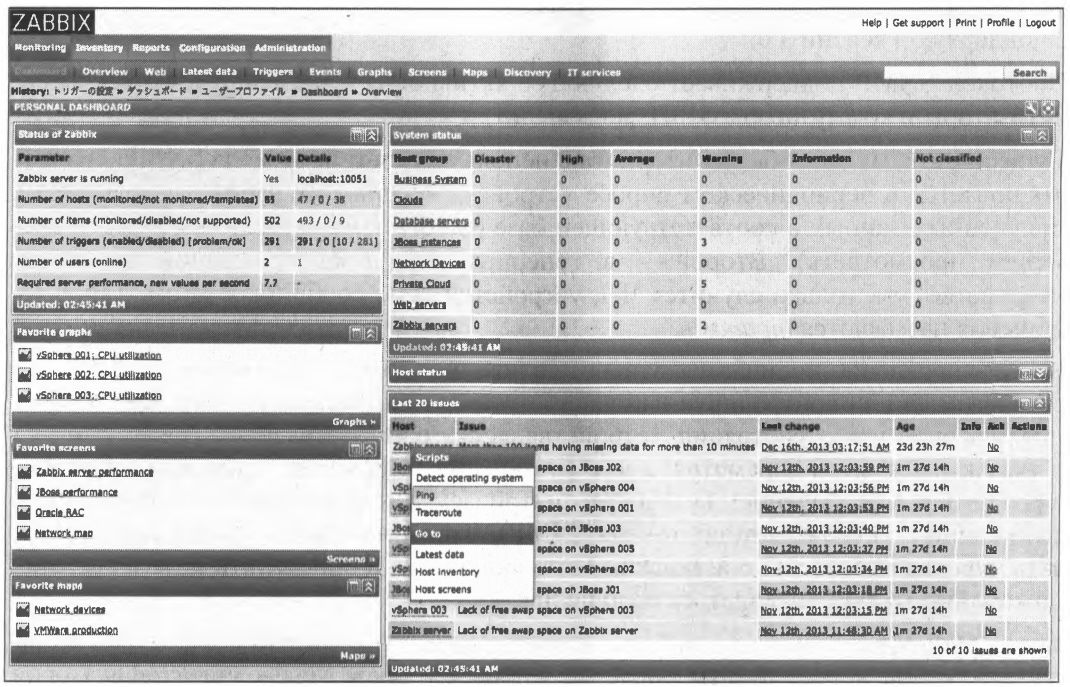


Рис. 7.1. Панель управления Zabbix

Мониторинг на основе протокола SNMP

Протокол SNMP (Simple Network Management Protocol) — простой протокол управления сетью. Впрочем, слово «простой» в названии этого протокола не совсем уместно, но так уж его назвали. Протокол используется для сбора информации от оборудования, подключенного к сети, и управления им. Другими словами, протокол SNMP служит не только для мониторинга, но и для управления сетевыми устройствами.

Устройства, поддерживающие SNMP, могут принимать команды по сети, выполнять их и передавать результаты выполнения. Как уже отмечалось, такие устройства стоят недешево — например, самый простой управляемый коммутатор всего лишь на пять портов стоит в восемь раз дороже аналогичного неуправляемого устройства того же производителя.

Для отправки управляющих сообщений протокол SNMP использует транспортный протокол UDP, который, в отличие от протокола TCP, работает без установки соединения и контроля доставки сообщения, благодаря чему снижается нагрузка на сеть.

Существуют разные версии SNMP (сейчас работают его версии 1.0 и 3.0). Недостаток SNMP-устройств версии 1.0 — нет никакой защиты, данные передаются по сети в открытом виде, их легко перехватить снифферами. Именно поэтому из соображений безопасности многое оборудование по умолчанию не поддерживает SNMP, и его в настройках оборудования нужно включать специально. Так что если вы будете разворачивать новую информационную систему, выбирайте устройства с поддержкой версии 3.0.

Протокол SNMP поддерживает следующее активное сетевое оборудование: маршрутизаторы и коммутаторы, ИБП, модемы и т. п.

Существуют два способа мониторинга с использованием протокола SNMP. Первый заключается в периодическом опросе устройств, анализе их работы и сохранении полученных данных в соответствующей базе (чтобы администратор мог их со временем просмотреть). Второй — в генерировании предупреждений на самом устройстве: как только случится ЧП, устройство само сообщит об этом. Такие сообщения называются *трапами*.

SNMP-управление отличается относительной простотой реализации. Каждый настраиваемый или контролируемый параметр имеет уникальный номер. Для получения информации о состоянии устройства достаточно отправить к нему команду с указанием номера параметра, а для управления — команду установки параметра с его номером и значением (мы не рассматриваем в этом контексте вопросы аутентификации и авторизации протокола SNMP). Чтобы настроить трапы, следует указать, для каких событий они должны быть включены, и определить адреса системы, на которую будут отправляться сообщения.

Все SNMP-совместимые устройства имеют стандартизованную конфигурацию параметров. Эта конфигурация представляет собой некое дерево идентификаторов, называемых OID (Object Identifier), — для доступа к какому-либо значению идентификатора необходимо указать полный путь к нему от самого корня. Структура

идентификаторов описывается в специальных файлах, которые называются MIB-файлами (Management Information Base). Основная часть структуры, как уже отмечено, стандартизована, но отдельные параметры описываются в проприетарных MIB-файлах (доступны к загрузке с сайтов разработчика оборудования).

> ***Пояснение***
>
> *Проприетарные* (от *англ.* proprietary) — частные, патентованные, разработанные внутри компании для собственных целей (о программных или аппаратных средствах).

MIB-файл позволяет вместо цифровых индексов использовать их символьные обозначения (это может быть более удобно для администратора, однако запрос по численному идентификатору можно выполнить всегда, а для использования символьного обозначения в программу должен быть импортирован соответствующий MIB-файл). Например, чтобы получить состояние порта коммутатора, надо запросить полное символьное значение для идентификатора:

```
.iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifOperStatus.101
```

При этом обычно разрешается опускать первую часть символов, одинаковых для контролируемых параметров: `.iso.org.dod.internet.mgmt.mib-2`. Иными словами, при запросе административного состояния порта коммутатора достаточно указать только:

```
interfaces.ifTable.ifEntry.ifOperStatus.101.
```

Интересующиеся читатели могут посетить страницу **http://www.mibdepot.com/index.shtml**, на которой собрано большое количество MIB-файлов как стандартных,

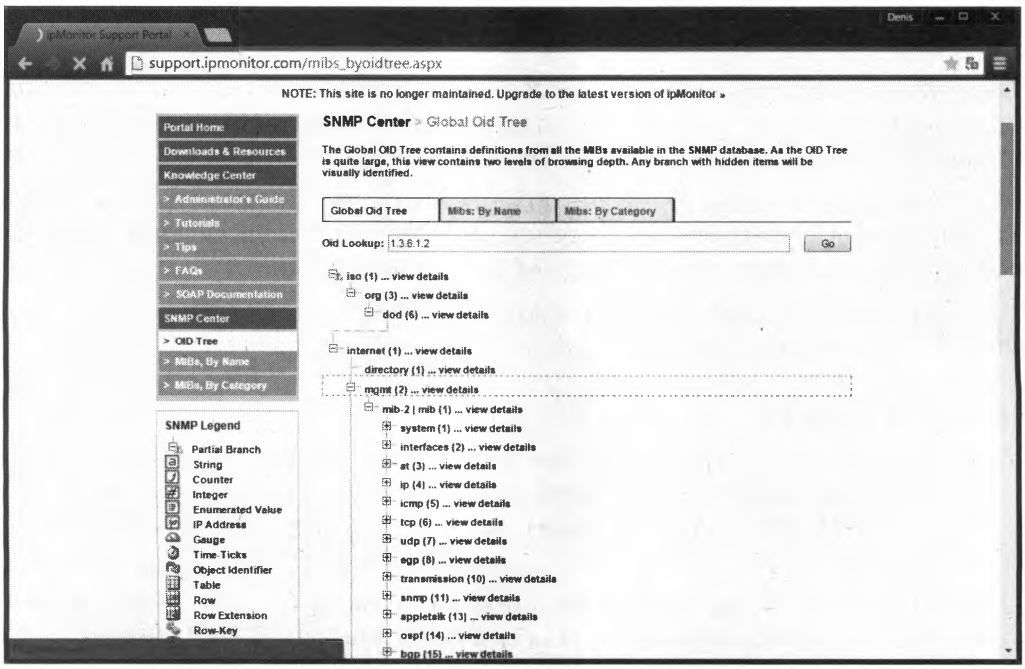


Рис. 7.2. Здесь показана страница одного из сайтов с отображением глобальной структуры MIB. Такие источники помогают правильно выбрать контролируемые параметры

так и разработки отдельных вендоров. Можно воспользоваться и любой из доступных утилит-просмотрщиков MIB-файлов, которые позволяют легко найти нужный параметр и/или идентификатор. Таких утилит очень много: HiliSoft MIB Browser, WinAgents MIB Browser, iReasoning MIB Browser и пр.

В запросах, как уже было сказано, можно использовать и символьные, и численные наименования идентификаторов. Так, указанному ранее значению соответствует индекс `.1.3.6.1.2.1.2.2.1.8.101`. Для повышения производительности системы контроля рекомендуется использовать именно численные значения, поскольку программе не придется тогда искать соответствие в файлах настроек. Хотя при символьном написании сами команды более удобочитаемы.

В большинстве случаев достаточно использовать стандартные параметры. То, какие из них соответствуют желаемой информации, легко найти в Сети по ключевым словам: `mib browser`. Например, на странице: **http://support.ipmonitor.com/mibs_byoidtree.aspx** (рис. 7.2) можно увидеть все дерево параметров и найти нужную ветвь.

Простейшие варианты мониторинга

Вы должны понимать, что профессиональные системы мониторинга, к сожалению, стоят дорого. Поэтому не все компании готовы выложить круглую сумму за такие решения. Посему вам придется или их не использовать, или использовать OpenSource-решения, которые, как правило, бесплатны.

Контроль журналов Windows

Операционная система постоянно регистрирует различные системные события и состояния выполнения тех или иных операций в журналах. Просмотреть журналы Windows можно с помощью оснастки **Просмотр событий**.

Когда компьютеров немного, можно подойти к каждому и просмотреть его журналы или же зарегистрировать их посредством RDP[1]. Но при увеличении числа компьютеров контролировать каждый из них будет очень сложно.

В этом случае администратору нужно использовать специальные возможности оснастки просмотра журналов в Windows 8/10/11 и Windows Server 2008/2022.

Привязка задачи

Администратор может настроить автоматический запуск какого-либо задания в случае возникновения события в журнале. Можно это сделать, явно указывая параметры события при создании задания, но удобнее перенести параметры из сообщения журнала.

Выделите сообщение, по появлению которого нужно выполнять некие действия, и перейдите по ссылке **Привязать задачу к событию** (рис. 7.3). Дальнейшие шаги

[1] RDP (от *англ.* Remote Desktop Protocol) — протокол удаленного рабочего стола.

будут происходить под управлением мастера операций. Вы можете назначить отсылку сообщения (в том числе по электронной почте) или запустить любую задачу.

После соответствующей настройки правила реагирования на события будут прописаны в качестве заданий в журнале планировщика (рис. 7.4).

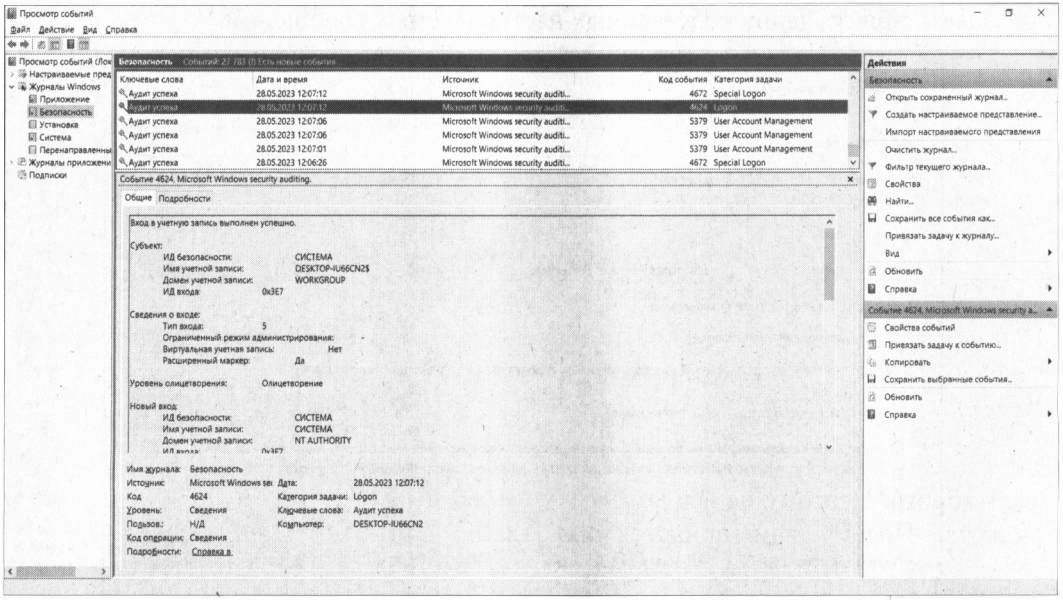


Рис. 7.3. Окно программы просмотра журнала событий

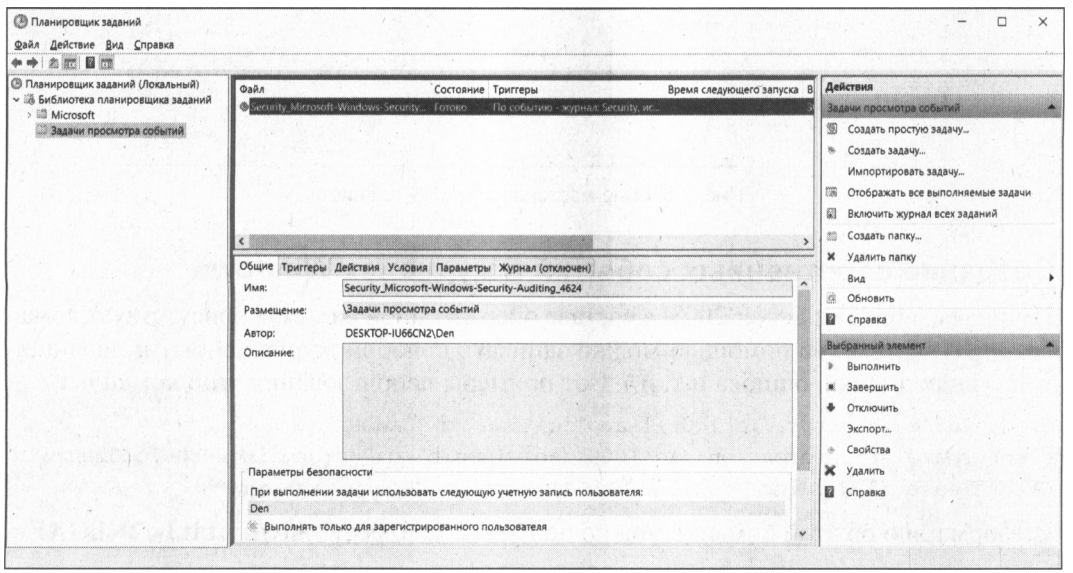


Рис. 7.4. Планировщик заданий Windows 11. Это задание отсылает сообщение по электронной почте на указанный адрес в случае появления нового сообщения в созданном администратором настраиваемом представлении журнала событий

Подписка на события

Оснастка просмотра событий позволяет собирать сообщения с других компьютеров. Для этого достаточно настроить *подписку* (рис. 7.5). При настройке подписки вы также указываете правила сбора сообщений (фильтрации), определяете компьютеры, с которых ведется сбор данных, и т. п. Обычно все собранные таким образом сообщения направляются в журнал **Пересланные события**, который можно использовать при создании собственных настраиваемых сообщений.

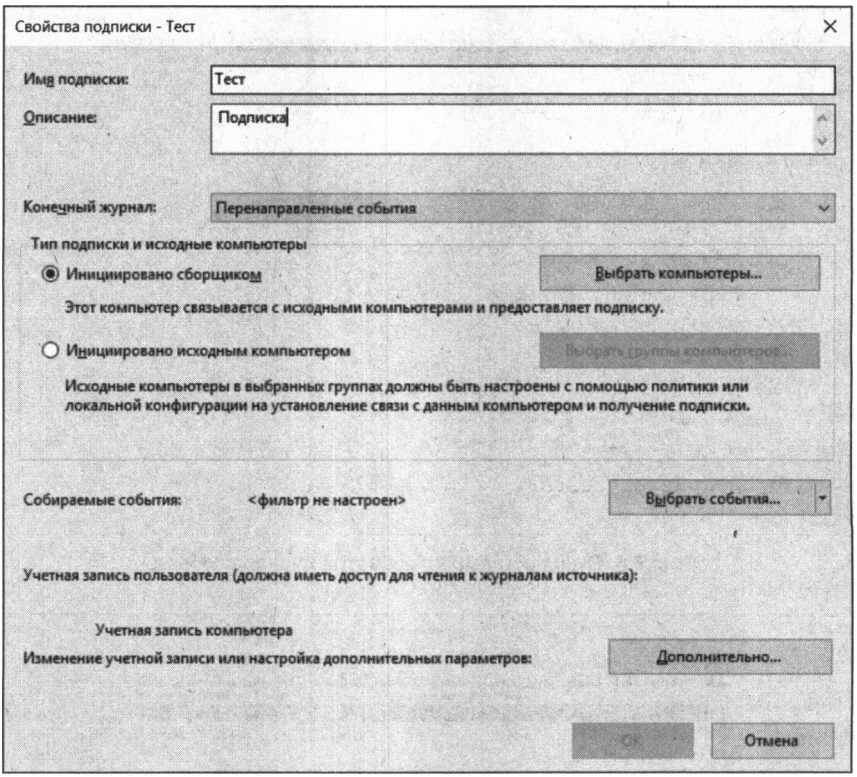


Рис. 7.5. Окно мастера настройки подписки

Создание собственных событий в журналах Windows

Начиная с Windows Server 2003, в составе операционной системы присутствует команда `EVENTCREATE`. С ее помощью можно записать в любой журнал событие заданного типа (информация, ошибка и т. п.). Вот примеры использования этой команды:

```
eventcreate /t error /id 100 /l application /d "Ошибка"
eventcreate /t information /id 1000 /so winmgmt /d "Информационное сообщение"
eventcreate /t warning /id 1000 /so winmgmt /d "Предупреждение"
```

Информацию об этой команде можно получить по адресу[1]: **https://bit.ly/2KhGAEu**.

[1] Полная ссылка: **https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-xp/bb490899(v=technet.10)?redirectedfrom=MSDN**.

Настройка журналирования в syslog

Системный журнал Linux — syslog — создается специальным демоном syslogd, которому программы отправляют свои сообщения. Подробно демон syslogd описан в *главе 11*.

Простейший мониторинг Apache

Так уж бывает, что веб-сервер Apache иногда «падает». Происходит это по разным причинам, и в большинстве случаев он требует более тонкой настройки, чем конфигурация по умолчанию. Пока администратор не разобрался, в чем причина, бывает полезным воспользоваться представленным в листинге 7.1 сценарием, опрашивающим сервер и перезапускающим сервис apache2, если сайт недоступен.

Листинг 7.1. Мониторинг и автоматический перезапуск Apache

```
#!/bin/bash
if curl -s --head --request GET https://сайт/ | grep "200 OK" > /dev/null; then
echo "Site is UP"
else
echo "Site is DOWN, restarting Apache"
date | mail -s "Site is Down" admin@example.com
/usr/sbin/service apache2 restart
fi\
```

Этот сценарий проверяет доступность сайта. Если тот недоступен, сценарий сначала отправляет сообщение об этом администратору, а затем перезапускает сервис apache2. Все достаточно просто. Такой сценарий нужно сделать исполняемым и добавить в расписание cron. Периодичность запуска — 1 минута. Да, это создаст лишние 1440 запросов к вашему сайту на протяжении суток. Если для вашего сайта это много, можно запускать сценарий один раз в 5 минут, что снизит количество обращений к сайту до 288 в сутки.

Утилиты мониторинга

Существует множество систем мониторинга — как платных, так и бесплатных. Некоторые из таких систем будут не по карману не только средним, но и многим крупным компаниям. Поэтому в этой книге основное внимание уделено OpenSource-проектам.

Среди таких решений можно порекомендовать уже упомянутые ранее Zabbix (**https://www.zabbix.com/ru/**), OpenNMS (**http://www.opennms.com**) и Nagios (**https://www.nagios.org/**). Последняя для мониторинга является стандартом де-факто, и мы ее сейчас рассмотрим подробно.

Система мониторинга Nagios

Необходимость мониторинга сети

Когда в сети один или два сервера, то достаточно просто понять, какой из них работает, а какой — нет. А вот когда в большой сети серверов несколько десятков и находятся они даже в разных городах, то хотелось бы иметь полную картину работоспособности серверов и предоставляемых ими сервисов (FTP, HTTP и пр.).

Можно написать систему мониторинга на bash — это не так уж и сложно. Впрочем, сложность, конечно, зависит от того, какую информацию вы хотите получить. Если нужно просто определить доступность сервера, то хватит простого сценария, перебирающего в цикле IP-адреса серверов и пингующего их. Однако такой простой сценарий не позволит определить, работают ли запущенные на сервере службы. Придется его усложнять... Но тратить время на разработку сложного сценария не имеет смысла — ведь все это за нас уже создано. А простой сценарий и вовсе писать незачем — уже существует сканер портов nmap, позволяющий просканировать всю сеть и определить, доступны ли ее узлы.

Так что здесь мы рассмотрим сложную систему Nagios, позволяющую производить мониторинг всевозможных сервисов сети: FTP, POP, HTTP, IMAP, SQL и пр. Система обладает модульной структурой, разрешающей добавлять новые опции мониторинга, имеется также возможность дописывать собственные модули на bash или Perl. Nagios умеет отправлять уведомления на электронную почту и подавать звуковой сигнал. Можно даже создать веб-страничку, на которой будет отображаться информация о доступности сервисов сети, история сбоев, отчеты о доступности серверов и т. д. Одним словом, Nagios — полноценная система мониторинга.

Для большего разнообразия рассматриваемых в книге систем, настройка сервера мониторинга будет производиться в условиях операционной системы FreeBSD (хотя по приведенному здесь образу и подобию вы настроите Nagios и в Linux).

Установка Nagios

Для работы Nagios нужен веб-сервер Apache. Установим Nagios:

```
# cd /usr/ports/net-mgmt/nagios
# make install clean
```

При установке Nagios следует ответить `y` на два вопроса (рис. 7.6):

You need a "nagios" group

Would you like me to create it [YES]? `y`

You need a "nagios" user

Would you like me to create it [YES]? `Y`

Организуем автоматический запуск Nagios, добавив следующую строку в файл /etc/rc.conf:

```
nagios_enable="YES"
```

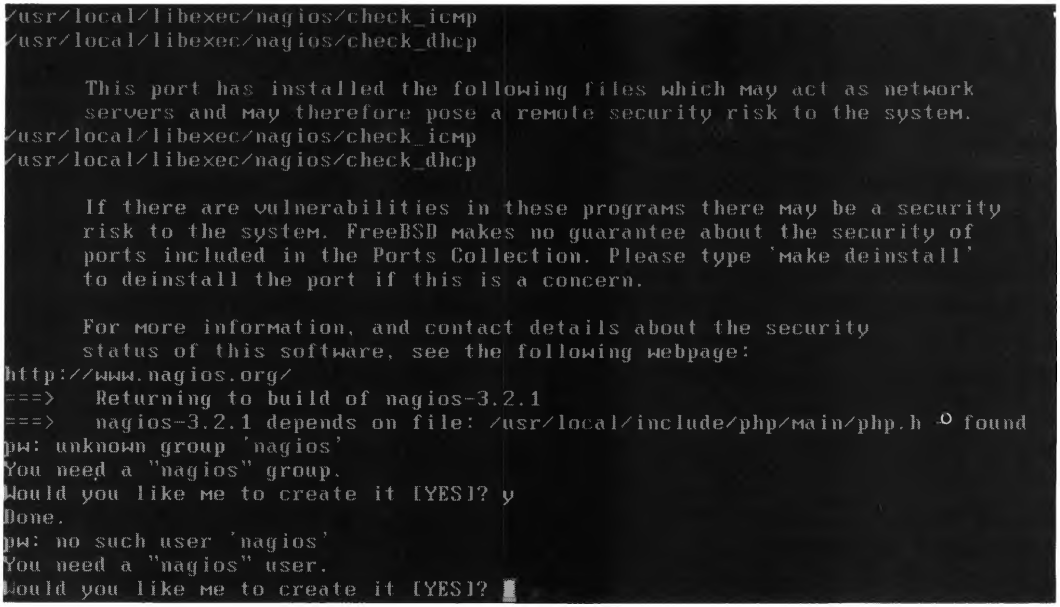


Рис. 7.6. Установка Nagios

Теперь откройте файл конфигурации Apache /usr/local/etc/apache22/httpd.conf и найдите в нем строки:

```
<Directory />
    AllowOverride None
    Order deny,allow
    Deny from all
</Directory>
```

Сразу после них добавьте следующие строки:

```
ScriptAlias /nagios/cgi-bin /usr/local/www/nagios/cgi-bin/

<Directory "/usr/local/www/nagios">
    Options ExecCGI
    AllowOverride None
    Order allow,deny
    Allow from all
    AuthName "Nagios Access"
    AuthType Basic
    AuthUserFile /usr/local/etc/nagios/htpasswd.users
    Require valid-user
</Directory>

Alias /nagios /usr/local/www/nagios/

<Directory "/usr/local/www/nagios/cgi-bin">
    Options None
    AllowOverride None
```

```
    Order allow,deny
    Allow from all
    AuthName "Nagios Access"
    AuthType Basic
    AuthUserFile /usr/local/etc/nagios/htpasswd.users
    Require valid-user
</Directory>
```

Этим вы защитите паролем доступ к каталогу nagios, чтобы никто, кроме вас, не смог промониторить вашу сеть. Информация о пользователях и паролях хранится в файле /usr/local/etc/nagios/htpasswd.users. У вас еще нет этого файла — создайте его и добавьте в него пользователей:

```
# htpasswd -c /usr/local/etc/nagios/htpasswd.users nagios
# htpasswd  /usr/local/etc/nagios/htpasswd.users admin
```

Перезапустите Apache и обратитесь к Nagios так:

```
http://адрес_сервера/nagios/
```

Настройка Nagios

Для настройки Nagios перейдите в каталог /usr/local/etc/nagios/. В нем вы найдете только файлы примеров, на основании которых следует создать реальные конфигурационные файлы.

Начнем с файла cgi.cfg-sample — в нем находится конфигурация CGI-части Nagios. Переименуйте этот файл в cgi.cfg. Весь файл со всеми комментариями мы здесь рассматривать не станем, тем более что много параметров там изменять не придется.

Прежде всего укажите путь к основному конфигурационному файлу:

```
main_config_file=/usr/local/etc/nagios/nagios.cfg
```

Затем — путь к файлам на веб-сервере:

```
physical_html_path=/usr/local/www/nagios
```

Часть URL — то, что будет после имени сервера:

```
url_html_path=/nagios
```

Включите аутентификацию:

```
use_authentication=1
```

Определите права для наших пользователей:

```
authorized_for_system_information=nagios,admin
authorized_for_configuration_information=nagios,admin
authorized_for_system_commands=nagios
authorized_for_all_services=nagios,guest,admin
authorized_for_all_hosts=nagios,guest,admin
authorized_for_all_service_commands=nagios
authorized_for_all_host_commands=nagios
```

В конфигурационном файле nagios.cfg прописываются конфигурационные файлы объектов сети, которые нужно мониторить. Например:

```
# Конфигурация для локального (FreeBSD) хоста
cfg_file=/usr/local/etc/nagios/objects/localhost.cfg

# Конфигурация для Windows-машины
cfg_file=/usr/local/etc/nagios/objects/windows.cfg

# Конфигурация для маршрутизатора/коммутатора
cfg_file=/usr/local/etc/nagios/objects/switch.cfg

# Конфигурация для сетевого принтера
cfg_file=/usr/local/etc/nagios/objects/printer.cfg
```

Далее вы выбираете один из файлов (в зависимости от типа объекта), находящихся в каталоге /usr/local/etc/nagios/objects, и на его основе создаете собственный конфигурационный файл. Давайте рассмотрим файл localhost.cfg, подходящий для тестирования компьютера под управлением FreeBSD (листинг 7.2).

Листинг 7.2. Файл localhost.cfg

```
# Определяем тестируемый узел

define host{
# Имя для шаблона – это имя можно использовать как переменную,
# с помощью которой мы будем ссылаться на этот узел
        use                     freebsd-server
# Имя тестируемого узла
        host_name               localhost
# Псевдоним
        alias                   localhost
# IP-адрес
        address                 127.0.0.1
        }

# Определим группу хостов, куда поместим все FreeBSD-машины
define hostgroup{
        hostgroup_name  freebsd-servers ; Имя группы
        alias           FreeBSD Servers ; Полное имя группы
        members         localhost       ; Список узлов, входящих
                                        ; в группу, элементы списка
                                        ; разделяются запятой
        }

# Пинг машины

define service{
# Имя сервиса (используется в этом шаблоне)
        use                             local-service
```

```
# Имя компьютера, который нужно пропинговать
        host_name                       localhost
# Описание проверки
        service_description             PING
# Команда для проверки
        check_command               check_ping!100.0,20%!500.0,60%
    }

# Определяем сервис, проверяющий свободное место на диске
# для корневого раздела локальной машины. Обычное предупреждение
# вы получите, если останется меньше 20%, а критическое — если
# меньше 10% свободного места на разделе

define service{
        use                             local-service
        host_name                       localhost
        service_description             Root Partition
       check_command                check_local_disk!20%!10%!/
        }

# Определяем сервис, проверяющий количество зарегистрированных
# в текущий момент в системе пользователей. Обычное предупреждение —
# если больше 20 пользователей, критическое — если больше 50

define service{
        use                             local-service
        host_name                       localhost
        service_description             Current Users
       check_command                check_local_users!20!50
        }

# Сервис, проверяющий кол-во запущенных процессов в текущий момент.
# Обычное предупреждение — если больше 250 процессов, критическое —
# если больше 400

define service{
        use                             local-service
        host_name                       localhost
        service_description             Total Processes
       check_command                check_local_procs!250!400!RSZDT
        }

# Проверяем загрузку локальной машины

define service{
        use                             local-service
        host_name                       localhost
```

```
        service_description             Current Load
        check_command                 check_local_load!5.0,4.0,3.0!10.0,6.0,4.0
        }

# Проверяем использование свопа на локальной машине.
# Обычное предупреждение – если осталось менее 20% свободного свопа
# Критическое – если меньше 10%

define service{
        use                             local-service
        host_name                       localhost
        service_description             Swap Usage
        check_command                    check_local_swap!20!10
        }
# Проверяем доступность SSH-сервиса на локальной машине.
# Уведомления по умолчанию отключены, поскольку не всегда
# сервис SSH запущен
define service{
        use                             local-service
        host_name                       localhost
        service_description             SSH
        check_command                   check_ssh
        notifications_enabled              0
        }
# Проверяем доступность HTTP-сервиса на локальной машине.
# Уведомления по умолчанию отключены, поскольку не всегда
# сервис HTTP запущен

define service{
        use                             local-service
        host_name                       localhost
        service_description             HTTP
        check_command                    check_http
        notifications_enabled              0
        }
```

Дополнительные примеры вы найдете в файле objects/templates.cfg-sample. Теоретически все объекты сети можно описать в одном конфигурационном файле, который потом нужно прописать в файле nagios.cfg, но такая практика не очень удобна. Гораздо удобнее для каждого объекта создать отдельный файл.

Вот, собственно, и все. Осталось только запустить Nagios:

```
# /usr/local/etc/rc.d/nagios start
```

Мониторинг в Nagios серверов Windows

Для мониторинга в Nagios систем на основе Windows разработано несколько различных агентов (плагинов). Наиболее часто используемыми из них являются NSClient++ (**http://www.nsclient.org/**), NC_NET (**http://sourceforge.net/projects/nc-net**) и OpMonAgent (**http://www.opservices.com/download/**). Функциональность этих агентов практически идентична, поэтому мы рассмотрим использование агента NSClient++, являющегося, на взгляд авторов, наиболее популярным из упомянутых.

Агент NSClient++ можно загрузить как в виде архива (*.zip), так и установочным файлом (*.msi), причем для 32- и 64-битных платформ следует использовать соответствующие версии агента. Загруженный архив необходимо распаковать в желаемую папку и установить службу Windows командой:

```
NSClient++ -install
```

Удобнее воспользоваться MSI-файлом, поскольку в этом случае мастер установки сразу внесет в конфигурацию агента часть настроек по результатам ваших ответов (рис. 7.7).

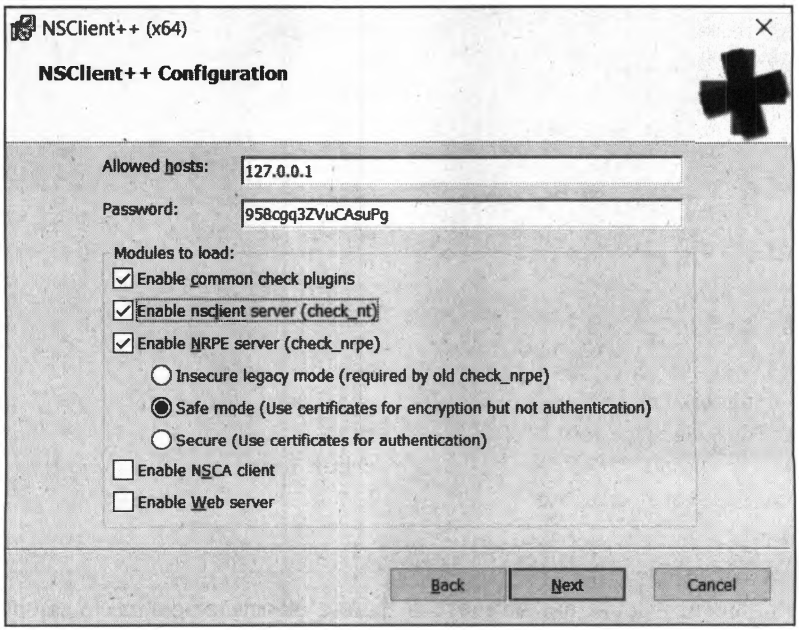


Рис. 7.7. Настройка параметров программы NSClient++. Настройки пользователя, введенные на этапе установки, будут сохранены программой в файле конфигурации

После установки необходимо разрешить взаимодействие службы с рабочим столом, для чего следует открыть свойства службы: **Панель управления | Администрирование | Службы**, найти службу **NSClientpp...** (полное название зависит от версии), открыть ее свойства и включить опцию **Разрешить взаимодействие с рабочим столом**.

Перед запуском службы следует *обязательно* проверить параметры ее работы. Для этого откройте файл nsc.ini (в папке установки агента) и снимите комментарий с тех строк, которые соответствуют модулям программы, предполагаемым к использованию для мониторинга системы. Достаточно подробные описания параметров конфигурации приведены в документации плагина по адресу: **https://docs.nsclient.org/**.

При настройке конфигурации следует исходить из принципа, что не следует включать больше опций, чем это необходимо в текущий момент. Например, если вы не планируете получать информацию посредством WMI-запросов, то и не стоит загружать модуль CheckWMI.dll (работа с этим модулем описана чуть далее).

Обратите внимание на возможность запуска агента в *диагностическом режиме*. При этом вы сможете как увидеть потенциальные ошибки в конфигурационном файле, так и отладить собственные запросы. Для запуска NSClient++ в диагностическом режиме достаточно в командной строке набрать:

```
NSClient++ /test
```

В окне **NSClient++** вы сможете, во-первых, увидеть результаты загрузки всех модулей, а во-вторых, вводить собственные команды и видеть результаты выполнения как запросов со стороны сервера Nagios, так и локальных команд. На рис. 7.8 показано окно отладки плагина, в котором введена команда:

```
CheckDriveSize ShowAll MinWarnFree=20% MinCritFree=10% Drive=D:\
```

и виден ответ системы.

```
C:\Tools\NSClient++>"NSClient++.exe" /test
Launching test mode - client mode
d NSClient++.cpp(1178) Enabling debug mode...
d NSClient++.cpp(551) Attempting to start NSClient++ - 0.3.8.76 2010-05-27
d NSClient++.cpp(969) Loading plugin: CheckDisk...
d NSClient++.cpp(969) Loading plugin: Event log Checker....
d NSClient++.cpp(969) Loading plugin: CheckSystem...
d NSClient++.cpp(969) Loading plugin: CheckWMI...
d \PDHCollector.cpp(73) Autodetected w2k or later, using w2k PDH counters.
d NSClient++.cpp(969) Loading plugin: NRPE server (w/ SSL)...
d \PDHCollector.cpp(110) Using index to retrive counternames
d \NRPEListener.cpp(91) Loading all commands (from NRPE)
d \NRPEListener.cpp(121) Starting NRPE socket...
d NSClient++.cpp(671) NSClient++ - 0.3.8.76 2010-05-27 Started!
d \Socket.h(669) Bound to: 0.0.0.0:5666
1 NSClient++.cpp(455) Using settings from: INI-file
1 NSClient++.cpp(456) Enter command to inject or exit to terminate...
d \PDHCollector.cpp(130) Found countername: CPU:    \Processor(_total)\% Process
or Time
d \PDHCollector.cpp(131) Found countername: UPTIME: \System\System Up Time
d \PDHCollector.cpp(132) Found countername: MCL:    \Memory\Commit Limit
d \PDHCollector.cpp(133) Found countername: MCB:    \Memory\Committed Bytes
```

Рис. 7.8. Окно программы NSClient++ в диагностическом режиме

Плагин NSClient++ позволяет контролировать параметры, приведенные в табл. 7.1. Подробности его использования детально описаны в технической документации (см. ранее приведенную ссылку), и по имеющимся там примерам легко составить собственные команды контроля состояния Windows.

Таблица 7.1. *Параметры Windows, контролируемые NSClient++*

Параметр	Описание
`CheckFileSize`	Контролирует размер файла или папки
`CheckDriveSize`	Контролирует размер свободного или использованного пространства жестких или сменных дисков (тип диска можно выбирать в команде)
`CheckFile`	Контролирует файлы по критериям даты их создания, времени последнего доступа, записи в файл или по размеру файла
`CheckEventLog`	Ищет сообщения об ошибках в файле журнала. Поскольку таких сообщений обычно много, использование этого вида контроля сильно загружает систему
`CheckCPU`	Контролирует загрузку процессора в течение задаваемого периода времени
`CheckUpTime`	Контролирует время работы системы
`CheckServiceState`	Контролирует состояние службы Windows (критическое сообщение формируется в случае несоответствия фактического состояния службы заданному в качестве параметра в команде). Можно контролировать все службы одновременно с заданием исключения. В качестве названия службы надо указывать то, которое отображается в свойствах службы
`CheckProcState`	Контролирует состояние процессов Windows. Фактически позволяет наблюдать за состоянием процесса, найденного по имени исполняемого файла. Можно контролировать также по числу одновременно запущенных процессов
`CheckMem`	Контролирует состояние виртуальной и физической памяти; доступен параметр количества записанных страниц памяти (commited pages)
`CheckCounter`	Контролирует значения счетчиков производительности. Объекты счетчиков желательно — в целях удобства использования — задавать в описаниях команд (служб)

`CheckAlwaysOK`
`CheckAlwaysCRITICAL`
`CheckAlwaysWARNING`
`CheckMultiple`
`CheckOK`
`CheckCRITICAL`
`CheckWARNING`
`CheckVersion`
	Так называемые *хэлперы*. Возвращают заранее определенное значение (какое — можно судить по названию команды). Используются в процессах настройки и отладки системы

Приведенным в табл. 7.1 списком не ограничиваются возможности контроля Windows-систем. Вы можете добавить контролируемые параметры, например, за счет использования внешних сценариев.

Мониторинг систем Windows может осуществляться на основе различных протоколов. Наиболее часто применяемыми являются протоколы NSClient и NRPE (для

«пассивного» мониторинга можно задействовать также протокол NSCA, о котором более подробно можно прочесть в онлайновой документации). На практике можно использовать любой из них — необходимо только включить/выключить соответствующие модули в файле настроек клиента nsc.ini. В то же время, на взгляд авторов, протокол NRPE несколько более гибок в использовании и обеспечивает шифрование данных обмена.

При работе с протоколом NRPE синтаксис команд строится следующим образом:

```
check_nrpe ... -c <команда> -a <аргументы>
```

Например, проверка доступной физической памяти может быть осуществлена так:

```
check_nrpe -H 192.168.0.9 -c CheckMem -a MaxWarn=70% MaxCrit=>80% type=physical
```

Мониторинг Windows-систем на основе WMI

В состав агента NSClient++ входит модуль CheckWMI.dll, позволяющий контролировать Windows-систему с использованием инструментария WMI.

Модуль CheckWMI.dll фактически состоит из двух подмодулей: CheckWMIValue и собственно CheckWMI. Подмодуль CheckWMIValue оптимизирован для контроля численных значений — например, текущей загруженности процессора (это число процентов загрузки) или разрешения монитора (число пикселов) и т. п. Работая с ним, вы можете просто указать контролируемые параметры и минимальные/максимальные допустимые для них значения, например, так:

```
CheckWMIValue "Query=Select PelsWidth from win32_DisplayConfiguration"
MinCrit=640 MinWarn=800 Check:Width=PelsWidth
```

Приведенная здесь команда составлена для использования в режиме отладки (`nsclient++ /test`). Она запрашивает разрешение дисплея по горизонтали и сообщает о критическом состоянии в случае, если оно равно или менее 640, и выдает предупреждение, если значение не превосходит 800. Из особенностей использования этой команды отметим, что после строки запроса (которая заключена в кавычки) нужно указать параметры минимальных/максимальных значений и только потом задавать название параметра, который контролируется командой (здесь: `PelsWidth`). Поясним также опцию `Check`, присутствующую в командной строке. После `Check` необходимо вписать название параметра, которое будет применяться в системе контроля (можно сохранить и название из описания в WMI, но часто более удобно ввести собственное название), и название, соответствующее объекту класса (то, которое отображается, например, в утилите просмотра WMI Object Browser).

Другие примеры (в том числе в вариантах для конфигурации Nagios) вы легко найдете поиском на странице документации агента NSClient++ (см. ранее приведенную ссылку).

Подмодуль CheckWMI нужно использовать в тех случаях, когда предполагается либо анализ строкового параметра, возвращаемого в результате WMI-запроса, либо запрос нескольких значений. При использовании подмодуля CheckWMI строки запроса несколько усложняются из-за необходимости применения фильтров. Синтаксис подмодуля CheckWMI вы также найдете на странице документации агента

NSClient++ (см. ранее приведенную ссылку). По своему построению запросы подмодуля CheckWMI сходны с фильтрами, используемыми для анализа журналов работы системы.

Мониторинг в Nagios серверов Linux

Контроль работы серверов Linux осуществляется с использованием плагина NRPE, причем на сервере Nagios он должен быть установлен как плагин, а на контролируемой системе Linux — в качестве демона. Для установки может быть использована как подготовленная версия, так и исходные коды плагина.

Кроме стандартного комплекта, администратор может задействовать при мониторинге любой из доступных плагинов, которые широко представлены в Интернете.

Используя протокол NRPE, можно на контролируемом хосте вызвать команду `check_nrpe` для проверки другого хоста. Этот способ дает возможность контролировать некоторую подсеть через один компьютер. При такой организации контроля на хосте, используемом в качестве прокси, обязательно должны быть установлены как демон протокола NRPE, так и плагин.

Мониторинг систем с использованием протокола SNMP

Для работы по протоколу SNMP в Nagios должен быть установлен соответствующий плагин. Он включен в состав плагинов Nagios, но воспользоваться им можно только в том случае, если предварительно был установлен пакет net-snmp. Поэтому, если предполагается использование SNMP-модуля, этот пакет необходимо загрузить с сервера **https://net-snmp.sourceforge.net/**, после чего заново перекомпилировать плагины и повторно установить их. Авторы рекомендуют при новой установке сначала выполнить команду `make clean`, которая очистила бы настройки предыдущей инсталляции.

> ***Примечание***
>
> На сайте **https://net-snmp.sourceforge.net/** необходимый пакет представлен только в исходных кодах или в RPM-формате.

После настройки контроля по протоколу SNMP необходимо протестировать работоспособность системы на простейших запросах. Например, проверить длительность работы устройства:

```
/usr/local/nagios/libexec/check_snmp -H <адрес_устройства> -C <community>
                                                    -o sysUpTime.0
```

> ***Примечание***
>
> В примерах использован протокол SNMP версии 1. В реальных условиях обычно используется протокол версии 3, поэтому примеры необходимо дополнить параметрами аутентификации.

В ответ вы должны получить примерно такое сообщение:

```
SNMP OK - Timeticks: (622339555) 72 days, 0:43:15.55 |
```

Команда `check_snmp` может запрашивать параметр, принимающий численное значение, и проверять соответствие его значения некоторому диапазону. Так, можно указать значения для состояния предупреждения и критического состояния (ключи: `-w` и `-c`) или диапазон значений (через двоеточие). Обратите внимание, что если вы хотите, чтобы, например, критическим значением интерпретировалось возвращаемое число в диапазоне от *a* до *b* (*b* > *a*), то диапазон нужно указывать так: `b:a`. Если указать диапазон в привычном виде: `a:b`, то, если возвращаемое значение *попадает* в этот диапазон, результат будет считаться нормальным состоянием, а если не попадает — то как предупреждение или критическое (в зависимости от использованного ключа). Кроме того, команда может проверять возвращаемое строковое значение (значение, с которым проверяется ответ, следует указать в ключе `-s`) или даже выполнять проверку с использованием регулярных выражений (ключи `-r`, `-R`). В запросе также можно проверять сразу несколько параметров, указывая их OID через запятую, — например, так:

```
//usr/local/nagios/libexec/check_snmp -H <адрес> -C <community> -o
.1.3.6.1.2.1.2.2.1.7.101,.1.3.6.1.2.1.2.2.1.7.102,.1.3.6.1.2.1.2.2.1.7.103
SNMP OK - 1 1 1 | iso.3.6.1.2.1.2.2.1.7.101=1 iso.3.6.1.2.1.2.2.1.7.102=1
iso.3.6.1.2.1.2.2.1.7.103=1
```

После того как запрос будет составлен и отлажен, достаточно описать новую команду в файле commands.cfg и добавить нужные службы в файлы описания контролируемых устройств.

В Сети можно найти достаточное число примеров настройки Nagios для контроля устройств с использованием протокола SNMP, которые можно применить на практике. Так, по адресу: **http://wiki.nagios.org/index.php/Howtos:snmp-apc-smart-ups** содержится описание настроек, с помощью которых можно контролировать состояние источников бесперебойного питания (UPS): состояние батареи, параметры напряжения, температуру и пр.

Сервер протоколов

Постановка задачи

Иногда нужно, чтобы протоколы со всех серверов сети аккуратно собирались на одном центральном сервере. Зачем? Просматривать протоколы серверов нужно далеко не всегда, а только в том случае, когда что-то «сломалось». Тогда можно удаленно зайти на интересующий нас сервер и просмотреть его журналы. Собственно, никакой необходимости в централизованном сервере протоколов нет.

Но представим другую ситуацию, когда нам нужно ежедневно не только собирать, но и обрабатывать протоколы. Каждый день заходить на каждый сервер и копировать его протоколы как-то не очень хочется. Проще заставить это сделать за нас компьютер. Точнее, несколько компьютеров — каждый сервер вместо того, чтобы записывать сообщение в собственный журнал, будет отправлять его на центральный сервер. В итоге мы получим некий архив протоколов на одном сервере. А там

осталось дело за малым — написать на bash/awk сценарий для их обработки (в зависимости от того, что нужно сделать).

Мы же немного усложним эту задачу и не станем не просто «сваливать в кучу» протоколы со всех серверов, а сразу будем помещать их в базу данных (MySQL) и анализировать программой loganalyzer.

Нам не известно, какие именно задачи вы перед собой ставите, но у этого решения есть два преимущества. Во-первых, вы получаете удобный веб-интерфейс, позволяющий просматривать логи серверов сети. Во-вторых, все журналы будут храниться в базе данных MySQL, что также весьма удобно. Ведь можно через phpMyAdmin[1] отправить любой запрос к этим данным и сделать любую выборку. Можно также написать приложение на PHP (или любом другом языке с поддержкой MySQL), что гораздо удобнее написания сценариев на bash/awk. Хранение журналов в базе данных открывает огромные возможности по их обработке, в противовес их хранению в обычных текстовых файлах.

Перед тем как приступить к настройке, рекомендуем ознакомиться с веб-интерфейсом, чтобы вы представляли, как все это будет выглядеть, и приняли решение, нужно ли это вам. Демоверсия анализатора loganalyzer доступна по адресу: **http://demo.phplogcon.org/**. За исключением рекламы, все будет выглядеть именно так.

Настройка основного (центрального) сервера

Прежде всего, нужно установить сервер rsyslog (забегая вперед, отметим, что rsyslog придется установить на всех серверах сети). Для этого выполните команды (напомним, что сервер работает под управлением FreeBSD):

```
cd /usr/ports/sysutils/rsyslog55
make install clean
```

Сразу устанавливаем модуль поддержки MySQL:

```
cd /usr/ports/sysutils/rsyslog55-mysql
make install clean
```

Затем останавливаем стандартный syslog:

```
/etc/rc.d/syslogd stop
```

И производим его замену на rsyslog путем редактирования файла /etc/rc.conf:

```
syslogd_enable="NO"
rsyslogd_enable="YES"
rsyslogd_flags="-c4"
rsyslogd_pidfile="/var/run/syslog.pid"
apache_enable="YES"
mysql_enable="YES"
```

[1] PHPMyAdmin — веб-приложение с открытым кодом, написанное на языке PHP и представляющее собой веб-интерфейс для администрирования СУБД MySQL.

Первая строка отключает запуск демона syslogd, следующие три строки обеспечивают запуск демона rsyslogd и устанавливают некоторые его параметры. Предпоследняя строка — это запуск Apache, который необходим нам для веб-интерфейса анализатора протоколов.

Настало время отредактировать файл конфигурации /usr/local/etc/rsyslog.conf (листинг 7.3).

Листинг 7.3. Файл /usr/local/etc/rsyslog.conf

```
# Модули
$ModLoad imuxsock
$ModLoad imklog
# Модуль поддержки MySQL
$ModLoad ommysql
$ModLoad imudp
# Номер UDP-порта
$UDPServerRun 514
$ModLoad imtcp
# Номер TCP-порта
$InputTCPServerRun 514

# Параметры доступа к БД MySQL
# Здесь 127.0.0.1 - адрес сервера БД
# log - название базы данных
# loguser - имя пользователя
# 123456 - пароль
# Укажите свои параметры доступа и не забудьте создать
# указанного пользователя и БД
*.*  :ommysql:127.0.0.1,log,loguser,123456

# Владелец и группа владельца
$FileOwner root
$FileGroup wheel
```

Файл конфигурации небольшой. Можно, конечно, настроить еще и уведомление по электронной почте (модуль ommail) — для тех случаев, когда сервер будет получать критические сообщения (crit, alert, emerg), но это создаст ненужный поток еще и почтового трафика. И, надо признаться, поток трафика окажется немалым, а скорость роста базы данных с протоколами составит несколько сотен килобайт в минуту. Так что прежде, чем настраивать подобный сервер, убедитесь, что у вас достаточно свободного пространства. Скажем, если у вас имеется 10 серверов, отправляющих свои журналы центральному серверу, база данных станет «раздуваться» примерно на 100 Кбайт каждую минуту. За один час — 6000 Кбайт, т. е. почти 6 Мбайт, а за одни сутки при надлежащей загрузке серверов вы получите прирост около 144 Мбайт. Несложный подсчет показывает, что за один месяц база вырастет на 4 Гбайт. Этот факт нужно учитывать. Ежели мы организуем еще и уведомление

по электронной почте, то станем раздувать и почтовый ящик — пусть не с такой скоростью, но все же...

Продолжим настройку. Теперь вам нужно установить Apache и MySQL, если вы это еще не сделали. А мы тем временем установим loganalyzer:

```
cd /usr/ports/sysutils/loganalyzer
make install clean
```

При установке loganalyzer следует выбрать поддержку MySQL (рис. 7.9).

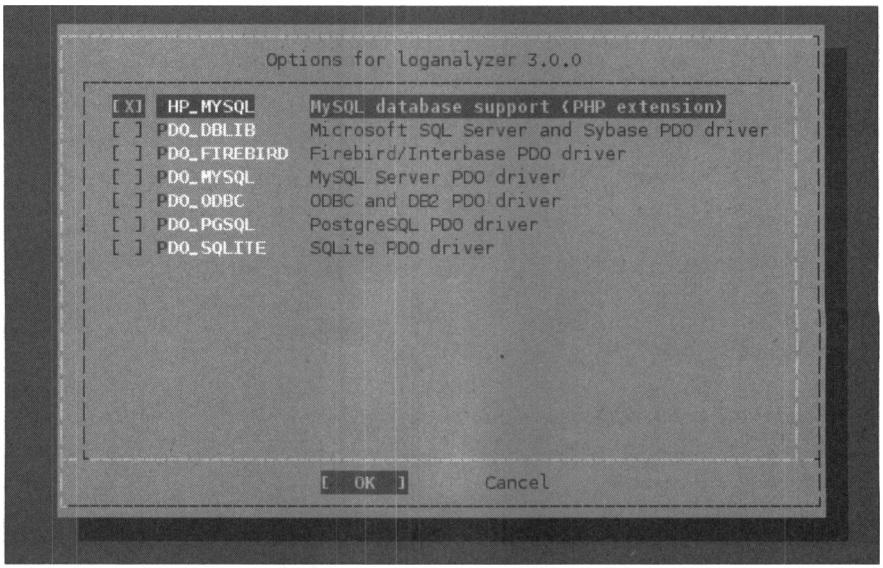


Рис. 7.9. Установка loganalyzer

Затем переходим в каталог /usr/local/www, находим в нем каталог анализатора журналов, заходим в него и копируем все, что есть в каталоге src, в любой из подкаталогов корневого каталога веб-сервера (можно создать, например, каталог logs и скопировать все в него — название, сами понимаете, значения не имеет).

Создаем конфигурационный файл config.php:

```
touch config.php
chmod 666 config.php
```

Не забудьте создать базу данных и пользователя, а также предоставить ему доступ к базе данных. После этого устанавливаем таблицы, необходимые для rsyslog:

```
sudo /usr/local/share/examples/rsyslog/mysql_createDB.sql
```

Запускаем Apache, если он еще не запущен:

```
sudo systemctl start apache2
```

Затем открываем браузер и переходим в каталог, в который поместили содержимое src, — в нашем случае это каталог logs:

```
http://127.0.0.1/logs
```

Начнется установка loganalyzer — дальнейшее понятно. При установке как раз и указываем адрес сервера БД, название БД, имя пользователя, пароль. Все эти данные будут записаны в файл config.php.

После установки желательно изменить права доступа к файлу config.php на 644. Вот, собственно, и все. Можно приступить к настройке серверов, с которых мы будем собирать протоколы.

Если при доступе к веб-интерфейсу вы увидите ошибку **No syslog records found**, откройте phpMyAdmin и отправьте следующий запрос к базе данных:

```
ALTER TABLE `systemevents` ADD `Checksum` int(11) NOT NULL
DEFAULT `0`; AFTER `SystemID`;
```

Настройка остальных серверов сети

Вам нужно установить демон rsyslogd на каждом сервере сети (при этом не имеет значения, под управлением какой операционной системы: FreeBSD или Linux, работает сервер — главное, чтобы был установлен rsyslogd) и отредактировать файл его конфигурации rsyslog.conf. Формат этого файла следующий:

```
селектор[;селектор]   действие
```

Параметр `селектор` определяет, какие сообщения должны быть запротоколированы. Вот список наиболее часто использующихся селекторов:

- `auth`, `security` — все, что связано с регистрацией пользователя в системе;
- `authpriv` — отслеживает программы, изменяющие привилегии пользователей (например, программу su);
- `cron` — сообщения планировщиков заданий;
- `kern` — сообщения ядра;
- `mail` — сообщения почтовых программ;
- `news` — сообщения новостного демона;
- `uucp` — сообщения службы Unix-to-Unix-CoPy, уже давно не используются, но файл конфигурации демона все еще содержит упоминание о ней;
- `syslog` — сообщения самого демона rsyslogd;
- `user` — сообщения пользовательских программ;
- `daemon` — сообщения различных сервисов;
- `*` — все сообщения.

При указании селектора можно определить, какие сообщения нужно протоколировать:

- `debug` — отладочные сообщения;
- `info` — информационные сообщения;

- `err` — ошибки;
- `warning` — предупреждения (некритические ошибки);
- `crit` — критические ошибки;
- `alert` — тревожные сообщения, требующие вмешательства администратора;
- `emerg` — очень важные сообщения (произошло что-то такое, что мешает нормальной работе системы);
- `notice` — замечания.

Впрочем, обычно селекторы указываются так:

```
название_селектора.*
```

Это означает, что будут протоколироваться все сообщения селектора. Вот еще несколько примеров:

- `daemon.*` — протоколируются все сообщения сервисов;
- `daemon.err` — регистрировать только сообщения об ошибках сервисов.

Теперь перейдем к параметру `действие` — это второе поле файла конфигурации. В большинстве случаев `действие` — это имя файла журнала, в который нужно записать сообщение селектора. Если перед именем файла стоит знак «минус» (-), то после каждой записи в журнал демон не будет выполнять синхронизацию файла, т. е. осуществлять системный вызов `fsync()`. Это повышает производительность системы, поскольку сообщений обычно много, и если после каждого выполнять синхронизацию журнала, то система будет работать медленно.

В большинстве случаев в файл конфигурации нужно добавить всего одну строку:

```
*.info;mail.none;authpriv.none;cron.none @@IP_центрального_сервера:514
```

Две «собачки» перед строкой означают, что сообщения протокола будут переданы удаленному серверу rsyslog (514 — это порт, который используется удаленным сервером).

Если вы какие-то сообщения желаете отправлять в файл, а не на сервер (для уменьшения размера БД сервера), то просто укажите имя файла, например:

```
mail.* -/var/log/maillog
```

Если есть желание выводить сообщения на консоль всех подключенных к системе пользователей, то вместо действия поставьте звездочку:

```
*.emerg  *
```

Протоколирование системой инициализации в Linux

Если вы уже работали с Linux, то знаете, что ранее протоколирование системы осуществляли демоны syslogd и rsyslogd. Сейчас же все устроено немного иначе — во многих современных дистрибутивах протоколированием системы занимается

сама система инициализации systemd, а точнее — ее сервис systemd-journald.service. При этом запрос системного лога (журнала) организуется через утилиту journalctl.

Протоколирование через сервис systemd-journald.service впервые появилось в Fedora 20, перешли на systemd и все современные дистрибутивы, среди которых Fedora, CentOS, Debian и Ubuntu (начиная с 15.04). Однако в дистрибутивах, основанных на системе инициализации, отличной от systemd, может использоваться демон syslogd, — именно поэтому его описание не удалено из книги (см. *главу 11*).

Вот что нужно знать о протоколировании в современных дистрибутивах:

- все журналы по-прежнему хранятся в каталоге /var/log;
- серверы (WWW, FTP и пр.) могут создавать собственные каталоги/файлы журналов в каталоге /var/log;
- для просмотра системных журналов используется утилита journalctl — привычные файлы вроде /var/log/messages больше недоступны. Конечно, вы можете параллельно установить демон rsyslogd, и он будет прекрасно работать в паре с journalcrl. Однако у journalctl гораздо больше возможностей — например, с помощью опции `-b` можно просмотреть логи текущей или предыдущей загрузки;

  > ***УТИЛИТА JOURNALCTL***
  >
  > Полное описание утилиты journalctl можно найти в руководстве *man* или по адресу: **http://www.freedesktop.org/software/systemd/man/journalctl.html**. Подробно эта утилита также рассматривается в книге Д. Колисниченко «Linux. От новичка к профессионалу» (7-е изд.) издательства «БХВ-Петербург»[1].

- существует графическая утилита просмотра журналов — gnome-system-log (рис. 7.10). Она не устанавливается по умолчанию, и чтобы ее установить, введите команду:

  ```
  sudo dnf install gnome-system-log
  ```

  Впрочем, учитывая, что просмотр основных журналов осуществляется через утилиту journalctl, особого эффекта от использования gnome-system-log вы не ощутите.

Для просмотра логов введите команду `journalctl` — будет выведен огромный список различных записей. Использовать команды постраничного вывода вроде `more` необходимости нет, поскольку подобные средства просмотра журнала уже встроены в саму утилиту journalctl (рис. 7.11).

Обратите внимание на самую первую строку — она говорит, с какого момента начинается ведение логов. Как правило, это дата установки системы. Понятно, что с самого начала будет очень много записей и их как-то нужно фильтровать.

---

[1] См. **https://bhv.ru/product/linux-ot-novichka-k-professionalu-7-e-izd-pererab-i-dop/**.

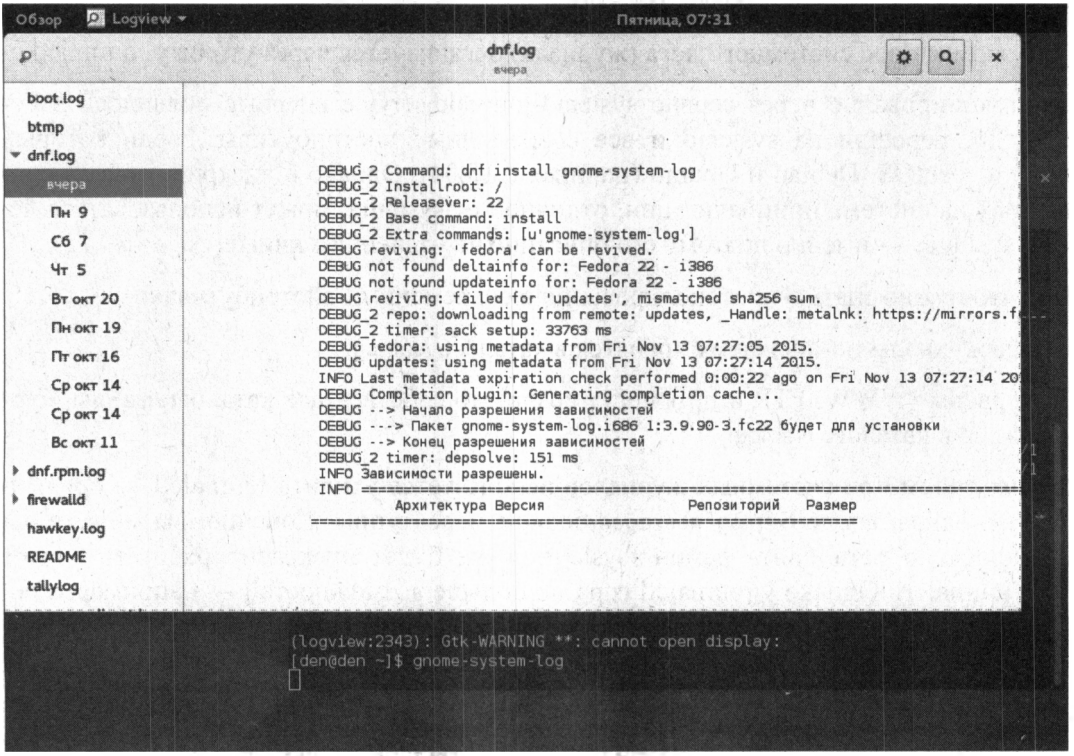


Рис. 7.10. Графическая утилита просмотра журналов gnome-system-log

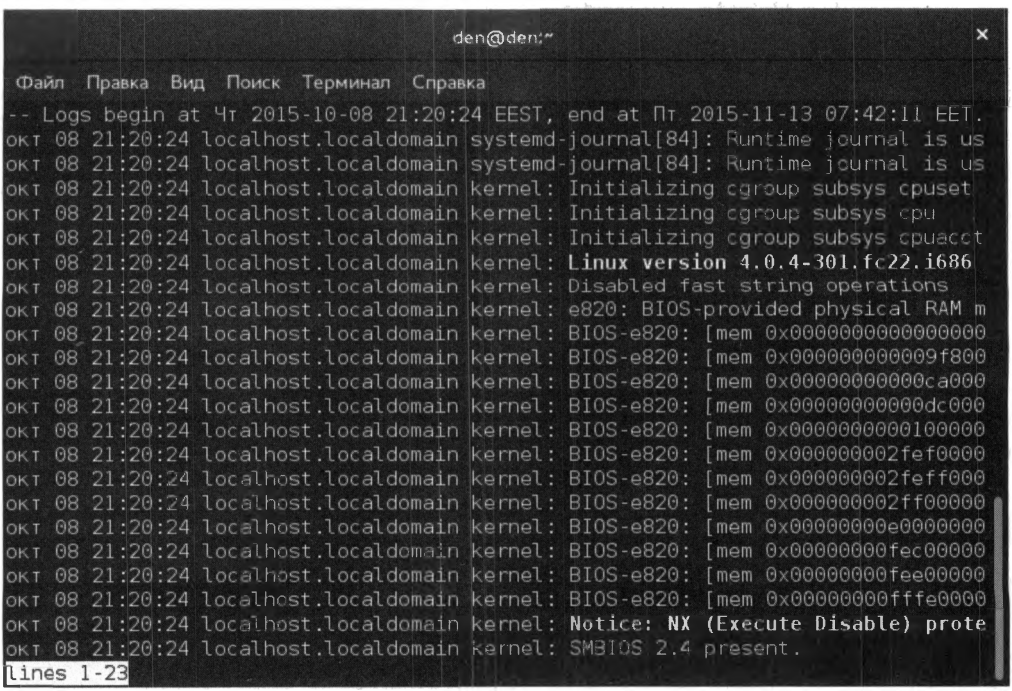


Рис. 7.11. Просмотр журнала утилитой journalctl

Системы мониторинга трафика

Проблема мониторинга трафика волнует каждого администратора. Может быть сейчас, когда соединения с безлимитным трафиком — реальность, вопрос о мониторинге трафика стоит не столь остро. Но ведь нужно же чем-то заняться администратору? BSD-машины нередко конфигурируются по принципу «настроил и забыл», а у администратора свой принцип: «админ спит, зарплата идет». Но такой образ жизни рано или поздно надоедает, поэтому иногда возникает желание «прикрутить» к своему серверу что-нибудь полезное.

В этом разделе мы рассмотрим две системы мониторинга трафика: достаточно простую систему darkstat, рисующую графики загрузки трафика, напоминающие графики всем известной программы MRTG, и полноценную систему мониторинга NetTAMS. Кому-то хватит первой системы, а у кого-то возникнет необходимость в использовании второй — более сложной и совершенной.

Простейшая система мониторинга трафика: darkstat

Первым делом нужно установить пакет с darkstat. Например, в FreeBSD (раз мы уже на примере FreeBSD рассматривали Nagios, не будем менять операционную систему в середине главы) это можно сделать так:

```
# pkg_add -r darkstat
```

Особой необходимости устанавливать darkstat из портов нет, поэтому устанавливаем ее из пакета, благодаря чему сэкономим немного времени. Сразу после установки открываем файл /etc/rc.conf и добавляем пока только эти строки:

```
darkstat_enable="YES"
darkstat_interface="em0"
```

Первая строка обеспечивает автоматический запуск darkstat, а вторая определяет интерфейс, который мы будем мониторить.

Запускаем darkstat:

```
# /usr/local/etc/rc.d/darkstat start
```

Проверяем, запущен ли darkstat:

```
# ps -ax | grep dark
```

Определяем порт, на котором работает darkstat:

```
# sockstat -4 | grep dark
```

Как можно видеть на рис. 7.12, darkstat запущен и работает на порту 667. Но обращаться к darkstat пока рано. Надо сгенерировать немного трафика, чтобы было, что показывать на графике. Интерфейс `em0` в этом примере используется для доступа к Интернету, поэтому мы можем сгенерировать трафик путем загрузки какого-нибудь большого файла:

```
# wget https://download.fedoraproject.org/pub/fedora/linux/releases/38/
Workstation/x86_64/iso/Fedora-Workstation-Live-x86_64-38-1.6.iso
```

```
denhost# pkg_add -r darkstat
Fetching ftp://ftp.freebsd.org/pub/FreeBSD/ports/i386/packages-8.1-release/Lates
t/darkstat.tbz... Done.
denhost# mcedit /etc/rc.conf

denhost# /usr/local/etc/rc.d/darkstat start
Starting darkstat.
denhost# ps -ax | grep dark
 1147  ??  Ss     0:00,06 /usr/local/sbin/darkstat -i em0 --chroot /var/run/dar
 1148  ??  Ss     0:00,01 darkstat: DNS child (darkstat)
denhost# sockstat -4 | grep dark
nobody   darkstat   1147  8  tcp4   *:667                 *:*
denhost#
```

Рис. 7.12. Установка и запуск darkstat

Примечание

Программа wget по умолчанию не установлена, для ее установки следует ввести команду: `pkg_add -r wget`.

Вот теперь можно открывать браузер и наслаждаться графиками (типичный график darkstat показан на рис. 7.13):

`http://ip_адрес_узла_где_запущен_darkstat:667/`

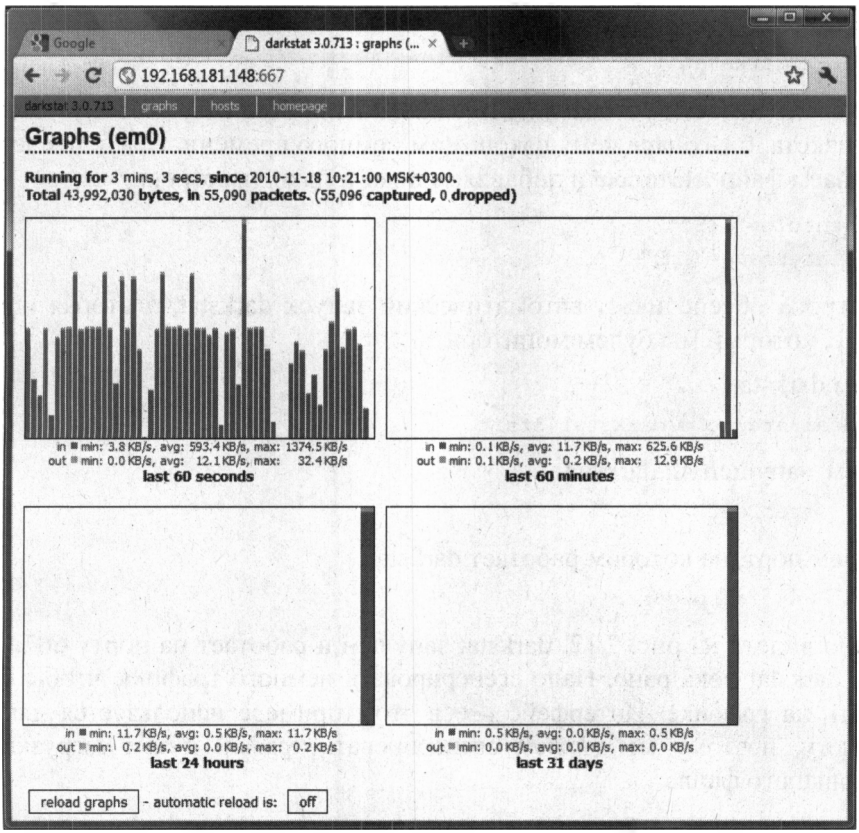


Рис. 7.13. Мониторинг трафика с помощью darkstat

Но это еще не все. Нужно добавить в файл rc.conf следующую строку:

```
darkstat_flags="--import em0.db --export em0.db"
```

Флаги `--import` и `--export` при запуске/останове демона darkstat управляют загрузкой/сохранением статистики в файл и из файла /var/run/darkstat/em0.db.

Следует также создать сценарий ротации файла em0.db. Код этого файла (назовем его em.sh) представлен в листинге 7.4.

Листинг 7.4. Файл em.sh

```
#!/bin/sh
DB="/var/run/darkstat/em0.db"

getpid() {
PIDFILE="/var/run/darkstat/darkstat.pid"
if [ -f $PIDFILE ]; then
  pid=`cat $PIDFILE`
fi
kill -SIGUSR1 $pid
}

getpid
mv $DB /var/run/darkstat/"darkstat-`date +%Y-%m`"
touch $DB && chmod 666 $DB
getpid
```

Этот файл — для его запуска каждый месяц (см. файл /etc/crontab) — нужно поместить в каталог /etc/periodic/monthly и сделать его исполняемым:

```
# chmod +x /etc/periodic/monthly/em0.sh
```

На этом все — ваш darkstat полностью готов к работе.

Система NeTAMS

NeTAMS (Network Traffic Accounting and Monitoring Software) — программа для учета и мониторинга IP-трафика. Она поддерживает разные методы сбора статистики, несколько баз данных для хранения информации о трафике (MySQL, PostgreSQL, Oracle, BerkleyDB, Radius) и обладает режимом оповещений. Позволяет производить блокировку на базе квот, авторизации, баланса (т. е. NeTAMS можно использовать как билинговую систему), дает возможность управлять пропускной полосой, контролировать подмену MAC-адреса, создавать гибкие политики учета и фильтрации трафика. Система весьма серьезная, особенно по сравнению с darkstat, у которой всех этих функций нет.

Для работы с NeTAMS нам понадобятся Apache и MySQL-сервер версии 5.0. Именно 5.0, а не 5.1 или 5.5, потому что с версиями 5.1 и 5.5 NeTAMS почему-то не работает, почему — мы не проверяли, не возникло такого желания.

Итак, будем считать, что серверы Apache и MySQL уже установлены и запущены.

Для работы NeTAMS также необходима библиотека libpcap, установим ее:

```
# cd /usr/ports/net/libpcap
# make install clean
```

Теперь установим NeTAMS, но вместо порта, который входит в состав FreeBSD, мы воспользуемся портом с сайта разработчиков:

```
# cd /usr/ports/net-mgmt
# fetch http://www.netams.com/files/netams-freebsd-port.tgz
# tar -zxvf netams-freebsd-port.tgz
```

В результате будет создан каталог freebsd-port, переименуем его в netams:

```
# mv freebsd-port netams
```

Настало время исправить ту самую ошибку с версиями MySQL, о которой говорилось ранее. Откройте файл Makefile:

```
# mcedit /usr/ports/net-mgmt/netams/Makefile
```

Найдите и удалите следующую строку:

```
mysqlclient.16:${PORTSDIR}/databases/mysql51-client \
```

Эта строка должна установить MySQL-клиент версии 5.1, но поскольку NeTAMS не работает с MySQL 5.1, то эта строка лишняя. NeTAMS также ничего не подозревает об установленном уже MySQL версии 5.0. И если не удалить эту строку, то для разрешения зависимости MySQL 5.0 будет удален, а вместо него установлена версия 5.1, но с ней NeTAMS работать не будет. Вот такая ситуация...

Теперь можно собрать порт:

```
# make install clean
```

При сборке зависимого порта GD следует выбрать опцию ICONV. Хотя, скорее всего, библиотека GD с этой опцией у вас уже установлена (она устанавливается при установке PHP).

После сборки добавьте строку автоматического запуска системы в файл /etc/rc.conf:

```
netams_enable="YES"
```

Скопируйте пример файла конфигурации в конфигурационный каталог NeTAMS:

```
# cd /usr/local/etc/netams/
# cp netams.conf.sample netams.conf
```

Пример конфигурационного файла представлен в листинге 7.5. Отредактируйте его по своему усмотрению. Значения, которые вам придется изменить (имена и IP-адреса узлов, порты, пароли и т. д.), выделены полужирным шрифтом.

Листинг 7.5. Пример файла netams.conf

```
# Отключаем отладку
debug none
```

```
# Определяем имя пользователя (root) и пароль (1) для доступа к netams
# пользователю root разрешаются все операции (permit all).
# Укажите нормальный пароль! Пароль "1" здесь использован, чтобы текст
# поместился в одной строке
user name root real-name Admin password 1 email root@localhost permit all

# Настройка сервисов
service server 0
login local
listen 20001
max-conn 6

service processor 0
lookup-delay 60
flow-lifetime 180

# Определяем порты, эти порты будут отображены на графике
# Это весь IP-трафик
policy name ip target proto
# WWW
policy name www target proto tcp port 80 8080 3128 443
# FTP
policy name ftp target proto tcp port 20 21
# POP3
policy name pop3 target proto tcp port 110
# SMTP
policy name smtp target proto tcp port 25
# SSH
policy name ssh target proto tcp port 22
restrict all drop local pass

# Сортируем порты по группам
unit group name admins acct-policy ip www ftp pop3 smtp ssh
unit group name other_users acct-policy ip www ftp pop3 smtp

# Определяем объекты (юниты), за которыми будем наблюдать:
# тип host — узел
# тип net — сеть
# unit host name comp1 ip A.A.A.A acct-policy ip www ftp pop3 smtp ssh
unit net name LAN ip 192.168.1.0/24 acct-policy ip www ftp pop3 smtp ssh

# Определяем пользователей
unit user name us1 ip 192.168.1.5 parent admin acct-policy ip www ftp pop3 smtp
ssh
unit user name us2 ip 192.168.1.7 parent other-users acct-policy ip www ftp
pop3 smtp ssh
```

```
# Статистику будем хранить в MySQL, здесь же указываем имя пользователя
# и пароль для доступа к MySQL
service storage 0
type mysql
user root
password пароль_для_mysql
accept all

# Указываем источники данных: откуда будут поступать пакеты
# В нашем случае есть только два источника: интерфейсы em0 и em1
service data-source 1
type libpcap
source em0
layer7-detect urls

service data-source 2
type libpcap
source em1
layer7-detect urls

# Запускаем сервис мониторинга
service monitor 0
monitor to storage 0
# Далее нужно указать наши объекты:
monitor unit comp1
monitor unit LAN

service alerter 0
report oid 06100 name rep1 type traffic period day detail simple
smtp-server localhost

# Определяем, где будем хранить файлы отчетов:
# в каталоге /usr/local/www/netams/stat
service html 0
path /usr/local/www/netams/stat
run 10min
htaccess yes
client-pages all
# Адрес веб-сервера
url http://192.168.1.1/netams/
language ru

service scheduler
# Обновление отчетов каждые 5 минут
oid 08FFFF time 5min action "html"
```

Конфигурационный файл готов. Запустим NeTAMS:

```
# /usr/local/etc/rc.d/netams start
```

Теперь осталось только настроить Apache. Перейдите в каталог /usr/local/etc/apache22/Includes и найдите там файл netams-apache-freebsd.conf. В этом файле хранятся параметры доступа к каталогам www/netams и www/netams/cgi-bin.

В каталоге /usr/local/www/cgi-bin находятся CGI-скрипты системы NeTAMS, сделаем их исполняемыми:

```
# chmod -R +x /usr/local/www/netams/cgi-bin
```

Отредактируем файл config.cgi:

```
# mcedit /usr/local/www/netams/cgi-bin/config.cgi
```

Найдите в этом файле две строки, содержащие соответственно пароль для доступа к SQL и пароль для доступа к NeTAMS:

```
$sql_password="MySQL-пароль"
$sc_passwd="1"                # В конфиге netams указан пароль 1
```

Теперь отредактируем файл admin/config.cgi — в нем надо произвести такие же изменения (изменить переменные `sql_password` и `sc_passwd`):

```
# mcedit /usr/local/www/netams/cgi-bin/admin/config.cgi
```

Перезапустим Apache:

```
# /usr/local/etc/rc.d/apache22 restart
```

Осталось только открыть браузер и зайти в панель управления NeTAMS[1]:

```
http://ваш_веб_сервер/netams/.
```

Утилита monit

Утилита monit предназначена для автоматического технического обслуживания — а именно: для системного мониторинга и исправления ошибок. Как правило, ее используют для автоматического перезапуска зависших сервисов. Конечно, подобную функциональность можно легко реализовать на bash, но для этого вы должны обладать навыками программирования на bash. А если таковых нет или не хочется тратить на это время, тогда проще использовать утилиту monit. Расценивайте эту утилиту как своеобразный «костыль», пока вы не разберетесь с причиной зависания сервисов. Сервисы в идеале не должны зависать, и автоматический перезапуск им, как правило, не нужен. Но на практике не бывает все идеально, поэтому такие утилиты имеют право на существование.

Для установки и обеспечения автоматического запуска monit введите команды:

```
sudo apt install monit
sudo systemctl enable monit
```

[1] Дополнительная информация (на русском языке) о системе доступна на сайте разработчиков: **http://www.netams.com/doc/index.html**.

Чтобы перезапустить, остановить, запустить или просмотреть статус утилиты, используйте привычные команды:

```
sudo systemctl restart monit
sudo systemctl stop monit
sudo systemctl start monit
sudo systemctl status monit
```

Основной файл конфигурации называется /etc/monit/monitrc. Как правило, в этом файле нужно задать только e-mail администратора, на который будут отправляться уведомления о нештатных ситуациях:

```
set alert <ваш email>
```

Утилита monit содержит настройки для мониторинга всех часто используемых сервисов. Все эти настройки хранятся в каталоге /etc/monit/conf-available, где каждому сетевому сервису соответствует отдельный файл с настройками. В каталоге /etc/monit/conf-enabled содержатся файлы (или ссылки на файлы каталога conf-available) тех сетевых сервисов, которые должна мониторить утилита.

Следующие команды заставляют monit контролировать состояние SSH, MySQL, nginx и Apache2 (как правило, у вас будет один веб-сервер, поэтому вам нужно выбрать нужную команду: или для nginx или для apache2):

```
cd /etc/monit/conf-enabled/
sudo ln -s /etc/monit/conf-available/openssh-server
sudo ln -s /etc/monit/conf-available/nginx
sudo ln -s /etc/monit/conf-available/mysql
sudo ln -s /etc/monit/conf-available/apache2
sudo monit -t
```

Сначала мы переходим в каталог conf-enabled, затем создаем символические ссылки на файлы конфигурации, которые находятся в каталоге conf-available, после чего запускаем тест конфигурации (`monit -t`), чтобы убедиться, что у нас все хорошо. В завершение нужно перезапустить monit.

Дополнительную информацию об использовании monit вы можете найти в ее документации **https://mmonit.com/monit/documentation/monit.html**.

Мониторинг жестких дисков. Коды S.M.A.R.T.

S.M.A.R.T. (от *англ.* Self-Monitoring, Analysis and Reporting Technology, технология самоконтроля, анализа и отчетности) — технология оценки состояния жесткого диска встроенной аппаратурой самодиагностики, а также механизм предсказания времени выхода его из строя.

Получить SMART-информацию о накопителе (будь то жесткий диск или SSD) можно посредством любой программы, поддерживающей S.M.A.R.T. Примеры таких программ: Crystal DiskInfo (рис. 7.14) и AIDA64 (рис. 7.15) — если нужно получить информацию локально, Nagios — если требуется получать информацию обо всех дисках на предприятии.

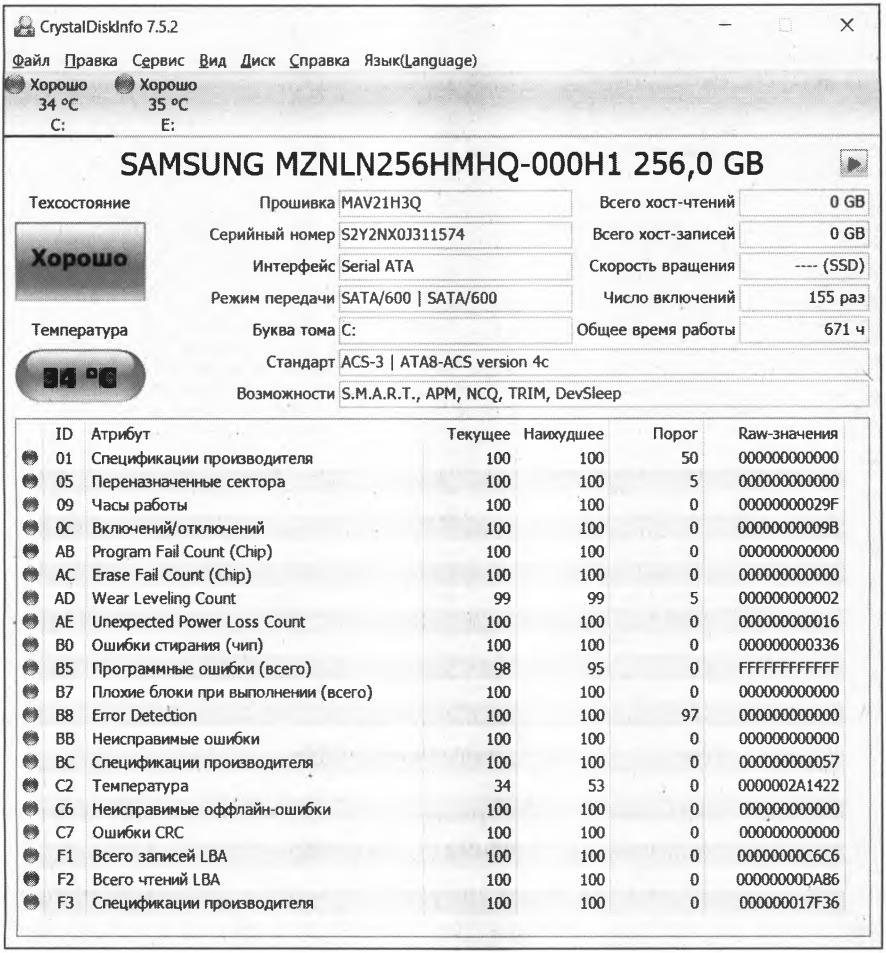


Рис. 7.14. Программа Crystal DiskInfo

Но что означает тот или иной код S.M.A.R.T.? Какие параметры (атрибуты) являются допустимыми, а какие — нет? Для разных дисков набор параметров самодиагностики может различаться. Попробуем разобраться, что есть что.

Любая программа, показывающая S.M.A.R.T., для каждого атрибута имеет несколько значений: ID, Value, Worst, Threshold и RAW — разберемся сначала с ними. Итак:

- **ID** (Number) — собственно, сам индикатор атрибута. Номера стандартны для значений атрибутов, но, например, из-за разницы перевода в разных программах один и тот же атрибут может называться по-разному, поэтому проще ориентироваться по ID, логично?
- **Value** (Current, текущее) — текущее значение атрибута в условных единицах (у. е.), никому, наверное, не ведомых. В процессе работы винчестера оно может уменьшаться, оставаться неизменным или увеличиваться. По показателю Value нельзя судить о «здоровье» атрибута, не сравнивая его со значением Threshold (порог) этого же атрибута. Как правило, чем меньше Value, тем хуже состояние

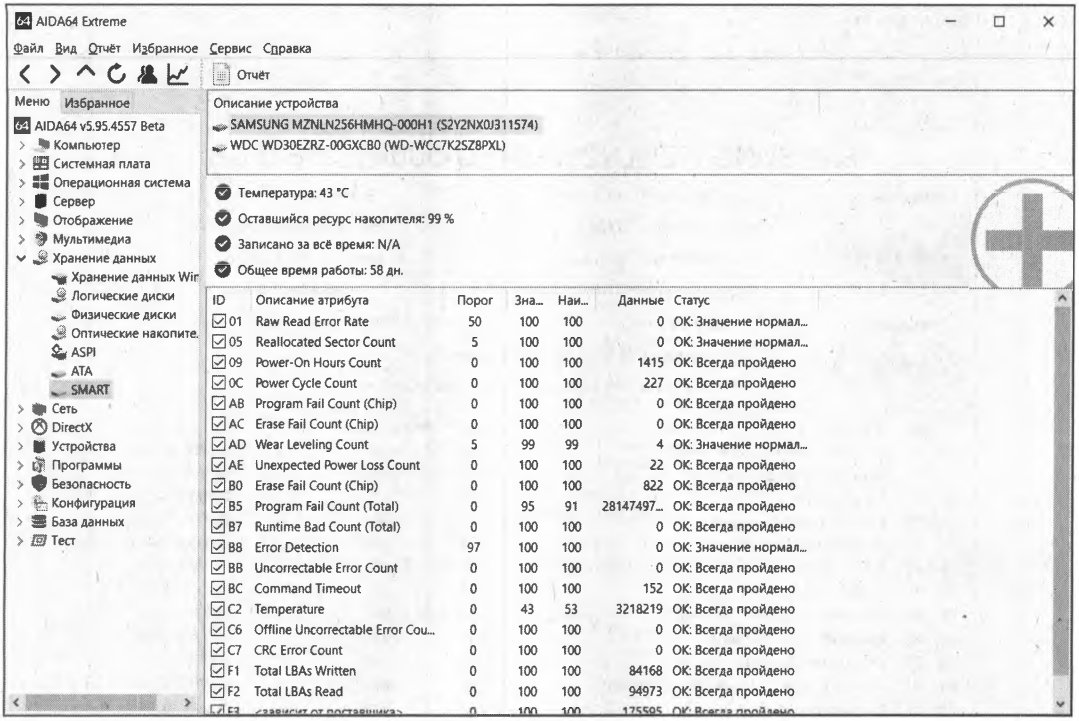


Рис. 7.15. Программа AIDA64

атрибута (изначально все классы значений, кроме RAW, на новом диске имеют максимальное из возможных значение — например, 100);

- **Worst** (наихудшее) — наихудшее значение, которого достигало значение Value за всю жизнь винчестера. Измеряется тоже в условных единицах. В процессе работы оно может уменьшаться либо оставаться неизменным. По нему тоже нельзя однозначно судить о «здоровье» атрибута — нужно сравнивать его с Threshold;
- **Threshold** (порог) — значение в (сюрприз!) условных единицах, которого должно достигнуть значение Value этого же атрибута, чтобы состояние атрибута было признано критическим. Проще говоря, Threshold — это пороговое значение: если Value больше Threshold — атрибут в порядке, если меньше либо равен — с атрибутом проблемы. Именно по такому критерию утилиты, читающие S.M.A.R.T., выдают отчет о состоянии диска либо отдельного атрибута вроде «Good» или «Bad».

  При этом они не учитывают, что даже при Value, большем Threshold, диск на самом деле уже может быть умирающим, с точки зрения пользователя, а то и вовсе «ходячим мертвецом», поэтому при оценке «здоровья» диска смотреть стоит все-таки на другой класс атрибута, а именно — на RAW. Однако именно значение Value, опустившееся ниже Threshold, может стать легитимным поводом для замены диска по гарантии (для самих гарантийщиков, конечно же) — кто же яснее скажет о «здоровье» диска, как не он сам, демонстрируя текущее значение атрибута хуже критического порога? То есть при значении Value, большем

Threshold, сам диск считает, что атрибут «здоров», а при меньшем либо равном — что «болен». Очевидно, что при Threshold = 0 состояние атрибута не будет признано критическим никогда. Следует учесть при этом, что Threshold — постоянный параметр, зашитый в диск производителем;

- **RAW** (Data) — самый интересный, важный и нужный для оценки показатель. В большинстве случаев он содержит в себе не условные единицы, а реальные значения, выражаемые в различных единицах измерения и напрямую говорящие о текущем состоянии диска. Основываясь именно на этом показателе, формируется значение Value (а вот по какому алгоритму оно формируется — это уже тайна производителя, покрытая мраком). Именно умение читать и анализировать поле RAW дает возможность объективно оценить состояние винчестера.

В табл. 7.2 приведены сами атрибуты.

Таблица 7.2. *Атрибуты самодиагностики*

Название (ID)	Описание
01 (01) Raw Read Error Rate	Частота ошибок при чтении данных с диска, происхождение которых обусловлено аппаратной частью диска. Для всех дисков Seagate, Samsung (семейства F1 и более новых) и Fujitsu 2,5" это число внутренних коррекций данных, проведенных до выдачи в интерфейс, следовательно, на пугающе огромные цифры можно реагировать спокойно
02 (02) Throughput Performance	Общая производительность диска. Если значение атрибута уменьшается, то велика вероятность, что с диском есть проблемы
03 (03) Spin-Up Time	Время раскрутки пакета дисков из состояния покоя до рабочей скорости. Растет при износе механики (повышенное трение в подшипнике и т. п.), также может свидетельствовать о некачественном питании (например, просадке напряжения при старте диска)
04 (04) Start/Stop Count	Полное число циклов запуск/остановка шпинделя. У дисков некоторых производителей (например, Seagate) — счетчик включения режима энергосбережения. В поле raw value хранится общее количество запусков/остановок диска
05 (05) Reallocated Sectors Count	Число операций переназначения секторов. Когда диск обнаруживает ошибку чтения/записи, он помечает сектор «переназначенным» и переносит данные в специально отведенную резервную область. Вот почему на современных жестких дисках нельзя увидеть bad-блоки — все они спрятаны в переназначенных секторах. Этот процесс называется remapping (ремаппинг), а переназначенный сектор — remap. Чем больше значение, тем хуже состояние поверхности дисков. Поле raw value содержит общее количество переназначенных секторов. Рост значения этого атрибута может свидетельствовать об ухудшении состояния поверхности блинов диска
06 (06) Read Channel Margin	Запас канала чтения. Назначение этого атрибута не документировано. В современных накопителях не используется
07 (07) Seek Error Rate	Частота ошибок при позиционировании блока магнитных головок. Чем их больше, тем хуже состояние механики и/или поверхности жесткого диска. Также на значение параметра может повлиять перегрев и внешние вибрации (например, от соседних дисков в корзине)

***Таблица 7.2** (продолжение)*

Название (ID)	Описание
08 (08) Seek Time Performance	Средняя производительность операции позиционирования магнитными головками. Если значение атрибута уменьшается (замедление позиционирования), то велика вероятность проблем с механической частью привода головок
09 (09) Power-On Hours (POH)	Число часов (минут, секунд — в зависимости от производителя), проведенных во включенном состоянии. В качестве порогового значения для него выбирается паспортное время наработки на отказ (MTBF, mean time between failure). Для многих современных дисков, в том числе WD, в качестве порога задано значение 0, поскольку значение MTBF не регламентируется производителем
10 (0A) Spin-Up Retry Count	Число повторных попыток раскрутки дисков до рабочей скорости в случае, если первая попытка была неудачной. Если значение атрибута увеличивается, то велика вероятность неполадок с механической частью
11 (0B) Recalibration Retries	Количество повторов запросов рекалибровки в случае, если первая попытка была неудачной. Если значение атрибута увеличивается, то велика вероятность проблем с механической частью
12 (0C) Device Power Cycle Count	Количество полных циклов включения/выключения диска
13 (0D) Soft Read Error Rate	Число ошибок при чтении по вине программного обеспечения, которые не поддались исправлению. Все ошибки имеют немеханическую природу и указывают лишь на неправильную разметку/взаимодействие с диском программ или операционной системы
180 (B4) Unused Reserved Block Count Total	Количество резервных секторов, доступных для ремаппинга
183 (B7) SATA Downshift Error Count	Содержит количество неудачных попыток понижения режима SATA. Суть в том, что винчестер, работающий в режимах SATA 3 или 6 Гбит/с (и что там дальше будет в будущем), по какой-то причине (например, из-за ошибок) может попытаться «договориться» с дисковым контроллером о менее скоростном режиме (например, SATA 1,5 или 3 Гбит/с соответственно). В случае «отказа» контроллера изменять режим диск увеличивает значение атрибута (Western Digital и Samsung)
184 (B8) End-to-End error	Этот атрибут — часть технологии HP SMART IV и означает, что после передачи через кеш памяти буфера данных паритета данных между хостом и жестким диском нет
185 (B9) Head Stability	Стабильность головок (Western Digital)
187 (BB) Reported UNC Errors	Ошибки, которые не могли быть восстановлены использованием методов устранения ошибки аппаратными средствами
188 (BC) Command Timeout	Содержит количество операций, выполнение которых было отменено из–за превышения максимально допустимого времени ожидания отклика. Такие ошибки могут возникать из-за плохого качества кабелей, контактов, используемых переходников, удлинителей и т. п., несовместимости диска с конкретным контроллером SATA/PATA на материнской плате и т. д. Из-за ошибок такого рода возможны BSOD (синий экран) в Windows. Ненулевое значение атрибута говорит о потенциальной «болезни» диска

Таблица 7.2 (продолжение)

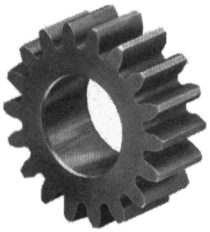
Название (ID)	Описание
189 (BD) High Fly Writes	Содержит количество зафиксированных случаев записи при высоте «полета» головки выше рассчитанной, скорее всего, из-за внешних воздействий — например, вибрации. Для того чтобы сказать, почему происходят такие случаи, нужно уметь анализировать логи S.M.A.R.T., которые содержат специфичную для каждого производителя информацию
190 (BE) Airflow Temperature (WDC)	Температура воздуха внутри корпуса жесткого диска. Для дисков Seagate рассчитывается по формуле: 100 – HDA temperature (см. далее). Для дисков Western Digital: 125 – HDA
191 (BF) G-sense error rate	Количество ошибок, возникающих в результате ударных нагрузок. Атрибут хранит показания встроенного акселерометра, который фиксирует все удары, толчки, падения и даже неаккуратную установку диска в корпус компьютера
192 (C0) Power-off retract count (Emergency Retry Count)	Для разных винчестеров может содержать одну из следующих двух характеристик: либо суммарное количество парковок блока магнитных головок (БМГ) диска в аварийных ситуациях (по сигналу от вибродатчика, обрыву/понижению питания и т. п.), либо суммарное количество циклов включения/выключения питания диска (характерно для некоторых дисков WD и Hitachi)
193 (C1) Load/Unload Cycle	Количество циклов перемещения БМГ в парковочную зону / в рабочее положение
194 (C2) HDA temperature	Здесь хранятся показания встроенного термодатчика для механической части диска — «банки» HDA (Hard Disk Assembly). Информация снимается со встроенного термодатчика, которым служит одна из магнитных головок, обычно нижняя в «банке». Не все программы, работающие со SMART, правильно разбирают эти поля, так что к их показаниям стоит относиться критически
195 (C3) Hardware ECC Recovered	Число коррекции ошибок аппаратной частью диска (чтение, позиционирование, передача по внешнему интерфейсу). На дисках с SATA-интерфейсом значение нередко ухудшается при повышении частоты системной шины — SATA очень чувствителен к разгону
196 (C4) Reallocation Event Count	Содержит количество операций переназначения секторов. Косвенно говорит о «здоровье» диска. Чем больше значение — тем хуже. Однако нельзя однозначно судить о «здоровье» диска по этому параметру, не рассматривая другие атрибуты. Этот атрибут непосредственно связан с атрибутом 05. При росте 196 чаще всего растет и 05. Если при росте атрибута 196 атрибут 05 не растет, значит, при попытке ремапа кандидат в бэд-блоки оказался софт-бэдом и диск исправил его, следовательно, сектор был признан здоровым и в переназначении не было необходимости. Если атрибут 196 меньше атрибута 05, значит, во время некоторых операций переназначения выполнялся перенос нескольких поврежденных секторов за один прием. Если атрибут 196 больше атрибута 05, значит, при некоторых операциях переназначения были обнаружены исправленные впоследствии софт-бэды

Таблица 7.2 (окончание)

Название (ID)	Описание
197 (C5) Current Pending Sector Count	Содержит количество секторов-кандидатов на переназначение в резервную область. Натолкнувшись в процессе работы на «нехороший» сектор (например, контрольная сумма сектора не соответствует данным в нем), диск помечает его как кандидата на переназначение, заносит его в специальный внутренний список и увеличивает параметр 197. Из этого следует, что на диске могут быть поврежденные секторы, о которых он еще не знает, — ведь на пластинах вполне могут быть области, которые винчестер какое-то время не использует. При попытке записи в сектор диск сначала проверяет, не находится ли этот сектор в списке кандидатов. Если сектор там не найден, запись проходит обычным порядком
198 (C6) Uncorrectable Sector Count	Число неисправимых ошибок при обращении к сектору (возможно, имелось в виду «число некорректируемых (средствами диска) секторов», но никак не число самих ошибок!). В случае увеличения числа ошибок велика вероятность критических дефектов поверхности и/или механики накопителя
199 (C7) UltraDMA CRC Error Count	Содержит количество ошибок, возникших по передаче по интерфейсному кабелю в режиме UltraDMA (или его эмуляции винчестерами SATA) от материнской платы или дискретного контроллера контроллеру диска. В подавляющем большинстве случаев причинами ошибок становятся некачественный шлейф передачи данных, разгон шин PCI/PCI-E компьютера или плохой контакт в SATA-разъеме на диске либо материнской плате/контроллере
200 (C8) Write Error Rate / Multi-Zone Error Rate	Показывает общее количество ошибок, происходящих при записи сектора, а также общее число ошибок записи на диск. Может служить показателем качества поверхности и механики накопителя
201 (C9) Soft read error rate	Частота появления «программных» ошибок при чтении данных с диска. Этот параметр показывает частоту появления ошибок при операциях чтения с поверхности диска по вине программного обеспечения, а не аппаратной части накопителя
203 (CB) Run out cancel	Количество ошибок ECC (Error Correcting Code, код, корректирующий ошибки)
228 (E4) Power-Off Retract Cycle	Количество повторов автоматической парковки БМГ в результате выключения питания
231 (E7) Temperature/ SSD Life Left	Температура жесткого диска. Для SSD-диска этот параметр называется SSD Life Left (остаток жизни SSD) — приблизительное количество оставшихся циклов перезаписи SSD
232 (E8) SSD Endurance Remaining	Количество завершенных физических циклов стирания на диске в процентах от максимально возможного
250 (FA) Read error retry rate	Число ошибок во время чтения жесткого диска
254(FE) Free Fall Event Count	Содержит зафиксированное электроникой количество ускорений свободного падения диска, которым он подвергался, т. е., проще говоря, показывает, сколько раз диск падал

Не все модели жестких дисков поддерживают атрибуты, приведенные в табл. 7.2, а некоторые диски могут поддерживать атрибуты, не представленные в ней. За толкованием атрибутов можно обратиться в службу поддержки производителя дисков.

ГЛАВА 8



Виртуализация и облачные технологии

Когда стали появляться первые виртуальные машины, к ним сначала относились весьма скептически: игрушки, захватывают много системных ресурсов, медленно работают и т. п. Однако в настоящее время виртуализация в том или ином виде применяется во многих решениях: виртуальные машины, виртуальные серверы, виртуальные рабочие станции, виртуальные сети VLAN и пр.

Секрет популярности виртуализации

Почему же виртуализация стала такой популярной? Секрет прост — экономия. Ресурсы современного сервера редко когда используются на все 100%. Что дает виртуализация? Мы можем создать несколько виртуальных серверов, работающих на одном физическом. Один из них оставить для собственных нужд, остальные — сдать в аренду другим компаниям. Так поступают многие крупные фирмы, в том числе и всем известный Amazon, — чтобы оборудование не простаивало, создаются и сдаются в аренду виртуальные серверы.

Однако перед внедрением виртуальных систем следует четко понимать, что мы хотим получить в результате и во что это нам обойдется. Проще всего сказать, что виртуализация — это выгодно. Но будет ли она выгодна именно вашей компании?

Стоит учесть, что программное обеспечение, позволяющее использовать преимущества виртуальной среды, в большинстве своем является коммерческим и довольно-таки недешевым продуктом. Нужно помнить и об определенной инфраструктуре, которая необходима для виртуализации, — например, вам понадобится система хранения данных, подключенная к нескольким серверам. На все это предстоит потратиться... Стоит ли игра свеч?

Как правило, экономическая выгода от перехода на виртуальную среду достигается, начиная с определенного количества серверов, как минимум с 10–15. Даже если вам сразу и не нужно такое количество серверов, покупать новое оборудование и программное обеспечение придется все равно. В результате именно в этом случае виртуализация окажется для вас невыгодной и вполне может статься, что она приведет лишь к дополнительным затратам на содержание ее инфраструктуры.

Глоссарий

Рассмотрим для начала используемую терминологию. Краеугольный камень любой системы виртуализации — *гипервизор* (hypervisor). Гипервизор — это программное обеспечение, реализующее виртуализацию ресурсов и позволяющее нескольким операционным системам работать одновременно на одном физическом компьютере, называемом *хостом*. Комплектующие «внутри» такой виртуальной машины (ВМ) называются *виртуальными*: виртуальные жесткие диски, виртуальные сетевые адаптеры, виртуальная память и т. д. Операционная система, работающая под управлением гипервизора, называется *гостевой*.

Гипервизор позволяет создавать и *виртуальные сети*. При этом виртуальная сеть может работать в разных режимах — например, в режиме NAT[1], быть сегментом сети без доступа к реальным адаптерам (т. е. просто внутренней сетью), в режиме моста и т. п.

Виртуальной машине передается контроль над клавиатурой и мышью хоста. Такая операция передачи управления называется *захватом*. В этом случае курсор мыши будет работать только в пределах окна виртуальной машины. Чтобы переместить курсор за пределы окна гостевой ОС, надо нажать специальную клавишу. Обычно такой клавишей является <Ctrl>, но в современных ВМ и так можно вывести мышь за пределы окна с гостевой ОС, поэтому больше нет необходимости в нажатии какой-либо специальной клавиши.

Вендоры виртуальных решений

Существует множество разработчиков технологий виртуализации. В этом разделе мы рассмотрим только самые популярные. Если вам нужна исчерпывающая информация, обратитесь к страничке Википедии, предоставляющей сравнение всех имеющихся виртуальных машин: **http://tinyurl.com/q5f33ce**[2].

Львиная доля на рынке виртуализации принадлежит компании VMware (**www.vmware.com**). Это лидер рынка виртуализации, представляющий продукты для всех имеющихся операционных систем: Windows, Linux, macOS и пр. Причем в линейке продуктов VMware есть как свободные, так и коммерческие продукты.

После VMware следует компания Oracle с ее виртуальной машиной VirtualBox. Последняя обрела популярность потому, что практически ничем не уступает коммерческой VMware Workstation, но при этом абсолютно бесплатна (**http://www.oracle.com/us/technologies/virtualization/index.html**).

На третьем месте — Xen (**www.xen.org**). Этот продукт представляет собой гипервизор на основе открытого кода и лежит в основе многих открытых решений. Так, на базе Xen компанией Citrix создан XenServer. Однако это решение уже является коммерческим.

---

[1] NAT (от *англ.* Network Address Translation, преобразование сетевых адресов) — механизм в сетях TCP/IP, позволяющий преобразовывать IP-адреса транзитных пакетов.

[2] Ссылка ведет на статью «Сравнение виртуальных машин».

Microsoft тоже заслужила свое место под солнцем виртуализации с ее гипервизором Hyper-V, входящим в состав Windows Server 2008 и более новых версий. Этот продукт может быть установлен совершенно бесплатно.

Существуют и бесплатные OpenSource-решения: KVM и OpenVZ, входящие в состав популярных современных дистрибутивов: Debian, Ubuntu, CentOS и пр. Далее в этой главе мы рассмотрим, в чем состоит принципиальная разница между KVM и OpenVZ.

> ***Примечание***
>
> Состояние проекта OpenVZ — неопределенное. Лет шесть назад появилась информация о том, что его закрывают, но по состоянию на 2023 год в его репозиториях есть обновления за 2021 год и доступны ядра 5.2 и 4.2 (кроме морально устаревших 2.6). В качестве развивающейся альтернативы рекомендуется использовать коммерческий продукт — Virtuozzo.

Выбор гипервизора

Как выбрать идеальное решение по виртуализации? Увы, идеального и универсального решения, которое можно было бы порекомендовать всем, не существует. Однако можно выбрать решение, максимально пригодное именно для вашего случая. При этом нужно учитывать много разных факторов.

Начнем, например, с поддержки технологий виртуализации собственно оборудованием. Ведь если ваше оборудование поддерживает виртуализацию, то гостевая ОС сможет работать с ресурсами оборудования напрямую, без эмуляции. Ряд гипервизоров (например, XenServer) требуют обязательной поддержки виртуализации оборудованием. И если ваше оборудование не поддерживает виртуализацию на аппаратном уровне, то использовать такие гипервизоры, увы, не получится. Некоторые гипервизоры требуют также наличия только *x*64-платформы (например, Hyper-V и тот же XenServer). Сейчас это не проблема, но если вы надумали в качестве сервера виртуализации использовать завалявшийся в углу 32-разрядный ПК, у вас ничего не выйдет.

Гипервизоры также часто бывают ограничены по типам гостевых ОС. Например, Hyper-V практически не поддерживает Linux. Если вам нужно работать с виртуальными Linux-серверами, то лучше выбрать KVM, Virtuozzo, Oracle VirtualBox или XenServer. Получить виртуальные macOS лучше всего с помощью сервера VMware.

Сегодня можно выделить четыре самых популярных решений: VMware vSphere, Microsoft Hyper-V, KVM и Virtuozzo. Первое — это, как уже было отмечено ранее, коммерческое решение от VMware. На рис. 8.1 показана логическая организация сети с использованием решений VMware vSphere. Решение от Microsoft (кстати, оно бесплатное) лучше всего подойдет, если вам нужны виртуальные Windows-системы. Из всего этого списка бесплатным OpenSource-решением является только KVM. В настоящее время нет бесплатной версии Virtuozzo, даже демо/триал версии, а то, что можно бесплатно скачать с сайта, — это обычный дистрибутив без средств виртуализации.

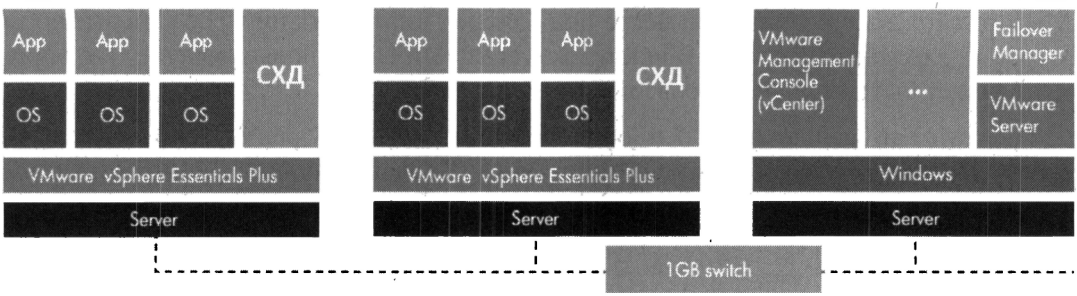


Рис. 8.1. Вариант логической структуры решения на продуктах компании VMware

Если вам нужно решение виртуализации для рабочей станции, то ничего лучше VMware Workstation еще не придумали. Это проверенное временем и отлично работающее решение. Конечно, если требуется решение бесплатное, то можно посмотреть и в сторону Oracle VirtualBox.

Гипервизоры различаются по типу установки на компьютер. Одни устанавливаются непосредственно на него в качестве основной операционной системы — это, например, XenServer и VMware ESXi vSphere. Другие интегрируются в уже существующую ОС — это, например, KVM, Hyper-V, VMware Workstation, Oracle VirtualBox.

Выбор типа гипервизора зависит и от решаемых задач, и от предпочтений администратора. Также нужно учитывать и их технические ограничения — в табл. 8.1 приведены сравнительные характеристики Hyper-V 2019 и VMware ESXi vSphere 6.7. Как видите, характеристики подобны, но у Free-версии от VMware (VMware vSphere Hypervisor) есть существенное ограничение по объему оперативной памяти и количеству виртуальных процессоров (vCPU). И если по объему оперативной памяти «упереться» в ограничение будет сложно, то по количеству vCPU — вполне возможно.

Помимо технических характеристик нужно принимать во внимание еще и функциональность гипервизоров.

Таблица 8.1. *Сравнительные характеристики гипервизоров Hyper-V 2019 и ESXi vSphere 6.7*

Система	Ресурс	MS Hyper-V	Версии VMware ESXi vSphere 6.7		
			Free Hypervisor	Essential Plus	Enterprise Plus
Хост	Логические процессоры	512	768	768	768
	Физическая память, Тбайт	24	4	4	16
	vCPU на 1 хост	2048	4096	4096	4096
	ВМ на 1 хост	1024	1024	1024	1024
	Вложенный гипервизор	+ (для некоторых ОС)	+	+	+

Таблица 8.1 (окончание)

Система	Ресурс	MS Hyper-V	Версии VMware ESXi vSphere 6.7		
			Free Hypervisor	Essential Plus	Enterprise Plus
Виртуальная машина (ВМ)	Виртуальные CPU на 1 ВМ	240 для поколения 2 или 64 для поколения 1	8	128	128
	Макс. размер ОЗУ для ВМ	12 Тбайт для поколения 2 или 1 Тбайт для поколения 1	6128 Гбайт	6128 Гбайт	6128 Гбайт
	Макс. дисковое пространство	64 Тбайт для формата VDHX, 2040 Гбайт для VHD	62 Тбайт	62 Тбайт	62 Тбайт
	Кол-во дисков	256	256	256	256
Кластер	Макс. кол-во узлов	64	–	64	64
	Макс. кол-во ВМ	8000	–	8000	8000

Основного недостатка Hyper-V в табл. 8.1 не увидеть. К сожалению, этот гипервизор до сих пор не поддерживает технологию USB Redirection, которая используется для «проброса» аппаратных USB-портов, что позволяет подключать к виртуальным машинам аппаратные USB-ключи. Вместо нее пытаются «сосватать» технологию Discrete Device Assignment, но это несколько не то. К тому же Hyper-V пока не умеет «на лету» добавлять CPU. Зато Hyper-V позволяет уменьшать размер диска, а не только увеличивать, как VMware. Сравнение функциональности этих двух ВМ приведено в табл. 8.2.

Таблица 8.2. Сравнение функциональности гипервизоров

Функция	MS Hyper-V	Версии VMware ESXi vSphere 6.5		
		Free Hypervisor	Essential Plus	Enterprise Plus
VM host live migration	+	–	+	+
VM storage live migration	+	–	–	+
QoS для хранилища/сети	+	–	–	+
«Проброс» оборудования	Discrete Device Assigntment	PCI VMDirectPath/ USB redirection	PCI VMDirectPath/ USB redirection	PCI VMDirectPath/ USB redirection
«Горячее» добавление	Диски/vNIC/ОЗУ	Диски/vNIC/USB	Диски/vNIC/USB	Диски/vNIC/USB/ CPU/ОЗУ

Таблица 8.2 (окончание)

Функция	MS Hyper-V	Версии VMware ESXi vSphere 6.5		
		Free Hypervisor	Essential Plus	Enterprise Plus
«Горячее» удаление	Диски/vNIC/ОЗУ	Диски/vNIC/USB	Диски/vNIC/USB	Диски/vNIC/USB/CPU
Изменение размера диска	Уменьшение и увеличение	Увеличение	Увеличение	Увеличение
Шифрование ВМ	+	–	–	+

Итак, если нужен «проброс» USB-портов в виртуальную машину, то однозначно — только VMware, даже ее бесплатная версия. С другой стороны, если необходимо шифрование виртуальной машины, то, возможно, дешевле будет использовать Hyper-V.

Кроме функциональности самого гипервизора, нужно оценить еще и средства управления. У каждого вендора есть свое решение для управления гипервизорами:

- Virtual Machine Manager (VMM) позволяет управлять серверами Hyper-V, а именно: создавать, клонировать, развертывать виртуальные машины и многое-многое другое;
- у VMware средство управления называется vSphere. Оно подразумевает использование ESXi-хостов и сервера vCenter Server для централизованного управления ими.

Какое средство управления более удобное — судить сложно. Все индивидуально, кто к чему привык. Однако нужно понимать, что в случае с VMware требуется обязательное наличие VMware vCenter, если вам нужен, например, кластер. А вот Virtual Machine Manager (VMM) является опциональным компонентом, который очень полезен, но совсем не обязателен.

Программное обеспечение и виртуальная среда

К сожалению, не каждое программное обеспечение сможет работать в виртуальной среде. Чтобы узнать, может ли то или иное программное обеспечение работать в виртуальной машине, нужно обратиться к документации по нему или задать вопрос в службу поддержки этого ПО. Вполне возможно, что использовать то или иное ПО в виртуальной среде не получится или придется установить какие-то патчи.

Особенности сетевых подключений виртуальных машин

Физическая машина (хост) имеет один или несколько сетевых интерфейсов, подключенных к физической (реальной) сети передачи данных. Число сетевых интер-

фейсов виртуальной машины может быть сколь угодно большим — вы можете создать в виртуальной машине любое количество сетевых адаптеров, и оно будет никак не связано с количеством адаптеров хоста. Например, на физическом компьютере у вас может быть один сетевой адаптер, а в виртуальной машине — три.

Виртуальный сетевой адаптер может работать в разных режимах. Наиболее частый режим — это трансляция сетевых адресов (NAT). В этом случае гипервизор создает сервер NAT, внешним интерфейсом которого служит реальный сетевой адаптер, а интерфейсы виртуальных машин подключаются к виртуальному интерфейсу, настройками которого (IP-адресом) можно управлять в ПО гипервизора. В этом режиме виртуальным машинам будет доступна работа в реальной сети (через адрес хоста), но обратиться к самой виртуальной машине будет весьма проблематично, поскольку сервер NAT также является и сетевым экраном, а настроить публикацию внутренних ресурсов в гипервизоре или весьма сложно, или вообще порой невозможно.

Если виртуальная машина должна работать с внешней сетью и наоборот, то лучше переключить виртуальный сетевой адаптер в режим *сетевого моста*. В этом случае пакеты, формируемые интерфейсом виртуальной машины, будут передаваться реальным физическим интерфейсом — как будто все интерфейсы: физические и виртуальные, подключены в один коммутатор. При этом можно будет обратиться к ресурсам виртуальной машины как к ресурсам обычной локальной системы, находящейся в одной локальной сети с хостом.

Есть и третий режим работы виртуального сетевого адаптера — только внутренние сети. В этом случае трафик может передаваться лишь между виртуальными машинами. Такой режим следует использовать, когда надо повысить безопасность внутренней сети виртуальных машин, — виртуальные машины никак не будут доступны: ни с хоста, ни из локальной сети.

Если в виртуальной машине создано несколько виртуальных сетевых адаптеров, то все они могут работать в разных режимах. Например, один сетевой адаптер может работать в режиме моста, а другой — в режиме внутренней сети.

К одному физическому интерфейсу можно подключить любое количество виртуальных интерфейсов. Практическое ограничение связано только с параметрами сетевой активности виртуальных систем — суммарные потребности виртуальных интерфейсов не должны превышать возможностей реального сетевого адаптера.

Последние версии ПО виртуализации включают в себя и виртуальные коммутаторы, реализованные программным способом. Эти коммутаторы по своим возможностям идентичны обычным коммутаторам 2-го и 3-го уровней.

Лицензирование программного обеспечения виртуальных машин

Не нужно забывать и о лицензировании выполняющегося в виртуальной машине программного обеспечения. В этой книге вопросы лицензирования не затрагиваются, но можем вас заверить, что не все так просто, как кажется на первый взгляд, —

особенно это касается лицензий Microsoft. Некоторые разъяснения по этому поводу можно получить в этом их документе:
http://download.microsoft.com/download/9/e/4/9e4ccec9-222b-4563-8dcd-43f941aba73f/microsoftservervirtualization_licensemobility_vlbrief.pdf.

Стоит отметить, что использование программного обеспечения в виртуальной машине не всегда требует лицензирования. Но тут все зависит от самого программного обеспечения и отношения к виртуализации его разработчиков. Некоторые из них требуют покупать дополнительные лицензии, некоторые разрешают использовать лицензионное ПО в виртуальных машинах без дополнительного лицензирования.

Если сравнивать два популярных гипервизора: Hyper-V и VMware ESXi vSphere, то вкратце дело с лицензиями обстоит так:

- в случае с VMware вы платите за сам гипервизор и нужно также покупать лицензию на каждую ОС, которая установлена внутри виртуальной машины (если это, конечно, не Linux или не другая бесплатная ОС);
- при использовании Hyper-V в составе Windows Server все зависит от редакции Windows Server. Если это Datacenter, то ОС внутри виртуальных машин не лицензируются. Если это Standard, то не лицензируются только две виртуальные машины. Обратите внимание, что лицензируется не факт установки ОС, а сама ОС, т. е. даже в Standard вы можете создать любое количество виртуальных машин с Linux;
- при использовании Hyper-V Server (устанавливается отдельно, непосредственно на «железо») лицензированию подлежит каждая виртуализированная Windows, хотя сам Hyper-V Server бесплатен. Если же вы используете в виртуальных машинах Linux, то решение виртуализации получается совсем бесплатным.

Создание виртуальных машин

Существует несколько способов создания новой виртуальной машины. Первый заключается в установке операционной системы с нуля на виртуальную машину. Второй подразумевает клонирование существующей виртуальной машины. Третий — снятие образа с физической машины и перенос его на виртуальный жесткий диск.

Понятно, что если у вас еще нет виртуальных машин, то вам подойдут только первый и третий способы.

Создание виртуальной машины путем чистой установки операционной системы

Первый способ является самым простым и мало чем отличается от обычной установки ОС. Разница лишь в том, что установка ОС выполняется не на физический жесткий диск, а на виртуальный.

Перед установкой ОС нужно создать саму виртуальную машину, определить ее параметры (количество процессоров, объем оперативной памяти, жесткие диски,

сетевые адаптеры, режимы работы сетевых адаптеров и пр.). После этого можно запускать установку гостевой ОС. Ее можно производить как с ISO-образа, хранящегося на жестком диске, так и с инсталляционного CD/DVD-диска.

После установки гостевой ОС необходимо установить *расширения*, предлагаемые соответствующим гипервизором. В случае с VMware — это так называемые VMware Tools. Расширения помогают оптимизировать работу гостевой ОС в виртуальной машине. Зачем устанавливать расширения? Все зависит от типа гипервизора и устанавливаемой гостевой ОС. Например, нами была замечена весьма медленная работа некоторых версий Windows в VMware Workstation. После установки расширений VMware Tools (которые представляют собой драйверы устройств виртуальной машины) скорость работы гостевой ОС существенно выросла. Что же касается Hyper-V, то по умолчанию в этой виртуальной машине недоступно управление мышью. И если вы не хотите использовать при работе с виртуальной машиной только клавиатуру, необходимо установить расширения для Hyper-V.

Если технические характеристики хоста позволяют запускать на нем обычные версии гостевых ОС, то можно обойтись и ими. В противном случае можно использовать специальные облегченные дистрибутивы — например, Windows Thin PC (облегченная версия Windows 7).

Конечно, у таких облегченных версий есть некоторые ограничения — например, в том же дистрибутиве Windows Thin PC не поддерживается .NET Framework, нельзя добавлять компоненты и т. п. Однако его функциональности в большинстве случаев достаточно, а некоторая ограниченность положительно сказывается на использовании системных ресурсов компьютера.

Клонирование виртуальной машины

Этот способ является самым быстрым способом создания виртуальной машины. Сначала создается эталонная виртуальная машина, на которую устанавливается необходимое программное обеспечение. Эта эталонная виртуальная машина и будет использоваться для клонирования виртуальных машин.

Клонирование можно выполнить как средствами гипервизора, так и вручную, — если скопировать файлы виртуального диска и при создании новой виртуальной машины указать, что будет использоваться уже существующий виртуальный диск.

Но не все так просто. Вам для клонированной ОС придется изменить все уникальные параметры: сетевое имя, параметры сетевых интерфейсов и т. п. Понадобится сменить и уникальный идентификатор безопасности Windows. Чтобы не изменять его вручную, можно воспользоваться утилитой NewSID, получить которую можно по адресу: **https://bit.ly/3bB7LpR**[1]. После запуска утилиты NewSID вы получите полностью работоспособную систему.

Впрочем, различные прикладные программы могут устанавливать собственные уникальные метки, о которых программа NewSID ничего не знает. В этом случае

[1] Полный адрес:
https://docs.microsoft.com/ru-ru/previous-versions/bb897418(v=msdn.10)?redirectedfrom=MSDN.

необходимо изменить такие метки вручную, но для этого нужно знать, что они есть. Как правило, об этом можно прочитать в документации на ПО. Полного списка таких программ нет, поэтому придется проверять каждую установленную в эталонной виртуальной машине программу. Особенно это касается утилит обеспечения безопасности, защиты от несанкционированного доступа, программ мониторинга и т. п.

Снятие образа физического сервера

Есть и третий способ создания виртуальной машины — снять образ с уже существующего сервера. Для этого некоторые разработчики виртуальных машин предоставляют собственные решения. Так, вы можете использовать следующие средства:

- Microsoft Deployment Toolkit;
- VMware vCenter Converter;
- Microsoft Disk2vhd;
- WinImage;
- Symantec Ghost.

Первые два решения весьма громоздкие. Третья утилита — небольшая, компактная и бесплатная. Она позволяет создать образ диска работающего сервера (VHD-файл). Однако не факт, что созданный образ диска заработает в виртуальной машине. Именно поэтому мы рекомендуем использовать программу WinImage, которая лишена подобных недостатков. Утилита не бесплатная, а условно-бесплатная — вы можете ее использовать бесплатно целый месяц. Полагаем, этого времени вполне достаточно, чтобы создать образ жесткого диска сервера, и не один.

Миграция между решениями различных производителей

Иногда бывает нужно использовать виртуальную машину, созданную средствами виртуализации одного разработчика, в гипервизоре другого разработчика. Например, вам прислали уже готовую виртуальную машину в формате VMware, а вы используете VirtualBox или наоборот.

Существуют решения, позволяющие конвертировать виртуальную машину из одного формата в другой. Например, вот так в Linux можно легко конвертировать образ виртуального жесткого диска VMware в образ VirtualBox:

```
qemu-img convert vmware.vmdk vmware.bin
VBoxManage convertdd vmware.bin vmware.vdi
```

Первая команда конвертирует образ VMware в промежуточный бинарный файл. Затем с помощью VBoxManage этот промежуточный файл конвертируется в образ VirtualBox.

Конвертировать образ VMware в образ Hyper-V можно с помощью утилиты V2V Converter (**https://www.starwindsoftware.com/converter**).

В общем-то, если поискать, можно найти конвертер для любых виртуальных машин. Даже если вы не сможете найти конвертер для преобразования формата имеющегося виртуального жесткого диска именно в ваш формат, можно попытаться преобразовать его в формат бесплатного решения виртуализации, — например, в формат VirtualBox. Думаем, особых проблем установить VirtualBox не составит.

Для миграции с облачного сервиса Microsoft Azure на VMware нужно установить Azure PowerShell на саму виртуальную машину, работающую под управлением Windows.

Самый простой способ получить VHD-файл по работающей виртуальной машине Microsoft Azure — это использовать команду `Save-AzureVhd`. Общий синтаксис выглядит так:

```
Save-AzureVhd [-Source] [-LocalFilePath] [[-NumberOfThreads] ] [[-StorageKey] ]
[[-OverWrite]]
```

Здесь:

- параметр `-Source` задает URI для хранилища BLOB в Azure;
- параметр `-LocalFilePath` — локальный путь для сохранения VHD-файла;
- параметр `-NumberOfThreads` указывает количество загружаемых потоков, которые будут использоваться при загрузке. Значение по умолчанию — 8;
- параметр `-StorageKey` указывает ключ хранилища. Если он не указан, команда попытается определить ключ хранилища учетной записи в исходном URI из Azure;
- наконец, параметр `-OverWrite` позволяет перезаписать существующий локальный VHD-файл.

Сохраняем BLOB в указанном файле с перезаписью такового, если он существует:

```
Save-AzureVhd -Source http://myaccount.blob.core.windows.net/
vhdstore/win7baseimage.vhd -LocalFilePath C:\vhd\Win7Image.vhd -Overwrite
```

Делаем то же самое, но указываем ключ хранилища для загрузки:

```
Save-AzureVhd -Source http://myaccount.blob.core.windows.net/
vhdstore/win7baseimage.vhd -LocalFilePath C:\vhd\Win7Image.vhd -Overwrite
-StorageKey <ключ>
```

Загруженный VHD-файл нужно преобразовать в формат VMDK. Для этого воспользуйтесь уже упомянутым ранее инструментом WinImage, который вы без проблем найдете в Интернете. Бесплатно доступна его 30-дневная ознакомительная версия, чего вполне хватит для переноса в VMware множества виртуальных машин, а вот если вы собираетесь использовать WinImage регулярно, то придется его купить. Стоит этот инструмент недорого — порядка 30 долларов, что для такой полезной утилиты немного.

> ***Примечание***
>
> Для файлов виртуальных дисков стандартизован формат VHD. Но на практике вендоры часто используют собственные форматы (например, VMware — формат VMDK).

Некоторые замечания к устройству виртуальных машин

Жесткие диски

Нужно сказать несколько слов о виртуальных жестких дисках. Во-первых, к одной виртуальной машине вы можете подключить несколько жестких дисков. Во-вторых, жесткие диски могут быть различных типов, даже если изначально эти типы не поддерживаются хостом. Например, у вас на хосте может быть только контроллер SATA, но в виртуальную машину вы можете добавить и SCSI-диски.

Типы виртуальных дисков

Для рабочей среды должен использоваться преимущественно фиксированный жесткий диск, а динамические и разностные диски могут применяться в тестовых и тому подобных целях.

- *Толстый* (Thick), или *фиксированный, жесткий диск*. При создании файла такого виртуального диска под него выделяется сразу весь объем. Этот тип диска рекомендуется выбирать в случае повышенных требований к производительности операций ввода-вывода (при этом ресурсы системы не затрачиваются на изменение размера файла).
- *Тонкий* (Thin), или *динамический, жесткий диск*. Исходно создается файл виртуального диска минимального размера, а затем (при необходимости) он автоматически увеличивается до заранее оговоренного максимального размера. Чтобы уменьшить размер файла тонкого диска (если часть дискового пространства в виртуальной машине освободилась по тем или иным причинам), нужно остановить виртуальную машину и выполнить операцию сжатия файла.
- *Разностные жесткие диски*. Такие диски могут использовать виртуальные машины Microsoft. На разностный диск пишутся только измененные данные по сравнению с некоторым образцом — *родительским* диском (родительский диск рекомендуется использовать в режиме *только для чтения*). Использование разностных дисков позволяет сэкономить дисковое пространство в случае создания нескольких подобных виртуальных машин (за счет исключения дублирования одинаковых данных).
- *Сквозное подключение физического диска* (pass-through). Гипервизоры позволяют подключить к виртуальной машине физический жесткий диск. Теоретически это самый быстрый вариант диска для виртуальной машины, хотя на практике различия в скорости между фиксированным диском и диском, подключенным напрямую, весьма незначительны.

  Примечание

  Для того чтобы подключить жесткий диск напрямую к виртуальной машине, он должен быть предварительно отключен от хостовой системы. Сделать это можно, например, с помощью менеджера дисков (или утилитой *diskpart*).

- *RAW-диски*. Описанные ранее тонкие, толстые и разностные диски представляют собой файлы, хранимые на хостовой системе. Некоторые гипервизоры могут ис-

пользовать непосредственный доступ к жесткому диску. Например, в VMware присутствует механизм прямого доступа клиента vSphere Client к устройствам хранения FC[1] или iSCSI[2]. Соответствующие описания необходимо уточнить по документации продукта.

Необходимость блочного доступа к виртуальному диску

Файл виртуального жесткого диска может быть создан на устройстве, понимаемом системой как *локальный* жесткий диск. Это могут быть диски как подключаемые локально, так и по технологии FC или iSCSI.

> ***Примечание***
>
> Существует еще технология передачи FC поверх сети Ethernet (FCoE), но она поддерживается сегодня лишь топовыми моделями коммутаторов и систем хранения и представляет в рамках этой книги более академический, чем практический интерес.

Некоторые коммерческие гипервизоры (например, ESX) позволяют работать и с устройствами, подключаемыми по сети (NAS/NFS), но это, скорее, исключение, чем правило.

Варианты подключения виртуального диска

В виртуальной машине жесткий диск можно подключить как к IDE-, так и SCSI-контроллеру. Часто рекомендуется для повышения производительности выбирать SCSI-вариант, хотя практической разницы между этими вариантами не наблюдается.

Обслуживание файлов виртуального диска

Файлы виртуальных дисков можно преобразовывать из одного типа в другой, дефрагментировать, сжимать (уменьшать в размере за счет исключения неиспользуемых участков). Для выполнения этих операций виртуальную машину необходимо предварительно выключить.

Учитывая существенные размеры файлов, эти операции следует заблаговременно планировать, поскольку выполняться они могут весьма длительное время.

Сохранение состояния виртуальной машины

Программы управления виртуальными машинами позволяют создавать *снимки* жестких дисков. Снимок (snapshot) является мгновенной копией текущего состояния системы и позволяет в случае необходимости восстановить виртуальную машину на этот момент времени.

---

[1] Fibre Channel (FC) (от *англ.* fibre channel, волоконный канал) — семейство протоколов для высокоскоростной передачи данных.

[2] iSCSI (от *англ.* Internet Small Computer System Interface) — протокол, который базируется на TCP/IP и разработан для установления взаимодействия и управления системами хранения данных, серверами и клиентами.

Обычно снимки используются в целях тестирования: создается копия рабочей виртуальной машины, после чего на нее, например, устанавливаются обновления программного обеспечения и проверяется правильность функционирования. В случае отсутствия ошибок на копии можно провести обновление и основной производственной системы.

Распределение вычислительных ресурсов

Виртуальная машина запускается как еще один процесс основной операционной системы. Несколько запущенных виртуальных машин будут делить между собой процессор(ы) хостовой системы.

ПО гипервизора обычно позволяет при создании виртуальной машины выделить ей один или несколько виртуальных процессоров. Не рекомендуется выделять виртуальной машине больше виртуальных процессоров, чем их установлено в хостовой системе. Если нет каких-либо особых причин, лучше предоставить виртуальной машине столько виртуальных процессоров, сколько физических процессоров (ядер) установлено в хостовой системе.

Администратор имеет возможность регулировать выделяемые каждой виртуальной машине вычислительные ресурсы, хотя и в ограниченных пределах: устанавливать относительные веса каждой виртуальной машины, гарантировать предоставление виртуальной машине некоторого минимального времени процессора и т. п. Эти настройки выполняются в ПО соответствующего гипервизора.

> ***Совет***
>
> Процессоры с поддержкой технологии Hyper-Threading отображаются в операционной системе как два процессора. Эта 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.

Оперативная память

Обычно именно память является ограничителем количества одновременно запускаемых на одном компьютере виртуальных машин. Для каждой виртуальной машины необходимо выделить в ее настройках некий 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 виртуальной машине памяти до допустимого предела, а 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 возможность запуска виртуального компьютера появляется.

Выделение виртуальным машинам излишней памяти приводит к увеличению количества операций чтения/записи на жесткий диск, что сказывается на производительности как основной системы, так и виртуальных.

Сервисные операции

Резервное копирование и антивирусная защита

Виртуальные машины, как и обычные системы, нуждаются в резервном копировании, защите от вирусов и т. п. Эти действия могут проводиться так же, как и обычно, — например, путем установки агента резервного копирования в операционную систему виртуальной машины с последующей настройкой операций.

Однако, учитывая возможность доступа к виртуальным машинам из среды гипервизора, в этих целях разработаны специальные программные решения. Так, для антивирусной защиты достаточно установить программное обеспечение только в гипервизор. Аналогично резервное копирование можно выполнить и без установки агентов в виртуальную машину. Подобные коммерческие решения предлагаются в настоящее время многими вендорами. Однако при их выборе следует предварительно проанализировать возможности этого ПО: для каких гостевых систем реализованы такие функции, с какими гипервизорами совместимы, дешевле ли такое решение или придется идти на дополнительные расходы и т. п.

Обмен данными

Примечание

Описываемые далее операции копирования доступны только после установки в гостевой операционной системе расширений виртуальной машины.

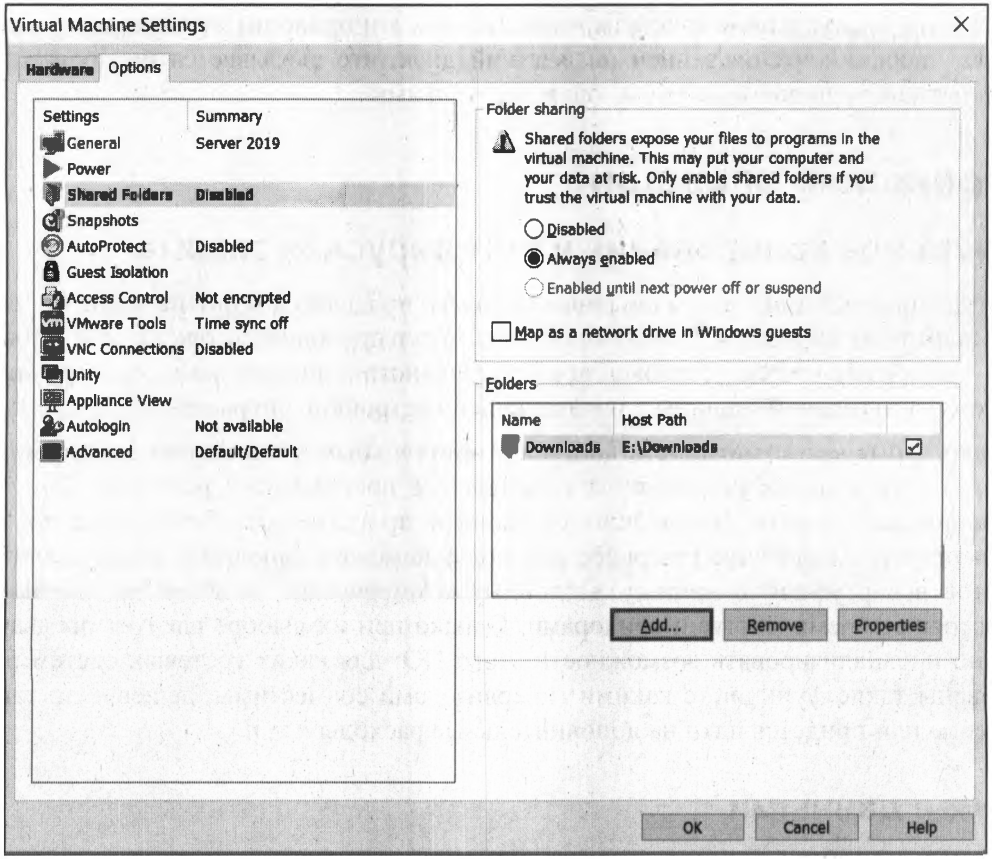
Копирование данных с машины на машину

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.

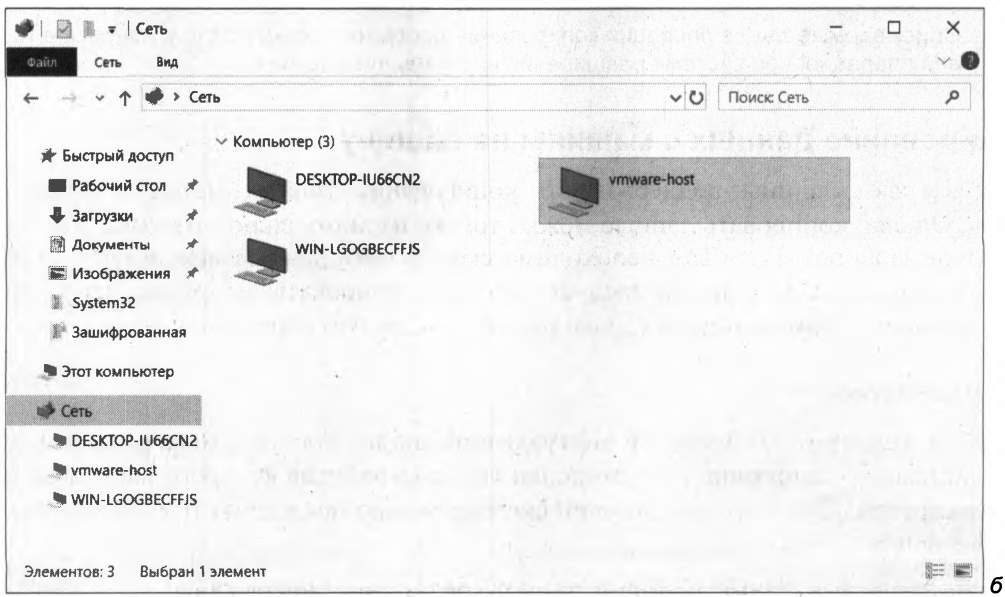
Общие папки

Часто необходимо обеспечить в виртуальной машине доступ к информации хостовой системы — например, для установки ПО, дистрибутив которого расположен на диске сервера. Для этого на хостовой системе можно предоставить в общий доступ любые папки.

Папки, предоставленные в общий доступ средствами гипервизора, подключаются так же, как и сетевые папки. Различия только в том, что общие папки могут быть созданы и без сетевого адаптера.



а



б

Рис. 8.2. *а* **— подключение папки хоста к гостевой машине для совместного использования;** *б* **— в виртуальной машине для доступа к «расшаренной папке» нужно просмотреть список ресурсов узла vmware-host**

Настройка общих папок выполняется в консоли управления гипервизора — достаточно указать предоставляемую в общий доступ папку и настроить режим доступа (полный или только для чтения). Подключение к общей папке в виртуальной среде происходит так же, как и подключение к общему ресурсу сети (рис. 8.2).

Миграция виртуальных машин

В этом разделе мы рассмотрим вопросы переноса виртуальной машины с одного гипервизора (сервера) на другой. Сразу оговоримся, что такая миграция не является средством обеспечения непрерывной работы системы. Это, скорее всего, один из вариантов обслуживания, при котором необходимо планово перенести вычисления на другой сервер, — например, при обслуживании сервера (проведении планово-профилактических работ, связанных с его выключением) или при переносе ВМ на более мощную вычислительную платформу.

> ***Примечание***
>
> Для того чтобы перенести виртуальную машину с одного гипервизора на другой, файл ее виртуального жесткого диска должен быть доступен как одному, так и другому серверу. Иными словами, необходимо использовать внешнюю систему хранения данных. Кроме того, с рабочего места, с которого осуществляется управление процессом миграции, должны быть доступны для администрирования оба гипервизора.

Возможность подобной миграции присутствует в большинстве гипервизоров. Реализуется она в консолях управления, причем наиболее просто — в коммерческих решениях (типа vSphere или Microsoft System Center Virtual Machine Manager). Однако администратор может осуществить перенос виртуальных машин и при помощи простейших сценариев. Например, в руководстве по миграции Hyper-V (**https://bit.ly/2Kxkb61**) пошагово описан весь процесс подготовки и переноса виртуальных машин.

Правильно подготовленная миграция позволяет практически не прерывать обслуживание. Так, при миграции Hyper-V во время переноса обычно происходит лишь потеря пары пакетов ping. Однако подобный перенос может не привести к успеху в случае высокой вычислительной нагрузки (большого изменения данных в оперативной памяти сервера). Кроме того, следует учесть, что часть параметров после завершения миграции должна быть вновь настроена вручную (подключения ISO-образов, параметры администрирования и т. п.).

Особо нужно отметить, что для успешности процесса лучше всего предусматривать *идентичные* конфигурации аппаратной и программной составляющих серверов (сервера-источника и сервера назначения): одинаковые модели процессоров, одно и то же их число, одинаковые версии операционной системы и т. д. и т. п. Постепенно число ограничений по идентичности параметров сервера-источника и сервера назначения с выходом новых версий ПО гипервизиров уменьшается. Но в любом случае, планируя процессы миграции, необходимо свериться с описанием поддерживаемых конфигураций в документации применяемого гипервизора.

Подключение к виртуальным машинам

Средствами управления гипервизора можно подключиться к рабочему столу виртуальной машины. Обычно консоль гипервизора легко можно поставить на станции администратора и управлять с ее помощью виртуальными машинами. Администраторы сразу же включают на виртуальных машинах опцию доступа к рабочему столу — в таком варианте доступны все функции управления, кроме включения питания виртуальной машины.

> ***Совет***
>
> Рекомендуется использовать управление виртуальной машиной только по защищенным каналам связи SSL (Secure Sockets Layer), как при работе на административной странице, 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 веб-сервере), порты 137 и 138 для TCP и UDP (используются при аутентификации).

Существуют некоторые особенности посылки специальных сочетаний клавиш. Так, вместо сочетания <Ctrl>+<Alt>+<Del> в консоли управления обычно используется <Ctrl>+<Alt>+<Ins>. Впрочем, эту команду, как правило, вызывают из меню управления. Переключение между режимами отображения виртуальной машины в окне и в полном экране осуществляется по нажатию правой клавиши <Alt> и <Enter>.

До установки расширений при щелчке мышью внутри окна виртуальной машины курсор мыши начинает перемещаться *только* в пределах виртуальной машины. Чтобы освободить курсор от какого-либо захвата, по умолчанию используется правая клавиша <Alt>.

Особенности выключения виртуальных машин

Существует несколько возможностей выключения виртуальной машины. Во-первых, можно завершить работу, выключив виртуальную машину с сохранением данных при помощи ее внутренней команды **Завершить работу**. Во-вторых, можно сохранить состояние виртуальной машины из консоли управления гипервизора. В этом случае ее работа как бы «заморозится», и 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`. Однако при последующем запуске может обнаружиться потеря несохраненной информации.

---

[1] Приведенные здесь примеры относятся к MS Virtual PC.

Если на вашем компьютере размещено несколько виртуальных машин, причем часть из них настроена на автоматический запуск при включении питания, то при выключении хостовой системы осуществляется сохранение состояния виртуальных машин. Этот процесс может существенно затянуться, если система будет сохранять много информации. В результате основная операционная система воспримет такую ситуацию как зависание прикладной программы с отсутствием ответа в течение заданного промежутка времени. Тогда виртуальная машина будет аварийно завершена, что может вызвать проблемы при ее следующей загрузке. Чтобы зарезервировать время на сохранение параметров виртуальных машин в случае перезагрузки хостовой системы, измените значение параметра реестра:

```
WaitToKillServiceTimeout
```

в ветви:

```
HKLM\SYSTEM\CurrentControlSet\Control\
```

установив необходимое время ожидания.

> ***Внимание!***
>
> **На некоторых облачных платформах необходимо двойное выключение виртуальной машины: сначала нужно выключить виртуальную машину средствами операционной системы (т. е. использовать команду `shutdown` или средства графического интерфейса пользователя), а затем нажать кнопку Выключить в панели управления виртуальной машиной. Если просто выключить «виртуалку», но не сообщить об этом панели управления, то за якобы использование виртуальной машины будут продолжать начисляться деньги. Если же нажать кнопку Выключить без предварительного выключения ее средствами ОС, то есть риск потери обрабатываемых данных.**

Виртуальные рабочие станции

Развитие технологий виртуализации позволило применить эти решения не только для серверов, но и для пользовательских рабочих станций (так называемые *desktop-решения*). Технологии виртуализации рабочих станций получили название VDI (Virtual Desktop Interface).

Сравниваем VDI-решения с терминальными клиентами

VDI-решения во многом напоминают терминальные подключения пользователей. Поэтому следующие основные преимущества терминалов свойственны и виртуальным рабочим столам:

- VDI-решения существенно снижают затраты на администрирование, поскольку вместо нескольких десятков рабочих станций работать приходится с несколькими серверами;
- конфигурации систем унифицированы, любые обновления выполняются быстрее и проще;

- сокращаются суммарные затраты на электроэнергию, оборудование используется более эффективно;
- все данные обрабатываются на сервере, и их легко защитить как для случая работы внутри локального сегмента, так и при доступе из публичной сети.

Так же как и у терминальных клиентов, у пользователей виртуальных рабочих столов могут возникнуть следующие сложности:

- невозможность использования функций аппаратных ускорителей (обработки графики на современных видеокартах, модулей аппаратного шифрования и т. п.);
- проблемы с использованием USB-устройств: видеокамер, сканеров, смарткарт и т. п.). Лучше использовать принтеры, имеющие сетевой (Ethernet) порт подключения.

При этом у пользователей виртуальных рабочих столов есть, на взгляд авторов, только одно, но весьма существенное преимущество. Каждый пользователь получает собственный виртуальный компьютер, который может быть настроен только для него и при этом совершенно не будет мешать другим сотрудникам. На виртуальный компьютер можно поставить любое необходимое программное обеспечение, что практически нереализуемо в условиях жестких настроек терминального сервера.

Немного об экономике VDI

Как и в любом ИТ-проекте, желательно сначала оценить, сколько будет стоить внедряемое решение и какую экономию (или убыток) оно принесет. Для сравнения приведем параметры, на которые ориентируются западные менеджеры и результаты расчета по которым приводятся на наших семинарах (табл. 8.3).

Как видно из данных табл. 8.3, экономия от внедрения решений VDI может быть достигнута только за счет разницы в стоимости рабочих станций и затрат на их обслуживание (электропитание, стоимость ремонта и т. п.). Поэтому экономически эффективным VDI-решение будет только при существенном числе рабочих станций и учете, например, не менее 3-летнего периода эксплуатации. Так, калькулятор эффективности от Oracle — Oracle Desktop Virtualization TCO Calculator[1] — устанавливает минимальную границу числа рабочих станций в 25 единиц.

Таблица 8.3. *Показатели экономической эффективности технологии VDI*

Параметр	Эффект	Примечание
Стоимость приобретаемого ПО (серверной и клиентских лицензий)	Затраты	Сумма варьируется для решений различных вендоров. Стоимость клиентских лицензий обычно составляет 100–150 $

[1] См. **http://www.oracle.com/us/media/calculator/vm/vm-home-2132015.html**.

Таблица 8.3 (окончание)

Параметр	Эффект	Примечание
Стоимость рабочей станции	Экономия (зависит от периода использования)	В качестве рабочих станций можно использовать упрощенные варианты («тонкие» клиенты и т. п.). Возможен отказ от приобретения индивидуальных источников аварийного питания. Кроме того, необходимо учесть разницу в ежегодных расходах на обслуживание (составляет примерно от 5 до 10% от стоимости станций)
Стоимость электропитания	Экономия (зависит от периода использования)	Экономия на электроснабжении рабочей станции (меньшая мощность), затраты на электропитание серверов, систем хранения
Стоимость оборудования: серверы, СХД, фермы	Затраты	Минимально от одного сервера и системы хранения, оптимально — отказоустойчивые решения с выделенными серверами управления, обеспечения доступа из Интернета и т. п.

Структура VDI-решений

VDI-решения объединяют различные элементы ИТ-структуры предприятия (рис. 8.3). Так, из службы каталогов берется информация о пользователях и группах. Например, некоторой группе пользователей можно поставить в соответствие определенный шаблон виртуального рабочего стола — в результате новому пользователю будет автоматически предоставляться конфигурация компьютера в соответствии с его функциональными обязанностями.

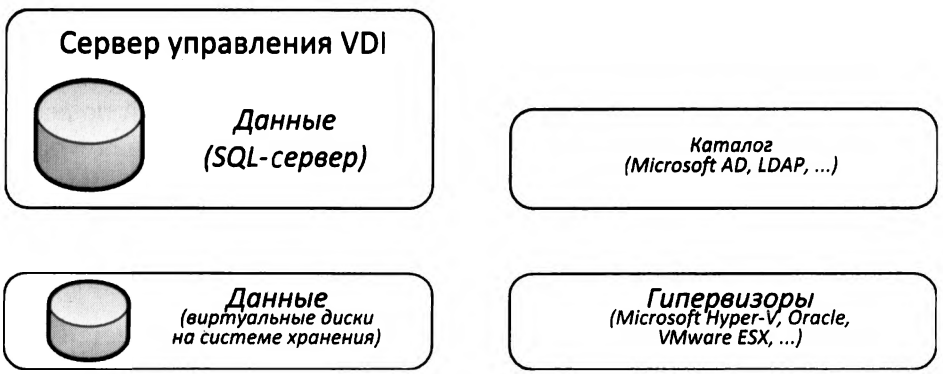


Рис. 8.3. Логическая структура VDI-решения

Программное обеспечение VDI может обеспечивать подключение (управлять) к виртуальным рабочим столам различных гипервизоров или к сессиям терминальных серверов.

Поскольку VDI-решения обслуживают большое количество рабочих столов, то они должны быть весьма надежными. Поэтому в производственной среде следует реализовывать отказоустойчивые решения: наряду с основным сервером управления

необходимо предусматривать резервные (один или несколько), нужно установить несколько серверов, на которых будут запускаться виртуальные рабочие столы, выбрать надежную систему хранения, построить резервированную сеть передачи данных (рис. 8.4).

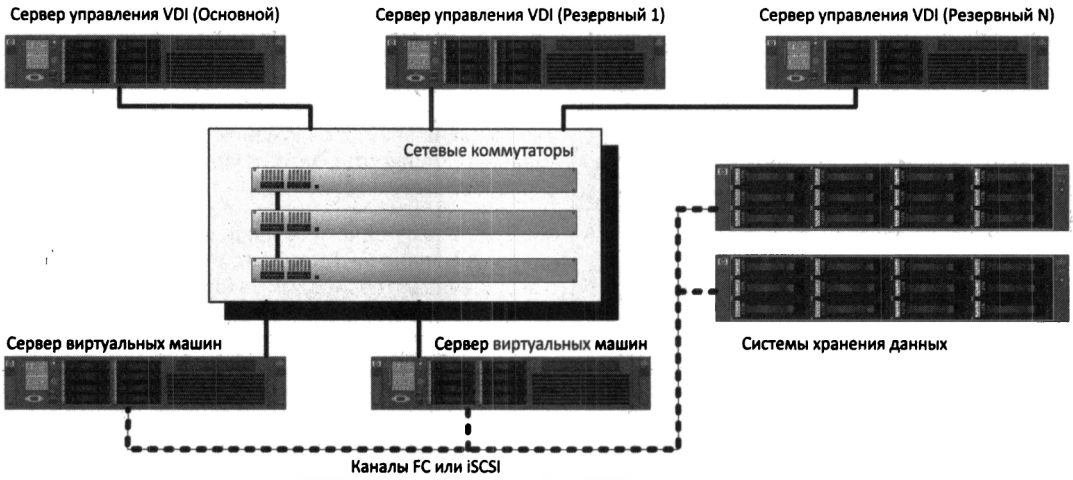


Рис. 8.4. Вариант аппаратной реализации VDI-решения

Некоторые особенности VDI-решений

VDI-решения обычно настраиваются на автоматическое создание виртуальных рабочих столов. Для этого администратором предварительно создаются шаблоны различной конфигурации, которые ставятся в соответствие группам пользователей из службы каталогов предприятия. При попытке подключения нового пользователя ПО предоставляет ему виртуальный рабочий стол, сформированный по соответствующему шаблону (для повышения производительности по шаблонам предварительно создается некоторое количество рабочих столов, которые находятся в неактивном состоянии). После отключения пользователя виртуальная машина, в зависимости от настроек, может сохраняться или уничтожаться для высвобождения ресурсов.

Поскольку однотипные конфигурации содержат значительное количество одинаковой информации на дисках и в памяти системы, то ПО VDI позволяет настроить совместное использование таких ресурсов.

Для подключения к VDI на рабочие места устанавливается клиентское ПО. При этом подключение к различным конфигурациям (различным виртуальным рабочим столам или терминальным сессиям) осуществляется через одну точку. Если пользователю разрешено подключение к нескольким рабочим столам/конфигурациям, то право соответствующего выбора предоставляется на экране подключения к VDI.

KVM и Virtuozzo (OpenVZ)

Разница между KVM и Virtuozzo

В Linux поддерживаются две технологии виртуализации на уровне ядра: KVM (Kernel Virtual Machine) и Virtuozzo (OpenVZ). У каждой из этих технологий есть свои преимущества и свои недостатки. При желании вы можете ознакомиться с ними в Интернете, где найдете множество статей, сравнивающих эти две технологии.

Но есть между ними одно очень важное различие — это возможность «оверселить» ресурсы Virtuozzo. Слово «оверселить» происходит от английского «oversell». Если вы совсем не знаете английского, поясним, что это означает «продать больше, чем было». Как такое возможно?

Рассмотрим пример. Представим, у вас есть сервер с 32 Гбайт оперативной памяти. Вы решили, что 2 Гбайт потребуется физическому серверу, а оставшиеся 30 Гбайт можно распределить между виртуальными машинами, — скажем, по 1 Гбайт (условно — для простоты расчетов) на каждый сервер. Вы создаете 30 серверов, каждому из которых отводите по 1 Гбайт оперативки. Но со временем вы обнаруживаете, что большинство серверов используют 500–600 Мбайт оперативной памяти, а то и меньше.

Следовательно, можно попытаться «продать» эту недобранную память. Вы делаете предположение, что в пики максимальной загрузки потребление оперативной памяти составит 750 Мбайт (не нужно забывать, что речь идет не о рабочей станции Windows, где последняя версия Skype легко забирает 500 Мбайт ОЗУ, а о Linux-сервере, который весьма скромно потребляет ресурсы компьютера). Оставшиеся от каждого сервера 250 Мбайт можно «продать» еще раз. В итоге к имеющимся 30 серверам у вас добавится еще 7:

$$250 \times 30 / 1024 \approx 7.$$

Все это будет выглядеть как 37 серверов по 1 Гбайт (максимально возможное потребление памяти), в то время как у вас есть всего 30 Гбайт доступной оперативной памяти. Это и есть оверселлинг.

О перерасходе памяти заботиться не нужно. Даже если сервер S1 израсходует 850 Мбайт оперативной памяти, то сервер S2 — всего 430. В итоге общее потребление оперативной памяти составит по 640 Мбайт на сервер. Если же все-таки произойдет ситуация, когда серверы начнут потреблять больше памяти, чем есть на самом деле, будет задействована подкачка. Да, это снизит производительность, но вся информационная система останется в работоспособном состоянии.

Чтобы не попасть на оверселлинг, желающие обзавестись виртуальным сервером (VPS) стараются приобрести KVM-сервер. Технология KVM жестко распределяет ресурсы сервера, и оверселлинг здесь невозможен. Поэтому хостеры чаще предлагают именно KVM-серверы, поскольку желающих на такой сервер больше.

Тем не менее, если вы создаете подобную информационную систему для своего предприятия, Virtuozzo позволит вам более эффективно использовать ресурсы сер-

вера. Да, можно было бы и в KVM создать 37 серверов — по 750 Мбайт оперативной памяти на каждый. Но тут суть в распределении ресурсов: максимальный лимит — 1 Гбайт, и если серверу S23, скажем, понадобится 990 Мбайт, он в условиях Virtuozzo их получит. Произойдет это за счет сервера, который не использует много ОЗУ, — например, за счет сервера S37, который потребляет всего 530 Мбайт. Общее потребление ОЗУ на два сервера не превысило 1,5 Гбайт, поэтому все в норме. А в случае с KVM, если бы всем было жестко выделено по 750 Мбайт, то сервер S23 «ушел бы в своп», но при этом в системе остались бы 220 Мбайт свободной оперативной памяти, которую можно было задействовать в Virtuozzo на условиях оверселлинга.

Большинство облачных провайдеров стараются использовать технологию KVM, поскольку клиентам не очень нравится, что ресурсы, за которые они заплатили, могут быть перепроданы, поэтому в этом издании будет рассмотрена именно KVM.

Виртуализация на основе технологии KVM

Установка KVM

Первым делом нужно узнать, поддерживает ли наш процессор виртуализацию, и можем ли мы вообще использовать KVM. Введите команду:

```
grep -E '(vmx|svm)' /proc/cpuinfo
```

Результат выполнения этой команды приведен на рис. 8.5. Вникать особо в вывод не нужно — главное, что он есть. А вот если в ответ на ввод этой команды последует тишина, значит, ваш процессор не поддерживает виртуализацию.

Дистрибутив Ubuntu поддерживает KVM на уровне ядра, а для работы с гипервизором рекомендует использовать библиотеку libvirt, что мы и будем делать далее. Но сначала нужно проверить поддержку аппаратной виртуализации, и для этого введем команду:

```
kvm-ok
```

В ответ вы должны увидеть следующий вывод:

```
INFO: /dev/kvm exists
KVM acceleration can be used
```

Осталось установить пакеты, необходимые для работы с KVM:

```
sudo apt install qemu-kvm libvirt-bin ubuntu-vm-builder bridge-utils
```

При желании также можно установить для libvirt графическую оболочку Virt Manager:

```
sudo apt install virt-manager
```

Оболочка Virt Manager чем-то напоминает VMware Workstation. Ее довольно просто освоить самостоятельно.

```
root@dedicated:~# grep -E '(vmx|svm)' /proc/cpuinfo
flags           : fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat pse36 clflush dt
s acpi mmx fxsr sse sse2 ss ht tm pbe syscall nx rdtscp lm constant_tsc arch_perfmon pebs bts rep_go
od nopl xtopology nonstop_tsc cpuid aperfmperf pni pclmulqdq dtes64 monitor ds_cpl vmx smx est tm2 s
sse3 cx16 xtpr pdcm pcid sse4_1 sse4_2 x2apic popcnt tsc_deadline_timer aes xsave avx f16c rdrand la
hf_lm cpuid_fault epb pti tpr_shadow vnmi flexpriority ept vpid fsgsbase smep erms xsaveopt dtherm i
da arat pln pts
vmx flags       : vnmi preemption_timer invvpid ept_x_only flexpriority tsc_offset vtpr mtf vapic ep
t vpid unrestricted_guest
flags           : fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat pse36 clflush dt
s acpi mmx fxsr sse sse2 ss ht tm pbe syscall nx rdtscp lm constant_tsc arch_perfmon pebs bts rep_go
od nopl xtopology nonstop_tsc cpuid aperfmperf pni pclmulqdq dtes64 monitor ds_cpl vmx smx est tm2 s
sse3 cx16 xtpr pdcm pcid sse4_1 sse4_2 x2apic popcnt tsc_deadline_timer aes xsave avx f16c rdrand la
hf_lm cpuid_fault epb pti tpr_shadow vnmi flexpriority ept vpid fsgsbase smep erms xsaveopt dtherm i
da arat pln pts
vmx flags       : vnmi preemption_timer invvpid ept_x_only flexpriority tsc_offset vtpr mtf vapic ep
t vpid unrestricted_guest
flags           : fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat pse36 clflush dt
s acpi mmx fxsr sse sse2 ss ht tm pbe syscall nx rdtscp lm constant_tsc arch_perfmon pebs bts rep_go
od nopl xtopology nonstop_tsc cpuid aperfmperf pni pclmulqdq dtes64 monitor ds_cpl vmx smx est tm2 s
sse3 cx16 xtpr pdcm pcid sse4_1 sse4_2 x2apic popcnt tsc_deadline_timer aes xsave avx f16c rdrand la
hf_lm cpuid_fault epb pti tpr_shadow vnmi flexpriority ept vpid fsgsbase smep erms xsaveopt dtherm i
da arat pln pts
vmx flags       : vnmi preemption_timer invvpid ept_x_only flexpriority tsc_offset vtpr mtf vapic ep
t vpid unrestricted_guest
flags           : fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat pse36 clflush dt
s acpi mmx fxsr sse sse2 ss ht tm pbe syscall nx rdtscp lm constant_tsc arch_perfmon pebs bts rep_go
od nopl xtopology nonstop_tsc cpuid aperfmperf pni pclmulqdq dtes64 monitor ds_cpl vmx smx est tm2 s
sse3 cx16 xtpr pdcm pcid sse4_1 sse4_2 x2apic popcnt tsc_deadline_timer aes xsave avx f16c rdrand la
hf_lm cpuid_fault epb pti tpr_shadow vnmi flexpriority ept vpid fsgsbase smep erms xsaveopt dtherm i
da arat pln pts
vmx flags       : vnmi preemption_timer invvpid ept_x_only flexpriority tsc_offset vtpr mtf vapic ep
t vpid unrestricted_guest
```

Рис. 8.5. Результат выполнения команды `grep -E '(vmx|svm)' /proc/cpuinfo`

Создание виртуальной машины

Создать виртуальную машину можно с помощью команды `virt-install`:

```
sudo virt-install \
  --virt-type=kvm \
  --name ubuntu2004\
  --ram 4096 \
  --vcpus=4 \
  --os-variant=ubuntu20.04 \
  --hvm \
  --cdrom=/iso/ubuntu-20.04.1-server-amd64.iso \
  --network network=default,model=virtio \
  --graphics vnc \
  --disk path=/var/lib/libvirt/images/ubuntu2004.img,size=40,bus=virtio
```

Разумеется, все эти параметры можно ввести в одну строку, но мы здесь используем символ \ для удобства читателя. Приведенная команда означает вот что: мы создаем виртуальную машину с именем `ubuntu2004`, имеющую 4 Гбайт оперативной памяти и 4 виртуальных процессора.

Гостевая операционная система задается параметром `--os-variant` (мы здесь будем работать в Ubuntu 20.04). Предварительно нужно скачать и поместить в каталог /iso

(это может быть точка монтирования внешней файловой системы для экономии места на основной файловой системе) ISO-образ этого дистрибутива. У нас он называется `ubuntu-20.04.1-server-amd64.iso`. Образ виртуального диска будет храниться в каталоге =/var/lib/libvirt/images. Параметр `size=40` задает размер виртуального диска в гигабайтах (т. е. 40 Гбайт). Сетевая карта — стандартная, т. е. виртуальная машина будет получать доступ к Интернету через NAT.

Также есть возможность загрузить ISO-образ по сети. Пример:

```
sudo virt-install --name ubuntu-guest --os-variant ubuntu20.04 --vcpus 4 --ram
4096 --location http://ftp.ubuntu.com/ubuntu/dists/focal/main/installer-amd64/
--network bridge=virbr0,model=virtio --graphics none --extra-
args='console=ttyS0,115200n8 serial'
```

Параметр `--os-variant`, как уже отмечалось, указывает гипервизору, под какую именно ОС следует адаптировать настройки. Список доступных вариантов ОС можно получить, выполнив команду:

```
osinfo-query os
```

Если такой утилиты нет в вашей системе, то ее нужно установить:

```
sudo apt install libosinfo-bin
```

После запуска установки в консоли появится вот такая надпись:

```
Domain installation still in progress. You can reconnect to the console to
complete the installation process.
```

Это вполне нормально. Продолжить установку мы сможем через VNC. Но сначала нужно посмотреть, на каком порту он работает. Введите команду:

```
virsh dumpxml ubuntu2004
...
<graphics type='vnc' port='5900' autoport='yes' listen='127.0.0.1'>
<listen type='address' address='127.0.0.1'/>
</graphics>
...
```

Здесь мы видим, что используется порт 5900 на локальном адресе 127.0.0.1. Чтобы подключиться к VNC, необходимо использовать Port Forwarding через SSH. Перед тем как это сделать, убедитесь, что tcp forwarding разрешен у демона ssh. Для этого нужно проверить настройки sshd:

```
cat /etc/ssh/sshd_config | grep AllowTcpForwarding
```

Если ничего не нашлось или форвардинг выключен:

```
AllowTcpForwarding no
```

Тогда нужно изменить файл так:

```
AllowTcpForwarding yes
```

После этого надо перезагрузить sshd.

Выполняем команду на локальной машине:

```
ssh -fN -l login  -L 127.0.0.1:5900:localhost:5900 server_ip
```

Здесь мы настроили ssh port forwarding с локального порта 5900 на серверный порт 5900. Вместо `server_ip` нужно указать ваш IP-адрес во внутренней сети. Теперь уже можно подключиться к VNC, используя любой VNC-клиент. Я предпочитаю UltraVNC из-за простоты и удобства.

После успешного подключения на экране отобразится стандартное окно приветствия начала установки Ubuntu (рис. 8.6).

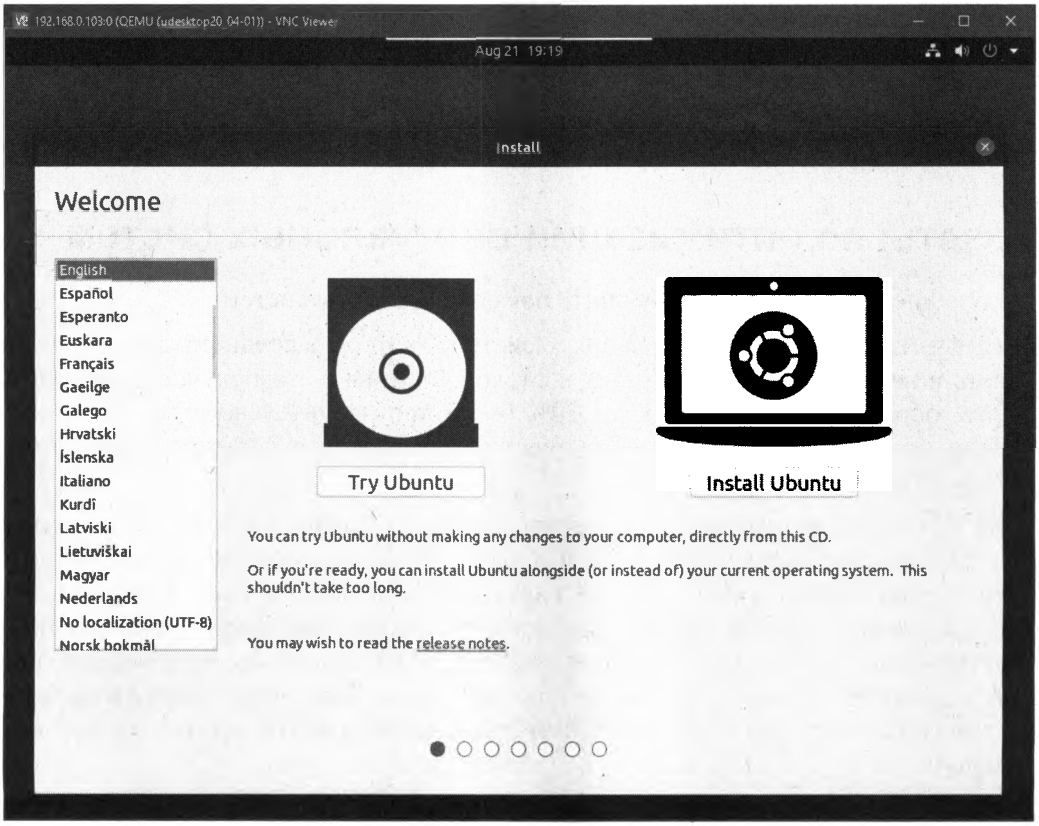


Рис. 8.6. Установка Ubuntu в виртуальной машине

Полезные команды

Для просмотра всех работающих виртуальных машин (все доступные можно получить добавив `--all`):

```
sudo virsh list
```

Перезагрузить хост можно командой `reboot`:

```
sudo virsh reboot $VM_NAME
```

Остановить виртуальную машину можно так:

```
sudo virsh stop $VM_NAME
```

Запустить:

```
sudo virsh start $VM_NAME
```

Отключить:

```
sudo virsh shutdown $VM_NAME
```

Добавить виртуальную машину в автозапуск (чтобы она запускалась автоматически при запуске физического сервера) можно командой:

```
sudo virsh autostart $VM_NAME
```

Очень часто требуется клонировать систему, чтобы в будущем использовать ее как каркас для других виртуальных ОС, — для этого используют утилиту virt-clone:

```
virt-clone -help
```

Советы по оптимизации виртуальных систем

Следующие советы помогут улучшить показатели работы систем:

- если есть аппаратные требования к системе, которую предполагается реализовать в виртуальной среде, то для хостовой системы в этом случае нужно выбирать оборудование примерно на 20% более производительное, чем рекомендовано. Это относится, например, к числу процессоров, их частоте, объему оперативной памяти и т. п.;
- не забывайте, что оперативная память нужна и операционной системе гипервизора. Так, для Microsoft Hyper-V требуется 500 Мбайт памяти. На первый гигабайт оперативной памяти каждой виртуальной машины нужно 32 Мбайта и на последующие — по 8 Мбайт. Если на хостовой системе установлена Windows, то это еще 512 Мбайт. Эти значения описывают невыгружаемую память ядра. В результате на хостовой системе должно быть на 500–1000 Мбайт оперативной памяти больше, чем сумма значений оперативной памяти каждой виртуальной машины;
- оптимально, если одному виртуальному процессору будет соответствовать один физический (это снизит затраты на переключение ресурсов);
- на гостевые машины устанавливайте преимущественно 64-разрядные операционные системы;
- для размещения файлов виртуальных дисков используйте самые быстрые накопители: SSD-диски, RAID-массивы уровня 0 и т. д.;
- вместо динамически расширяемых виртуальных дисков используйте диски фиксированного размера — они работают быстрее. Часто рекомендуют использовать SCSI-адаптеры гипервизора для монтирования виртуальных дисков. Связано это с тем, что такие адаптеры доступны *только* после установки гостевых расширений виртуальных машин. Тем самым гарантируется оптимальность

конфигурации гипервизора. Если производительность диска является критическим параметром для виртуальной машины, то используйте прямое подключение жесткого диска;

- отключите поддержку технологии Hyper-Threading в BIOS хостового компьютера;
- отключите в хостовой системе все неиспользуемые роли (службы);
- для гостевых систем используйте «усеченные» версии операционных систем;
- обязательно устанавливайте расширения для виртуальных машин, в том числе и для хостовой операционной системы (если она установлена);
- периодически дефрагментируйте виртуальные диски средствами установленных на них операционных систем, после чего выполняйте дефрагментацию файла виртуального диска средствами программы управления;
- не включайте на виртуальных машинах различные визуальные эффекты, 3D-эффекты и т. п.;
- используйте несколько сетевых адаптеров: один для доступа к хостовой системе, другие разделите между всеми виртуальными машинами.

Виртуализация в сетях передачи данных

Как уже отмечалось ранее, виртуализировать можно практически все. В этом разделе мы поговорим о виртуализации в сетях передачи данных.

Виртуальные частные сети

Виртуальная локальная сеть (VLAN, Virtual Local Area Network) — группа устройств, взаимодействующая напрямую на канальном уровне, при этом на физическом уровне все эти устройства подключены к разным коммутаторам. Устройства, находящиеся в разных виртуальных сетях, невидимы друг для друга на канальном уровне, даже если они подключены к одному и тому же коммутатору, а взаимодействие между устройствами осуществляется только на сетевом или других, более высоких уровнях.

Виртуальные локальные сети используются для создания логической топологии сети, которая никак не зависит от ее физической топологии.

VLAN можно создать только на управляемых устройствах. Бюджетные устройства (также их часто называют *офисными*) VLAN не поддерживают.

Зачем нужны виртуальные сети?

Все виртуальное, оказывается, находит в реальном мире вполне конкретное применение. Виртуальная локальная сеть — это не какой-нибудь эмулятор или игрушка для админа, а вполне реальный инструмент построения современной сети.

- Во-первых, VLAN позволяет гибко компоновать устройства по группам. Например, можно с легкостью объединить устройства, находящиеся в разных мес-

тах, в одну сеть или же разделить устройства одной сети на разные виртуальные подсети.

- Во-вторых, виртуальная локальная сеть может уменьшить количество широковещательного трафика в сети. С помощью VLAN можно разбить коммутатор на несколько широковещательных доменов и отправить широковещательное сообщение только одной группе устройств (одной виртуальной сети).
- В-третьих, VLAN позволяет повысить безопасность и управляемость сети. VLAN активно используются для борьбы с ARP-спуфингом[1] и существенно упрощают применение политик и правил безопасности. С помощью виртуальных сетей можно применять правила к целым подсетям, а не к каждому устройству.

Маркировка кадров

Когда компьютер передает данные, он ничего не подозревает ни о своей принадлежности к какой-либо виртуальной сети, ни о существовании VLAN. Он просто передает информацию. А вот всем остальным занимается коммутатор, который «знает», что компьютер, подключенный к тому или иному порту, принадлежит той или иной виртуальной сети.

Что делать, если на порт приходит трафик разных VLAN? Как его различить? Для этого используется *маркировка кадров*. Маркировка (tagging) позволяет идентифицировать трафик, т. е. установить, к какой виртуальной сети он принадлежит.

Существуют различные варианты маркировки кадров. Иногда производители оборудования, в частности Cisco, разрабатывают собственные протоколы маркировки кадров. Но чаще используется стандарт IEEE 802.1Q. Согласно этому протоколу во внутрь кадра помещается специальная метка — *тег*, которая передает информацию о принадлежности трафика к определенной VLAN.

Размер этой метки всего 4 байта, и она состоит из следующих полей:

- TPID (Tag Protocol Identifier) — идентификатор протокола маркировки. Идентифицирует протокол, использующийся для маркировки кадра. Идентификатор протокола 802.1Q — 0x8100. Размер этого поля равен 16 битам;
- Priority — задает приоритет передаваемого трафика. Используется стандартом IEEE 802.1p. Размер — 3 бита;
- CFI (Canonical Format Indicator) — индикатор канонического формата. Проще говоря, задает формат MAC-адреса: 1 — канонический, 0 — неканонический. Размер поля — всего 1 бит;
- VID (VLAN Identifier) — задает индикатор виртуальной сети. Указывает, к какой виртуальной сети принадлежит кадр. Размер — 12 битов.

Маркер вставляется перед полем `Тип протокола` — понятное дело, после этого пересчитывается контрольная сумма, поскольку кадр уже изменился (рис. 8.7).

---

[1] ARP-спуфинг — один из методов взлома сетей.

Исходный кадр

Адрес получателя	Адрес отправителя	Тип протокола	Данные	Контрольная сумма

Маркированный кадр

Адрес получателя	Адрес отправителя	**Маркер**	Тип протокола	Данные	**Контрольная сумма**

Рис. 8.7. Исходный и измененный (маркированный) кадры

Порты и VLAN

Обратимся к портам коммутатора и виртуальным сетям. Порты коммутатора, которые поддерживают виртуальную сеть, можно разделить на две группы: маркированные порты (в терминологии Cisco — транковые порты, от *англ.* trunk ports) и немаркированные порты (порты доступа, access ports).

- *Маркированные порты* нужны, чтобы через один порт можно было передавать и получать трафик от нескольких виртуальных сетей. При этом виртуальных сетей может быть несколько, а порт — всего один. Как уже было отмечено ранее, информация о принадлежности трафика той или иной виртуальной сети указывается в специальном поле кадра. Без этого поля коммутатор не сможет различить трафик от разных сетей.
- *Немаркированные порты* (порты доступа) используются для передачи немаркированного трафика. Порт доступа может быть только в одной виртуальной сети. Порт может быть маркированным в нескольких VLAN и одновременно являться портом доступа в какой-то другой одной виртуальной сети. Если порт является портом доступа для какой-то виртуальной сети, то эта сеть называется *родной* для этого порта (native VLAN).

Когда на порт доступа приходит маркированный трафик, то он обычно должен удаляться, но это происходит не всегда — все зависит от настроек коммутатора. По умолчанию все порты коммутатора считаются портами доступа для сети VLAN 1. В процессе настройки администратор может изменить тип порта на маркированный и определить принадлежность портов к разным VLAN.

Порты коммутатора могут привязываться к определенной виртуальной сети статически или динамически. В первом случае администратор вручную определяет, какой порт будет принадлежать к какой VLAN. При динамическом назначении узлов принадлежность порта к той или иной виртуальной сети определяется коммутатором. Процедура назначения портом описана в стандарте 802.1X. Этот стандарт предусматривает аутентификацию пользователя на RADIUS-сервере для получения доступа к порту.

Практика настройки VLAN на коммутаторах Cisco

Думаем, всем уже ясно, что VLAN — штука полезная, и пора все настроить на практике. Чтобы не «изобретать колесо заново», воспользуемся примерно такой же топологией сети, какая описана в документации Cisco, но с небольшими усовершенствованиями.

Итак, у нас есть два коммутатора: **switch1** и **switch2**. К каждому из коммутаторов подключено по две виртуальные сети. Для подключения к коммутаторам компьютеры виртуальной локальной сети используют порты доступа (fa0/N), а для связи между коммутаторами служит транковый (маркированный) порт. На рис. 8.8 приведена конфигурация виртуальной локальной сети, а на рис. 8.9 — та же сеть, но уже оснащенная роутером для доступа к Интернету.

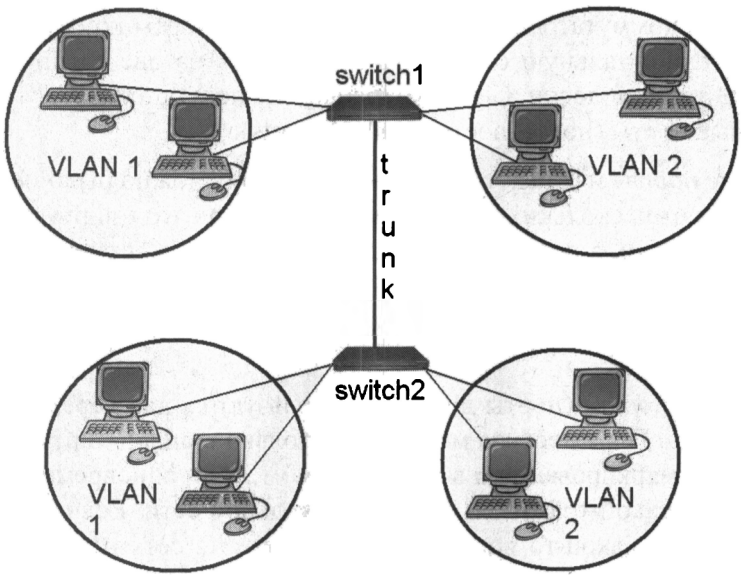


Рис. 8.8. Усовершенствованная топология сети Cisco

Теперь следует указать IP-адрес маршрутизатора (192.168.1.1) — этот адрес будет шлюзом по умолчанию для компьютеров первой виртуальной сети (**VLAN 1**, или `default`):

```
switch1(config)#interface default
switch1(config-if)#ip address 192.168.1.1 255.255.255.0
switch1(config-if)#no shutdown
```

Аналогично можно задать:

```
switch1(config)#interface vlan2
switch1(config-if)#ip address 192.168.1.1 255.255.255.0
switch1(config-if)#no shutdown
```

Теперь настроим интерфейс fa0/20, который соединен с маршрутизатором (см. рис. 8.9). Трафик, который не предназначен нашим виртуальным сетям, должен

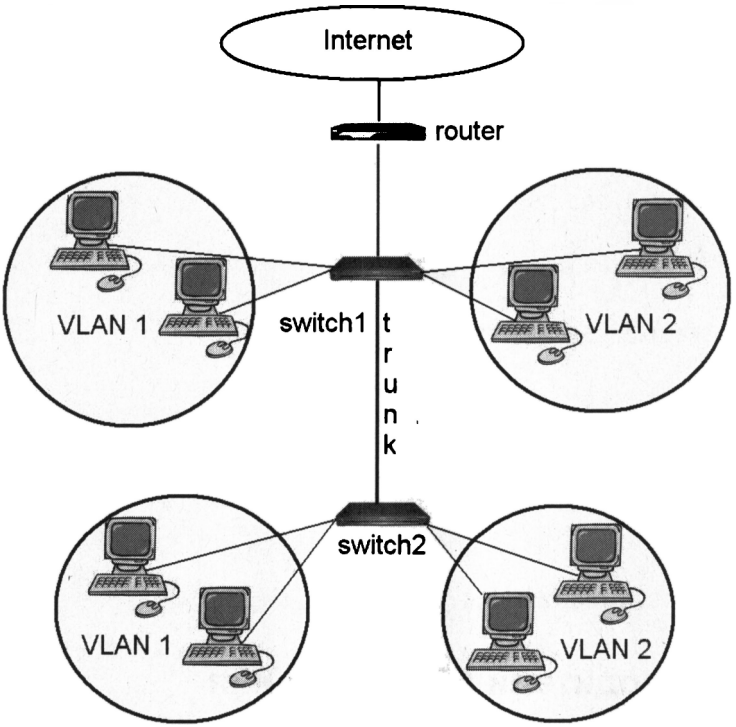


Рис. 8.9. Конфигурация виртуальной локальной сети с доступом к Интернету

перенаправляться на маршрутизатор, а он уже сам пусть разбирается, что с ним делать.

Вот необходимые команды конфигурации:

```
switch1(config)#interface fa0/20
switch1(config-if)#no switchport
switch1(config-if)#ip address 192.168.1.1 255.255.255.0
switch1(config-if)#no shutdown
```

Осталось еще прописать сам маршрут:

```
switch1(config-if)#ip route 0.0.0.0 0.0.0.0 192.168.1.1
```

Рассмотрим окончательную конфигурацию коммутатора **switch1**:

```
!
ip routing
!
interface fa0/3
switchport mode access
switchport access vlan 2
!
interface fa0/4
switchport mode access
switchport access vlan 2
```

```
!
interface fa0/24
switchport encapsulation dot1q
switchport mode trunk
!
interface default
ip address 192.168.1.1 255.255.255.0
no shutdown
!
interface vlan2
ip address 192.168.1.1 255.255.255.0
no shutdown
!
interface fa0/20
no switchport
ip address 192.168.1.1 255.255.255.0
no shutdown
!
ip route 0.0.0.0 0.0.0.0 192.168.1.1
```

Другие производители оборудования

Понятно, что Cisco — далеко не единственный производитель сетевого оборудования. Учитывая, что оборудование от Cisco стоит дорого, желающие сэкономить наверняка будут искать более дешевые аналоги. Один из таких аналогов — это оборудование от D-Link. Простенькое, иногда зависает (ничего личного — говорим как есть), но зато ощутимо дешевле.

Обратите внимание, что далеко не все оборудование от D-Link поддерживает виртуальные локальные сети.

О настройке VLAN на коммутаторах D-Link можно прочитать вот на этой страничке: **http://xgu.ru/wiki/VLAN_в_D-LINK**, или в руководстве пользователя.

Настройка VLAN в Linux

А теперь рассмотрим настройку виртуальных сетей в ОС Linux. Этот раздел вам понадобится, если вы надумали построить программный маршрутизатор между двумя VLAN на базе Linux или хотите обеспечить присутствие одного и того же сервера в нескольких VLAN: такой себе Фигаро тут, Фигаро там.

Первым делом надо добавить модуль 802.1Q, обеспечивающий маркировку кадров:

```
# modprobe 8021q
```

Модуль не найден? Тогда следует перекомпилировать ядро, включив поддержку этого модуля. Вот заветные команды:

```
# cd /usr/src/linux
# make menuconfig
```

```
# make modules
# make modules_install
```

Модуль включается в разделе: `Network options / 802.1Q VLAN Support`.

После перекомпиляции ядра перезагружаем систему и снова вводим команду:

```
# modprobe 8021q
```

Модуль должен быть загружен. Затем надо выключить сетевой интерфейс и «поднять» его, но уже без IP-адреса:

```
# /sbin/ifconfig eth0 down
# /sbin/ifconfig eth0 0.0.0.0 up
```

Теперь укажем, к какому интерфейсу какая из виртуальных сетей подключена. Для этого используется команда `vconfig` (пакет vlan или vconfig — название пакета, содержащего программу vconfig, зависит от дистрибутива). Формат вызова команды такой:

```
# /sbin/vconfig add интерфейс VLAN_ID
```

Например:

```
# /sbin/vconfig add eth0 1
# /sbin/vconfig add eth0 2
```

В этом случае мы связали VLAN 1 и VLAN 2 с одним сетевым интерфейсом — eth0. Далее нужно указать IP-адрес и сетевую маску для каждого интерфейса:

```
# /sbin/ifconfig eth0.1 192.168.1.x netmask 255.255.255.0 up
# /sbin/ifconfig eth0.2 192.168.2.x netmask 255.255.255.0 up
```

Можно задать маршрут по умолчанию (если необходимо):

```
# /sbin/route add default gw 192.168.1.x
```

Получить исчерпывающую информацию о «виртуальных» интерфейсах можно через псевдофайловую систему `/proc`:

```
cat /proc/net/vlan/eth0.N
```

Например:

```
cat /proc/net/vlan/eth0.1
```

Это еще не все. VLAN мы вроде бы настроили, но при перезагрузке потеряем все настройки. Чтобы этого не случилось, нужно прописать модуль 802.1Q в файле /etc/modules.conf, а настройки VLAN — в файле /etc/network/interfaces, например:

```
auto myvlan
iface myvlan inet static
        address 192.168.1.1
        netmask 255.255.255.0
        vlan_raw_device eth0
```

Можно также создать сценарий и добавить его вызов в сценарий автозапуска системы — это уже как кому больше нравится.

Выбор сервера: физический или виртуальный

Нужен ли вашему проекту сервер?

Часто бывает так, что человек мучается над выбором физического сервера, а он ему вообще не нужен. Поэтому первым делом надо определиться, нужен ли сервер вообще, а потом уже думать, какой из них покупать: физический или виртуальный.

Вот несколько причин, согласно которым проекту (предприятию/организации) нужен собственный сервер:

- крупный интернет-проект: игровой сервер, большой интернет-магазин, хостинг-провайдер и т. п.;
- необходимость удаленной совместной работы с каким-либо приложением вроде бухгалтерской программы «1С:Предприятие» или любым другим подобным;
- наличие большого количества пользовательского контента — например, если это социальная сеть;
- сайт с высокой посещаемостью, с которой обычный хостинг уже не справляется, и его нередко отключают за превышение лимита ресурсов.

Впрочем, в последнем случае сервер не всегда и нужен. Возможно, следует оптимизировать программное обеспечение, чтобы уменьшить нагрузку на хостинг, или попробовать перейти к другому хостеру с более «мягкими» лимитами.

А вот в первых трех случаях сервер нужен. Вот только заметьте, что мы пока не говорим, какой именно. Для других вариантов проектов (четвертый случай из рассмотренных, как уже было указано, — под вопросом) дешевле и проще приобрести хостинг. Учитывая среднюю стоимость физического сервера, средств, потраченных на него, хватит лет на 50 аренды хостинга.

Если же ваш проект соответствует приведенным здесь критериям, сервер все-таки нужен. Осталось решить, будет это физический сервер или можно обойтись виртуальным. Для начала рассмотрим коммерческую сторону вопроса.

Стоимость физического сервера

Давайте подберем сервер средней конфигурации, который бы подошел под наши нужды. При выборе сервера ориентируйтесь на модели в стандартных корпусах 1U или 2U, что будет полезно, если вы надумаете установить сервер в дата-центре.

Вот примерная конфигурация такого сервера:

- Proliant DL180 Gen9 E5-2620v4 Hot Plug Rack (2U);
- Xeon 8C 2,1 GHz (20 Mb);
- 1×16 Gb R1D_2400;
- RAID-контроллер P440FBWC (2 Gb кеш, поддерживаемые уровни RAID1/10/5/6);
- 2×300 Gb 12G10K (8/16 up) SFF;

- noDVD;
- 2 HPFans;
- iLOstd (w/o port);
- 2×1 Gb Eth;
- EasyRK + CMA;
- 1×900 W.

Конфигурация средняя, но есть определенные положительные моменты: стандартный корпус 2U, серверный процессор Xeon, регистровая память 16 Гбайт, два накопителя по 300 Гбайт каждый (подойдет для создания RAID-массива).

Стоимость этого сервера, по данным Яндекс.Маркет, составляет 146 851 рубль. От этой суммы мы и будем отталкиваться в дальнейших расчетах.

Стоимость виртуального сервера

Посмотрим, во сколько обойдется адекватный виртуальный сервер. Стоимость виртуального сервера будет зависеть от его конфигурации и выбранной платформы. Авторы этой книги имели опыт работы со следующими платформами: Microsoft Azure, Hetzner, Xelent Cloud. Платформа Hetzner отличается весьма демократичными ценами. Самые высокие цены у Microsoft. В среднем виртуальный сервер конфигурации CX41 (4 процессора, 16 Гбайт памяти и 160 Гбайт дискового пространства) обойдется всего лишь в 19 евро (примерно 1900 рублей) в месяц. В тариф включено 20 Тбайт трафика — в большинстве случаев этого будет достаточно, поэтому можно сказать, что трафик бесплатный.

Если разделить стоимость физического сервера (146 851 рубль) на стоимость ежемесячной аренды, то этих денег хватит более чем на 70 (!) месяцев аренды сервера. Другими словами, вы можете арендовать виртуальный сервер почти 6 лет.

> ***Примечание***
>
> Потребности в ресурсах, так же как и цены на физические устройства и виртуальный хостинг, все время растут, а курсы валют колеблются, и ко времени выхода книги из печати и рассматриваемые конфигурации, и расчеты их стоимости могут устареть, однако соотношения цен на физические серверы и виртуальный хостинг, как правило, остаются стабильными, соответственно и излагаемые здесь соображения — актуальными.

Также учтите, что, приобретая физический сервер, всю сумму придется заплатить сразу. Заметьте: мы говорим сейчас не об аренде физического сервера, а именно о покупке собственного за собственные средства. В случае с заемными средствами сервер обойдется еще дороже, поскольку надо будет выплачивать проценты по кредиту. В качестве капиталовложения физический сервер для небольших и средних проектов — тоже не вариант, т. к. за непродолжительное время он очень быстро потеряет в цене и вы не сможете продать его даже за половину затраченной суммы, если обнаружите, что он вам больше не нужен.

Да, вы можете возразить, что на физическом сервере в два раза больше дискового пространства, но:

- во-первых, далеко не всегда вам сразу нужны будут все его 300 Гбайт (второй накопитель используется в качестве «зеркала», поэтому вторые его 300 Гбайт не считаются);
- во-вторых, в случае с виртуальным сервером вам не нужно будет сразу оплачивать стоимость аренды на 6 лет вперед. Вы можете платить так, как вам угодно: раз в месяц, почасово (0,017 евро в час для нашей конфигурации), можно уменьшить количество ресурсов и платить меньше. Так, аренда конфигурации с 8 Гбайт памяти стоит 10,68 евро в месяц — тогда ваших средств хватит на еще более продолжительный срок аренды.

Стоимость содержания физического сервера

Конечно, физический сервер приятнее тем, что его можно подержать в руках, — видишь, за что платишь деньги. Однако, как и со всем физическим, мало его купить, его нужно еще и содержать.

В стоимость содержания физического сервера входят следующие составляющие:

- *стоимость программного обеспечения* — арендуя виртуальный сервер, вы автоматически приобретаете и лицензию на право использования того или иного программного обеспечения — например, Microsoft Windows Server. В случае с физическим сервером за «математику» придется доплатить. Впрочем, и при аренде виртуального сервера этот вопрос лучше уточнить — разные платформы считают по-разному: Linux, как правило, бесплатный, а вот в случае с Windows стоимость ПО может не входить в стоимость аренды. Как правило, она входит, но стоимость виртуальной машины с Windows может оказаться выше, чем аналогичной с Linux;
- *зарплата администратору* — в зависимости от обязанностей администратора, графика его работы и вашего региона эта сумма будет составлять от 25 тыс. рублей в месяц;
- *стоимость основного и резервного интернет-канала* — в стоимость виртуального сервера уже входит один выделенный IP-адрес и канал со скоростью от 10 Мбит/с. И будьте уверены — канал резервируемый. Никто не захочет, чтобы серверы клиентов остались без Интернета. Вам же для своего физического сервера придется обеспечить резервный канал самостоятельно;
- *стоимость электричества* — сервер оснащен блоком питания на 900 Вт (при полной нагрузке). Стоимость потребляемой им электроэнергии несложно подсчитать самостоятельно. Сюда же добавьте затраты на кондиционирование помещения, в котором стоит сервер, — ему не должно быть слишком жарко, что особенно актуально для летнего периода;
- *стоимость системы резервного электропитания* — вы же не хотите, чтобы работа вашего предприятия остановилась, если пропадет электричество? А скачки

этого самого электричества очень опасны для «железа», поэтому система резервного питания должна быть, пусть самая простенькая — хотя бы для защиты от перепадов напряжения.

С последним пунктом могут быть проблемы. Серверные источники бесперебойного питания (ИБП), способные «продержать» сервер несколько часов, пока электропитание не будет восстановлено, стоят дороже, чем сам сервер. Бюджетный вариант — например, APC by Schneider Electric Smart-UPS XL Modular 1500 VA 230 V Rackmount Tower, обеспечивающий всего 28 минут работы при половинной нагрузке, обойдется вам от 1100 евро. Полноценное серверное решение вроде APC by Schneider Electric Smart-UPS SRT 8000 VA RM 230 V стоит уже от 3200 евро.

Если позволяют условия — например, у вас собственное здание, можно попробовать установить дизель-генераторы — это дешевле. Но в офисном центре ваши соседи вряд ли это оценят — шум и запах никто не отменял. Про пожарные нормы мы вообще упоминать не станем.

Выход один — колокация (colocation), т. е. размещение собственного сервера в дата-центре (ДЦ). Выглядит эта услуга так: вы покупаете физический сервер и передаете его в дата-центр, где обеспечиваются все условия для его бесперебойной работы: есть резервный интернет-канал, система резервного питания, система кондиционирования. Стоимость размещения сервера в дата-центре Hetzner (Германия) выше, чем стоимость аренды виртуального сервера. Самый дешевый вариант размещения обойдется в 120 евро в месяц. За эти деньги вы можете арендовать виртуальный сервер целых полгода!

С другой стороны, в отечественных дата-центрах (а вы наверняка будете размещать сервер «дома» — никто не станет отправлять свой сервер в другую страну) размещение обойдется гораздо дешевле. Так, в дата-центре Xelent[1] (Москва и Санкт-Петербург) размещение сервера стоит 3500 рублей в месяц.

Итак, если разместить свой физический сервер в ДЦ, то у вас станет гораздо меньше головной боли и из всех расходов останется стоимость колокации, стоимость ПО (если нужно) и зарплата администратору. Конечно, спустя два года добавится и стоимость технического обслуживания. Гарантия на узлы сервера составляет как раз два года, а в составе сервера есть много механических частей, которые могут выйти из строя: вентиляторы, жесткие диски и т. д. В случае с виртуальным сервером вам об этом заботиться не придется, впрочем, об этом мы еще поговорим.

И в результате, если не учитывать плату за программное обеспечение (ведь можно использовать бесплатное ПО), стоимость содержания физического сервера в месяц выглядит так:

- 3500 рублей — услуги колокации;
- 25 000–30 000 рублей — минимальная зарплата администратора (конечно, эту сумму можно не платить, если «сам себе администратор»).

---

[1] См. **https://www.xelent.ru/services/colocation/**.

Выбор облачного провайдера

Очень важно не допустить ошибку при выборе облачного провайдера. Такие ошибки могут очень дорого обойтись предприятию — потраченными нервами, деньгами, но еще хуже, если ненадежный Центр обработки данных (ЦОД) потеряет данные. В этом случае предприятие может ожидать настоящее финансовое фиаско. Сейчас мы рассмотрим список факторов, на которые нужно обратить внимание при выборе облачного провайдера.

Прежде всего следует учесть три основных момента: площадка, собственно сама услуга «облака» и поддержка.

Площадка

Самое важное — это ЦОД, где будут физически храниться ваши данные. Если вы недосмотрите и окажется, что некоторые услуги (например, лицензия на операционную систему) платные, ничего страшного. Гораздо хуже, если вы выберете провайдера с ненадежным ЦОД.

Итак, нужно проверить:

- сертифицирован ли ЦОД, какой уровень (Tier) надежности ему присвоен?
- где расположен ЦОД: в России или за границей?
- кому принадлежит ЦОД? Можно ли посмотреть, как все устроено?
- случались ли ранее на этой площадке аварии?

Теперь рассмотрим все эти вопросы подробнее.

Сертификация ЦОД

Сертификация ЦОД по UTI[1] — это не просто бумажка. В процессе сертификации ЦОДу присваивается определенный уровень надежности. Дополнительную информацию об уровнях надежности (Tier) можно найти в Интернете, но, в общем, картина выглядит так:

- Tier I — самый простой уровень, предполагается отсутствие (!) систем резервирования электропитания и охлаждения машинного зала, отсутствие резервирования серверных систем. Уровень доступности — 99,671%, что означает примерно 28,8 часа простоев ежегодно. Учитывая отсутствие резервирования электропитания, это все равно, что разместить серверы у себя в офисе.

  Мы бы не стали выбирать ЦОД с Tier I — некоторые провайдеры указывают, что имеют сертификат по UTI, но не показывают уровень (пока вы их об этом не просите), — оно и понятно, гордиться особо нечем;

[1] Uptime Institute (UTI) — независимый поставщик консалтинговых услуг, сертификации и обучения в области центров обработки данных (ЦОД).

- Tier II — основан на Tier I, но предполагает резервирование всех активных систем. Это уже что-то, но все же 22 часа простоя (99,75% доступности) в год вам гарантированы;
- Tier III — вот это то, что нужно. ЦОД 3-го уровня считаются работающими непрерывно. Резервируются все инженерные системы, обеспечиваются возможности ремонта и модернизации без остановки сервисов. Tier III предполагает постройку второго ЦОД внутри того же здания — ведь все нужно дублировать, в том числе структурированные кабельные системы (СКС), электричество, системы охлаждения, у всего серверного оборудования должны быть независимые подключения к нескольким источникам питания и т. д. Допускается не более 1,6 часа простоя в год (99,98% доступности);
- Tier IV — дальнейшее развитие Tier III. Предполагает сохранение уровня отказоустойчивости даже при аварии. Гарантирует непрерывность работы при любых умышленных поломках, допуская простой не более 0,8 часа ежегодно (99,99%).

  Сами понимаете, что это будет самый дорогой вариант, мы бы даже сказали — мегадорогой. Многие ограничиваются Tier III, чего нужно придерживаться и нам, если не хочется переплачивать.

> ***Примечание***
>
> Можно ли доверять сертификации UTI? Однозначно да. Сертификация начинается еще на этапе проектирования, и сертификации подлежат даже чертежи будущего ЦОД. После постройки и запуска ЦОД производится его выездная проверка специалистами UTI, чтобы понять, насколько результат соответствует чертежам. Методика оценки у UTI собственная и включает проверку всех подсистем ЦОД. Выездная проверка обходится дорого, т. к. кроме стоимости самой проверки нужно оплачивать перелет и проживание команды экспертов.

Итак, можно смело выбирать ЦОД с Tier III как оптимальное решение по цене и надежности. А что касается 1,6 часа простоя в год, то это не так много, да и их может не быть вовсе.

> ***Внимание!***
>
> Категорически не рекомендуется связываться с ЦОД, сертифицированным по Tier I или вовсе без сертификата!

Где расположен ЦОД: в России или за границей?

Физическое расположение ЦОД очень важно, поскольку нужно учитывать два момента: ping до ЦОД и всеми любимый ФЗ № 152. С пингом все понятно — если ваш сервер программы «1С:Предприятие» будет расположен на каких-то там островах, то вряд ли подключение к нему можно будет назвать быстрым, бухгалтерия начнет жаловаться, и придется искать другого провайдера, заморачиваться с переносом и пр. Но все это не так страшно, как нарушение ФЗ № 152, в котором говорится, что персональные данные нельзя выносить за пределы РФ. Если вы не собираетесь в «облаке» хранить и обрабатывать персональные данные — пожалуйста, покупайте виртуальные серверы, где вам угодно, — хоть в Японии. Но если вы об-

рабатываете персональные данные, будьте добры, храните их на серверах, которые находятся только в России.

Кому принадлежит ЦОД? Можно ли войти и посмотреть, как все устроено?

ЦОД может принадлежать или самому облачному провайдеру, или же провайдер может арендовать площадку у ее собственника. В арендованной площадке нет ничего плохого — главное, чтобы вас все устраивало, в том числе и цены (ведь за аренду нужно платить, следовательно, цена услуг провайдера-посредника может быть выше, чем у компании, которая является собственником ЦОД). С другой стороны, некоторые компании просто предоставляют ЦОД в аренду, но не предоставляют самих облачных услуг, т. е. купить «облако» по цене собственника не получится вообще.

Если площадка открыта для экскурсий, то провайдеру скрывать нечего и с площадкой все в порядке. Если же экскурсия невозможна, то это может означать, что или с площадкой что-то не так, или экскурсии запрещены из соображений безопасности.

С другой стороны, ЦОД может находиться довольно далеко, а экскурсии могут быть групповыми, а не индивидуальными (согласитесь, что индивидуальные экскурсии — дело весьма хлопотное). Поэтому ждать придется, пока не наберется группа желающих, а она может и не набраться вовсе. Но если экскурсии в принципе возможны, то это уже хорошо.

Облачная платформа

Здесь важно убедиться, что вы получите то, что хотите получить, т. е. чтобы действительность полностью соответствовала вашим ожиданиям. Как минимум нужно уточнить следующие моменты:

- как можно подключиться к «облаку»? Есть ли панель управления;
- что представляет собой виртуальное ядро;
- какие используются дисковые ресурсы? Соответствует ли скорость ресурсов заявленной;
- есть ли сервис резервного копирования;
- какова пропускная способность интернет-соединения и сколько будет стоить ее расширение;
- входит ли в стоимость услуги лицензия на программное обеспечение;
- как выполняется тарификация;
- есть ли тестовый режим;
- сколько стоит собственная VPN-сеть и какие имеются ограничения;
- наличие каких-либо скрытых платежей — например, за панель управления сервером и т. п.?

Цель такой проверки заключается в том, чтобы узнать точную стоимость вашей виртуальной инфраструктуры в месяц.

Как можно подключиться к «облаку»? Есть ли панель управления?

Как правило, провайдеры предоставляют целые панели управления всей виртуальной инфраструктурой, с помощью которых можно в реальном времени создавать и удалять серверы (виртуальные машины), изменять их конфигурацию и т. д. Но есть и исключения, когда необходимые вам объекты создаются по вашему запросу специалистами технической поддержки или же предоставляется командная строка, команды которой еще предстоит изучить...

Не помешает и наличие веб-консоли для каждого сервера, отображающей все, что с ним происходит, — с самого момента загрузки. Наличие такой консоли — огромное преимущество. Если что-то пойдет не так и «благодаря» неправильной настройке сети виртуальная машина потеряет связь с Интернетом, то обычным способом вы не сможете к ней подключиться. Тогда на помощь придет как раз веб-консоль. В противном случае (если ее нет) придется обращаться в службу поддержки провайдера, и вполне вероятно, что за исправление своих «ко́сяков» (ведь это не ошибка провайдера) вам придется платить какие-то деньги.

Также уточните, как именно осуществляется управление самими виртуальными серверами. Для Linux, как правило, это вход по ssh, а для Windows — по RDP.

Что представляет собой виртуальное ядро?

Вот тут начинается самое интересное. Вы запускаете конфигуратор «облака» и пытаетесь определить стоимость сервера. И у вас там есть ползунок, позволяющий выбрать количество ядер процессора виртуальной машины. Но что представляет собой виртуальное ядро?

Облачные провайдеры измеряют процессорную мощность своих серверов в *виртуальных ядрах* (vCPU). Одно vCPU может равняться одному физическому ядру процессора, а может быть и четвертью такого ядра. Этот вопрос нужно уточнить заранее. Покупая виртуальную машину с процессором на четыре ядра, получите ли вы четыре процессорных ядра или всего одно ядро — если одно виртуальное ядро vCPU = 0,25 процессорного?

Какие используются дисковые ресурсы? Соответствует ли скорость ресурсов заявленной?

Очень часто провайдеры завлекают дешевыми предложениями то ли SSD-«облака», то ли SSD-хостинга. Нас интересует SSD-«облако» — т. е. предполагается, что на арендуемой вами виртуальной машине будет установлен твердотельный диск (SSD). В реальном мире (когда используется реальный сервер) скорость записи на самый бюджетный SSD-диск примерно равна 250 Мбайт/с. От этого и нужно отталкиваться. Если у вас Linux-сервер, то измерить производительность диска можно стандартной командой `dd`, а если сервер под управлением Windows, то можно использовать CrystalDiskMark.

В нашей практике нам не раз встречались провайдеры, заявляющие, что у них используются SSD-диски, а на самом деле в результате замеров реально были получены показатели на уровне 110 Мбайт/с, что равно скорости обычного жесткого диска на 5400 оборотов... Кстати, в технической поддержке провайдера нам потом доказывали, что это нормально... Может, у них и на самом деле используются SSD-диски, но конечному пользователю важен не тип накопителя, а реальная скорость его работы.

Есть ли сервис резервного копирования?

Уточните, есть ли сервис резервного копирования или резервирование данных придется осуществлять своими силами, т. е. докупать еще один виртуальный накопитель, устанавливать и настраивать программное обеспечение для бэкапа и пр. Если сервис есть, то нужно уточнить, сколько он стоит, чтобы вы могли планировать свои месячные затраты на содержание виртуальной инфраструктуры.

Какова пропускная способность интернет-соединения и сколько будет стоить ее расширение?

По умолчанию провайдеры предоставляют не очень широкий канал — например, 10 Мбит/с. Для кого-то этого достаточно, для кого-то — нет. Уточните, во сколько обойдется расширение пропускной способности.

Также узнайте, придется ли вам доплачивать за постоянный IP-адрес и трафик. У некоторых провайдеров низкие цены на виртуальные машины, но зато они компенсируют это счетами за использование выделенного IP-адреса и за каждый гигабайт принятого/переданного трафика.

Входит ли в стоимость услуги лицензия на программное обеспечение?

Арендуя сервер под управлением Windows, нужно учитывать, входит ли в стоимость аренды лицензия на саму операционную систему? Также невредно уточнить, во сколько обойдутся дополнительные терминальные лицензии.

В случае с Linux-сервером следует узнать, предоставляется ли какая-либо панель управления самим сервером. Впрочем, если нет, то всегда можно «прикрутить» бесплатные VestaCP или Webmin.

Как выполняется тарификация?

Тарификация — это тема для отдельного разговора. Первое, что надо бы уточнить, — это единицу тарификации: минута, час, день и т. д. Что произойдет, если вы выключите сервер на некоторое время? Будет ли такой простой бесплатным, или только лишь за хранение информации все равно придется платить?

Что будет, если вы измените конфигурацию сервера в меньшую сторону? Как и когда это отразится на стоимости его аренды? Допустим, вы заказали сервер с 16 Гбайт оперативной памяти, а спустя некоторое время решили, что 16 Гбайт — это много и будет достаточно 12. И например, в 11:00 вы уменьшаете размер опера-

тивной памяти. Когда это отразится на тарификации? Моментально, через час или в начале следующего дня?

Есть ли тестовый режим?

Тестовый, или деморежим — самый хороший способ протестировать, подходит ли вам рассматриваемая площадка или нет. Узнайте у провайдера, есть ли тестовый режим и как им можно воспользоваться.

Сколько стоит собственная VPN-сеть и какие есть ограничения?

Обычно виртуальная частная сеть создается бесплатно, но есть и случаи, когда сама операция создания VPN стоит каких-то денег. К тому же нужно уточнить, сколько серверов могут входить в состав сети и какова скорость обмена данными внутри нее.

Есть ли какие-либо скрытые платежи — например, за панель управления сервером и т. п.?

Полагаем, особых комментариев этот вопрос не требует. Постарайтесь по максимуму вычислить, сколько будет стоить содержание виртуальной инфраструктуры в месяц, чтобы в конце месяца это не стало для вас неприятным сюрпризом — когда серверы отключат из-за недостатка на балансе средств, которые израсходовались раньше запланированного срока.

Поддержка

Здесь нас интересуют следующие вопросы:

- доступна ли поддержка в режиме 24/7 (т. е. круглосуточно), или она работает только в рабочее время;
- каким языком владеет служба поддержки (хорошо бы русским);
- нужно ли обращаться в поддержку за мониторингом ресурсов и баланса, или же все интересующие вас данные будут доступны через панель управления услугой?

Эти вопросы тоже в комментариях особо не нуждаются. Надеемся, приведенная информация поможет выбрать лучшего облачного провайдера и избежать лишних расходов.

Виртуализация физического сервера

Сегодня все чаще и чаще физические серверы переносят в «облако». Более того, виртуализируют не только серверы, но и всю инфраструктуру сети.

Собственно, перенос сервера с «железа» в «облако» — технически не очень сложная задача. Просто до начала самого переноса надо четко понимать, зачем это все нужно.

- Во-первых, «железо» облачной платформы гораздо надежнее, чем «железо» любого отдельно взятого сервера. Особенно это актуально для владельцев старых серверов (старше 5 лет) — в любой момент может произойти непоправимое, например выход из строя жесткого диска или, что еще хуже, выход из строя материнской платы. Даже если у вас настроено резервное копирование и сами данные вы не потеряете, вы точно получите многочасовой простой сервера — пока нужное «железо» не будет заказано, куплено, оплачено и установлено.

  На больших предприятиях, даже частных, порой имеется несколько слоев бюрократии, с которой сталкивается любой администратор, — нельзя просто пойти и купить замену вышедшему из строя устройству. Нужно сначала получить счет, объяснить, за что он, доказать, что цена оптимальная, а уже потом, после оплаты (а банковский перевод, как все мы знаем, может затянуться до трех дней), ехать и получать необходимую «железку». Поэтому изначально виртуализацию можно рассматривать как страховку от всех неприятностей, связанных с выходом из строя оборудования. У облачной платформы оборудование тоже не вечное, но за него отвечает сама платформа, а учитывая наличие у них запасных частей, в большинстве случаев вы даже не заметите, что что-то ломалось.

- Во-вторых, переезд в «облако» — лучший (и самый дешевый) способ обеспечить бесперебойную работу сервера, если необходима его доступность в режиме 24/7. Вашему предприятию не придется покупать дорогостоящие ИБП (стоимость которых превышает стоимость сервера), организовывать (и оплачивать) резервный интернет-канал и т. п.

- В-третьих, управлять облачным сервером просто удобнее: можно настроить резервное копирование сразу всего сервера, можно сделать мгновенный снимок (snapshot) сервера перед внесением изменений в конфигурацию или установкой нового ПО, можно выполнить клонирование сервера и т. д.

Виртуализация выводит администрирование сервера на совершенно другой уровень, а в качестве приятного бонуса вы получаете страховку от всех неприятностей, которые могут произойти с вашим сервером.

Представим, что у нас есть сервер терминалов (Windows Server 2012/2019), на котором работает СУБД и к которому подключаются не только бухгалтеры из главного офиса, но и бухгалтеры филиалов — база данных-то общая.

И для обеспечения отказоустойчивости сервера было принято решение о переносе его в «облако». Как уже отмечалось, сама процедура переноса относительно простая.

Прежде всего нужно сделать образ нашего физического сервера. В Microsoft уже давно позаботились о нас и разработали бесплатную утилиту Disk2vhd, позволяющую создать VHD-образ нашего сервера для его размещения в «облаке». Утилиту эту можно бесплатно скачать по адресу: **https://docs.microsoft.com/ru-ru/sysinternals/downloads/disk2vhd**.

Запустите утилиту. В ее открывшемся окне (рис. 8.10) нам нужно выбрать тома, которые будут включены в VHD-файл. По умолчанию Disk2vhd попытается создать VHD-файл в домашней папке пользователя (на диске C:\), но, учитывая, что, как

можно видеть, на нем осталось только 13,8 Гбайт свободного места, было принято решение создавать VHD-файл на отдельном, неиспользуемом томе, где дискового пространства достаточно, — это том E:\ (он и не включен в состав VHD-файла).

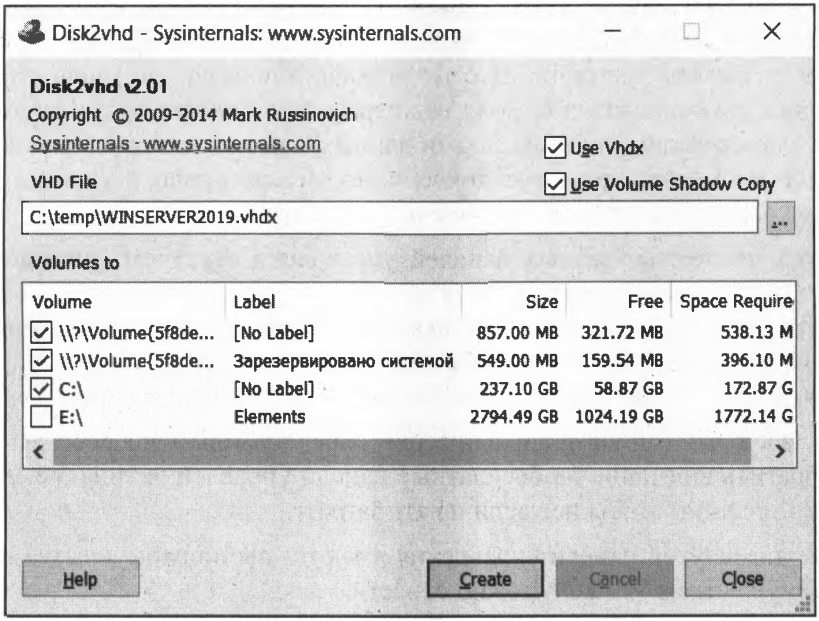


Рис. 8.10. Утилита Disk2vhd

Далее осталось нажать кнопку **Create** и дождаться завершения процесса. Процесс создания VHD-файла не очень быстрый (особенно при использовании не SSD-дисков), поэтому можно отлучиться и выпить не одну чашечку кофе.

Затем нужно любым удобным способом передать полученный файл образа в службу поддержки облачного провайдера. Например, загрузить файл в облачный сервис вроде Mega (ограничение 50 Гбайт) или разместить его на FTP-сервере и сообщить службе поддержки сервиса параметры доступа.

Получив VHD-образ нашего сервера, служба поддержки создаст на его базе виртуальный сервер. Вам ничего не придется делать (и заметьте — все это совершенно бесплатно). По завершении создания наш сервер появится в панели управления.

Теперь нужно его настроить. Сам процесс настройки виртуального сервера мы здесь рассматривать не станем, поскольку он зависит от конфигурации сервера и в каждом конкретном случае будет иным. В нашем самом простейшем случае (сервер терминалов без ActiveDirectory) процесс настройки виртуального сервера весьма несложен: нужно просто изменить на RDP-клиентах его IP-адрес — ведь у облачного сервера он будет другим (его вы увидите в панели управления сервером). Возможно, придется сменить настройки сети, но если ваш сервер не был интернет-шлюзом, а свои сетевые параметры получал по DHCP, то кроме изменения IP-адреса сервера на RDP-клиентах делать больше ничего не придется.

Установка панели управления на виртуальный Linux-сервер

Панель управления виртуальным сервером, предоставляемая провайдером, позволяет управлять «железом» сервера: включать/выключать сервер, просматривать его состояние, создавать снапшоты. Все это хорошо и полезно, но многим пользователям хотелось бы большего контроля над сервером — например, управлять пользователями, веб-сервером, почтой, базами данных, заданиями cron. При наличии ssh-доступа все это можно сделать из консоли, но гораздо проще и удобнее выполнять управление сервером посредством панели управления.

Существует множество разных панелей управления сервером (их еще называют *веб-интерфейсом администрирования сервером*). Часть из них платные, например: cPanel, ISPmanager, DirectAdmin, Parallels Plesk Panel. Такие панели стоит покупать в тех ситуациях, когда вы сами являетесь хостинг-провайдером и планируете предоставлять место на своих физических серверах другим пользователям.

Если же у вас обычный виртуальный сервер, арендованный для собственных нужд, можно обратить внимание на бесплатные панели управления типа VestaCP, Cloxo, Webmin и ISPconfig, чтобы не увеличивать затраты.

У каждой упомянутой панели управления имеются свои преимущества и недостатки. К преимуществам VestaCP можно отнести:

- готовность к работе сразу после установки — вам ничего не придется в ней донастраивать. Все готово к использованию сразу же, а дальнейшую настройку сервера можно продолжить уже через панель управления;
- простой и красивый интерфейс пользователя. Людей встречают по одежке, а программные продукты — по интерфейсу. Если есть выбор, то конечный пользователь выберет программный продукт с интерфейсом, который ему покажется более симпатичным;
- открытый исходный код — это позволяет независимым экспертам убедиться в отсутствии в продукте всякого рода уязвимостей;
- свободное бесплатное распространение — нет никаких условий или каких-либо ограничений (если не считать поддержки, но об этом — позже). Вы можете удалить панель в любой момент, если она вам не понравилась, и установить другую. В случае с платным ПО пришлось бы решать еще один неприятный вопрос — возврат денег, который по условиям договора может быть частичным. Здесь же вы ничем не рискуете: установили, попробовали, если не понравилось — удалили. Но мы уверены, что VestaCP вам понравится.

Конечно, у всего есть недостатки. Так, у VestaCP — платная техподдержка. Впрочем, было бы странно ожидать, что к бесплатной панели прилагается и бесплатная поддержка, — разработчикам ведь нужно на что-то жить... Стоимость техподдержки обходится в 60 долларов в час (можно купить 15 часов за 540 долларов — выйдет по 36 долларов за час), но поскольку все сразу работает «из коробки», в большинстве случаев техподдержка вам не понадобится.

С другой стороны, к некоторым другим бесплатным панелям техподдержка вообще не прилагается, — и если возникнут проблемы, решение придется искать на форумах или рассчитывать на собственные силы.

Второй недостаток VestaCP — отсутствие файлового менеджера по умолчанию. За него просят или 3 доллара в месяц, или 50 долларов единовременно. С другой стороны, всегда можно подключиться по ssh и запустить бесплатный файловый менеджер mc, так что и это особо не проблема.

Установку панели управления нужно производить на «чистый» сервер, на котором еще не было установлено какое-либо программное обеспечение. Преимущество VestaCP в том, что ее инсталлятор сам установит и настроит все необходимое ПО. Наоборот, если что-то уже было установлено, инсталлятор сообщит, что установку нужно производить на «чистый» сервер (рис. 8.11), и прервет процесс установки (чтобы продолжить установку, нужно или удалить пакеты, которые мешают установщику, или запустить процесс с опцией `--force`).

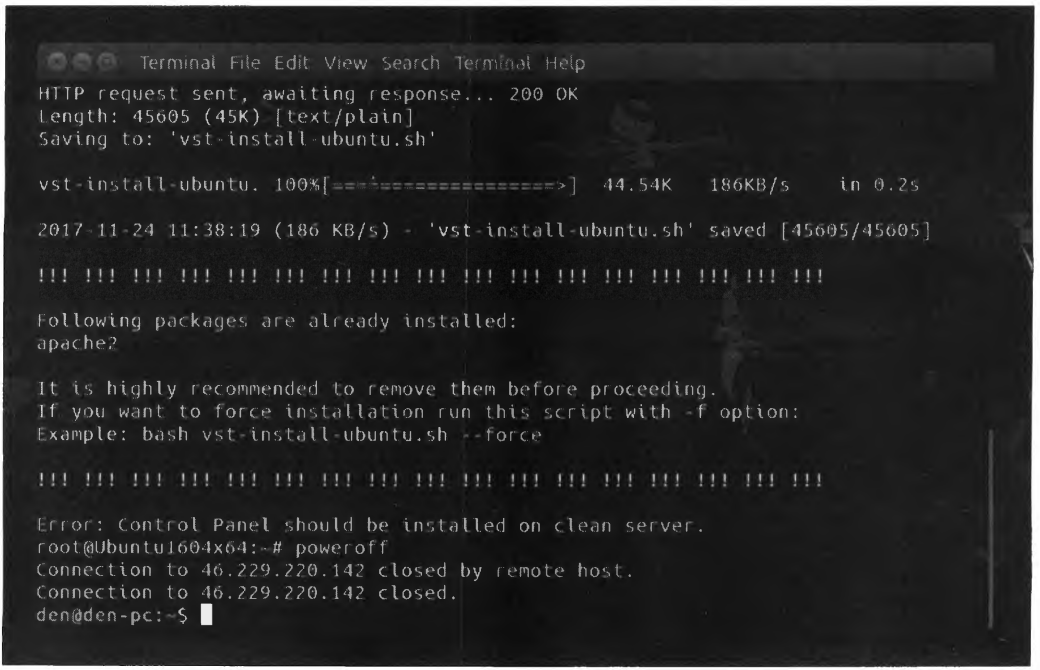


Рис. 8.11. Установку нужно производить на чистый сервер

Итак, начнем установку панели управления. Подключитесь по SSH и загрузите инсталлятор «Весты» (рис. 8.12):

```
wget http://vestacp.com/pub/vst-install.sh
```

Теперь запустите загруженный сценарий инсталлятора. Поскольку инсталлятор будет устанавливать дополнительное ПО, ему нужны права root, поэтому запускайте его или от имени root, или же через команду `sudo`:

```
# bash vst-install.sh
```

Рис. 8.12. Инсталлятор загружен

Далее инсталлятор сообщит, какое программное обеспечение собирается установить, и запросит вашего подтверждения — нужно ответить: y. После этого инсталлятор попросит указать ваш e-mail и доменное имя сервера (рис. 8.13).

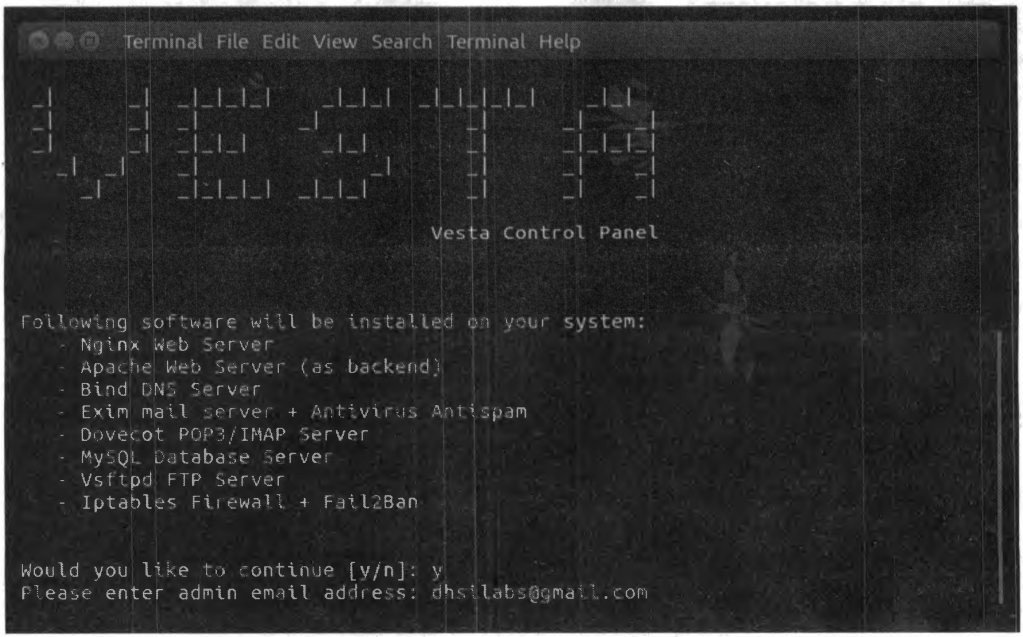


Рис. 8.13. Подтверждение установки

Начнется установка, которая, по мнению инсталлятора, занимает около 15 минут (рис. 8.14). У нас же на виртуальном сервере минимальной конфигурации (2 ядра, 5 Гбайт RAM, 40 Гбайт SAS-диска) установка заняла менее 10 минут.

По окончании установки инсталлятор сообщит, как войти в панель управления сервером (рис. 8.15).

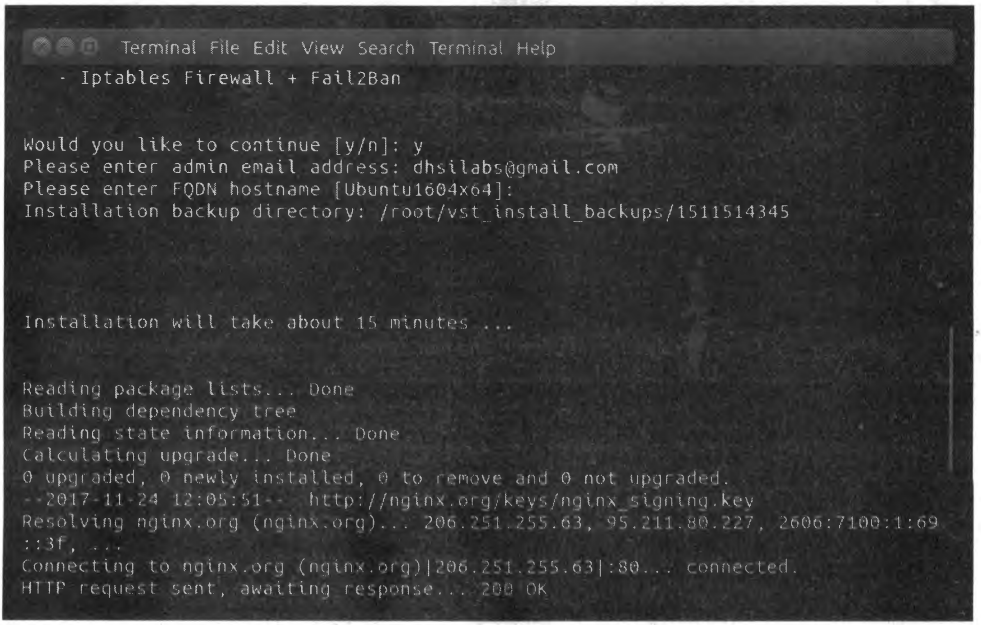


Рис. 8.14. Началась установка

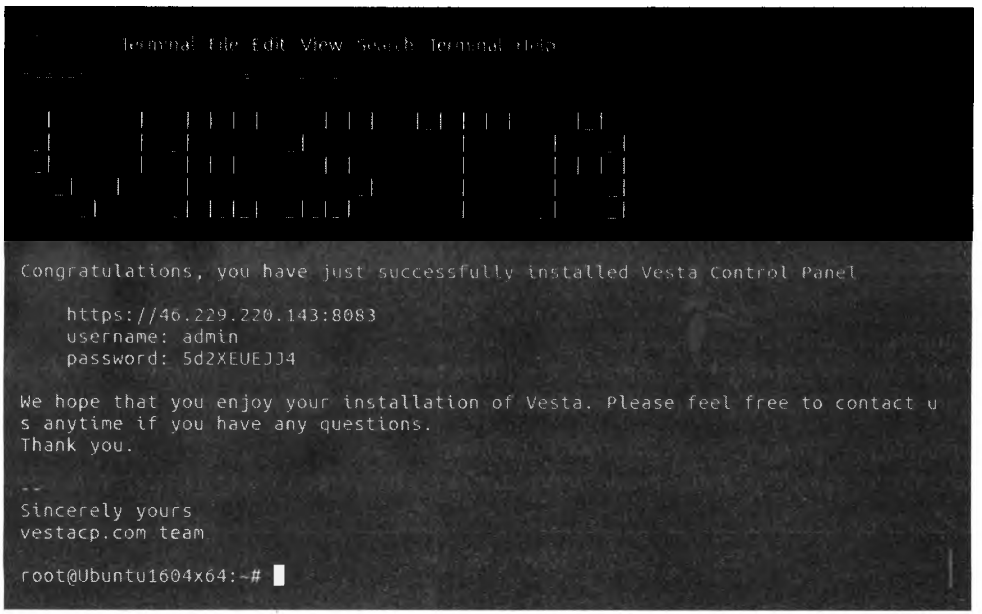


Рис. 8.15. Установка завершена

Что ж, давайте посмотрим, что представляет собой установленная нами панель. Откройте браузер, перейдите по адресу, указанному инсталлятором (**https://имя_сервера:8083**), и на открывшейся странице введите имя пользователя и пароль, предложенные инсталлятором (рис. 8.16).

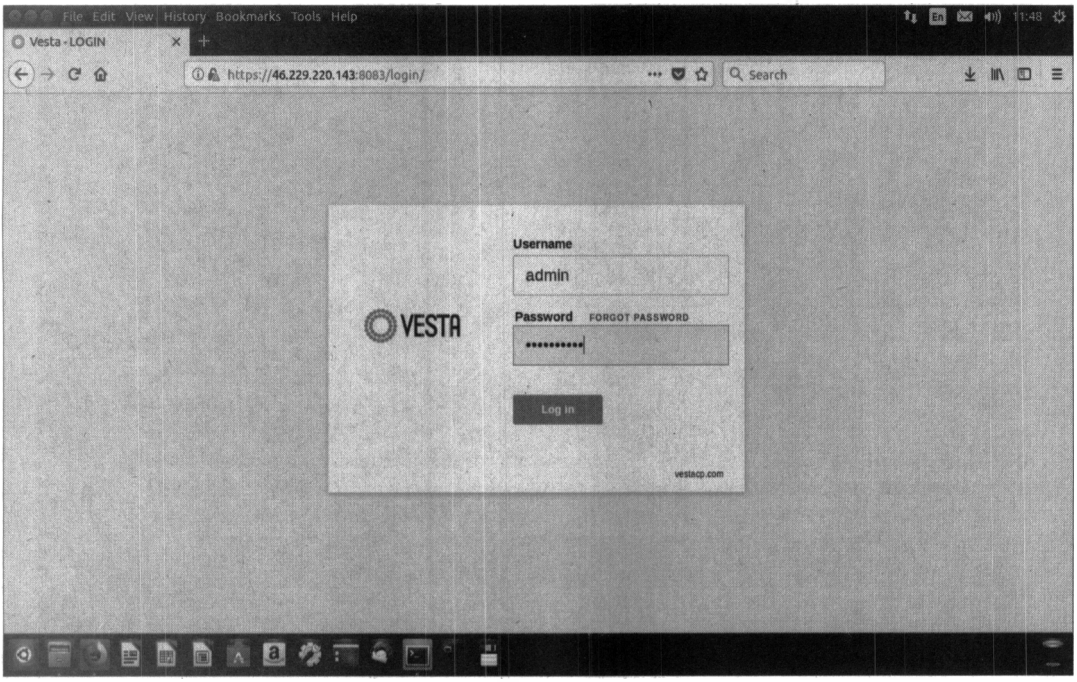


Рис. 8.16. Вход в панель управления

Главная страница панели управления VestaCP показана на рис. 8.17. Все настройки здесь разделены по категориям, которые находятся вверху окна:

- **USER** — управление пользователями;
- **WEB** — настройки доменов и поддоменов;
- **DNS** — настройка служб DNS и серверов имен;
- **MAIL** — настройки почтовых серверов и аккаунтов;
- **DB** — управление базами данных;
- **CRON** — управление расписанием Cron;
- **BACKUP** — резервное копирование системы.

Что делать дальше? Вы можете приступить к администрированию своего сервера. Интерфейс понятен, все предельно просто. Кстати, для русификации интерфейса не нужно предпринимать никаких действий, кроме как выбрать русский язык из меню панели управления (рис. 8.18).

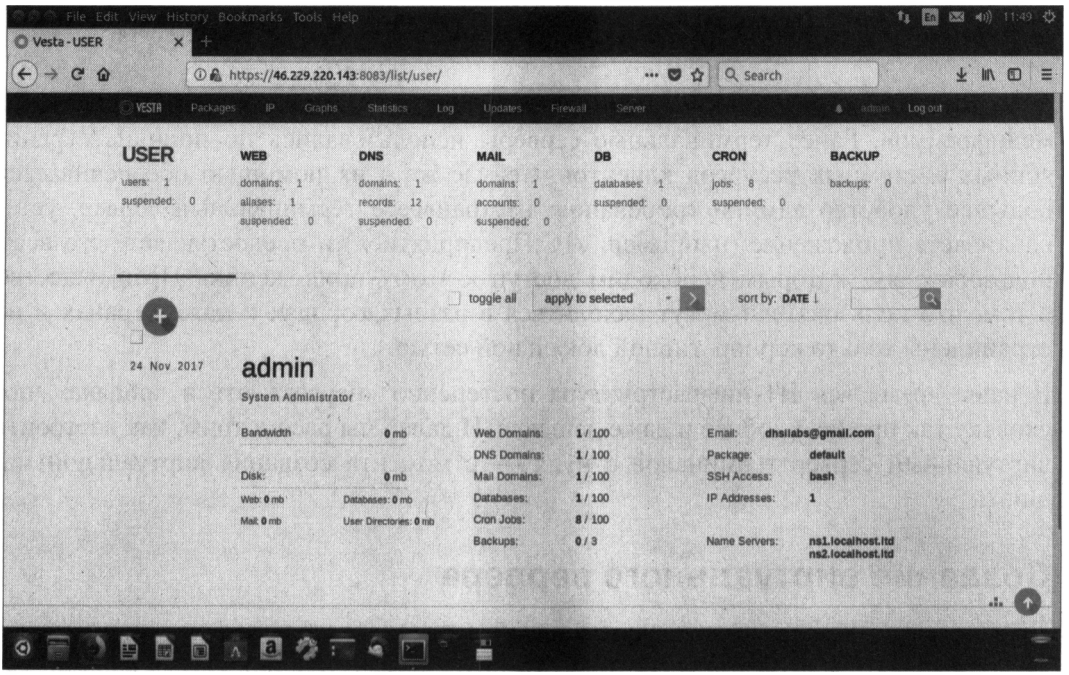


Рис. 8.17. Главная страница панели управления

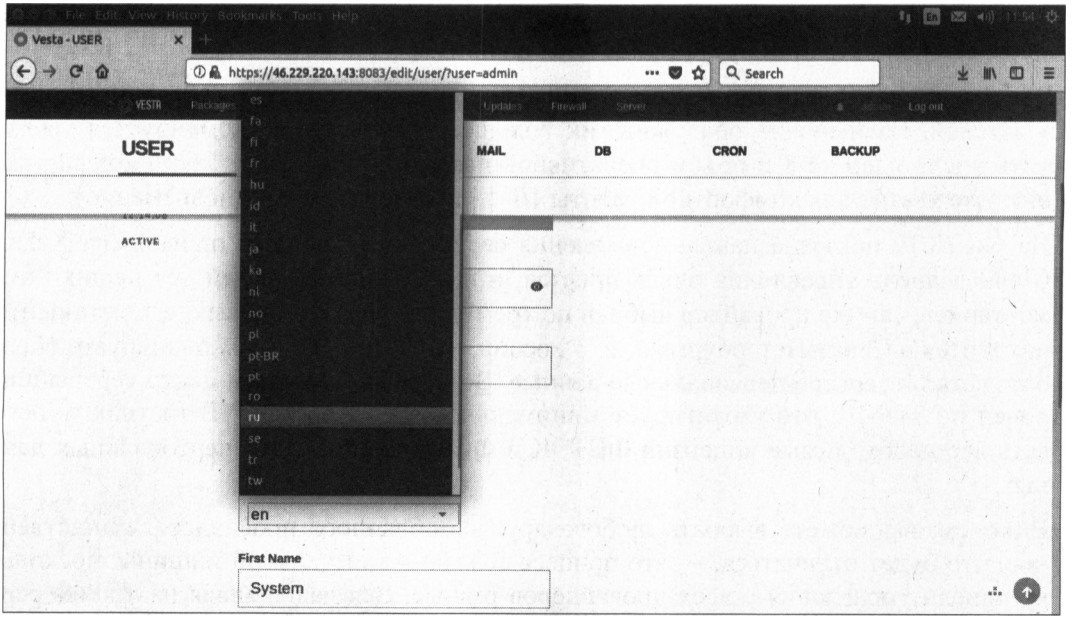


Рис. 8.18. Выбор языка интерфейса

Настройка терминального Windows-сервера

Терминальные серверы — не новинка и существуют еще со времен огромных мейнфреймов. Ранее терминальные серверы использовались по причине ограниченных системных ресурсов клиентов. Сейчас же с их помощью обеспечивается большее удобство администрирования: настраиваете терминальный сервер, устанавливаете приложение (например, «1С:Предприятие») и предоставляете его всем пользователям, которым необходим доступ к этому приложению. Преимущество в том, что пользователи могут находиться в разных городах и даже странах и не ограничены только корпоративной локальной сетью.

В наше время вся ИТ-инфраструктура постепенно «переезжает» в «облака», поскольку так проще, удобнее и даже дешевле. И далее мы рассмотрим, как настроить виртуальный сервер терминалов с нуля — с момента создания виртуальной машины.

Создание виртуального сервера

Прежде всего нужно создать виртуальный сервер. Поскольку нам нужен сервер терминалов, то надо заказать соответствующую конфигурацию. Двумя ядрами уже не обойдешься — как минимум четыре ядра, 12 Гбайт оперативки и SAS-диск на 120 Гбайт. Слишком большой диск заказывать необходимости нет — всегда можно дозаказать больший объем. Операционная система — Windows Server 2012 R2. В принципе, вы можете выбрать любую другую версию (2008 или даже 2022), но далее все иллюстрации будут приведены на примере Windows Server 2012 R2.

Выбранной конфигурации вполне достаточно для одновременной работы пяти пользователей. Если нужно обслужить их большее количество, рекомендуется увеличить число ядер до 8 и объем оперативной памяти до 16 Гбайт. Такой конфигурации уже хватит для комфортной работы 10–15 пользователей (одновременно).

На рис. 8.19 показана панель управления серверами облачного провайдера Xelent Cloud. Панель управления очень простая, и вы разберетесь с ней без наших комментариев, сам же провайдер выбран по трем причинам. Во-первых, его дата-центр находится в Санкт-Петербурге, т. е. в России, что важно, если вы планируете обрабатывать на сервере персональные данные. Во-вторых, этот дата-центр сертифицирован по Tier-III, что гарантирует минимальное время простоя. В-третьих, у него есть все необходимые лицензии ФСТЭК и ФСБ для обработки персональных данных.

Впрочем, вы можете выбрать любого другого облачного провайдера. Единственное, что будет отличаться, — это процесс создания виртуальной машины, поскольку панели управления у всех провайдеров разные. Вся дальнейшая настройка сервера терминалов от описанной в этой главе отличаться не будет.

Итак, наш сервер создан. Кстати, на его создание понадобилось всего 2 минуты и 57 секунд. Интересно, сколько времени займет доставка физического сервера и его первоначальная настройка?

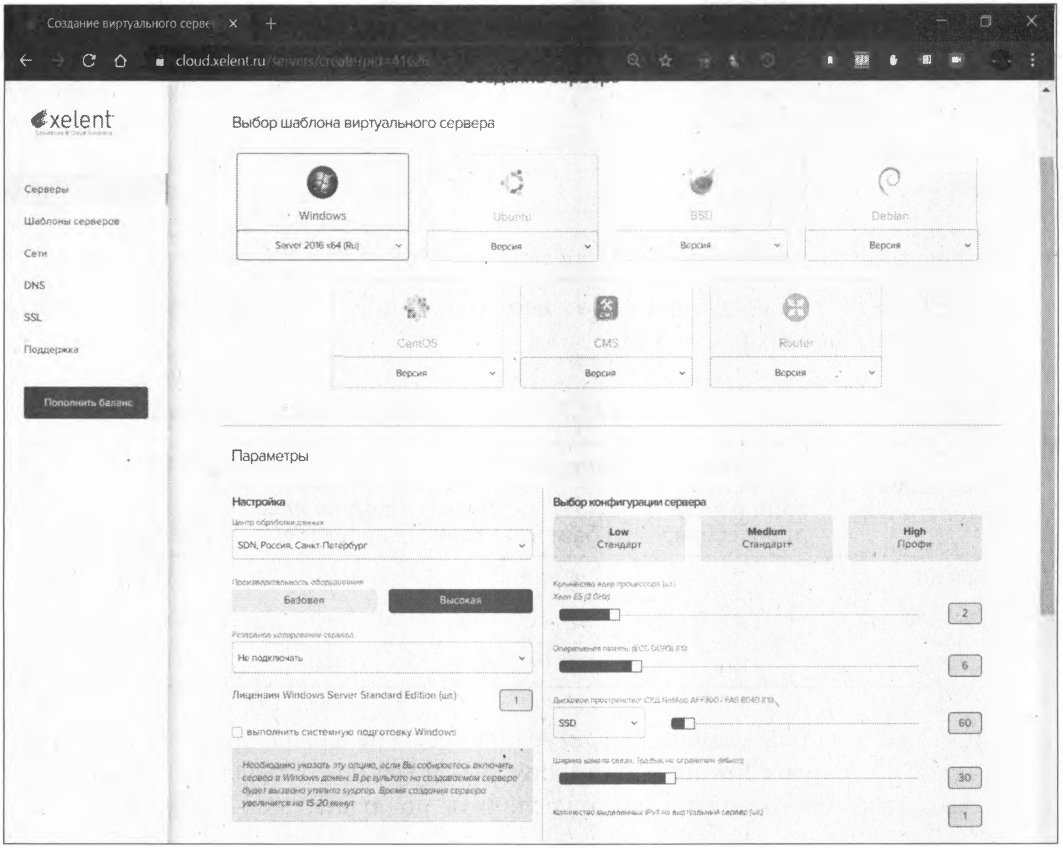


Рис. 8.19. Создаем виртуальный сервер

Подключитесь к серверу, используя данные, предоставленные в панели управления.

Оптимальная конфигурация виртуального сервера для бухгалтерской программы «1С:Предприятие»

Основной фактор, влияющий на конфигурацию нашего будущего виртуального сервера, — это количество пользователей, которым понадобится одновременно обращаться к серверу. Также нужно понимать, какие операции еще будут выполнять пользователи на сервере: или они станут работать только с «1С:Предприятие», или же использовать еще какие-то другие приложения. Понятно, что нужно учитывать нагрузку на сервер от тех приложений тоже.

При большом количестве пользователей (от 50 человек) рекомендуется использовать два сервера: один в качестве сервера СУБД, второй — как сервер «1С:Предприятие». Обратите внимание, что при этом конфигурации этих серверов будут разными.

В табл. 8.4 приводится конфигурация виртуального сервера при условии, что количество пользователей будет небольшим.

Таблица 8.4. Конфигурация виртуального сервера при небольшой нагрузке

Количество пользователей	Кол-во ядер процессора	ОЗУ, Гбайт	Диск, Гбайт
до 10	2	5–6	100
10–25	2	12–14	120
25– 50	4	24	200

При большой нагрузке картина будет несколько иной — появится еще один сервер — для базы данных (табл. 8.5).

Таблица 8.5. Конфигурации серверов при большой нагрузке

Количество пользователей	Сервер «1С:Предприятие»			Сервер БД		
	Кол-во ядер процессора	ОЗУ, Гбайт	Диск, Гбайт	Кол-во ядер процессора	ОЗУ, Гбайт	Диск, Тбайт
50–100	2	24	100	8	16	0,5
100–500	4	32	200	12	60	1
от 500	10	64	500	40	512	3

Помните, что в любой момент конфигурацию сервера можно изменить как в лучшую, так и в худшую (downgrade) сторону. Исключение составляет только накопитель, емкость которого можно только увеличить, но нельзя уменьшить.

Установка службы удаленных рабочих столов

Откройте **Диспетчер серверов**, если вы его закрыли. Для этого запустите его с ярлыка на панели задач или выполните команду `servermanager.exe` — как кому больше нравится.

В меню **Управление** выберите команду **Добавить роли и компоненты** (рис. 8.20) — откроется **Мастер добавления ролей и компонентов** (рис. 8.21).

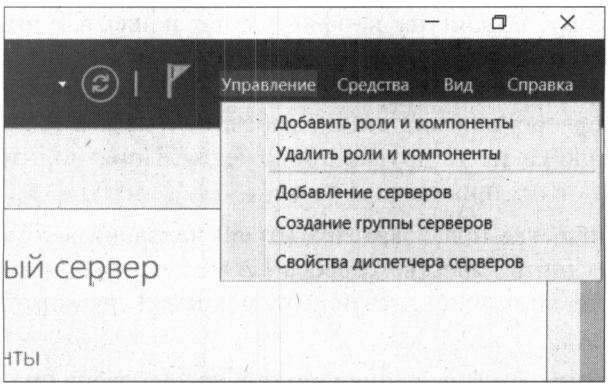


Рис. 8.20. Меню Управление

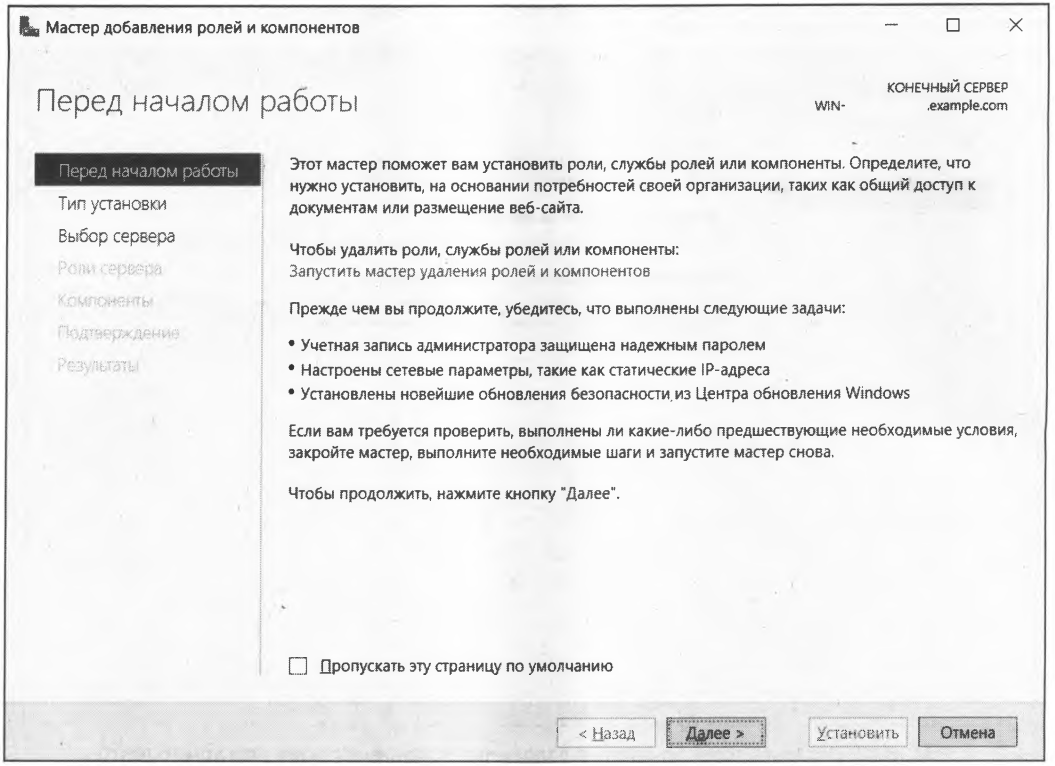


Рис. 8.21. Мастер добавления ролей и компонентов

Далее выполните следующие действия:

1. Нажмите кнопку **Далее**.
2. Оставьте переключатель в положении **Установка ролей или компонентов** (рис. 8.22) и снова нажмите кнопку **Далее**.
3. Выберите из пула сервер, на который нужно установить службу терминалов. В нашем случае там будет один сервер (рис. 8.23). Нажмите кнопку **Далее**.
4. Отметьте роль **Службы удаленных рабочих столов** (рис. 8.24) и нажмите кнопку **Далее**.
5. Компоненты оставьте без изменения, т. е. на следующем экране мастера добавления ролей и компонентов просто нажмите кнопку **Далее**.
6. Мастер отобразит описание роли **Службы удаленных рабочих столов**. Нажмите кнопку **Далее**.
7. В открывшемся окне (рис. 8.25) выберите устанавливаемые **Службы ролей** и выберите из списка **Лицензирование удаленных рабочих столов**. Сразу после выбора этой службы необходимо согласиться на установку дополнительных компонентов, нажав кнопку **Добавить компоненты** (рис. 8.26).
8. Нам понадобится также служба **Узел сеансов удаленных рабочих столов** или **Remote Desktop Session Host**. Как и в предыдущем случае, нужно согласиться на добавление дополнительных компонентов.

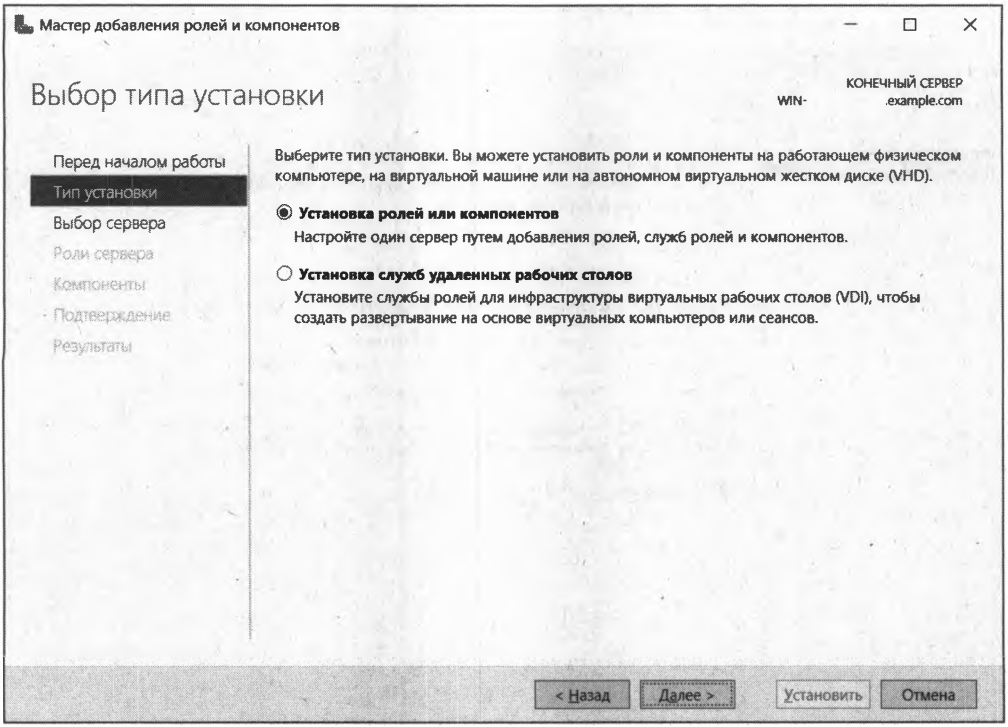


Рис. 8.22. Оставьте переключатель в положении **Установка ролей или компонентов**

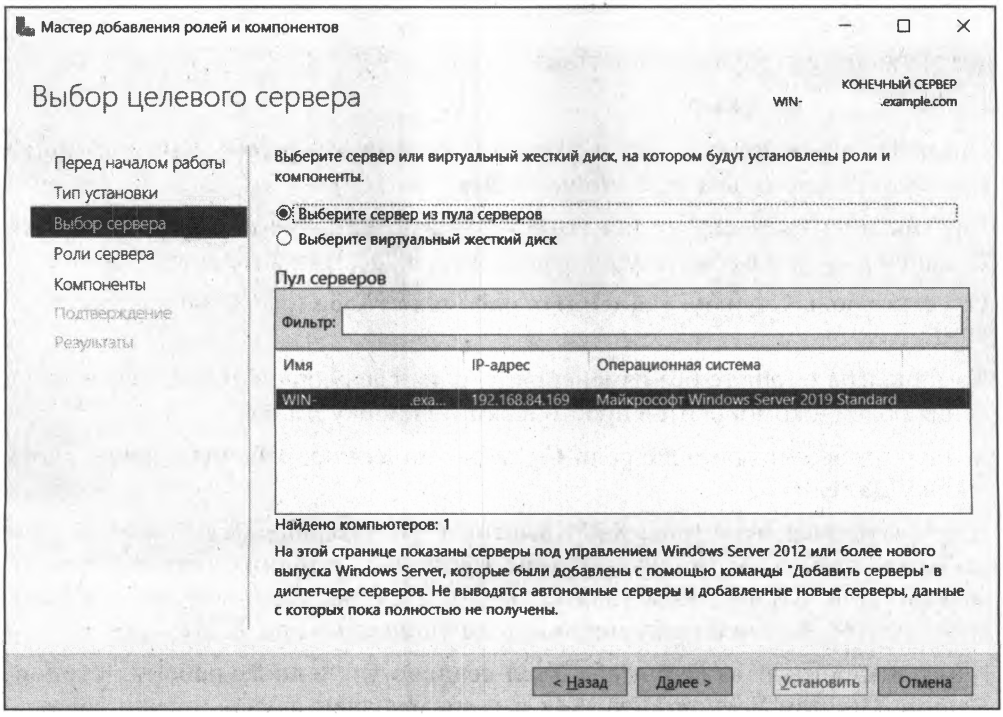


Рис. 8.23. Выберите сервер

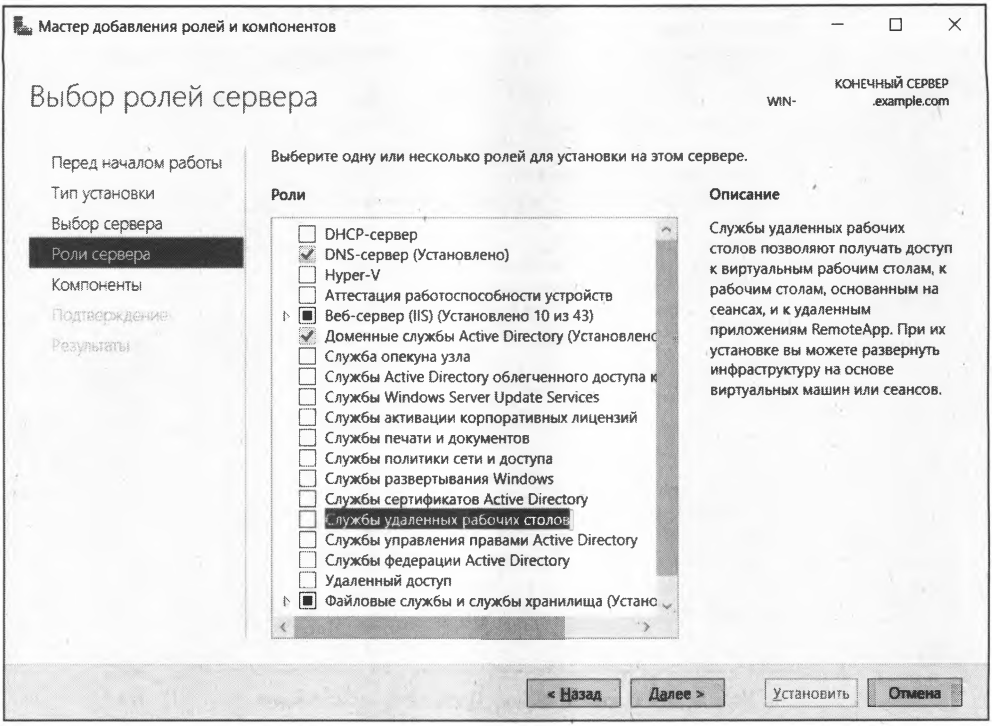


Рис. 8.24. Выберите **Службы удаленных рабочих столов**

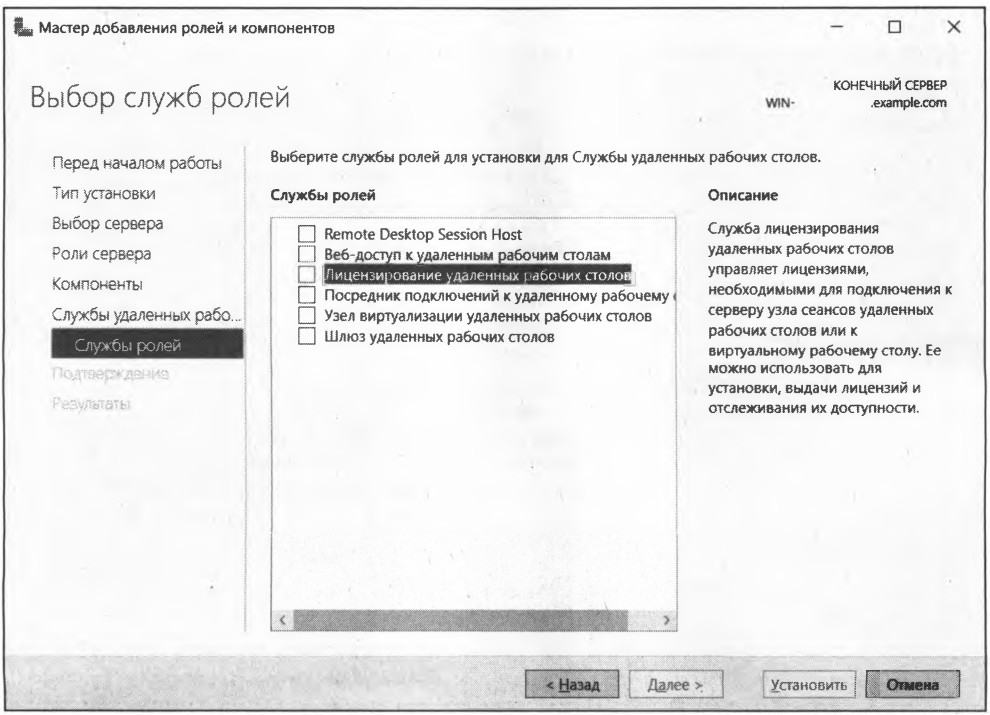


Рис. 8.25. Выберите **Лицензирование удаленных рабочих столов**

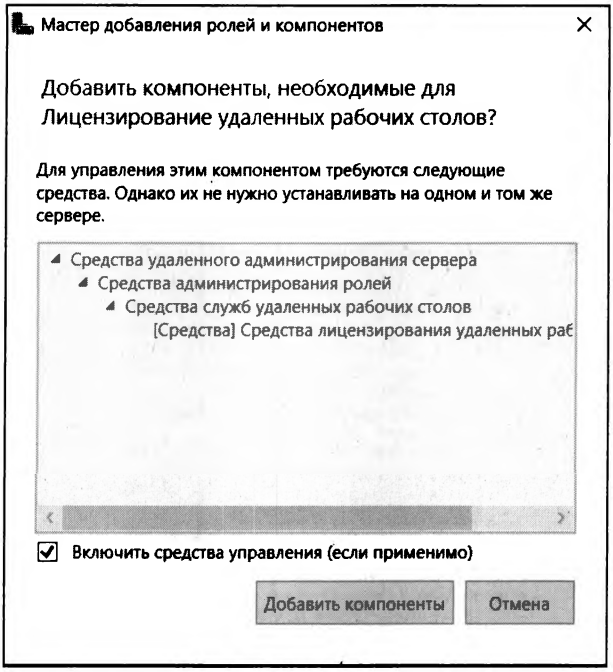


Рис. 8.26. Нажмите кнопку **Добавить компоненты**

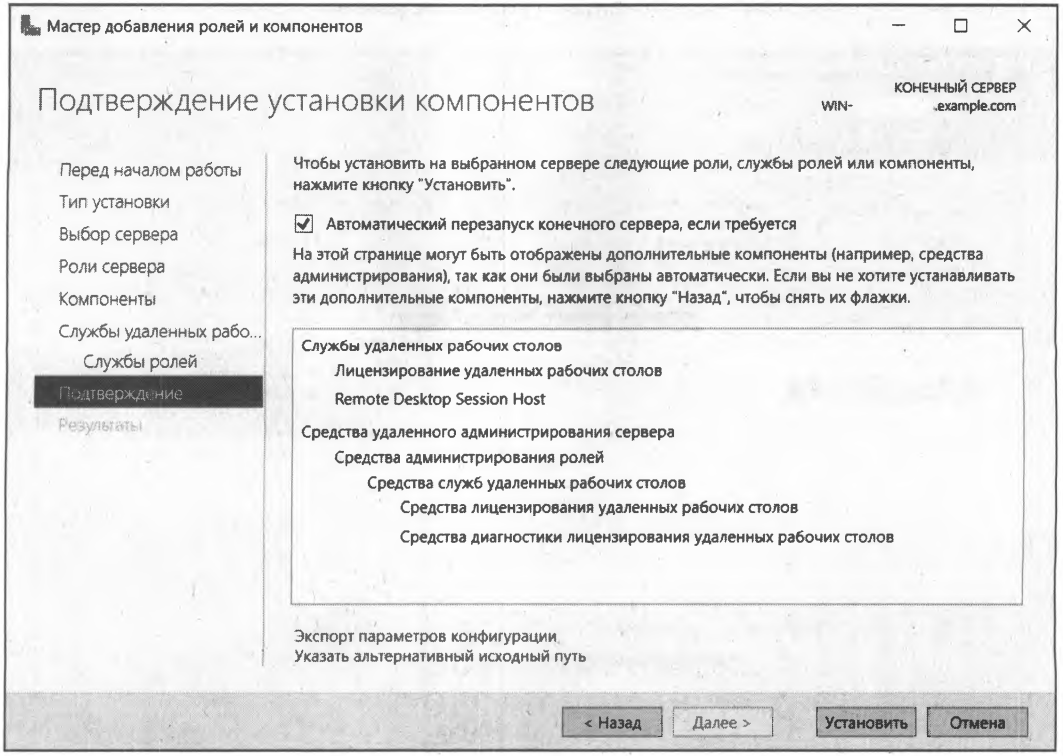


Рис. 8.27. Нажмите кнопку **Установить**

9. Мы определили все параметры установки роли. На последней странице мастера включите параметр **Автоматический перезапуск конечного сервера, если требуется** и нажмите кнопку **Установить** (рис. 8.27).

Осталось дождаться установки ролей. Если все пройдет хорошо, после перезагрузки вы увидите сообщение об успешной установке всех выбранных служб и компонентов. Просто нажмите кнопку **Закрыть** для завершения работы мастера.

Настройка сервера лицензирования для удаленных рабочих столов

После перезапуска сервера вы увидите уведомление, что режим лицензирования удаленного стола не настроен (рис. 8.28). Этим мы сейчас и займемся. Запустите **Средство диагностики лицензирования удаленных рабочих столов**. Для этого выберите соответствующую команду из меню **Средства | Remote Desktop Services** Диспетчера серверов (рис. 8.29).

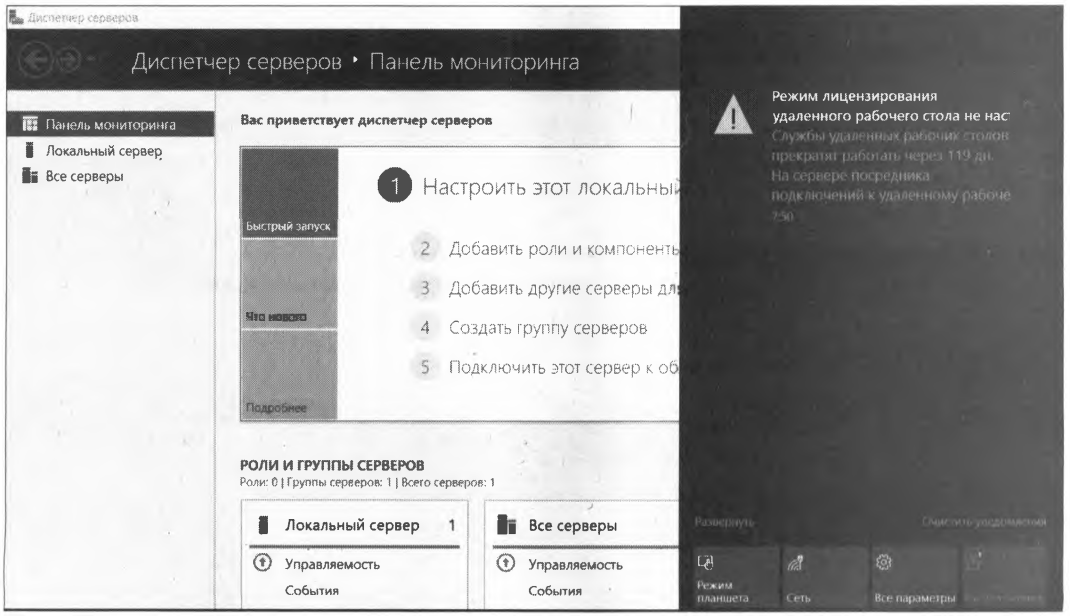


Рис. 8.28. Требуется дополнительная настройка

Средство диагностики оповестит, что доступных лицензий пока нет, поскольку не задан режим лицензирования для сервера узла сеансов удаленных рабочих столов (рис. 8.30). Оно также сообщит, что льготный период (по умолчанию 120 дней) еще не истек, но сам сервер пока не настроен на использование хотя бы одного сервера лицензирования.

Относительно льготного периода нужно знать следующее:

- существует льготный период, в течение которого сервер лицензирования не требуется, однако после его истечения для подключения к серверу клиенты должны

использовать действительную клиентскую лицензию служб удаленных рабочих столов, выданную сервером лицензирования;

- удаленный рабочий стол поддерживает два одновременных подключения для удаленного администрирования компьютера. Для этих подключений сервер лицензирования не требуется.

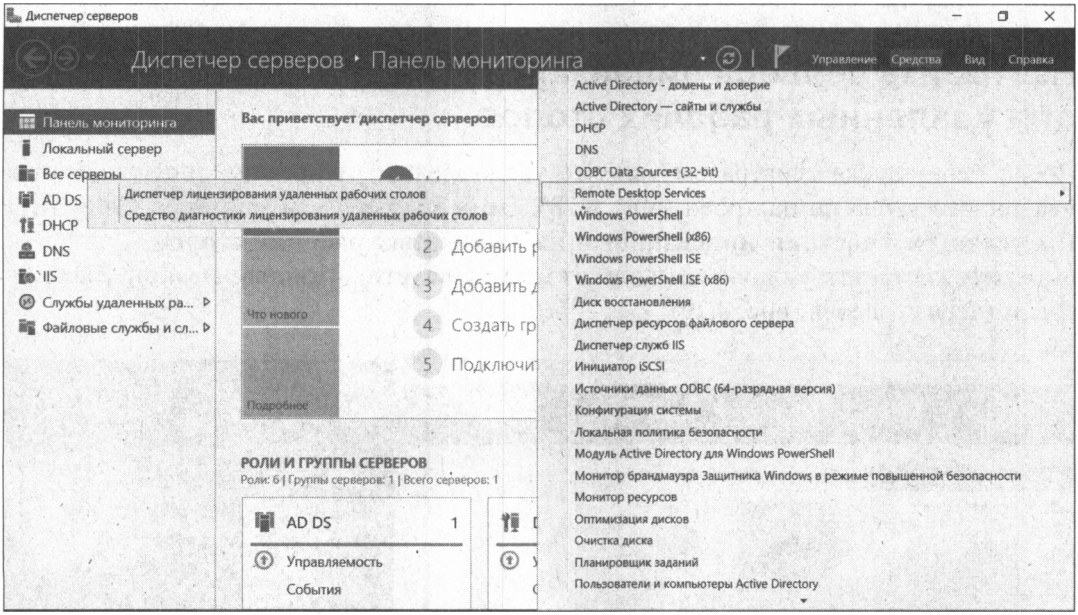


Рис. 8.29. Запуск средства диагностики лицензирования удаленных рабочих столов

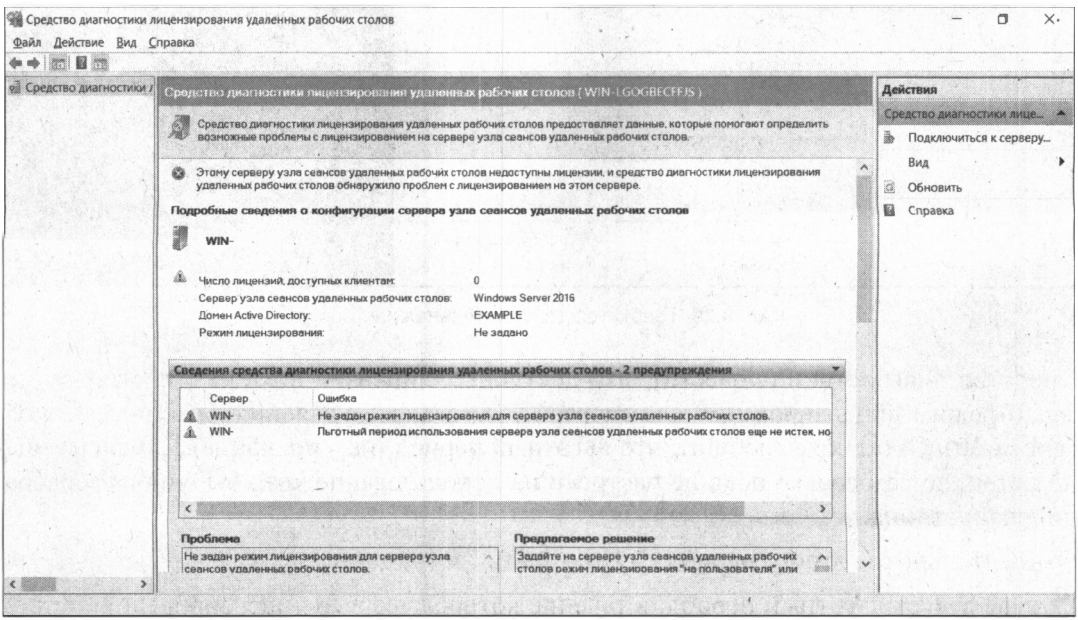


Рис. 8.30. Нет доступных лицензий

Другими словами, пока вы еще не купили лицензии для терминального доступа, вы можете воспользоваться льготным периодом. Почему бы не использовать терминальный сервер бесплатно целых четыре месяца? Кроме того, если вам нужно всего два удаленных подключения — например, у вас всего два удаленных офиса, — тогда сервер лицензирования вообще не потребуется, да и конфигурацию виртуального сервера можно упростить — хватит 8 Гбайт оперативки.

В Windows Server 2016/2019/2022 сервер лицензирования указывается в локальных групповых политиках, поэтому выполните команду `gpedit.msc`, чтобы открыть редактор локальной групповой политики. Перейдите в нем в раздел **Конфигурация компьютера | Административные шаблоны | Компоненты Windows | Службы удаленных рабочих столов | Узел сеансов удаленных рабочих столов | Лицензирование** (рис. 8.31).

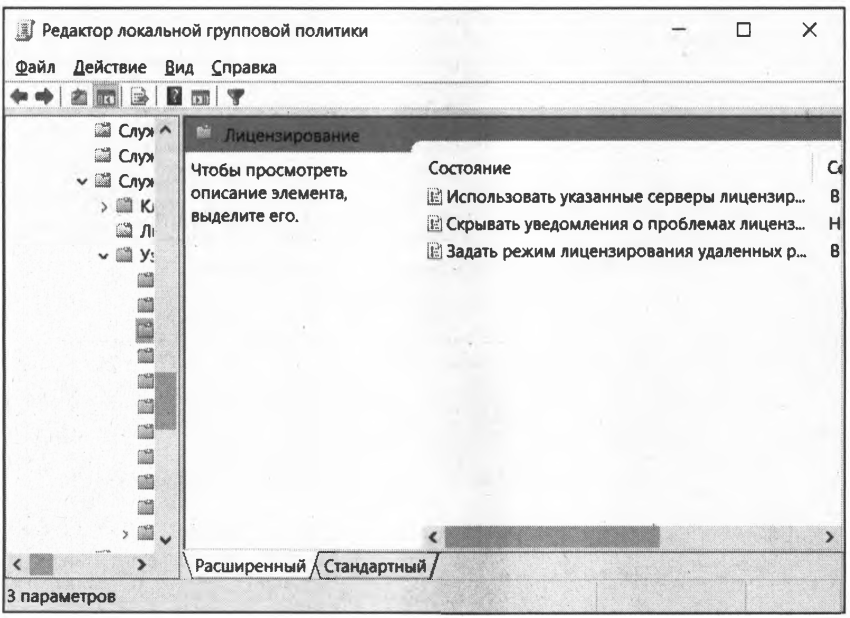


Рис. 8.31. Редактор локальной групповой политики

Откройте параметры **Использовать указанные серверы лицензирования удаленных рабочих столов** — просто щелкните двойным щелчком мыши на названии параметра. В открывшемся окне (рис. 8.32) установите переключатель в положение **Включено** и укажите, какой сервер лицензирования использовать (мы воспользуемся им же). Введите имя сервера или его IP-адрес и нажмите кнопку **OK**.

Затем откройте параметр **Задать режим лицензирования удаленных рабочих столов** (см. рис. 8.31). В открывшемся окне (рис. 8.33) установите переключатель в положение **Включено** и укажите режим лицензирования сервера узла сеансов удаленных рабочих столов. Возможны два варианта: **На устройство** или **На пользователя**. Представим, что у вас есть 10 лицензий. В режиме **На устройство** вы можете создать на сервере неограниченное число пользователей, которые смогут подключаться через удаленный рабочий стол только с 10 компьютеров, на которых

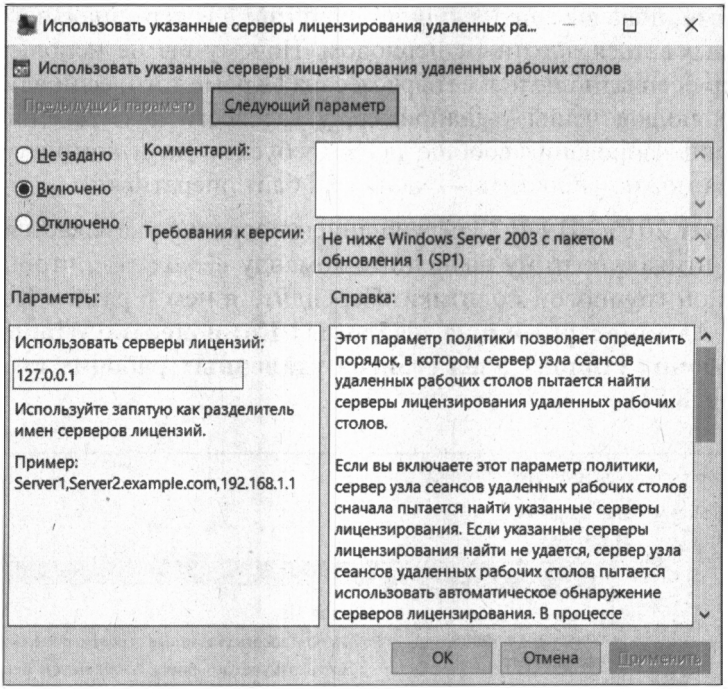


Рис. 8.32. Параметры сервера лицензирования

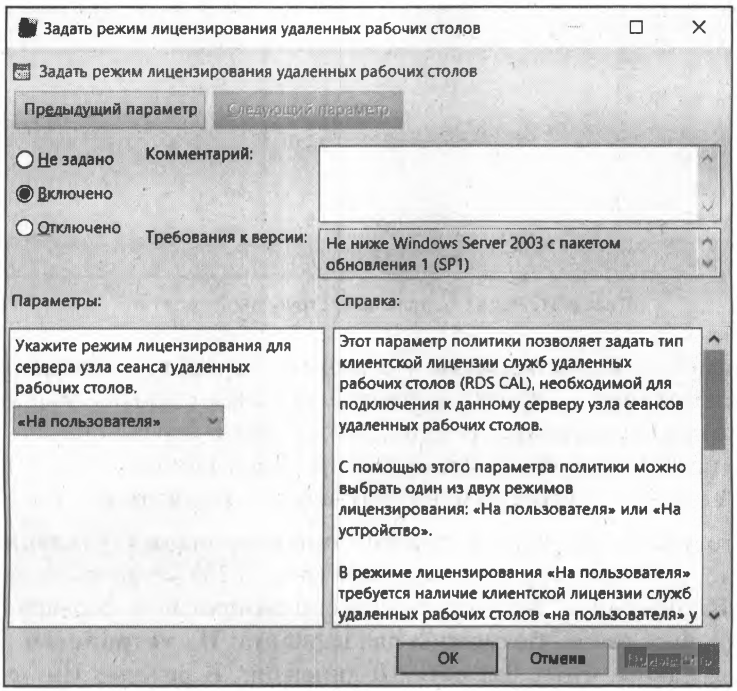


Рис. 8.33. Выбор режима лицензирования

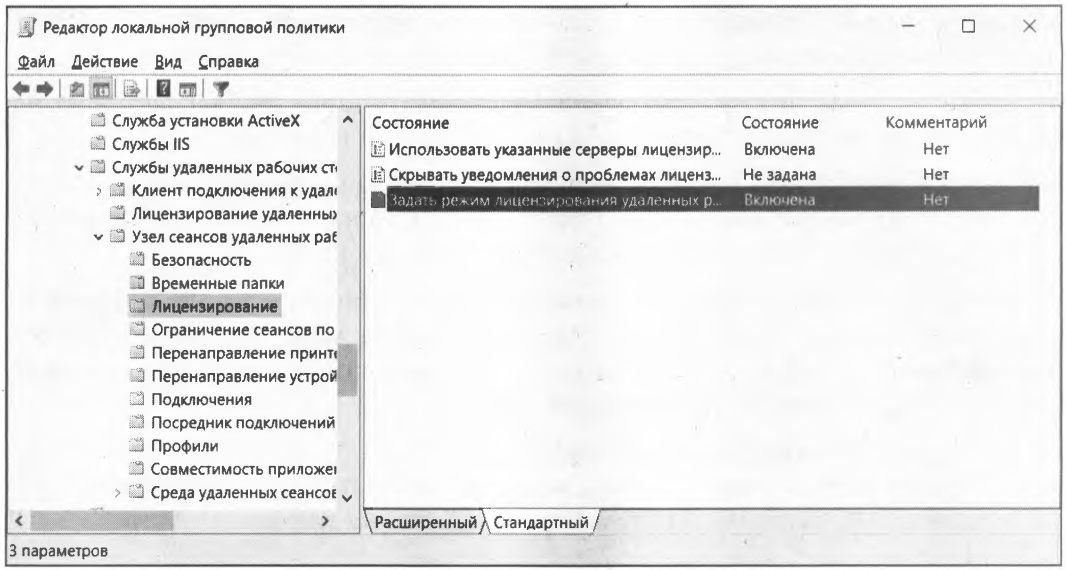


Рис. 8.34. Результат установки параметров

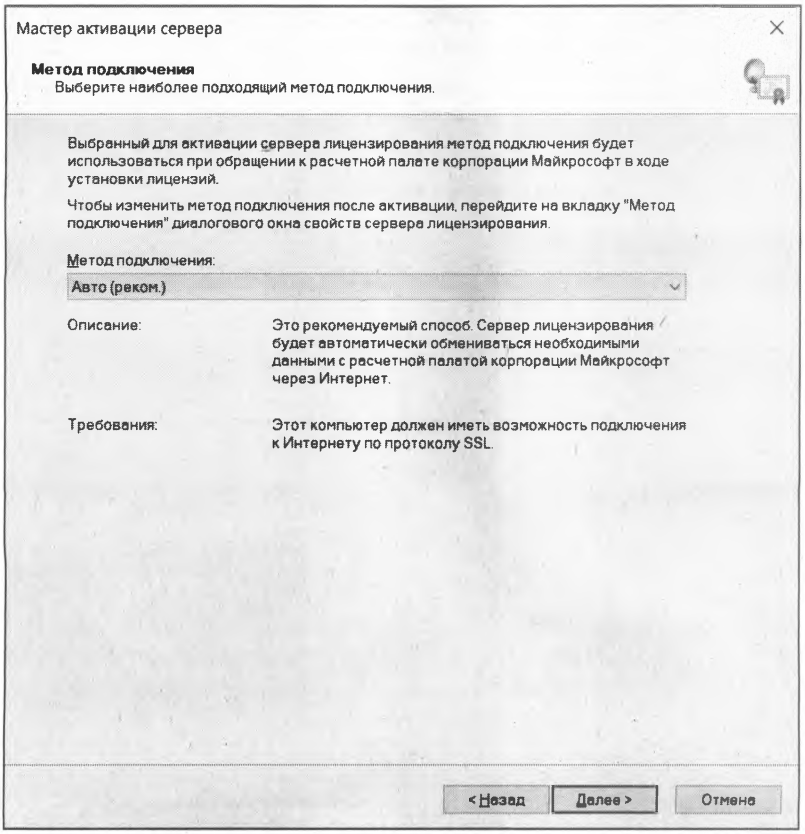


Рис. 8.35. Мастер активации сервера: выбор метода подключения

установлены эти лицензии. Если выбрать режим **На пользователя**, то зайти на сервер смогут только 10 выбранных пользователей, но с любых устройств. Часто режим **На пользователя** более предпочтительный, поэтому его и выбираем.

В результате у вас должны быть установлены параметры так, как показано на рис. 8.34. Закройте окно редактора локальной групповой политики.

Вернитесь в окно средства диагностики лицензирования удаленных рабочих столов (см. рис. 8.31) и нажмите кнопку **Обновить**. Вы увидите новое сообщение об ошибке, связанной с тем, что сервер лицензирования не включен.

Чтобы запустить сервер лицензирования, перейдите в **Диспетчер лицензирования удаленных рабочих столов** — его можно вызвать в меню **Средства | Remote Desktop Services**. Найдите наш сервер в списке, щелкните на нем правой кнопкой мыши и выберите команду **Активировать сервер**.

Откроется окно **Мастер активации сервера**, в котором — на первой странице мастера — нужно нажать кнопку **Далее** и в следующем открывшемся окне (рис. 8.35) выбрать метод подключения. Рекомендуется оставить все как есть — **Авто**.

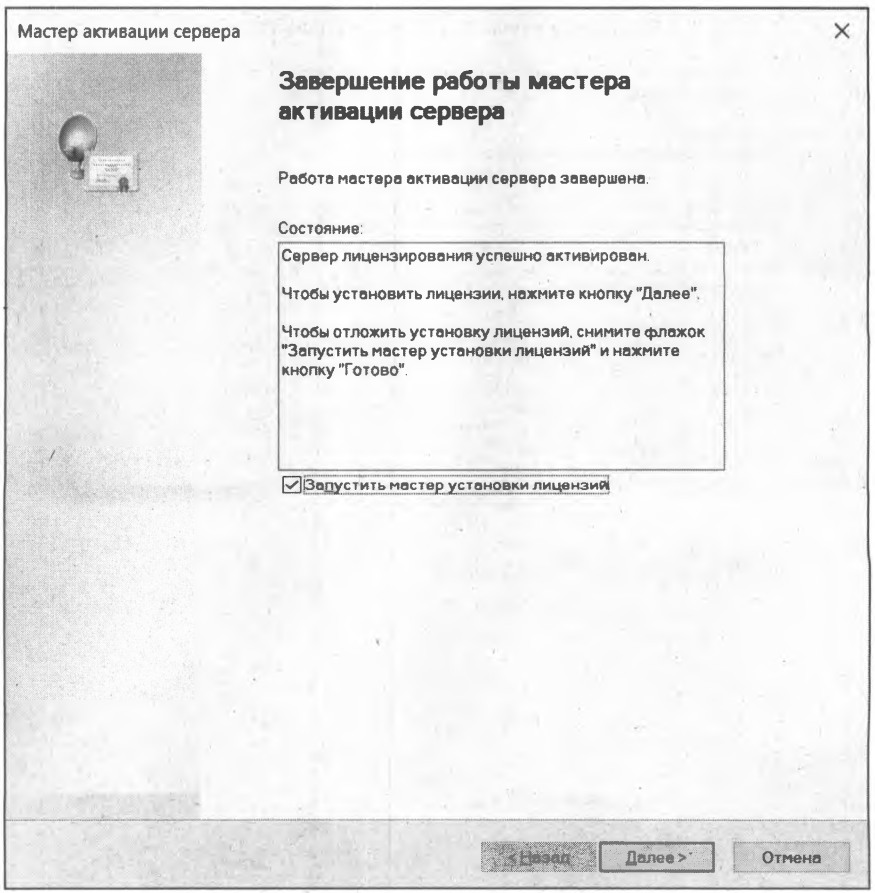


Рис. 8.36. Сервер лицензирования активирован

В следующем открывшемся окне введите сведения об организации и нажмите кнопку **Далее**. Дополнительные сведения об организации заполнять не рекомендуется — просто нажмите кнопку **Далее**.

Что ж, сервер лицензирования успешно активирован (рис. 8.36). Теперь нужно запустить мастер установки лицензий. Не выключайте флажок **Запустить мастер установки лицензий** и нажмите кнопку **Далее**.

Установка лицензий службы удаленных рабочих столов

Итак, в предыдущем разделе вы нажали кнопку **Далее** при активном флажке **Запустить мастер установки лицензий**. В открывшемся окне просто нажмите кнопку **Далее**.

В следующем окне выберите нужную вам программу лицензирования. Чтобы только лишь продемонстрировать вам настройку сервера, мы выбрали программу **Соглашение "Enterprise Agreement"** (рис. 8.37), — вы же должны выбрать именно вашу программу лицензирования. Нажмите кнопку **Далее**.

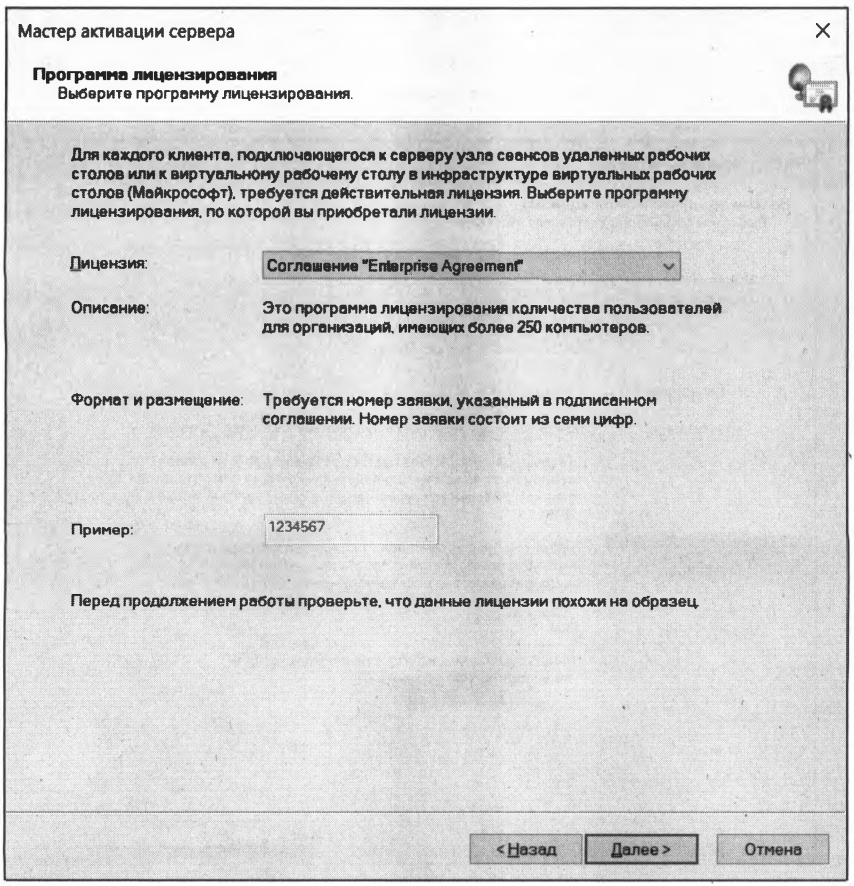


Рис. 8.37. Выбор программы лицензирования

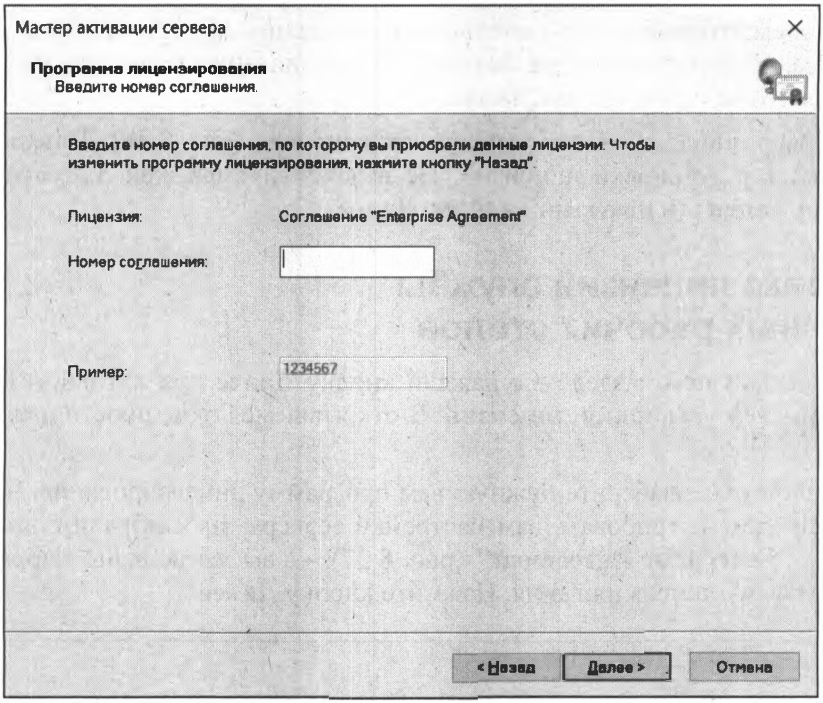


Рис. 8.38. Ввод номера соглашения

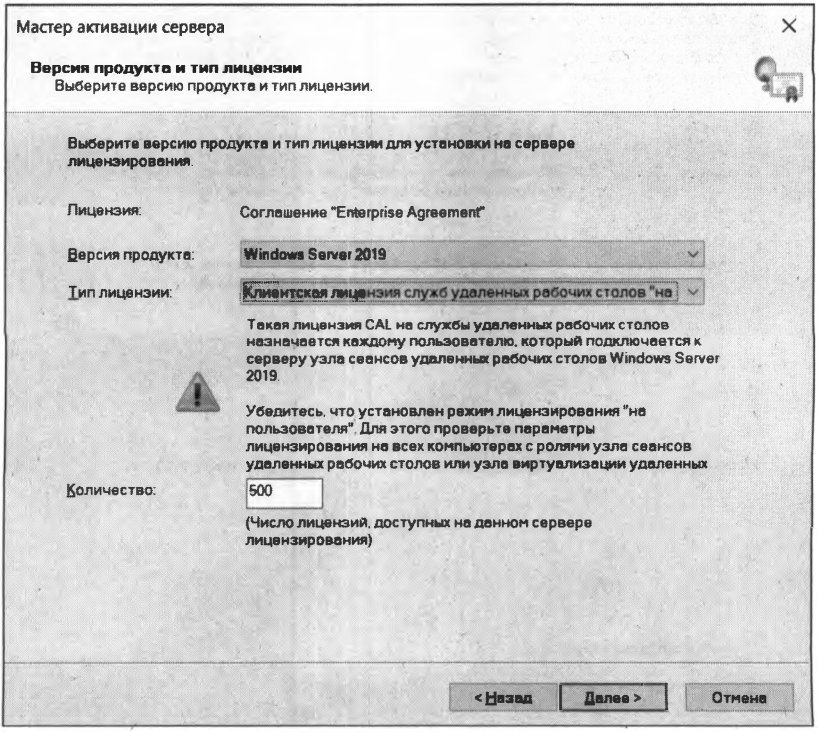


Рис. 8.39. Версия продукта и тип лицензии

В следующем окне (рис. 8.38) введите номер соглашения — обычно он состоит из семи цифр. Нажмите кнопку **Далее**.

В следующем окне (рис. 8.39) нужно выбрать версию продукта (мы выбираем **Windows Server 2019**), тип лицензии и количество лицензий. Ранее мы выбрали тип лицензирования **На пользователя**, поэтому здесь должны выбрать **Клиентская лицензия служб удаленных рабочих столов "на пользователя"**. Введите число лицензий, доступных на этом сервере лицензирования, нажмите кнопку **Далее** и дождитесь успешного завершения работы мастера установки лицензий. Если вы все сделали правильно, то получите сообщение о том, что все запрошенные лицензии установлены (рис. 8.40).

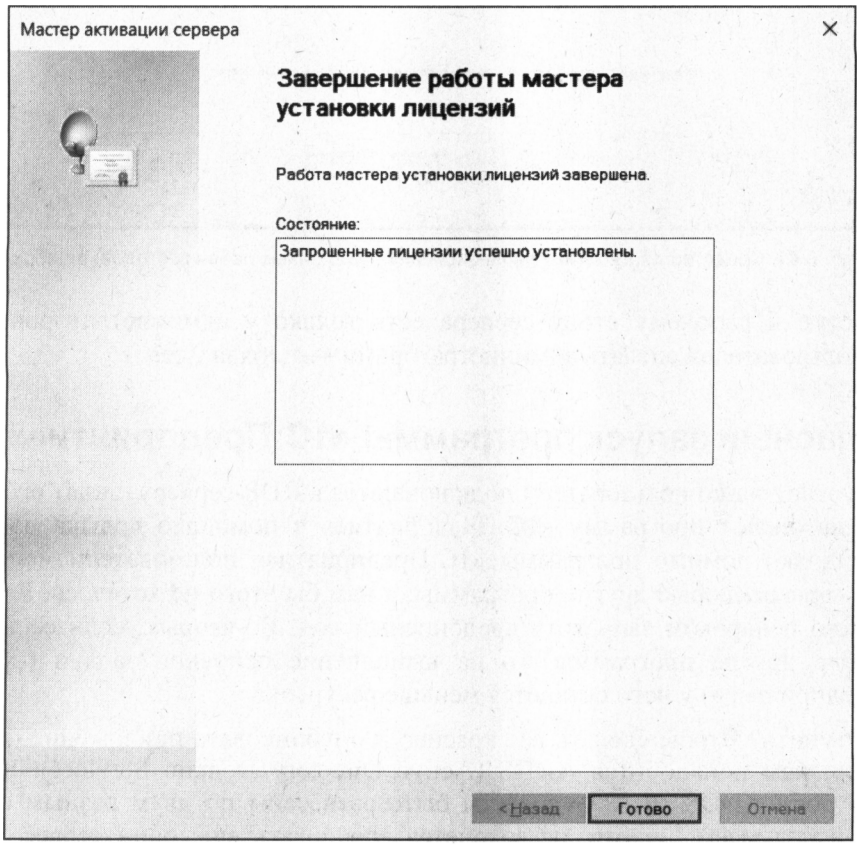


Рис. 8.40. Запрошенные лицензии успешно установлены

Вернитесь в **Средство диагностики лицензирования удаленных рабочих столов** (рис. 8.41) и убедитесь, что никаких ошибок нет. Заодно вы увидите информацию об установленных лицензиях.

На этом настройка сервера терминалов завершена. Вам осталось только добавить в группу **Пользователи удаленного рабочего стола** (Remote Desktop Users) тех пользователей, которым разрешен удаленный доступ к серверу. Ведь по умолчанию

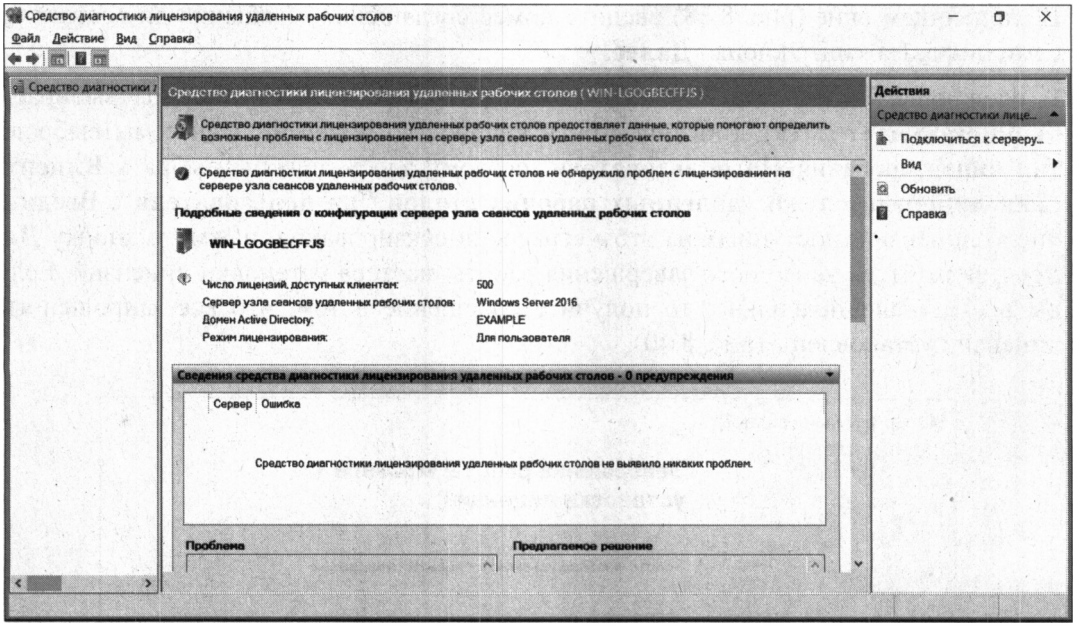


Рис. 8.41. Средство диагностики лицензирования удаленных рабочих столов: ошибок нет

RDP-доступ к рабочему столу сервера есть только у администраторов сервера, а всех пользователей сделать администраторами — плохая идея.

Безопасный запуск программы «1С:Предприятие»

На этом этапе наши пользователи подключаются к RDP-серверу, видят его рабочий стол и запускают программу «1С:Предприятие» с помощью ярлыка на рабочем столе. Однако помимо программы «1С:Предприятие» пользователи могут запустить на сервере любые другие программы, а нам бы этого не хотелось. Во-первых, так можно ненароком запустить вредоносный код. Во-вторых, если сервер будет выполнять другие программы, то на выполнение основной задачи (программа «1С:Предприятие») у него останется меньше ресурсов.

Как поступить? Чтобы сделать все красиво и опубликовать приложение «1С:Предприятие», нам понадобится ADDS (Active Directory Domain Services). Но по-хорошему роли ADDS и RDS должны быть разнесены по двум разным серверам. Сейчас же, думаем, никому не захочется арендовать еще один сервер под роль ADDS (только арендовали один сервер и сразу же нужно арендовать второй!).

Выход есть — использование групповой политики **Запускать программу при подключении**. Откройте редактор групповой политики. Там есть два варианта:

- или установить групповую политику для всего компьютера:

  Конфигурация компьютера | Административные шаблоны | Компоненты Windows | Службы удаленных рабочих столов | Узел сеансов удаленных рабочих столов | Среда удаленных рабочих столов | Запускать программу при подключении;

- или — для конкретного пользователя (тогда придется установить политику для всех пользователей, которые будут использовать программу «1С:Предприятие»):

  Конфигурация пользователя | Административные шаблоны | Компоненты Windows | Службы удаленных рабочих столов | Узел сеансов удаленных рабочих столов | Среда удаленных рабочих столов | Запускать программу при подключении.

Правильнее, конечно же, второй вариант — устанавливать политику для пользователя. К тому же если установить эту политику для всего сервера, то программа «1С:Предприятие» будет запускаться даже для администратора, а это нам не нужно, хотя можно и переопределить эту политику для учетной записи администратора — при желании:

1. На вкладке **Локальные ресурсы** RDP-клиента для параметра **Клавиатура** установите значение **На удаленном компьютере**.
2. Нажмите кнопку **Подключить** для установки соединения с терминальным сервером.
3. Нажмите комбинацию клавиш <Ctrl>+<Shift>+<Esc> для запуска диспетчера программ на удаленном сервере.
4. Выполните команду меню **Файл | Запустить новую задачу**.
5. Запустите редактор групповой политики (`gpedit.msc`) и либо выключите политику запуска программ, либо отключите ее только для своей учетной записи в разделе **Конфигурация пользователя**.

Песочница Windows

В Windows 10 (начиная с версии 1903) появилась встроенная *песочница* (Windows Sandbox) (разумеется, в Windows 11 эта функция также есть), представляющая собой изолированное окружение рабочего стола для безопасного запуска приложений. Сама идея не нова, в UNIX уже давным-давно была такая возможность (chroot-окружения), но в Windows ее реализовали только в 2019 году.

Для работы песочницы необходимо выполнение следующих условий:

- выпуск Windows Pro или Enterprise;
- архитектура *x*86-64;
- включение виртуализации в BIOS;
- минимум 4 Гбайт ОЗУ и 1 Гбайт свободного дискового пространства;
- минимум двухъядерный процессор.

Но это минимальные требования. Рекомендуется же 8 Гбайт ОЗУ, SSD-накопитель и четырехядерный (или лучше) процессор с поддержкой технологии Hyper-Threading.

Прежде чем включать песочницу, нужно активировать поддержку виртуализации в BIOS. О том, как это сделать, вы сможете прочитать в документации к компьюте-

ру или его материнской плате. В крайнем случае, если не разберетесь, можно обратиться к производителю компьютера/материнской платы.

Если же вы используете виртуальную машину, включить виртуализацию можно командой PowerShell:

```
Set-VMProcessor -VMName {VMName} -ExposeVirtualizationExtensions $true
```

Для включения самой песочницы достаточно включить компонент Песочница Windows: **Панель управления | Программы и компоненты | Включение и отключение компонентов Windows** (рис. 8.42).

Включить песочницу можно и с помощью PowerShell-команды:

```
Enable-WindowsOptionalFeature -FeatureName "Containers-DisposableClientVM" -All
-Online
```

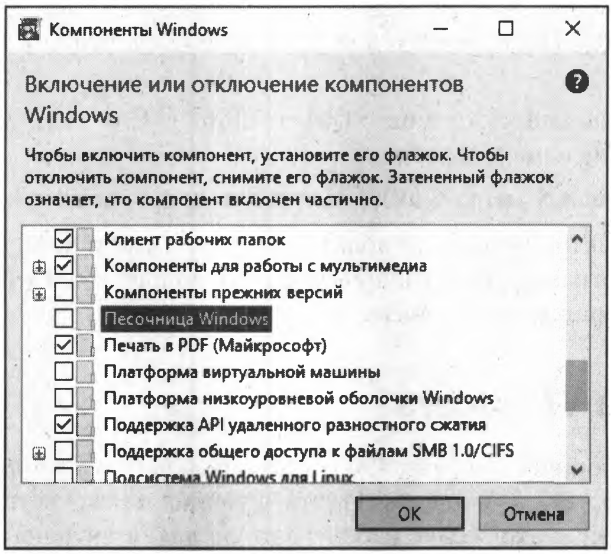


Рис. 8.42. Включение песочницы

Для отключения служит другая команда:

```
Disable-WindowsOptionalFeature -FeatureName "Containers-DisposableClientVM"
-Online
```

Дальше все просто:

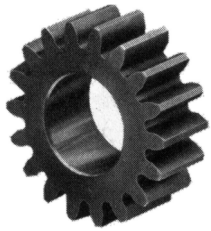
1. В главном меню найдите пункт **Windows Sandbox** и выберите его. Разрешите повышение привилегий.
2. Скопируйте подозрительный файл в окно песочницы (оно появится на рабочем столе) — просто перетащите туда файл (файлы).
3. Запустите файл в песочнице.
4. Если вы скопировали исполнимый файл, то или запустится программа, или же ее установщик. Если вы запустили установщик, продолжайте установку.

5. Закончив экспериментировать, вы можете просто закрыть приложение Windows Sandbox — все содержимое песочницы будет безвозвратно удалено.

Песочница позволяет запускать portable и другие подозительные приложения, не опасаясь за хост-систему. Вы можете проверить приложение в песочнице и, убедившись, что оно безопасно, установить его на основную систему.

Постоянно задействовать песочницу для работы с одним и тем же приложением неудобно — ведь его придется каждый раз переустанавливать. Если есть такая потребность, тогда лучше использовать полноценную виртуальную машину. В ней вы можете установить приложения, которые не будут удалены после завершения работы виртуальной машины. В то же время все изменения, внесенные в виртуальную машину, не отразятся на основной хост-системе.

Песочница служит не для постоянной работы с приложением в изолированном окружении. Ее цель — помочь вам убедиться, что приложение безопасно, после чего вы сможете установить его на основной системе. Песочница пригодится и разработчикам, которые смогут проверять в ней работу инсталлятора своего программного продукта без необходимости устанавливать/удалять приложение после каждой пересборки инсталлятора.



ГЛАВА 9

Безопасность

В наши дни в обеспечение безопасности информации вкладываются серьезные суммы, а на крупных предприятиях создаются целые отделы информационной безопасности. В некоторых случаях, к сожалению, реальная ценность информации не соизмеряется с мерами по ее защите, в результате чего затраты на защиту информации превышают ее реальную стоимость. Бывает и так, что перед администраторами сети ставится невыполнимая задача достижения абсолютной надежности, которая даже в наше время выглядит как нечто из разряда научной фантастики.

Разумнее всего перед началом внедрения мер по защите информации определить список возможных угроз, а также степень и актуальность каждой угрозы. На некоторых предприятиях даже создается специальный документ — «модель угроз», в котором описываются все возможные угрозы: от несанкционированного доступа из Интернета и вирусов до физической кражи ПК и/или их компонентов. Перечислены в нем и мероприятия по устранению этих угроз, которые либо уже выполнены, либо должны быть выполнены.

Если вам нужен именно такой документ, то вы можете взять за основу базовую «Модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденную ФСТЭК России 15 февраля 2008 года (ее без проблем можно найти в Интернете). Вы будете удивлены тем, сколько существует угроз, о которых вы даже и не подозреваете. Но это не самая «страшная» модель угроз — есть еще секретная ИТР-2020, которой нет в открытом доступе. Впрочем, обычным предприятиям вполне достаточно и упомянутой базовой модели. В нашей же книге, чтобы не переписывать сюда эту модель (вы и так ее сможете скачать и прочитать), мы будем руководствоваться только собственным опытом. Вы, однако, можете совместить прочитанное здесь с базовой моделью угроз и создать оптимальный для своего предприятия план действий по защите информации.

Безопасность и комфорт

К сожалению, эти два понятия мало сочетаются на практике. Вы только представьте себе спортивный автомобиль с каркасом безопасности и встроенной системой

пожаротушения. Такой автомобиль гарантирует большую безопасность водителю и пассажирам в случае переворота и пожара, чем большинство привычных нам автомобилей. Но почему-то автопроизводители не спешат оснащать этими опциями прочие свои «продукты». Почему? Потому что их наличие в салоне не добавит ни комфорта, ни какого-либо шика. Вот и сдвигается «ползунок» в сторону комфорта, а не безопасности. На спортивных же машинах, где повышен риск перевернуться, каркас устанавливается. С ним неудобно, он не «смотрится», но он нужен.

Аналогичная ситуация наблюдается и в информационных системах. Можно защитить систему по максимуму, но работать в ней будет неудобно. И вы, как системный администратор, должны это понимать и донести свое мнение до руководства. Чем безопаснее система, тем сложнее с ней работать, — ведь она накладывает больше ограничений на текущую работу. Поскольку далеко не все сотрудники предприятия являются специалистами по информационной безопасности или имеют отношение к конфиденциальным данным, у вас окажется много недовольных. Хотя бы по той причине, что не все умеют работать со средствами защиты и не все понимают их важность и необходимость. Когда защищаемая информация того стоит, приемлемы любые меры — хоть рентген на входе. Если же на предприятии нет секретной информации, то зачем усложнять жизнь всем, в том числе и себе?

Задайте себе вопросы: что произойдет в случае утечки информации? Какие возникнут от этого последствия для предприятия? Если никаких или ущерб окажется минимальным, то, может, и не стоит пытаться «городить огород» безопасности? Ведь утечки может и не произойти. Если на предприятии нет ценной или интересной кому бы то ни было информации, то никто не станет взламывать ее информационную систему, никто не будет подкупать сотрудников, чтобы они «вынесли» обрабатываемую ими информацию и пр. Вполне возможно, что для такого предприятия оптимальным набором обеспечения безопасности станут лишь средства антивирусной защиты, межсетевого экранирования и резервного копирования.

Попытаемся разложить по полочкам

Чтобы не перестараться с защитой информации и не сделать информационную систему некомфортной для пользователей, вам нужно ответить себе на вопросы: что, где и от чего? Почти как в «Что? Где? Когда?»

- Вам следует знать, *что* мы будем защищать. Есть ли вообще на предприятии информация, которая того стоит. Или же мы просто выстроим защиту даже не самой информации, а работоспособности информационных систем, чтобы утром, придя в офис, сотрудники не обнаружили свое рабочее место в неработоспособном состоянии — где тогда они будут играть в «Тетрис» или раскладывать пасьянс?

  Итак, администратор должен иметь четкое представление о том, **что защищать**. Всю информацию можно разделить на *публичную* — ее защищать ни к чему, она должна быть доступна всем, и *конфиденциальную*: персональные данные клиентов и сотрудников, коммерческая тайна и т. п. А некоторые предприятия могут

также работать и с *секретной* информацией — например, со сведениями, составляющими государственную тайну. Надо понимать, кому и к какой информации может быть предоставлен доступ, — не всем сотрудникам требуется доступ к секретной и конфиденциальной информации, не у всех есть соответствующие допуски и т. д.

- Нужно также определиться, **где защищать** информацию. Одно дело, если вся информация находится на локальных серверах, другое дело — если в «облаке». Вы должны понимать, как обрабатывается и где хранится информация, как данные из одной программы передаются в другую, как ограничивается доступ в Интернет и т. п. Чем точнее вы с этим разберетесь, тем легче организовать защиту.
- Надо определиться и с тем, **от чего защищать**. Существует множество угроз, о чем уже говорилось в начале этой главы. Составьте список предполагаемых угроз, актуальных для вашего предприятия, — в зависимости от них и следует реализовать методы защиты информации. Например, если вы считаете, что актуальна угроза утечки данных через электромагнитное излучение, то вам нужно получить схемы электропитания с указанием расположения кабелей (насколько близко они проложены от информационных линий), схемы заземления, пожарной и охранной сигнализаций и т. д.

Как будем защищать?

При разработке мер безопасности нужно учитывать стоимость не только пусконаладочных работ, но и обслуживания установленного оборудования. Бывает так, что стоимость пусконаладки совсем небольшая, а вот обслуживание может вылиться в приличную сумму. Так, охранную сигнализацию «по акции» вам устанавливают за 1 рубль, а обслуживание ее будет стоить 5 тыс. рублей в месяц. При этом у конкурентов стоимость пусконаладочных работ составляет 20 тыс. рублей, зато в месяц надо будет платить только 3500. Теперь подсчитайте, какой вариант вам будет выгоднее. Стоимость первого года по «акционному» варианту составит 60, а по второму — 62 тыс. рублей. Зато второй год при выборе второго варианта окажется намного выгоднее.

Если вы ознакомились с базовой моделью угроз, упомянутой в начале этой главы, то у вас уже может быть составлен внушительный список угроз для вашей компании. Однако на реализацию мероприятий по устранению *всех* возможных угроз не хватит никакого бюджета. Вы потратите все средства компании и превратите офис в огромный сейф, в котором сотрудникам будет некомфортно работать.

На практике существует правило 30/70: реализовав лишь 30% мероприятий, вы закроете 70% угроз, — вам надо лишь верно расставить приоритеты и выбрать «правильные» угрозы. Остальные 30% угроз будет предотвратить очень сложно и/или очень дорого.

При выборе решений информационной безопасности нужно точно расставить приоритеты: защищаетесь ли вы для «бумажки», или вам действительно нужна безопас-

ность. Некоторые предприятия обращаются к специалистам по информационной безопасности только с одной целью — для получения аттестата соответствия требованиям информационной безопасности. Естественно, при этом приобретаются самые дешевые средства защиты информации — лишь бы они имели сертификат. В результате: и деньги потрачены, и речи ни о какой безопасности идти не может.

Три «кита» безопасности

Работы по обеспечению безопасности информационной системы можно условно разделить на три этапа, которые следует выполнять параллельно, а не последовательно.

- **Организационные мероприятия** — нужно подготовить ряд внутренних документов, четко регламентирующих действия пользователей и администраторов в различных ситуациях. Вот примерный перечень таких документов:
  - приказ о назначении администратора информационной безопасности — регламентирует, кто будет отвечать за информационную безопасность;
  - инструкция администратора информационной безопасности — определяет, что должен делать ответственный за информационную безопасность;
  - инструкция по действиям пользователей в нештатных ситуациях — определяет, что есть нештатная ситуация: пропажа данных, потеря работоспособности рабочего места, оповещение антивируса или системы обнаружения вторжений и т. п., и регламентирует действия пользователей;
  - инструкция по резервному копированию — определяет, резервное копирование какой именно информации и как часто следует производить. Если на место администратора придет другой человек, эта инструкция подскажет ему, какую информацию надо резервировать и как ее восстановить в случае сбоя;
  - инструкция по порядку проведения проверок безопасности — регламентирует, какие проверки безопасности должны производиться на предприятии и как часто.
- **Реализация многоуровневой системы обороны** — несколько уровней защиты значительно сложнее взломать, чем один. Известно, что замок часто устанавливается только на входной двери. Аналогично этому раньше брандмауэры устанавливались лишь на серверах. Однако сейчас принято устанавливать брандмауэры на каждой машине — так злоумышленнику для взлома конкретной машины придется вскрыть два «замка». На серверах нужно устанавливать системы контроля доступа — наподобие SELinux, LIDS и т. п. Даже если злоумышленник каким-то образом получит права root, навредить системе ему помешает такая система контроля доступа.
- **Постоянный мониторинг системы** — только производя постоянный мониторинг системы, вы сможете заметить некоторые отклонения от нормы. По статистике, как раз «некоторые отклонения от нормы» — это свидетельства готовя-

щейся атаки. Например, вас должен насторожить рост трафика в ночное время, когда активности не должно быть, а она есть.

Полной гарантии безопасности данных вам никто не даст. Да, вы можете вообще пренебречь мерами безопасности — мол, любую систему можно взломать. Согласны. Но почему вы тогда все еще продолжаете запирать дверь в собственную квартиру? — ведь любой замок можно открыть. Но если не закрыть дверь, то войти сможет *каждый*, а если закрыть — то только тот, кто может открыть «любой замок». А поскольку таких гораздо меньше, чем обычных людей, замок на двери существенно снижает риск кражи. Вот поэтому вы и закрываете дверь. Так почему тогда нужно пренебрегать средствами защиты информации?

Организационное обеспечение информационной безопасности

На практике существенных результатов можно достичь одними только организационными мероприятиями, польза от которых в несколько раз превосходит полезность технических мер защиты.

Первым делом на уровне всего предприятия следует сформулировать четкие положения его информационной безопасности. Нужно создать *концепцию информационной безопасности*, в которой определить категории обрабатываемой информации, описать предполагаемые риски, установить направления и объем защиты данных для каждой категории.

Каждой компьютерной системе надо присвоить *категорию конфиденциальности*, а также разработать для нее *паспорт информационной безопасности*, в котором определить установленное программное обеспечение и категории информации, которая на ней хранится и обрабатывается. После этого можно будет разработать комплекс мер по обеспечению безопасности каждого отдельного компьютера.

В организационно-распорядительных документах предприятия необходимо зафиксировать правила взаимодействия пользователя с информационной системой. Пользователь должен знать, с чем он работает, какие программы он может использовать, а какие на предприятии запрещены (например, утилиты сканирования сети) и т. п. В инструкциях необходимо оговорить правила работы с электронной почтой предприятия, поведение пользователя в случае возникновения предположения о наличии вируса, требования к взаимодействию с Интернетом и т. п.

Чем точнее определены права пользователя и его 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).

План обеспечения непрерывности функционирования информационной системы

Важно также составить и утвердить план обеспечения непрерывности функционирования информационной системы. Обратите внимание — не только составить план, но и *утвердить* его у руководства компании, иначе толку от него не будет.

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 которых можно отказаться на время ремонта основного компьютера? Где должны храниться дистрибутивы, чтобы операция восстановления ПО 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.

Такой план, утвержденный руководством, с одной стороны, огородит вас от неоправданных требований немедленного восстановления работы, поскольку для каждой ситуации период восстановления будет в нем четко оговорен. С другой стороны, этот план станет инструкцией, определяющей, что нужно делать в аварийной ситуации.

Безопасность паролей

Самым узким местом безопасности являются пользовательские пароли. Некоторые из них очень простые, а некоторые пользователи (о ужас!) вообще не используют никаких паролей.

Пароль не только предотвращает несанкционированный доступ, но и может использоваться в качестве ключа шифрования. Представим ситуацию: вы установили простой пароль — типа 111 — и зашифровали свои данные с помощью EFS. Ваш пароль будет подобран за считанные секунды программой Advanced EFS Data Recovery или подобной и данные окажутся расшифрованы. Если же пароль сложный, расшифровать данные с помощью таких программ не получится — проверено на практике. Какой пароль можно считать устойчивым к подбору?

- Во-первых, минимальная длина пароля должна быть не менее шести символов, еще лучше, если их будет восемь.
- Во-вторых, не должно быть никаких чисто цифровых паролей вроде 12345678. Пароль должен содержать и буквы, и цифры. Причем буквы не должны представлять собой словарное слово. Если вы все же хотите использовать словарное слово, то чередуйте в нем буквы с цифрами. Небольшой пример — есть два пароля: audi2015 и a2u0d1i5. Как вы думаете, какой пароль будет сложнее подобрать?

- В-третьих, для усложнения подбора паролей нужно использовать символы, отличные от алфавитных: знак подчеркивания, знаки препинания (тире, запятая, точка). Усложняем наш второй пароль с учетом этих требований: @a2,u0,d1,i5_.
- В-четвертых, желательно использовать символы различного регистра, например: @A2,u0,d1,i5_.
- Можно в пароле использовать и чередование английских и русских букв. В нашем пароле букву А можно написать, включив русскую раскладку, что значительно усложнит пароль. Вот только не надо писать русские слова при включенной английской раскладке — например: ghbdtn (привет). Словари таких слов уже давно созданы и используются злоумышленниками при подборе паролей. А вот указывать похожие символы алфавитов на разных языках — хорошая идея. Например, чтобы еще усложнить наш пароль @A2,u0,d1,i5_, можно букву i взять из украинского алфавита. Правда, в таком случае он станет очень неудобным для ввода: сначала придется переключиться на русский, потом на английский и уже затем — на украинский. Поэтому оптимальным с точки зрения комфорта и безопасности нам представляется предыдущий вариант.

> ***Совет***
>
> Никогда не используйте пароль, применяемый для входа в систему, в качестве паролей для входа на различные сайты, социальные сети и т. д. Для входа на такие ресурсы должны использоваться другие пароли.

Помните, что существуют очень эффективные программы «восстановления» паролей пользователей, за считанные секунды подбирающие простой пароль.

Вот что не следует использовать в качестве паролей:

- имена родных и близких;
- клички своих домашних животных;
- номера и названия своих автомобилей;
- даты из своей биографии и своих близких;
- другую общедоступную информацию о себе.

Такие пароли ваши недоброжелатели смогут подобрать даже безо всяких программ.

И вообще, если вы не хотите, чтобы ваш пароль подобрали, лучше, чтобы он состоял хотя бы из 15 символов. Такие пароли очень сложно подобрать, во всяком случае за умеренное время. Мы, конечно, понимаем, что 15 символов — это очень много, поэтому вместо пароля используйте парольную фразу, разбавленную различными цифрами, знаками пунктуации, как было показано ранее.

Пароль нужно изменять регулярно, скажем, раз в месяц. Если вы подозреваете, что кто-то может попытаться взломать вашу систему, тогда и того чаще — например, раз в неделю. При желании можно использовать средства автоматической смены паролей. Одно из таких описано на страничке: **https://habr.com/ru/sandbox/65040/** — сценарий автоматически меняет пароли пользователей и отправляет новые на SMS/e-mail пользователя. Он может пригодиться, если нужно быстро сменить пароли для всех пользователей, например, когда есть подозрение, что система скомпрометирована.

Новый пароль должен быть действительно новым, а не модификацией старого путем дописывания к нему новых цифр.

> ***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 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.

Токены и смарт-карты

Существуют различные технические решения, которые позволяют аутентифицировать пользователя, не прибегая ко вводу пароля, — например, по каким-либо биометрическим показателям. Но наиболее используемым на практике методом является аутентификация на основе *смарт-карты*.

Смарт-карта имеет вид пластиковой карты, наподобие банковской, на которую можно с помощью специальных устройств записывать (и считывать) информацию. Обычно на смарт-карте сохраняется сертификат пользователя, предназначенный для аутентификации его в системе. Чтобы сертификат не мог быть использован злоумышленником, смарт-карта защищается специальным PIN-кодом. PIN-код — это не пароль пользователя в системе, а лишь защита сертификата на случай утери или кражи смарт-карты. Он не передается по сети (поэтому не может быть перехвачен анализаторами трафика) и служит для доступа к сертификату, записанному на смарт-карту только локально. Поэтому он может быть достаточно коротким и удобным для запоминания.

Однако использование смарт-карт предполагает установку на всех компьютерах устройств для их считывания, что не всегда удобно или возможно. Например, компьютеры могут быть на гарантии, а решение о внедрении смарт-карт принимается после их приобретения.

Конечно, проблему считывателей смарт-карт решить можно, но есть способ более эффективный, — использование *токенов*. Токен (он же аппаратный токен, USB-ключ, криптографический токен) — небольшое устройство, предназначенное для идентификации его владельца и обеспечения информационной безопасности пользователя (рис. 9.1).

Рис. 9.1. Аппаратный токен eToken

При желании токены можно создать и из обычных флешек, но лучше все же приобрести настоящие — стоят они не так уж и дорого, особенно для предприятия. Стоимость токена соизмерима со стоимостью считывателя смарт-карт, но если на предприятии необходимо обеспечить повышенный уровень безопасности для каких-либо отдельных пользователей, это решение будет экономически оправданным.

Подключение токена в USB-порт воспринимается системой как вставка смарт-карты, однако перед использованием токена нужно установить на систему дополнительный драйвер этого устройства.

Rainbow-таблицы

Операционные системы используют не пароли, а их *хеши*, созданные по известным правилам. Параметры вычислительной техники настолько выросли, что у хакеров появилась возможность не перебирать пароли, а составить базу данных хешей паролей и затем просто выбирать из нее по полученным данным необходимые значения. В результате им достаточно узнать (например, перехватить по сети) хеш пароля, выполнить запрос к подобной базе, называемой Rainbow-таблицей, и получить значение пароля практически сразу.

Программы для использования Rainbow-таблиц доступны в Интернете, и 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 (**www.oxid.it**) позволяет построить таблицу хешей для паролей, состоящих из всех букв латинского алфавита и цифр, длиной до восьми символов включительно менее чем за полтора дня. Эта программа была обновлена разработчиком в 2014 году и стала поддерживать Windows 8. К сожалению, в настоящее время (8 августа 2023 года) сайт программы недоступен, но вы без труда найдете в Интернете множество источников, с которых сможете ее скачать. Обратите только внимание на то, что программа эта распознается антивирусными программами и браузером Chrome как вирус, поэтому загружать ее нужно при выключенном антивирусе и в браузере Firefox. В качестве альтернативы можно использовать программу Windows Password Recovery[1], пригодится вам и программа Reset Windows Password[2], поддерживающая самую новую версию Windows — Windows 11.

Блокировка учетной записи пользователя

Самый эффективный способ борьбы с подбором пароля — блокировка учетной записи пользователя после некоторого числа неудачных попыток входа. Эта опция

---

[1] См. **https://www.passcape.com/windows_password_recovery_passcape_rainbow_table_generator_rus**.

[2] См. **https://www.passcape.com/index.php?section=news&cmd=details&newsid=766**.

включается через групповую политику предприятия с помощью Active Directory или настраивается посредством PAM-модулей при использовании Linux.

Блокировать учетную запись рекомендуется после 3–5 неудачных попыток ввода пароля. Полагаем, этого количества попыток должно хватить пользователю, который просто ошибся при вводе пароля — например, выбрал неправильную раскладку клавиатуры, просто нажал не на ту клавишу и т. п. Для сложных паролей можно увеличить количество неправильных попыток ввода до семи. Лучше пусть учетные записи будут чаще блокироваться и администраторы будут чаще отвлекаться на допуск в систему слишком много раз ошибшегося, но «своего» пользователя, чем кто-то подберет чей-то пароль. При этом период, в течение которого считаются попытки входа, а также время, через которое произойдет автоматическая разблокировка заблокированной учетной записи пользователя, можно установить порядка одного часа. Другими словами, если пользователь установленное количество раз (допустим, пять) ввел неправильный пароль, его учетная запись будет заблокирована. Если администратор недоступен и разблокировать эту учетную запись некому, она будет автоматически разблокирована через час. После чего у пользователя опять будет пять попыток ввода пароля.

> ***Примечание***
>
> Если к учетной записи предъявляются особые требования безопасности, то можно оставить только вариант ее ручного разблокирования администратором, хотя это и приведет к увеличению нагрузки на него, в том числе потребует и расследования каждого такого инцидента.

Блокировка учетных записей достаточно часто может возникать вследствие тех или иных неверных настроек, ошибок сохраненных паролей и т. п. Для расследования таких ситуаций можно загрузить комплект утилит Account Lockout and Management Tools ALTools.exe[1], 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.

Восстановление пароля администратора

Существует несколько утилит, позволяющих сменить пароль администратора (в том числе и администратора домена). Среди коммерческих вариантов едва ли не самая популярная — это программа ERD Commander (сегодня входит в состав Microsoft Desktop Optimization Pack). Программа позволяет создать загрузочный компакт-диск, с помощью которого можно не только заменить пароль администратора, но и отредактировать настройки реестра системы.

Существуют и бесплатные решения — наподобие Offline NT Password & Registry Editor[2]. Несмотря на присутствие в названии обозначения NT, последняя версия программы поддерживает все версии Windows, начиная с NT3.5 до Windows 10.

---

[1] См. **http://www.microsoft.com/downloads/details.aspx?familyid=7af2e69c-91f3-4e63-8629-b999adde0b9e&displaylang=en**.

[2] См. **http://pogostick.net/~pnh/ntpasswd/**.

Поддерживаются и серверные версии: 2003, 2008 и 2012. К сожалению, версия 2016 и более новые этим продуктом пока не поддерживаются, но, учитывая, что поддержка Windows 10 имеется, полагаем, в скором времени разработчики добавят поддержку и Windows Server 2016/2019/2022 и Windows 11.

В случае утери пароля от Linux-сервера для его восстановления можно использовать системные средства. Порядок восстановления пароля root будет примерно таким:

1. Перезагрузить систему и передать ядру (используя средства загрузчика) параметр `single`. Если система при загрузке в однопользовательском режиме запросит пароль root (запросит или нет — зависит от настроек системы), опять перезагрузить систему и передать ядру параметр `init=/bin/bash`.
2. Перемонтировать корневую файловую систему в режиме `rw`.
3. Установить пароль root командой `passwd`.
4. Перезагрузить систему командой `reboot`.

Если редактирование конфигурации загрузчика запрещено, порядок восстановления пароля будет следующим:

1. Загрузить компьютер, используя любой Live-носитель: LiveCD, LiveDVD или LiveUSB.
2. Получить права root. Обычно для этого нужно просто ввести команду `su` — пароль на Live-дисках не требуется.
3. Выполнить команду `chroot` для изменения корневой файловой системы. Корневой должна стать файловая система установленного на жестком диске дистрибутива Linux.
4. Ввести команду `passwd` для изменения пароля root.
5. Перезагрузить систему командой `reboot`.

Методы социальной инженерии

В связи с постоянно совершенствующимися техническими мерами обеспечения безопасности злоумышленники все активнее начинают использовать для получения данных об информационной системе методы так называемой *социальной инженерии*.

Например, злоумышленник может представиться ничего не подозревающему сотруднику предприятия новым специалистом службы техподдержки, коммерческим агентом или интервьюером и попытаться получить у него сведения о структуре сети и расположении информационных сетевых служб, о действующих мерах обеспечения безопасности данных и т. п.

Если от одного сотрудника будет получено недостаточно информации, злоумышленник легко может обратиться ко второму, третьему и т. д. Широко распространены попытки использования в целях социальной инженерии различных анкет, запросов по электронной почте и пр.

Сотрудники предприятия должны четко придерживаться следующих правил:

- не давать никакой информации в ответ на любые обращения по телефону, по электронной почте, при личных контактах каким бы то ни было 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 сервисов Интернета или пришедших по электронной почте;
- не отвечать на любые неожидаемые 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 интернет-адресами (URL) сайтов, чтобы быть уверенными в работе с конкретной и нужной 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 той или иной фирмы, впервые представившемся вам по электронной почте, принять меры к проверке его данных. При этом не следует пользоваться контактными данными, опубликованными в Интернете, — проверьте данные об этой фирме иными путями, например через справочные службы.

Меры защиты от внешних угроз

Первое, с чего нужно начать, — это ограничить доступ к информационной системе как физически, так и по каналам связи. Физическое ограничение доступа начинается с охраны помещений, а защита каналов связи осуществляется с помощью межсетевых экранов и систем предотвращения/обнаружения вторжений (IPS/IDS).

Физическая безопасность

Физический доступ к системе очень опасен. Например, ранее было показано, как легко можно изменить пароль администратора Linux-сервера (пароль пользователя root). Всего лишь был нужен физический доступ к серверу. Если бы у злоумышленника не было физического доступа, то у него бы ничего не вышло, — во всяком случае, приведенный сценарий не сработал бы, — это уж точно.

В Windows с безопасностью в случае физического доступа дела обстоят не лучше. 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 или отключить контроль записи на сменные устройст-

ва). При этом его действия останутся незамеченными для администратора и для пользователей.

Ограничение доступа к рабочим станциям

Что можно сделать для ограничения доступа к рабочим станциям? Пакет «минимум» должен включать в себя набор следующих мероприятий:

- установить пароль на вход в BIOS SETUP (не на загрузку ОС, а именно на вход в SETUP);
- запретить загрузку со сменных носителей — система должна загружаться только с собственного жесткого диска;
- поскольку стереть параметры BIOS можно, отключив батарейку материнской платы или использовав на ней специальный джампер (при этом все запреты снимаются), нужно предусмотреть либо специальные замки, препятствующие открытию корпуса системного блока, либо использовать систему пломбирования. Взломать можно любой замок, однако это не окажется незамеченным, равно как и распломбирование системного блока;
- на всех ПК переименовать стандартную учетную запись **Администратор** и установить для нее сложный пароль, а также создать ложную учетную запись **Администратор** с правами обычного пользователя;
- для входа в систему использовать сложный пароль. Не использовать гостевые учетные записи и учетные записи без пароля.

С одной стороны, это минимум, а с другой — максимум. Ведь тот же замок при желании можно взломать бесследно и точно так же закрыть после сброса параметров BIOS. Пломбы также можно восстановить. А узнаете вы об этом только лишь тогда, когда к BIOS SETUP не подойдет ваш пароль.

И даже если отключить все USB-порты (что довольно проблематично при использовании множества нужных USB-устройств: мыши, клавиатуры, принтеры и пр.) и приводы CD/DVD, все равно останется вероятность того, что кто-либо принесет внешний DVD-привод или внешний жесткий диск и воспользуется этими устройствами для кражи информации. Да и мобильные смартфоны сейчас оснащены картами памяти по 64 Гбайт, чего вполне достаточно для «слива» информации, не говоря уже о возможности передачи файлов по Интернету.

Конечно, если ресурсы позволяют, можно установить камеры, наблюдающие за действиями пользователя, или же использовать DLP-систему[1] (что будет, пожалуй, эффективнее, чем камера) — во многих таких системах есть возможность записи экрана пользователя или хотя бы периодического создания скриншотов. Потом, просматривая видеозаписи, можно будет узнать, что делал пользователь и был ли слив информации.

---

[1] DLP (от *англ.* Data Leak Prevention) — технологии предотвращения утечек конфиденциальной информации из информационной системы вовне, а также технические устройства (программные или программно-аппаратные) для такого предотвращения утечек.

Можно, конечно, установить и программу блокировки доступа к сменным устройствам (например, DeviceLock от SmartLine) или вообще пойти по пути максимального сопротивления и использовать электронный замок — тот же «Соболь» от фирмы «Код безопасности»[1]. Но все равно останутся способы обойти и эти решения. Другое дело, что на такой «обход» понадобится гораздо больше времени и у администратора будет возможность заметить попытку несанкционированного доступа.

Полностью ограничить физически можно разве что серверы, которые размещаются в отдельных помещениях, в специальных шкафах под замком и под видеонаблюдением.

Уровень физической защиты зависит от конкретных условий. Авторы встречали ситуации, когда в небольшом предприятии сервер просто устанавливался в сейф. Более крупные предприятия 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 для извлечения конфиденциальной информации могут быть использованы и данные резервного копирования. 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.

Межсетевые экраны

Для ограничения доступа к системе по каналам связи традиционно применяются межсетевые экраны (брандмауэры). Использование их мы подробно обсуждали в *главе 5*.

Обратим только еще раз внимание читателя, что, во-первых, нужно контролировать как входящий, так и исходящий трафик. Во-вторых, межсетевой экран не препятствует использованию злоумышленником разрешенных протоколов для доступа к системам (пример доступа извне через межсетевой экран также приведен в *главе 5*). И в-третьих, межсетевые экраны должны быть задействованы как на периметре информационной системы, так и на каждой рабочей станции и на каждом сервере.

Ограничения подключения нового оборудования

Сегодня пользователям доступно множество компактных USB-устройств: 3G/4G-модемы, адаптеры Wi-Fi, внешние жесткие диски и пр. Подключение 3G/4G-модема к компьютеру делает этот компьютер частью Интернета, и брандмауэр, установленный на корпоративном шлюзе, уже не будет его защищать. А внешние жесткие диски сейчас таких размеров, что на них могут поместиться все данные сервера.

---

[1] См. **http://www.securitycode.ru/products/pak_sobol/**.

Поэтому доступ к внешним устройствам нужно ограничивать. Первый вариант — это использование групповой политики Windows, позволяющей контролировать USB-устройства. Подробно этот способ описан в статье KB555324 на сайте Microsoft.

Второй вариант — сторонние программные продукты, например уже упоминавшийся DeviceLock. Опциями контроля доступа к съемным носителям оснащены и программные комплексы защиты узла. Типичный пример такого комплекса — Symantec EndPoint Protection.

При выборе варианта защиты следует учитывать:

- позволяет ли продукт контролировать различные классы устройств (не только USB-устройства, но и, например, модемы, видеокамеры и т. п.);
- можно ли обойти защиту простыми средствами (например, отключив службу или загрузившись в безопасном режиме и т. п.);
- имеется ли возможность, запретив устройства по их классу, разрешить использование исключений по серийному номеру (реально всегда необходимо обеспечить такие исключения для администраторов, служебных устройств и т. п.).

Сама Windows протоколирует все подключавшиеся к системе USB-носители данных. Можно просмотреть, какие устройства подключались к системе. Косвенно это может служить доказательной базой против пользователя. Данные хранятся в следующих ключах реестра:

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR\
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USB\
```

Избавиться от них не так уж и просто, но можно. Для этого достаточно использовать приложение USB Oblivion[1].

Обеспечение сетевой безопасности информационной системы

Внешний доступ к информационной системе может быть получен и по каналам связи. Соответственно администратор должен обеспечить такую защиту, чтобы к сети нельзя было подключить чужое устройство и чтобы попытки взлома информационной системы по используемым каналам не оказались успешными.

Контроль проходящего трафика

По каналам связи могут осуществляться попытки взлома информационной системы с использованием как известных, так и неизвестных на текущий момент уязвимостей. Обычно средствами предотвращения вторжений оснащаются системы защиты хоста. Но существуют способы и контроля всего трафика предприятия — специализированные *средства обнаружения вторжений* (IDS, Intrusion Detection System).

---

[1] См. **https://www.cherubicsoft.com/en/projects/usboblivion**.

Решения по обнаружению попыток взлома могут быть как программными, так и аппаратными. Поскольку для такой работы нужна очень высокая скорость вычислений, то обычно используются специализированные аппаратные устройства, позволяющие обновлять алгоритмы поиска зловредного кода.

Системы IDS ведут анализ трафика, фиксируют предполагаемые отклонения и формируют соответствующие предупреждения администратору. Существуют также и активные системы — Intrusion Prevention System (IPS), — они в режиме реального времени могут блокировать трафик при обнаружении подозрительных кодов.

Примеров IDS/IPS можно привести достаточно много — как коммерческих, так и бесплатных: Check Point IPS, LIDS (Linux IDS), TippingPoint Next-Generation IPS[1], Security Studio Endpoint Protection (сертифицированная система, содержащая IPS) и др.

Контроль устройств по MAC-адресам

Самый простой и бесполезный способ контроля подключаемых к сети устройств — это проверка MAC-адреса устройства. Такой контроль поддерживается всеми управляемыми коммутаторами. Когда включен режим контроля MAC-адресов, коммутатор запоминает MAC-адрес из первого пришедшего пакета и в дальнейшем пропускает данные только с этого устройства (конечно же, только по тому порту, к которому подключено устройство).

Включение проверки MAC-адреса позволяет защититься от уязвимости, называемой ARP-spoofing[2], при реализации которой злоумышленник может «расположиться» между двумя компьютерами, обменивающимися данными, и перехватывать весь трафик.

Недостаток способа контроля путем проверки MAC-адреса заключается в том, что коммутатор блокирует порт до явного вмешательства. Именно поэтому администраторы не любят включать эту функцию — ведь тогда им приходится перенастраивать коммутатор. Бесполезность же этого способа в том, что MAC-адрес устройства очень просто изменить, как в Windows (рис. 9.2), так и в Linux. Опытный взломщик может воспользоваться такой возможностью и подключиться к порту коммутатора.

> ***Примечание***
>
> **Если настройки сетевого адаптера не содержат возможности смены MAC-адреса, его можно изменить через реестр системы — изменив параметр `NetworkAddress` ключа `HKLM\SYSTEM\CurrentControlSet\Control\Class\<GUID сетевого адаптера>`. После изменения MAC-адреса желательно перезапустить сетевой интерфейс: отключить его и снова включить.**

Проверку MAC-адреса устройства часто используют интернет-провайдеры для контроля своих клиентов. При изменении MAC-адреса (замена сетевой карты, под-

---

[1] Разработка HP, см. **http://www8.hp.com/ru/ru/software-solutions/ips-intrusion-prevention-system/**.

[2] Эта атака использует особенности реализации протокола разрешения имен (ARP) и не зависит от реализации программного обеспечения.

ключение другого компьютера или установка роутера) требуется звонить провайдеру и сообщать новый MAC-адрес. Провайдер перенастраивает коммутатор, и только после этого становится возможным подключиться к Интернету.

На наш взгляд, это бесполезно. Например, представьте себе ситуацию: подключились вы к Интернету, маршрутизатора Wi-Fi у вас не было, и сотрудники провайдера записали MAC-адрес вашего компьютера. Спустя время вы купили маршрутизатор или новый компьютер — MAC-адреса у них другие, и надо дозваниваться до службы поддержки, а там как обычно: «все операторы заняты». Гораздо проще изменить MAC-адрес своего устройства программно, благо эта возможность есть в прошивке практически любого маршрутизатора. Поэтому в такой защите смысла нет — от квалифицированных взломщиков вы не защититесь, а лишь создадите неудобства и себе, и самым обычным пользователям.

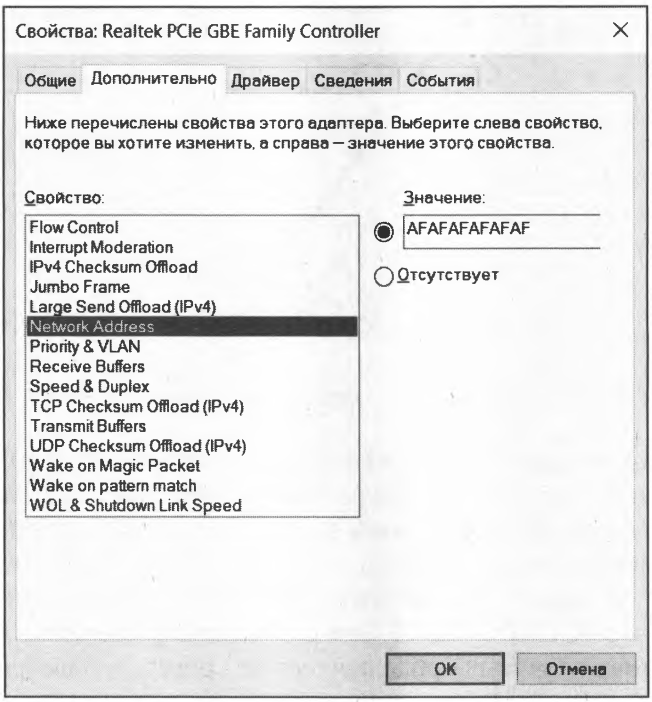


Рис. 9.2. Изменение MAC-адреса путем редактирования свойств адаптера

Протокол 802.1*x*

Наиболее безопасным средством контроля подключения к сети в настоящее время является использование протокола 802.1*x*, предназначенного 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 (рис. 9.3). Первоначально порт, к которому подключается устройство, находится в отключенном состоянии и может пропускать *только* пакеты процесса аутентификации (эти

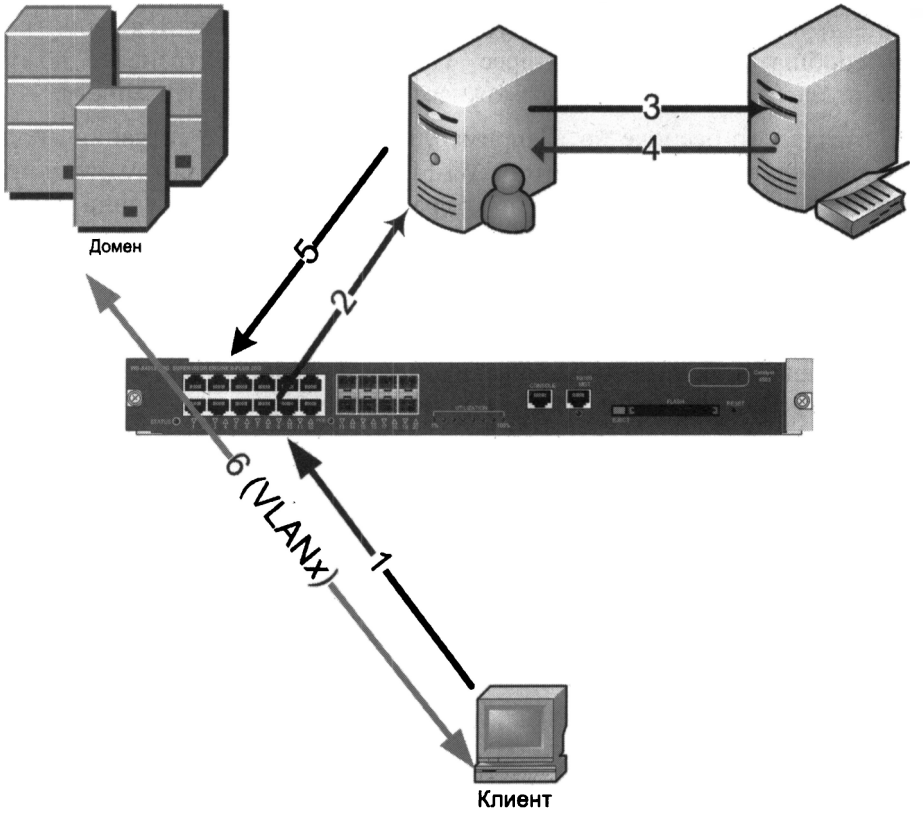


Рис. 9.3. Последовательность подключения клиента по протоколу 802.1*x*

пакеты передаются между подключаемым устройством и службой аутентификации). Подключаемое устройство можно идентифицировать (1) 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 сервер RADIUS (2). В сетях с централизованным каталогом сервер RADIUS проверяет параметры подключения на сервере каталогов (3), от которого получает данные аутентификации пользователя (4) и передает на коммутатор разрешение на открытие порта (5). После получения подтверждения от RADIUS порт коммутатора открывается для передачи информации в обоих направлениях (6). При этом RADIUS-сервер может сообщить коммутатору и номер VLAN, в которую должен быть помещен клиент.

В процессе аутентификации могут быть использованы различные технологии подтверждения устройства. Наиболее безопасным считается идентификация на основе сертификатов. Настройки этого варианта мы далее и рассмотрим.

Особенности применения протокола 802.1*x*

Протокол 802.1*x* следует использовать только на портах подключения *конечных* устройств. Применить его на уровне распределения и выше невозможно.

Стандарт предусматривает открытие порта после получения подтверждения идентификации устройства. Но если к порту коммутатора подключить небольшой сетевой концентратор с несколькими компьютерами, то после открытия порта аутентифицированным компьютером другие компьютеры, подключенные к этому концентратору, также смогут беспрепятственно работать в локальной сети.

Для предупреждения такой опасности можно применить несколько решений. Во-первых, включить на портах хотя бы тот же 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 — этот режим реализован не для всех моделей коммутаторов. Например, коммутаторы Cisco поддерживают режим single-host — когда через порт может работать только одно устройство, а описанный же в стандарте режим multiple-hosts допускает подключение к одному порту нескольких устройств, от чего и приходится дополнительно защищаться.

Если предприятие использует IP-телефонию, то подключение телефонных аппаратов и компьютера обычно осуществляется 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.

Есть ряд устройств, которые не поддерживают этот протокол: во-первых, это компьютеры, на которых установлены старые версии операционных систем; во-вторых, сетевые принтеры и аналогичные устройства. В таких случаях на соответствующих портах следует использовать иные методы контроля подключенных устройств (например, по MAC-адресам).

Настройка протокола 802.1*x*

Самый безопасный вариант настройки этого протокола — использование сертификатов при аутентификации компьютеров и пользователей.

В этом случае администратор должен обеспечить следующие настройки:

- ❒ настройку Центра сертификации;
- ❒ настройку службы каталогов;
- ❒ настройку службы RADIUS;
- ❒ настройку клиентского компьютера;
- ❒ настройку коммутатора.

Для аутентификации по протоколу 802.1*x* вам необходимо, чтобы, во-первых, клиенты имели соответствующие сертификаты; во-вторых, сертификат должен получить RADIUS-сервер.

Выдача сертификатов компьютерам

Для компьютеров, входящих в домен, удобно организовать автоматическую выдачу сертификатов. Это делается с помощью настройки групповой политики по следующему пути: **Конфигурация компьютера | Конфигурация Windows | Параметры безопасности | Политики открытого ключа | Параметры автоматического запроса сертификатов | Создать необходимый автоматический запрос**.

RADIUS-серверу также необходим специальный сертификат, который можно использовать при аутентификации по протоколу 802.1*x*. Этот сертификат могут выдать только центры сертификации, установленные на Enterprise-версии Windows-сервера. Их необходимо сначала опубликовать в центре сертификации[1], а затем на сервере, где запущена служба IAS (реализация службы RADIUS в Windows), открыть оснастку управления сертификатами *локального компьютера* с правами соответствующей учетной записи и запросить сертификат этого типа. После выполнения операции следует проверить наличие сертификата в соответствующем контейнере (рис. 9.4).

> ***Примечание***
>
> Если оснастка *certsrv.msc* у вас недоступна, необходимо установить службы сертификатов. Для этого откройте Windows PowerShell ISE и введите две команды:
>
> ```
> Add-WindowsFeature Adcs-Cert-Authority -IncludeManagementTools
> Install-AdcsCertificationAuthority -CAType EnterprisesRootCA
> ```

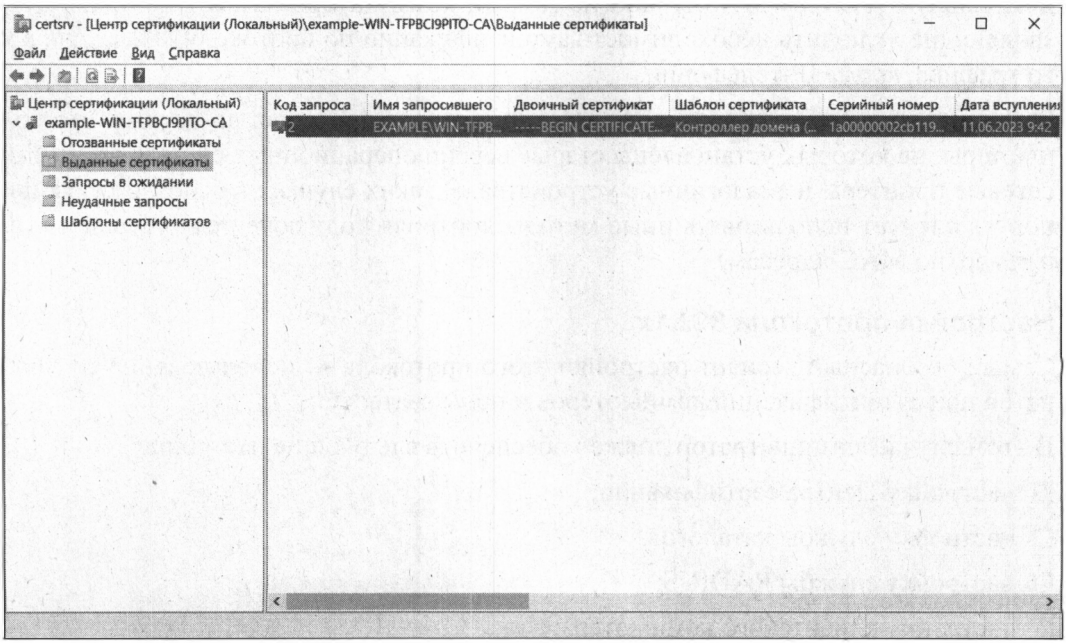


Рис. 9.4. Центр сертификации (certsrv.msc)

[1] Если эта оснастка у вас недоступна, инструкции по ее установке можно получить на сайте Microsoft: **https://docs.microsoft.com/ru-ru/windows-server/networking/core-network-guide/cncg/server-certs/install-the-certification-authority**.

Настройка службы каталогов

При подключении по протоколу 802.1*x* аутентифицироваться могут как компьютеры (их учетные записи в домене), так и сами пользователи. Политики подключения RADIUS-сервера проверяют членство соответствующих учетных записей в группах безопасности. Поэтому для предоставления права доступа создайте в службе каталогов соответствующие группы безопасности и включите в них требуемые объекты.

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 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.*

- *Клиент* — это коммутатор, который запрашивает у сервера RADIUS разрешение на включение порта. Каждый клиент должен быть зарегистрирован на RADIUS-сервере. Для этого необходимо ввести его IP-адрес и ключ. *Ключ* — это пароль, который должен быть одинаковым в настройках и 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.
- Возможность получения клиентом аутентификации от службы IAS всецело определяется *политиками удаленного доступа.* Обычно таких политик достаточно много (для различных вариантов подключения) — 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 той или иной VLAN в соответствии с данными аутентификации. Для этого данные от службы IAS должны возвращать соответствующие параметры. Покажем, как это сделать.

Создав политику удаленного доступа, откройте ее свойства и нажмите кнопку редактирования профиля. Выберите вкладку **Advanced** (Дополнительно) и добавьте следующие три атрибута (рис. 9.5):

- **Tunnel-Medium-Type** — со значением **802 (includes all 802 media plus Ethernet canonical format)**;

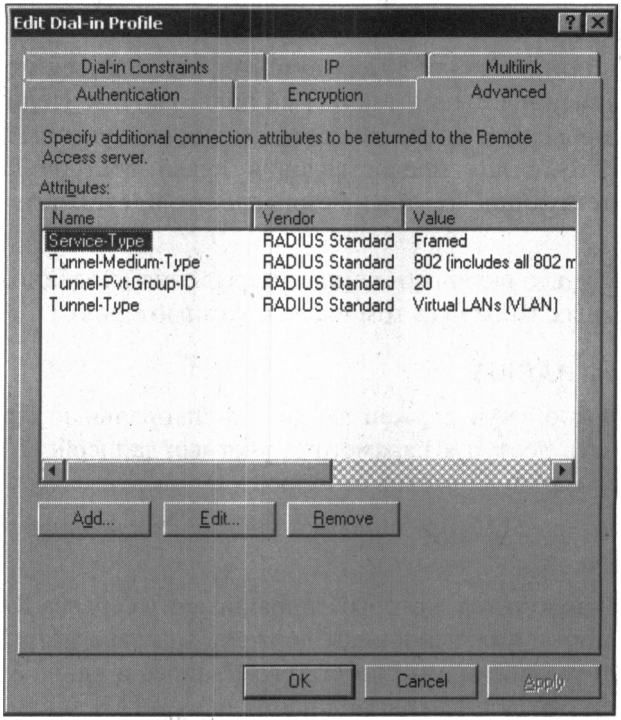


Рис. 9.5. Настройка атрибутов, используемых для автоматического назначения порта коммутатора в VLAN

- **Tunnel-Pvt-Group-ID** — со значением номера VLAN, в которую должен быть помещен порт в случае удачной аутентификации (на рис. 9.5 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.

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*. По умолчанию настройки предполагают использование для аутентификации именно сертификатов, так что никаких изменений данных параметров не требуется.

> ***Совет***
>
> Проще всего настроить эту службу на режим автоматического запуска с использованием групповой политики. Для этого следует открыть меню **Конфигурация компьютера | Конфигурация Windows | Параметры безопасности | Системные службы** и указать для службы **Беспроводная настройка** вариант автоматического запуска.

На следующем шаге 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**.

Настройка коммутатора

Настройки коммутаторов у разных вендоров различаются. Приведем в качестве примера вариант настройки коммутатора Cisco.

В этом 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
```

Затем 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*.

Технология NAP

Описанная ранее технология подключения по протоколу 802.1*x* подразумевает проверку только сертификата компьютера (или пользователя). Понятно, что этого мало, и ей на смену пришла технология NAP (Network Access Protection).

> ***Примечание***
>
> Название Network Access Protection используется корпорацией Microsoft, продукты других фирм могут носить иное имя — например, Network Access Control для продуктов Symantec Endpoint Protection.

Эта технология поддерживается серверами Windows Server 2008/2022, а в качестве клиентов могут выступать даже машины с Windows XP, но с установленным SP3 (хотя на сегодняшний день это мало кому интересно).

Технология NAP предусматривает ограничение использования ненадежными системами следующих сетевых служб:

- служб IPsec (Internet Protocol security protected communication);
- подключений с использованием протокола 802.1*x*;
- создания VPN-подключений;
- получения конфигурации от DHCP-сервера.

Идея очень проста — клиент, который хочет получить один из упомянутых здесь сервисов, должен предоставить о себе определенные данные. Существует возможность и проверки параметров, определенных центром безопасности сервера: наличия антивирусной программы, обновлений, настроек брандмауэра и т. п. Все эти данные предоставляются программой-агентом, которая запущена на клиентском компьютере. Если компьютер проходит проверку (его настройки соответствуют параметрам, заданным администратором), он получает сертификат, дающий право на использование запрашиваемых услуг. Если проверка не пройдена, все зависит от выбранных администратором настроек: или будет проведено обновление до нужного уровня безопасности, или будут наложены определенные ограничения в работе.

Подробно о внедрении NAP рассказано на сайте Microsoft по адресу: **https://technet.microsoft.com/ru-ru/network/bb545879**.

Обнаружение нештатной сетевой активности

Вирусная эпидемия или атака на информационную систему не возникают «вдруг». Обычно им предшествует некий период, характеризующийся повышенной нештатной сетевой активностью. Периодический анализ файлов протоколов систем и использование тех или иных *обнаружителей сетевых атак* могут предупредить администратора и дать ему возможность предпринять встречные шаги.

Хотя профессиональные программы, предназначенные для обнаружения сетевых атак, весьма 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. 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.

Приведем несколько бесплатных программ, которые часто применяются для сканирования сети:

- 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.

Следует отметить, что преобладание Linux-версий объясняется большими возможностями настройки этой операционной системы на низком уровне по сравнению с Windows-вариантами.

Контроль состояния программной среды серверов и станций

При эксплуатации системы администратор должен быть уверен в том, что на серверах и рабочих станциях отсутствуют известные уязвимости и что установленное программное обеспечение выполняет свои функции без наличия каких-либо закладок, недокументированных обменов данными и т. п. Понятно, что собственными силами проверить это невозможно, поэтому мы вынуждены доверять изготовителям программ и обеспечивать со своей стороны идентичность используемого комплекта ПО оригинальному дистрибутиву.

Индивидуальная настройка серверов

В большинстве случаев типичная (по умолчанию) конфигурация операционной системы позволяет сразу же приступить к ее использованию. При этом, также в большинстве случаев, система будет содержать лишние функции — например, службы, которые запущены, но не нужны вам. Такие функции в целях повышения безопасности следует отключать. Например, по умолчанию при установке Linux часто устанавливается веб-сервер (некоторые дистрибутивы грешат этим). Но он вам не нужен, — следовательно, вы его на безопасную работу не настраивали, и у него осталась конфигурация по умолчанию. Злоумышленник может использовать ненастроенные службы для атаки на вашу систему. Более того, поскольку вы считаете, что на том или ином компьютере веб-сервера нет, вы даже не будете контролировать на нем эту службу.

Именно поэтому все неиспользуемые службы нужно отключить. Включить их обратно, как только они вам понадобятся, — не проблема. Какие именно службы отключить, зависит от применения компьютера, поэтому привести здесь универсальные рекомендации на этот счет не представляется возможным.

Security Configuration Manager

В составе Windows Server присутствует программа Security Configuration Manager (SCM). Как видно из ее названия, SCM предназначена для настройки параметров безопасности сервера. Практически программа предлагает применить к системе один из шаблонов безопасности, выбрав ту или иную роль вашего сервера.

SCM привлекательна тем, что предлагает применить *комплексно* все те рекомендации, которые содержатся в объемных руководствах по безопасности. Однако в реальных системах редко можно найти серверы с «чистой» ролью — обычно присутствуют те или иные их модификации, заставляющие администратора тщательно проверять предлагаемые к назначению настройки. Поэтому установку SCM следует рассматривать только как первый шаг настройки сервера.

Security Compliance Manager

Microsoft разработала специальное средство для анализа и разворачивания на предприятии групповых политик безопасности — Microsoft Security Compliance Manager. Утилита доступна к бесплатной загрузке со страницы: **http://go.microsoft.com/fwlink/?LinkId=182512**. Установить ее можно на системы под управлением Windows 8/10/11 и Windows Server 2008/2022. При этом продукт требует сервера базы данных (бесплатная его версия может быть загружена и настроена в процессе установки утилиты).

> ***Совет***
>
> При установке продукта необходимо наличие подключения к Интернету — возможно, придется загрузить SQL Server Express. Кроме того, после установки продукт загружает с сайта Microsoft последние версии рекомендуемых параметров безопасности.

Microsoft подготовила и рекомендуемые параметры настроек безопасности для систем, предназначенных для эксплуатации в типовых условиях, в условиях предприятия и для организаций с повышенным уровнем безопасности. Эти рекомендации представляют собой наборы рекомендуемых параметров групповой политики для рабочих станций (Windows 8/10/11) и серверов (Windows Server 2008/2022). Обычно в конкретных условиях применить все рекомендации невозможно — например, какие-то компоненты, рекомендуемые для отключения, у вас предполагается использовать. Утилита Security Compliance Manager и предназначена для того, чтобы сравнить текущие параметры групповой политики с рекомендациями, отредактировать их и применить на предприятии эту групповую политику.

Исключение уязвимостей программного обеспечения

Ошибки наличествуют во всех программных продуктах, они свойственны как самим операционным системам, так и прикладному программному обеспечению. Уязвимость в программном обеспечении потенциально позволяет злоумышленнику получить доступ к данным в обход защиты. Поэтому установка обновлений 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.

> ***Примечание***
>
> 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 «заплаток», но и некоторые усовершенствования и дополнения основных программ и т. п. В рассматриваемом контексте для нас не актуальны эти различия.

Уязвимости и эксплойты

Каждый день в том или ином программном обеспечении обнаруживаются какие-нибудь уязвимости. А вот «заплатки», позволяющие закрыть «дыры» в информационной безопасности, выпускаются не так регулярно, как этого бы хотелось.

Другими словами, с момента обнаружения уязвимости и до установки «заплатки» (заметьте, не до выхода, а до установки — «заплатка» уже вышла, а администратор ничего о ней и не подозревает) может пройти внушительное время. За это время кто-либо может воспользоваться уязвимостью и взломать вашу систему.

Чтобы воспользоваться уязвимостью, не нужно быть «крутым хакером» — достаточно подобрать *эксплойт* (специальную программу, которая реализует эту уязвимость) и применить его к вашей системе. Найти эксплойт довольно просто — надо лишь уметь пользоваться поисковыми системами. В результате обычный пользователь получает инструмент, позволяющий ему, например, повысить свои права до уровня администратора или «свалить» сервер предприятия. Можно рассуждать о причинах такого поведения, но авторам неоднократно приходилось сталкиваться с наличием подобного пользовательского интереса. На сайте **http://www.metasploit.com/** доступен бесплатный сканер уязвимостей, который можно использовать как для тестирования «дыр», так и для выбора метода атаки системы.

Информация о найденных уязвимостях разработчиками ПО тщательно скрывается до момента выпуска исправлений программного кода. Однако этот факт не гарантирует отсутствие «прорех» в защите систем, которые уже начали эксплуатироваться злоумышленниками.

Поэтому своевременная установка «заплаток» является необходимым, но недостаточным средством обеспечения безопасности данных.

Как узнать об обновлениях?

Информация об уязвимостях публикуется на специальных сайтах. Вот некоторые из них:

- SecurityFocus: **http://www.securityfocus.com**;
- CERT vulnerability notes: **http://www.kb.cert.org/vuls/**;
- Common Vulnerabilities and Exposures (MITRE CVE): **http://cve.mitre.org**;
- SecurityLab: **http://www.securitylab.ru/vulnerability/**;
- IBM Internet Security Systems: **http://xforce.iss.net**.

Эти сайты нужно регулярно просматривать или же подписаться на существующие у них рассылки.

Проверка системы на наличие уязвимостей

При желании можно самостоятельно произвести проверку системы на наличие уязвимостей. Программ для такой проверки предостаточно: RkHunter, OpenVAS, SATAN, XSpider, Jackal, Strobe, NSS — как платных, так и бесплатных. Информацию об этих сканерах вы без проблем найдете в Интернете. Например, следующие статьи объясняют, как использовать RkHunter и OpenVAS соответственно:

- **http://habrahabr.ru/company/first/blog/242865/**;
- **http://habrahabr.ru/post/203766/**.

Администратор может воспользоваться и любой программой, предназначенной для анализа безопасности компьютерных систем. Сегодня на рынке подобных продуктов представлено множество. 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.

Если необходимо сертифицированное решение, то можно использовать программу XSpider, которая имеет сертификат ФСТЭК России. Окно этой программы показано на рис. 9.6.

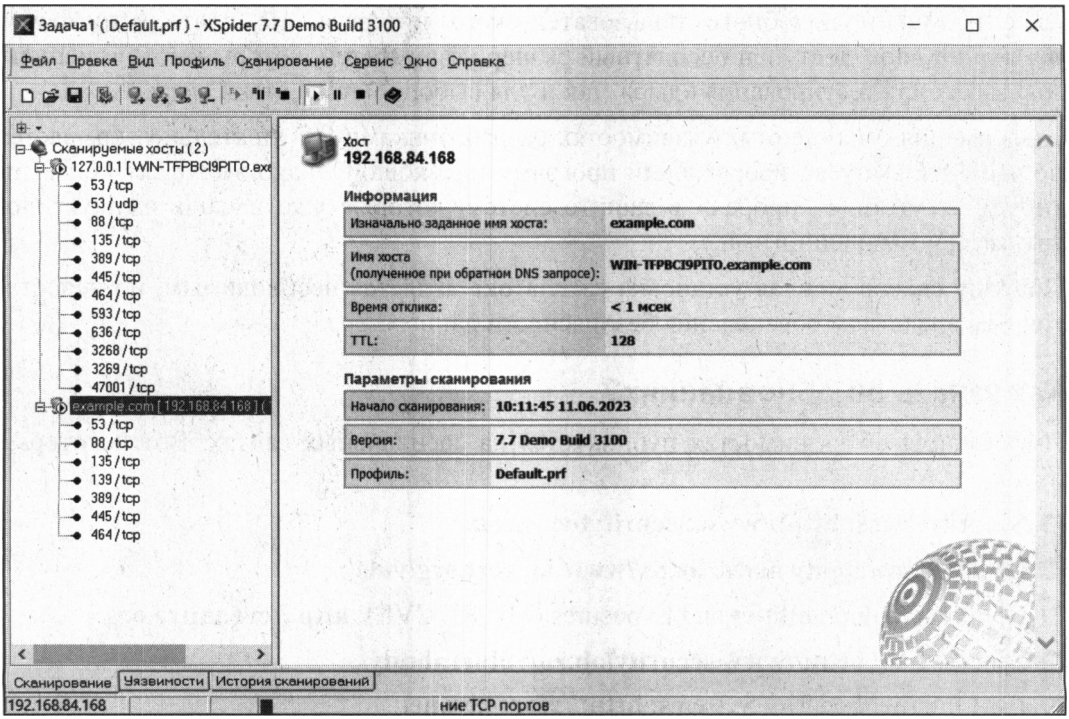


Рис. 9.6. Программа XSpider

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 обновлений

К сожалению, сами обновления также 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. Авторам 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 предприятия.

Поэтому администратор поставлен перед дилеммой: применить обновление и рисковать стабильностью работы системы или не применять и ждать, что атака злоумышленника минует компьютеры небольшого и незаметного предприятия.

Разработчики программного обеспечения советуют в обязательном порядке *тестировать* все устанавливаемые на рабочие компьютеры обновления. Тестирование должно проводиться в типовой для вашего предприятия 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 малого или среднего предприятия практически нереально, но проверить хотя бы возможность загрузки компьютера и правильность выполнения основных бизнес-процессов — вполне возможно.

> ***Совет***
>
> Ставьте полученные обновления сначала не на основные компьютеры — в частности, попробуйте провести 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 предприятия, если такое восстановление придется проводить сразу после применения обновления?

Обновления операционных систем Linux

Современные операционные системы Linux поддерживаются выпуском «заплат» на обнаруженные уязвимости. Этот процесс можно автоматизировать (запускать обновления по графику с использованием демона cron) или же устанавливать обновления вручную.

Операции выполняются по правилам соответствующей версии операционной системы. Например, для операционной системы Ubuntu ручное обновление выполняется двумя командами:

```
# apt-get update
# apt-get upgrade
```

Первая команда обновляет локальный список информации о пакетах, вторая — устанавливает новые версии пакетов, т. е. производит само обновление.

В отличие от Windows-систем, при установке обновлений на серверы Linux (без графической подсистемы) крайне редко требуется перезагрузка. Что же касается стабильности, то нами были замечены редкие проблемы только при обновлении программ с графическим интерфейсом, а поскольку такие программы на сервере не устанавливаются, беспокоиться об этом вообще не стоит.

Для обновления в графическом режиме рабочих станций Linux задействуются мастера операций, автоматически запускаемые в случае обнаружения исправлений.

Индивидуальные обновления Windows-систем

Обновления систем Windows 8/10/11 и Windows Server 2008/2022 организуются через Центр обновления, который проверяет наличие обновлений и производит их установку. Как можно видеть на рис. 9.7, Центр обновления показывает количество важных и необязательных обновлений, а также позволяет просмотреть и выборочно установить обновления (рис. 9.8).

Для серверов режим автоматической установки не является оптимальным, поскольку сервер обычно достаточно плотно нагружен: в рабочее время обслуживает поль-

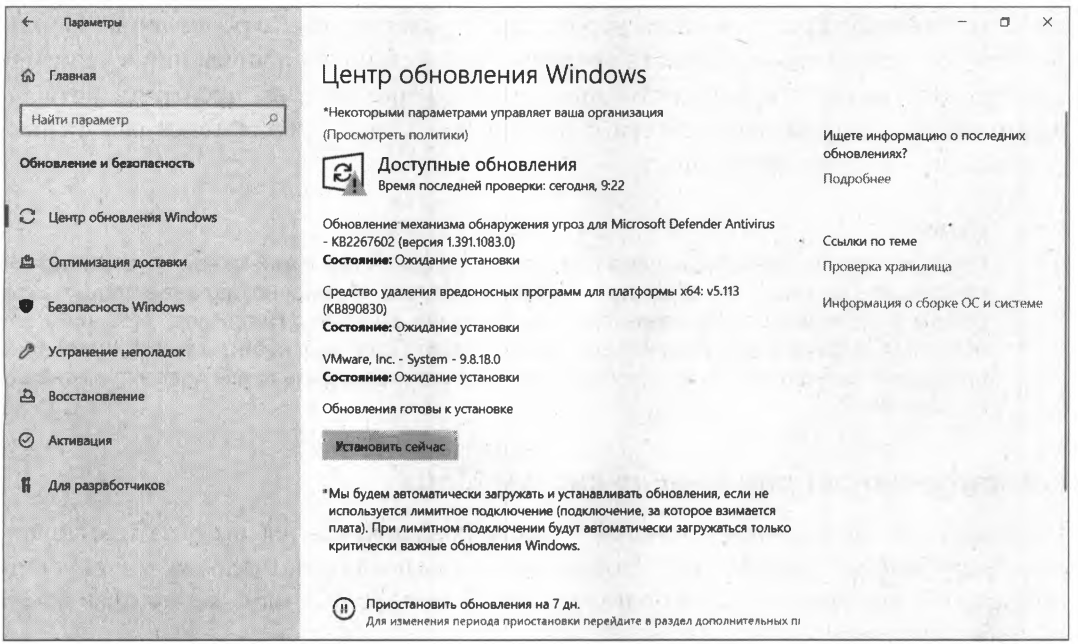


Рис. 9.7. Центр обновления Windows (Windows Server 2022)

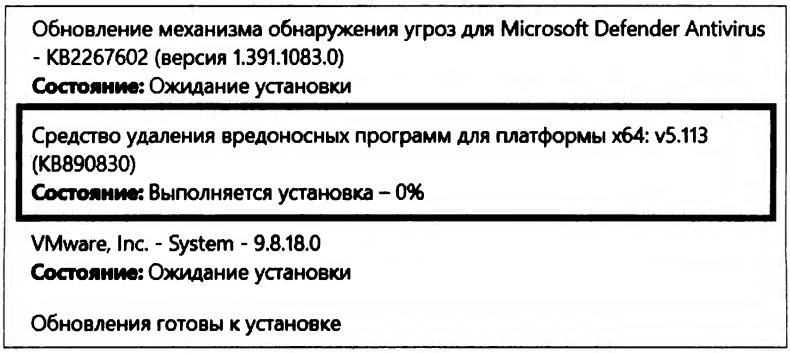


Рис. 9.8. Установка обновлений (Windows Server 2022)

зователей, ночью выполняются сервисные операции. Поэтому незапланированная операция перезагрузки может быть нежелательна. Вследствие этого мы советуем выполнять установку обновлений только в ручном режиме под контролем оператора сервера.

Обновление Windows-систем на предприятии

Обновление Windows-систем на предприятии имеет несколько особенностей:

- во-первых, обновления от Microsoft часто весьма объемны по размеру, и их одновременная загрузка на несколько систем может негативно сказаться на доступе в Интернет даже на безлимитных тарифах, не говоря уже про экономию для тарифов с оплатой за трафик;
- во-вторых, установка обновлений должна быть контролируемой: обновления должны авторизоваться (получать разрешение от администратора на установку, лучше всего — после тестирования), операции нужно проводить по графику, с учетом типа компьютеров (отбор по группам, площадкам и т. п.), весь процесс должен протоколироваться с возможностью легкого составления отчетов по результатам.

В этих целях целесообразно использовать *службу автоматического обновления* — Windows Software Update Services (WSUS). Она распространяется бесплатно и предназначена для установки как обновлений операционной системы Windows, так и ряда других продуктов Microsoft.

Сама служба представляет собой приложение, работающее на веб-сервере IIS. Поэтому для ее установки необходимо выполнить ряд условий (установить компоненты). Для установки службы воспользуйтесь мастером добавления ролей и компонентов в Windows Server 2008/2022 (рис. 9.9).

Архитектуру обновления можно построить по нуждам предприятия: служба допускает виртуализацию, каскадирование (загрузку обновления с другого сервера WSUS), балансировку нагрузки (обслуживание инфраструктуры несколькими серверами) и т. п.

Основные настройки службы (параметры прокси-сервера, выбор продуктов, для которых закачиваются обновления, настройка языков, графика синхронизации и пр.) выполняются во время установки продукта, но их можно уточнить и в консоли службы. После установки компьютеры необходимо разбить по группам (в зависимости от требований к установке обновлений) и настроить режимы (например, автоматическое согласие на установку определенной категории обновлений и т. п.).

Чтобы клиенты выполняли установку обновлений с сервера WSUS, надо в групповой политике явно указать имя сервера, с которого будет осуществляться обновление.

Для индивидуальной настройки системы на локальный сервер WSUS (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 WSUS-сервер (например, **http://wsus**).

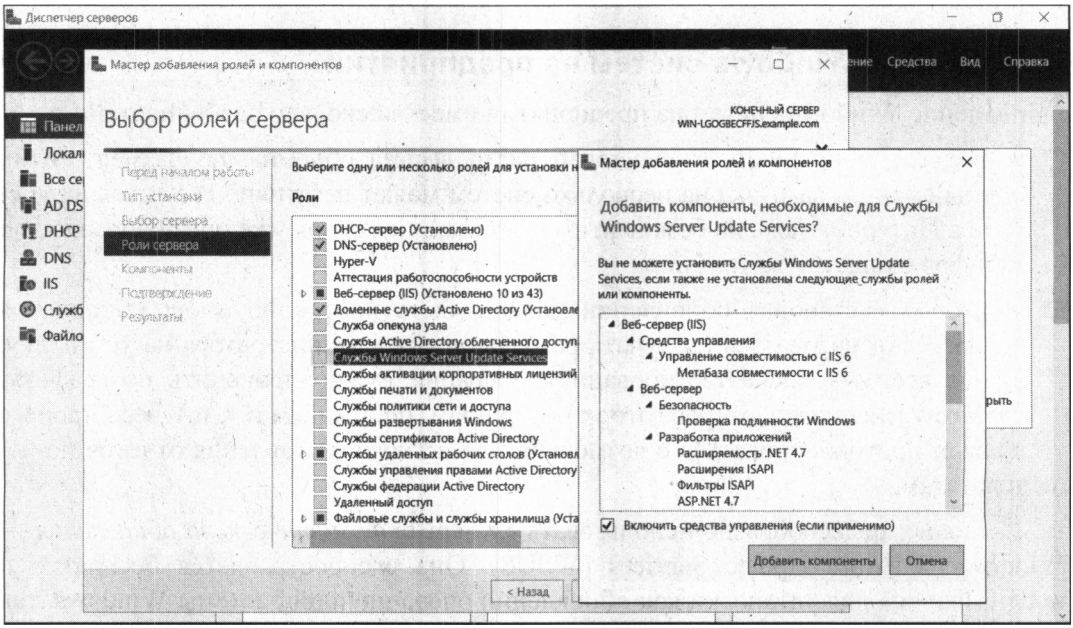


Рис. 9.9. Установка Службы WSUS в Windows Server 2022

Установка обновлений через групповые политики

Обновления можно устанавливать с помощью групповых политик. К такому способу допускается прибегать, например, при необходимости срочного развертывания «заплатки».

Специально для автоматизации установки обновления выпускаются в MSI-формате. Загрузив файл обновления, его следует распаковать в папку на локальном диске, запустив с ключом `-x`. Затем, используя программу редактирования групповой политики, можно создать пакет установки, импортировав MSI-файл из этой папки. Единственное неудобство такого решения — необходимость создания различных политик, учитывающих установленную версию операционной системы и программ MS Office. Но поскольку в малых и средних предприятиях обычно придерживаются однотипности устанавливаемого ПО, подобные действия не должны вызвать у администратора затруднений.

Защита от вредоносных программ

Часто с целью кражи или уничтожения информации совершаются попытки установки на компьютер какой-либо вредоносной программы. Этих программ настолько много, что для исключения таких ситуаций создан специальный класс программ — программы защиты хоста.

Программы защиты хоста позволяют заблокировать запуск вредоносных программ, а также исключить установку троянов и руткитов (вредоносного кода, который может использоваться для кражи данных). Обычно весь вредоносный код вместе с троянами и руткитами называется *malware-программами* — от *англ.* malicious software (буквально «вредоносное ПО»).

На рис. 9.10 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.

Рис. 9.10. Интерфейс программы Symantec Endpoint Protection

Примечание

Руткит (rootkit) — программа, использующая технологии маскировки своих файлов и процессов. Эта технология широко применяется, и не только злоумышленниками. Например, антивирусная программа Kaspersky Antivirus использует эту технологию для сокрытия своего присутствия при чтении NTFS-данных.

В корпоративной среде для централизованного управления защитой всех рабочих станций можно использовать программу Symantec Endpoint Protection Manager (рис. 9.11). Помимо централизованного управления программа поддерживает развертывание программы Symantec Endpoint Protection на рабочих станциях.

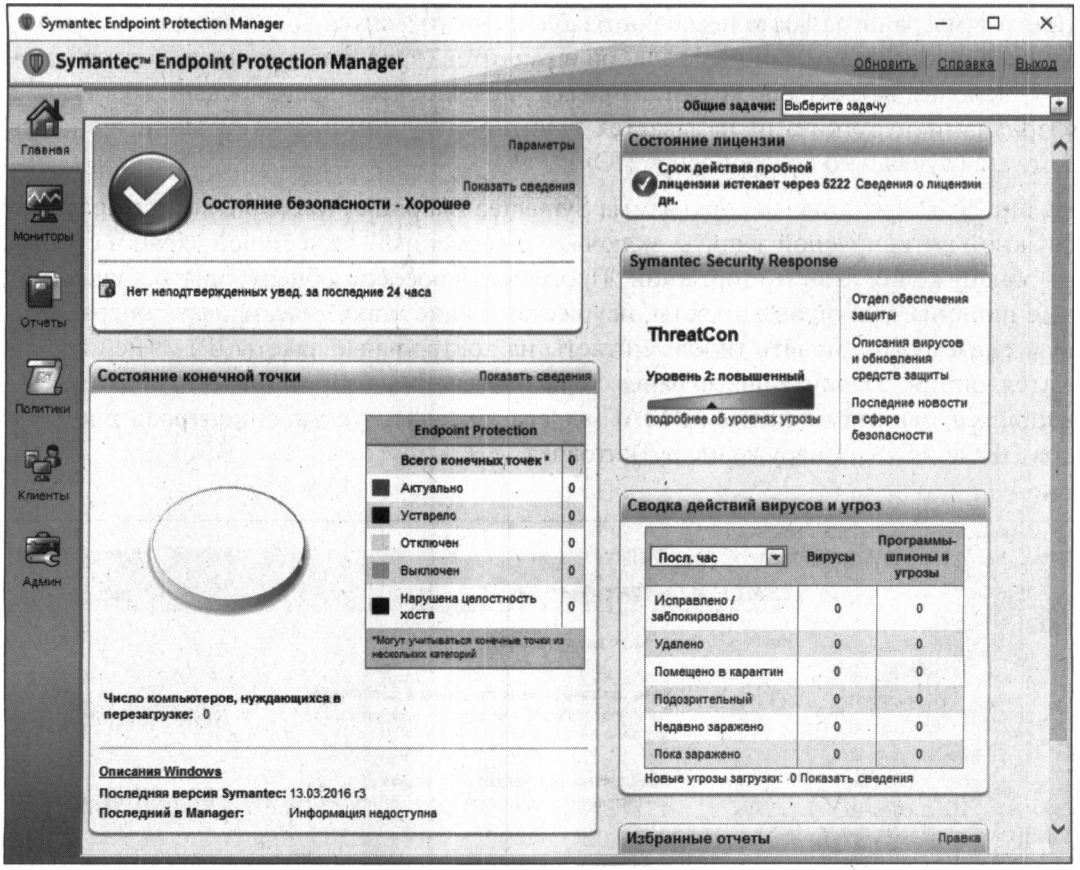


Рис. 9.11. Интерфейс программы Symantec Endpoint Protection Manager

Использовать в корпоративной среде индивидуальные версии антивирусных программ нецелесообразно — они пригодны только для небольших предприятий. Корпоративные же решения, подобные Symantec Endpoint Protection Manager, позволяют настроить единые правила защиты (например, профили для работы в локальной сети и в публичной с автоматическим переключением при смене места нахождения и т. п.), снизить объем загружаемых обновлений (обновления будут получены из Интернета только один раз, а потом просто распространены по локальной сети), централизованно настроить опции антивирусной защиты и т. п.

Symantec Endpoint Protection Manager — не единственное корпоративное решение. Аналогичные решения есть у Dr.Web (Dr.Web Enterprise Security Suite), у Лаборатории Касперского (Kaspersky Endpoint Security для бизнеса) и у других разработчиков средств защиты информации.

В процессе выбора средства защиты конфиденциальной информации обращайте внимание на наличие сертификата ФСТЭК. Как правило, разработчики предлагают как обычные, так и сертифицированные версии. Последние стоят дороже. Если вы уже приобрели лицензионную версию программы, то, как правило, вам предоставляется возможность докупить сертифицированную версию или пакет сертифика-

ции, — как, например, у Касперского (причем, нужно отметить, что цена пакета сертификации более чем лояльная).

График обновления антивирусных баз

В последнее время вирусы в мире распространяются очень быстро — на второй-третий день после начала распространения они захватывают большинство существующих компьютерных систем. Как правило, обновления антивирусных баз появляются через несколько часов после обнаружения вирусов, поэтому имеет смысл настроить автоматическое обновление антивирусных баз несколько раз в сутки, — скажем, каждые 5 часов. Однако не каждая антивирусная программа позволяет настроить точный (и малый) интервал времени обновления баз данных — предлагаются варианты: раз в день, раз в неделю и т. д. Так что выбирайте минимальный предлагаемый интервал обновления. Например, из приведенных вариантов — ежедневное обновление.

Внимательность пользователя

Во многом уровень безопасности системы зависит от сознательности и внимательности пользователей. Пользователям не следует переходить по сомнительным ссылкам, в том числе в электронных письмах, нельзя также открывать любые вложенные в письма файлы. Таким путем можно перекрыть один из самых часто используемых способов распространения компьютерных вирусов — по электронной почте.

Среди сотрудников предприятия надо распространить инструкции по предотвращению инфицирования вирусами. Вот один из вариантов такой инструкции — вы можете дополнить ее в зависимости от специфики вашего предприятия:

- запрещается как-либо вмешиваться в работу антивирусных программ;

  Пояснение

  Как правило, такого вмешательства можно избежать, если соответствующим образом настроить систему и саму антивирусную программу. Тем не менее интерфейс программы может предоставлять выбор различного режима работы программы, в том числе и отключение антивирусной защиты. Ни в коем случае нельзя разрешать пользователям изменять режимы работы антивируса.

- запрещается переходить по ссылкам в социальных сетях «ВКонтакте», «Одноклассники» и пр., какими бы текстами они ни заманивали. Сами социальные сети не содержат вирусов, однако они могут содержать ссылки, ведущие на страницы с вирусами;
- нельзя открывать файлы, отправленные вам в качестве вложений. Если кто-либо должен отправить вам файл с вложением по электронной почте, пусть он вас каким-то образом предупредит (например, по телефону, через Skype, через другие какие-либо мессенджеры или по электронной почте — в предварительном письме). Если вы не ждете никаких вложений (документов, фото и т. д.), лучше их не открывать;

- нельзя переходить по ссылкам, содержащимся в электронном письме, особенно от неизвестного адресата. Однако даже компьютер ваших коллег может быть инфицированным, поэтому — никаких ссылок! Как и в случае с вложениями — если вам должны отправить ссылку, пусть сначала предупредят об этом;
- все съемные диски (CD/DVD, USB) перед использованием размещенной на них информации нужно проверять антивирусом, даже SD-карты фотоаппаратов!
- запрещается загружать и запускать так называемые Portable-версии программ.

> ***Пояснение***
>
> Подразумевается, что сотрудники работают в системе с правами обычного пользователя и устанавливать программы стандартным способом не могут. Зато они могут скачать Portable-версии программ, которые, как правило, распространяются на сайтах, содержащих пиратское ПО. Часто бывает, что вместе с таким ПО распространяются и вирусы, «зашитые» или в саму программу, или в генератор ключа для нее. Если нужно запустить такую программу, делайте это в виртуальной машине без подключения к сети. Только после тщательного анализа программы можно начать использовать ее на реальных машинах.

Выполнение этих простых правил поможет существенно снизить риск инфицирования системы.

Обезвреживание вирусов

Если компьютер оказался поражен вирусом, 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 антивирусной программы и выполнить полную проверку системы. Для выявления имени вируса следует воспользоваться сканированием системы — например, с флешки или посредством онлайнового антивирусного сервиса. 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.pandasecurity.com/activescan/index/**

  и многие другие.

При работе в составе локальной компьютерной сети можно воспользоваться также возможностью антивирусных программ осуществлять проверку сетевых ресурсов.

Если антивирусная программа на компьютере не установлена, то следует первоначально провести его проверку на вирусы, используя заведомо «чистое» программ-

ное 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» флешки или с компакт-диска. Вот примеры таких программ:

- Dr.Web CureIt: **http://www.freedrweb.com/cureit/** — поможет, если Windows еще запускается и относительно нормально работает;
- Dr.Web LiveDisk: **http://www.freedrweb.ru/livedisk/** — загрузочный диск. Преимущество этого способа в том, что вирус на жестком диске будет находиться в незапущенном состоянии и не только не сможет вам помешать, но и не будет дальше размножаться. Следует загрузить файл LiveDisk на неинфицированный компьютер, записать образ на «болванку» и загрузиться с него на инфицированной системе;
- AdwCleaner: **https://ru.malwarebytes.com/adwcleaner/** — средство очистки от рекламного программного обеспечения. Порой такое ПО досаждает не меньше вирусов.

После ликвидации вирусов нужно установить/переустановить (если она была повреждена вирусом) антивирусную программу и обновить ее антивирусную базу данных.

Защита от вторжений

Антивирусные программы проверяют файлы, сохраняемые на носителях, контролируют почтовые отправления и т. п. Но они не могут предотвратить атаки, базирующиеся на уязвимостях служб компьютера. В таких случаях опасный код содержится в передаваемых по сети данных, а не хранится в файловой системе компьютера.

Программы защиты хоста включают и 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 этих сигнатур нуждается в постоянном обновлении с центрального сервера. Обычно обновление осуществляется единой операцией.

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 с локального компьютера и отсылают в Сеть информацию — например, о предпочтениях пользователя при посещениях сайтов. А иногда и передают злоумышленнику данные, вводимые пользователем при работе с сайтами интернет-банкинга.

Часть таких программ обнаруживается системами защиты, и их работа блокируется. Но многие программы не детектируются как вирусы, поскольку их действия часто идентичны типовым операциям пользователя. Обнаружить такие *программы-трояны* весьма сложно. Поэтому важно периодически осуществлять контроль запущенного на компьютере программного обеспечения.

Существует специальный класс программ, специализированных на поиске троянов. В качестве примера можно привести Adaware от компании LavaSoft, которую можно найти на сайте **https://www.adaware.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.

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 Интернета, разрешить выполнение только подписанных электронной подписью сценариев и т. п.

Поскольку администраторам достаточно часто приходится самостоятельно заниматься поиском троянских программ, опишем основные способы их автоматического запуска. Итак, вредоносный код может быть запущен с использованием:

- файлов autoexec.bat и config.sys — такой вариант используется нечасто, поскольку новые операционные системы обычно не учитывают параметры этих файлов. Они задействовались при старте компьютера в Windows XP и более ранних версиях системы, в Windows 7 остались по инерции, а в новых версиях (8/10/11) этих файлов нет;
- файла win.ini — хотя этот файл сохраняется лишь в целях обратной совместимости, но включение программ в строки `run` и `load` этого файла позволяет обеспечить их запуск системой;
- папки **Автозагрузка** для всех пользователей и профиля текущего пользователя — достаточно просто проверить содержимое этой папки, чтобы обнаружить такую программу;
- ключей реестра, описывающих автоматически загружаемые программы:

```
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
HKCU\Software\Microsoft\Windows\CurrentVersion\Run
StartUp Folder
HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce
```

Примечание

Параметры `RunServices` **и** `RunServicesOnce` **не используются в новых версиях ОС.**

Администратор домена через групповую политику может отключить при старте системы автоматический запуск программ, определенный в параметрах `Run` и `RunOnce`. Для этого используется меню **Конфигурация компьютера | Административные шаблоны | System | Logon** | с параметрами **Do not process...** и аналогичное меню 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
```

- браузера Browser Helper Object (BHO) — в Windows имеется возможность встраивать в Internet Explorer специально разработанные программы, призванные расширить функциональность этого обозревателя. Поскольку такие программы имеют практически неограниченные права доступа к локальной системе, хакеры часто используют эту технологию для отслеживания действий пользователя, для показа рекламы, перенаправления на порносайты и т. п.

  Эти программы подключаются по их GUID через ветвь реестра:

  ```
  HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper
  Objects
  ```

  Поскольку среди таких программ присутствуют и полезные расширения, то при анализе системы необходимо найти в реестре программу, зарегистрировавшую тот или иной GUID. Помочь в быстром поиске BHO могут такие утилиты, как HijackThis[1];

- некоторых других ключей, которые обычно не приводятся при описании возможных вариантов автозапуска программ, однако возможность использования которых также нельзя исключать:

[1] См. **http://www.spywareinfo.com/~merijn/files/hijackthis.zip**.

```
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
```

Авторам 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[1] (рис. 9.12);

- запуска программ через назначения 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 наличии у модуля

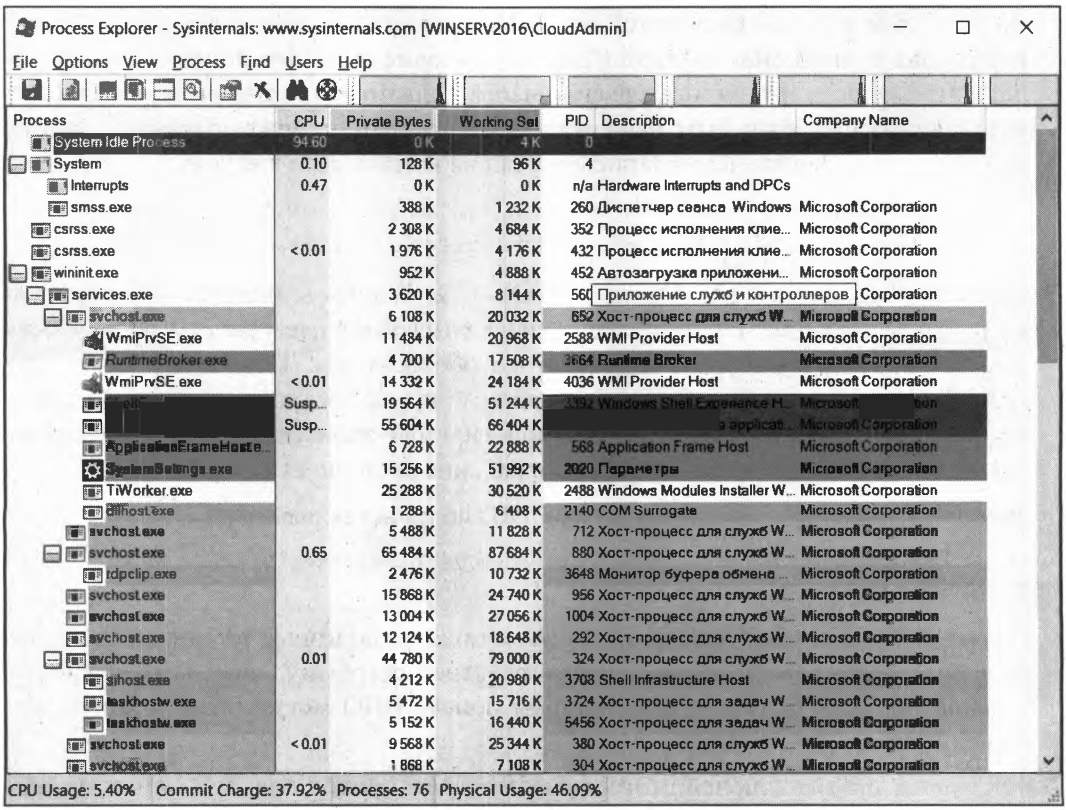


Рис. 9.12. Программа Process Explorer позволяет увидеть иерархию запущенных в системе процессов

[1] См. **https://learn.microsoft.com/en-us/sysinternals/downloads/process-explorer**.

электронной подписи. Кроме того, в любой момент можно просмотреть установленные модули (меню **Свойства обозревателя** | вкладка **Общие** | **Параметры** | кнопка **Просмотр объектов**) и удалить ненужные;

- служб и драйверов — 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. Обнаружить такой код крайне сложно. Здесь следует использовать специализированные средства (если программа защиты хоста не блокирует код) по обнаружению руткитов — например, RootkitRevealer[1].

Редактирование списка автоматически загружаемых программ

Список автоматически загружаемых программ можно редактировать при помощи утилиты msconfig или вкладки **Автозагрузка** Диспетчера задач, что характерно для Windows 10/11 (рис. 9.13). Утилита показывает как элемент автозагрузки, так и

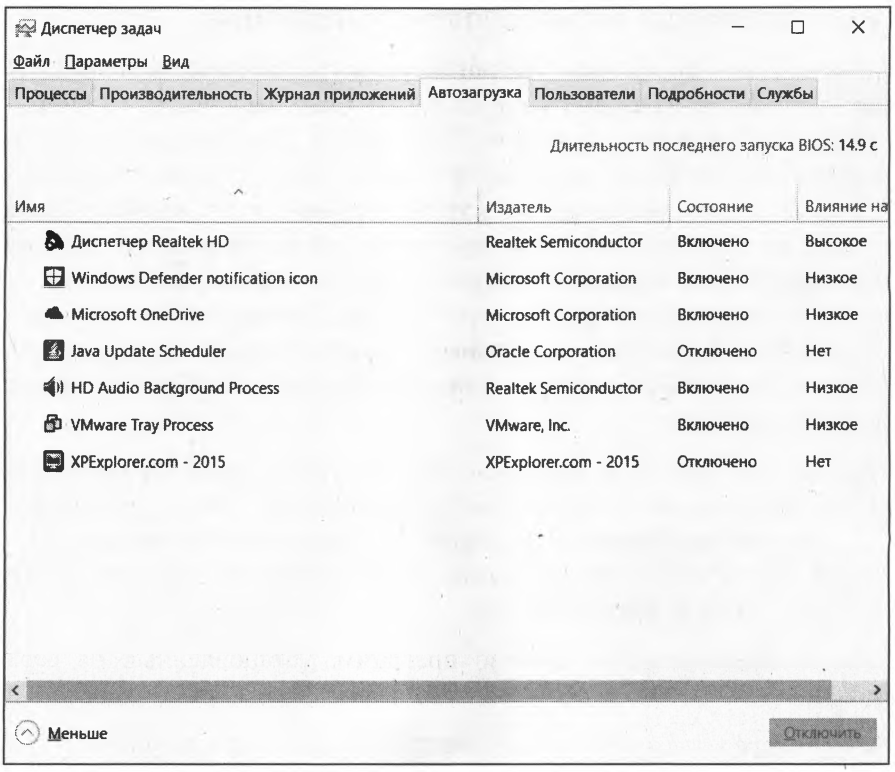


Рис. 9.13. Диспетчер задач: вкладка **Автозагрузка**

[1] См. **https://technet.microsoft.com/ru-ru/sysinternals/bb897445**.

путь его запуска и позволяет отключать загрузку элемента. В Windows 7 эта утилита позволяет отключать даже службы. Правда, в более новых версиях Windows для управления службами используется только оснастка services.msc (впрочем, ее можно использовать и в Windows 7). В Windows 10/11 службами можно управлять с помощью вкладки **Службы** Диспетчера задач (см. рис. 9.13).

Безопасность приложений

Сколь бы хорошо ни защищалась операционная система, сколь бы правильно ни были написаны фильтры и политики брандмауэров, но если прикладное программное обеспечение или его уязвимости позволят получить доступ к защищенным данным, то все предпринятые усилия окажутся напрасными. Примеры такого поведения программ легко можно найти в Интернете: в смартфоны встроены программы, мониторящие активность пользователя, клиент Skype позволяет принять вызов от человека, не входящего в список контактов (это означает, что из внешней сети есть доступ к локальному компьютеру с возможностью выполнения действий, не разрешенных пользователями) и т. п.

Основные принципы безопасности приложений

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, не предназначенные 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 с 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 вашего предприятия.

Проконтролировать действия установленных программ практически невозможно. Наиболее рациональный выход — это использование ПО с открытым кодом, поскольку залогом его безопасности является независимая экспертиза. Но в силу объективных обстоятельств это возможно далеко не всегда. Поэтому следует придерживаться нескольких принципов:

- ограничьте минимумом количество программ, установленных на серверах и станциях;
- используйте средства контроля запуска программного обеспечения;
- исключите возможность передачи данных с серверов в сеть Интернета (заблокируйте, например, по их IP-адресам);
- по возможности используйте программы анализа поведения.

Единый фонд дистрибутивов и средства контроля запуска программного обеспечения

Для обеспечения безопасности приложений также необходимо:

- во-первых, добиться, чтобы на предприятии существовал единый фонд дистрибутивов и все установки программ на рабочие станции и серверы выполнялись только из проверенного источника;
- во-вторых, включать средства контроля запуска программ. Максимально безопасный вариант — запретить запуск любых программ по умолчанию и создать исключения: те программы, которые необходимы для работы. Контроль запуска программ можно реализовывать через групповые политики (вариант описан в *главе 6*), но более тонкие настройки можно выполнить, применяя программы защиты хоста.

На рис. 9.14 показан пример выбора параметров, которые можно использовать при формировании правил запуска в программе Symantec Endpoint Protection. При помощи подобных настроек: контроля доступа к параметрам реестра, к файлам и папкам, попыткам запуска или прекращения процесса, загрузки библиотек — можно очень точно настроить правила разрешения и блокирования.

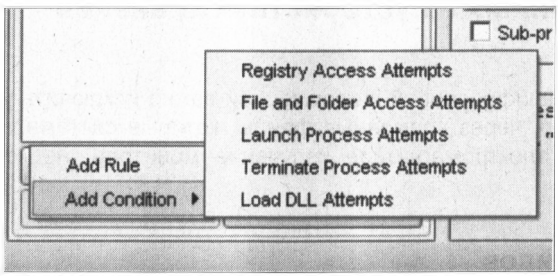


Рис. 9.14. Выбор критериев правил контроля запуска ПО

Неизменность системы

Одним из способов защиты системы от вредоносного кода является запрет на внесение изменений на локальный диск. Традиционный совет для тех, кто не хочет «подхватить» что-либо в Интернете, заключается в загрузке при путешествиях по Сети с какого-либо LiveCD. Кстати, Microsoft подготовила специальную модификацию для Windows, предназначенную для интернет-кафе и игровых клубов, которая возвращает состояние системы к начальному после каждой перезагрузки.

Аналогичные решения присутствуют и среди бесплатных продуктов. Например, по адресу **http://www.bitdisk.ru/** доступна программа BitDisk, которая также может контролировать запись изменений во время работы системы. Бесплатная версия программы после перезагрузки системы возвращает состояние к тому моменту, на котором эта функция была включена. Платная версия позволяет переключаться между режимами без перезагрузки и выбирать режимы сохранения изменений на локальный диск.

Защита от утечки данных

Во время работы компьютера доступ к информации контролируется средствами операционной системы и программного обеспечения. Порядок настройки прав доступа не представляет особой сложности и успешно реализуется администраторами. Но как только данные выходят из-под контроля операционной системы (например, компьютер выключается или данные переносятся на сменный носитель), то исключить их попадание в чужие руки крайне сложно.

Шифрование данных

Шифрование данных на сегодня является самым надежным способом обеспечения конфиденциальности информации.

Применение шифрования ограничено действующим законодательством (например, требуется лицензия, необходимо применять только сертифицированные алгоритмы шифрования и т. п.), но на практике существует и применяется много иных вариантов кодирования данных.

Шифрование данных на устройствах хранения

> ***Примечание***
>
> При работе с зашифрованной информацией важно исключить утечку по другим каналам — например, через временные файлы, которые система создает при обработке данных, через электромагнитное излучение монитора, на котором воспроизведен текст, и т. п.

Шифрование архивов

Шифрование при архивировании — самый простой способ, но далеко не самый надежный. Для многих архиваторов существуют программы подбора паролей, и, учитывая склонность пользователей к простым вариантам паролей, информация из архивов может быть вскрыта за конечное время.

Нужно также учитывать, что коммерческие варианты архиваторов могут иметь так называемые *инженерные* пароли, с помощью которых соответствующие службы при необходимости прочтут зашифрованные вами данные.

Бесплатные программы шифрования данных

Существует несколько программ, которые позволяют шифровать данные с высокой степенью надежности. Мы же хотим здесь порекомендовать форк популярной утилиты TrueCrypt — программу шифрования VeraCrypt[1]. Это бесплатное кроссплатформенное решение, версии которого есть для Windows, macOS и Linux. Косвенно качество программы подтверждает факт ее применения в вооруженных силах

[1] См. **https://www.veracrypt.fr/en/Home.html**.

Израиля. При желании вы можете использовать и саму TrueCrypt (если раздобудете), но скачать ее с официального сайта уже не получится.

> ***Примечание***
>
> К сожалению, разработчики прекратили поддержку TrueCrypt, о чем официально объявили на своем сайте: **http://www.truecrypt.org/**, при этом обвинив свою программу в ненадежности. Сообщество пользователей программы усомнилось в справедливости этих обвинений и провело независимый аудит, подтвердивший нескомпрометированность TrueCrypt (**http://habrahabr.ru/post/254777/**). Так что вы можете пользоваться этой программой совершенно спокойно.

Утилита VeraCrypt создает виртуальный зашифрованный диск и монтирует его как реальный. Шифрование данных осуществляется в режиме реального времени и не требует никаких дополнительных операций. При этом виртуальный зашифрованный диск может быть просто файлом на диске или сменном носителе компьютера или же полностью преобразованным логическим диском (в том числе и системным). Программа использует строгие алгоритмы (AES-256, Twofish и др.) и имеет кроме прочих и русский интерфейс.

Среди особенностей программы отметим возможность создания *скрытого тома*. Дело в том, что вы можете попасть в такую ситуацию, когда будете вынуждены раскрыть пароль зашифрованного диска (специалисты смогут обнаружить на вашем компьютере контейнер, используемый для хранения зашифрованной информации, и вынудить вас выдать пароль). Для такого случая VeraCrypt позволяет создать для одного контейнера *два* последовательно зашифрованных диска, доступ к которым осуществляется по различным паролям. Вы можете сообщить вымогателям первый пароль и расшифровать диск, на котором будете хранить ничего не значащую информацию. Обнаружить же на свободной части этого диска наличие зашифрованных данных второго диска *невозможно* — там будут просто случайные данные, шум.

> ***Примечание***
>
> Скрытый том создается вторым этапом на свободном месте первого зашифрованного диска. Программа никак не может контролировать запись данных на это место при работе с первым диском. Поэтому сначала нужно создать «открытый» вариант зашифрованного диска, заполнить его некими данными, а потом на оставшемся свободном месте создать скрытый том. И больше не записывать данные на первый диск.

Максимум, чем вы рискуете в такой ситуации, так это потерей данных на скрытом томе, поскольку не знающий о такой возможности специалист может дописать данные на первый диск и исключить тем самым возможность дешифрования скрытого тома.

Программу VeraCrypt можно использовать и без установки на компьютер — это обеспечивает ее переносной (portable) вариант. Для этого на этапе установки программы нужно на втором шаге выбрать опцию **Extract** и распаковать в нужную папку переносную версию.

На рис. 9.15 показана программа VeraCrypt, запущенная на Windows Server 2022 (это видно по обрамлению окна).

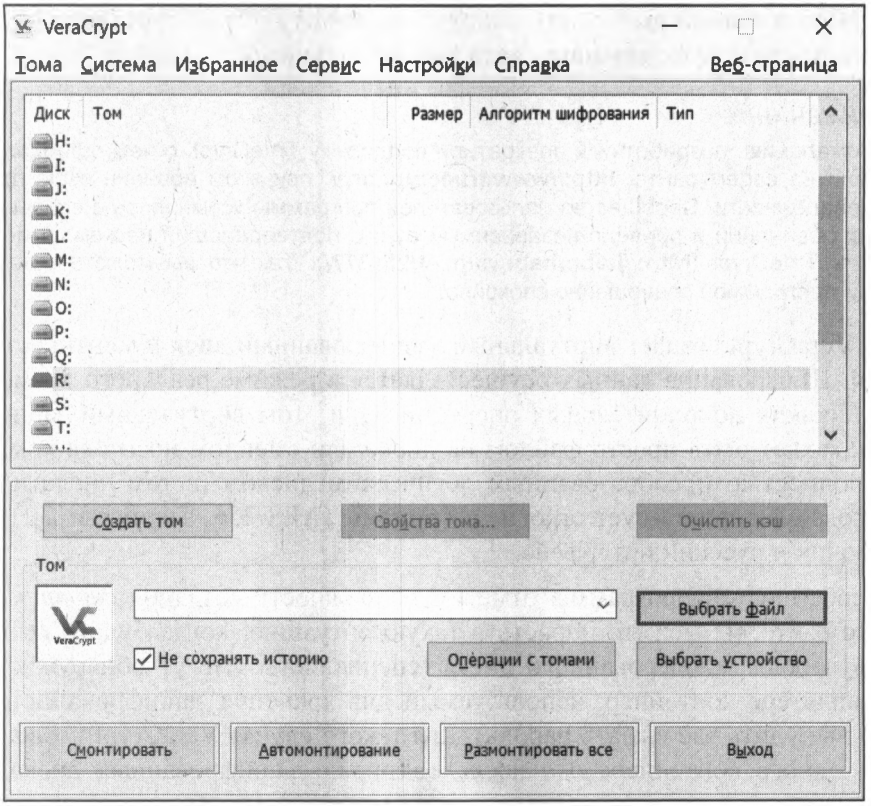


Рис. 9.15. Программа VeraCrypt

Шифрование дисков: коммерческие программы

Существует несколько программ сторонних фирм, позволяющих реализовать возможность шифрования *всего* диска. Однако в настоящее время наблюдается какой-то кризис на рынке коммерческого ПО для шифрования данных. Если несколько лет назад выбор был весьма большой, то на сегодняшний день хороших коммерческих решений не так уж и много.

Ранее потребности в шифровании дисков с успехом обеспечивал программный продукт PGP Desktop. К сожалению, его выпуск прекращен, и официально он недоступен для загрузки. Использовать программы (любые), загруженные из неофициальных источников, не рекомендуется по соображениям безопасности. Поэтому мы больше не можем рекомендовать эту программу для использования.

Вместо PGP Desktop достойно рекомендации приложение AxCrypt Premium (рис. 9.16), которое можно скачать по адресу: **https://www.axcrypt.net/ru/**. Его особенности:

- поддержка облачного шифрования — есть возможность зашифровать файлы, хранящиеся в Dropbox, Google Drive и других облачных дисках;
- поддержка мобильной версии — вы можете получить доступ к защищенным файлам на вашем мобильном устройстве;

- «расшаривание» доступа к файлам — вы можете поделиться с кем-то зашифрованным файлом для безопасного просмотра (требуется, чтобы у того, с кем вы этим файлом делитесь, также была установлена эта программа).

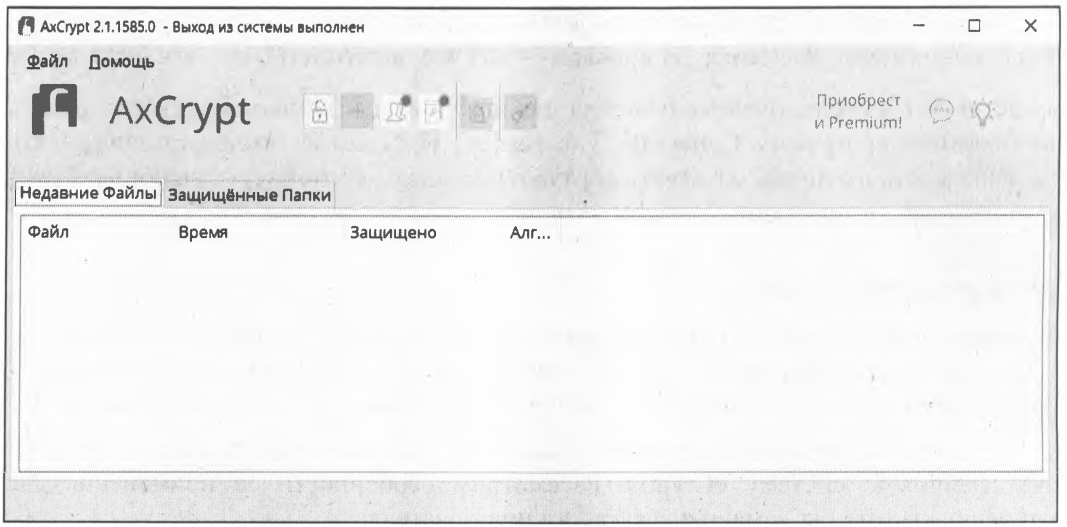


Рис. 9.16. Приложение AxCrypt

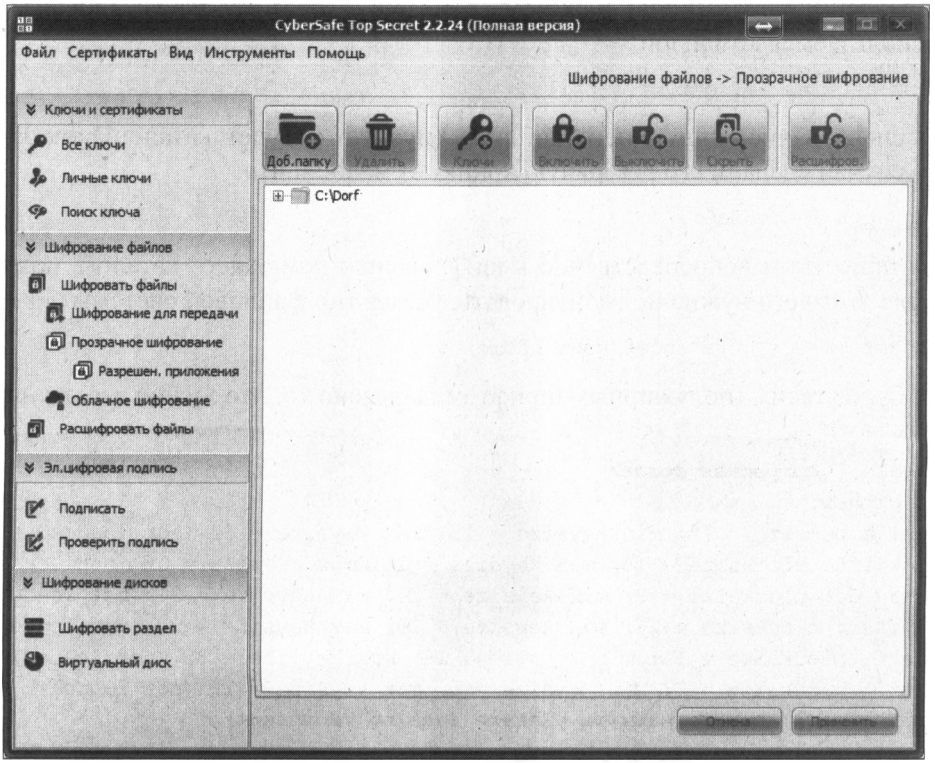


Рис. 9.17. Программа CyberSafe Top Secret, позволяющая шифровать не только диски и файлы, но и электронную почту

Шифрование в AxCrypt Premium осуществляется посредством 256-битного AES-кодирования, что является стандартом на сегодняшний день. Да, согласно ФЗ № 152 на предприятии для шифрования персональных данных эту программу использовать не получится, но для защиты данных, представляющих коммерческую тайну частного предпринимателя, или для личного использования — вполне. Стоимость приложения также невысока: 34 доллара — для частных лиц и 86 — для бизнеса.

Существуют и отечественные решения для шифрования данных. Среди них нельзя не отметить программу CyberSafe Top Secret[1]. Программа позволяет шифровать разделы жесткого диска, создавать виртуальные диски-контейнеры, выполнять прозрачное шифрование папок и шифровать отдельные файлы (рис. 9.17).

Шифрование в Linux

Функции шифрования в Linux поддерживаются на уровне ядра операционной системы. В последних версиях, например, дистрибутива Ubuntu шифрование домашнего каталога предлагается в качестве выбора при установке операционной системы.

В случае необходимости шифрования всего диска можно задействовать шифрованную файловую систему eCryptfs. Рассмотрим особенности ее применения для зашифровки хотя бы домашнего каталога пользователя.

Прежде всего нужно установить утилиты eCryptfs. Пусть наш компьютер работает под управлением операционной системы Debian 6 — поэтому для установки утилит мы воспользуемся командой `apt-get`:

```
sudo apt-get install ecryptfs-utils
```

Перед шифрованием домашнего каталога (пусть это будет каталог **/home/user**) на всякий случай сделаем его резервную копию — мало ли что:

```
sudo cp -pfr /home/user /tmp
```

Теперь приступим непосредственно к шифрованию домашнего каталога пользователя. Для этого его нужно подмонтировать, указав тип файловой системы `ecryptfs`:

```
sudo mount -t ecryptfs /home/user /home/user
```

Вывод будет таким (полужирным шрифтом выделено то, что нужно ввести или выполнить вам):

```
Passphrase: <секретная фраза>
Select cipher:
 1) aes: blocksize = 16; min keysize = 16; max keysize = 32 (not loaded)
 2) blowfish: blocksize = 16; min keysize = 16; max keysize = 56 (not loaded)
 3) des3_ede: blocksize = 8; min keysize = 24; max keysize = 24 (not loaded)
 4) twofish: blocksize = 16; min keysize = 16; max keysize = 32 (not loaded)
 5) cast6: blocksize = 16; min keysize = 16; max keysize = 32 (not loaded)
 6) cast5: blocksize = 8; min keysize = 5; max keysize = 16 (not loaded)
Selection [aes]: просто нажмите <Enter> (aes по умолчанию)
```

[1] См. **http://cybersafesoft.com/product.php?id=1.**

```
Select key bytes:
 1) 16
 2) 32
 3) 24
Selection [16]: нажмите <Enter>
Enable plaintext passthrough (y/n) [n]: n
Enable filename encryption (y/n) [n]: n
Attempting to mount with the following options:
  ecryptfs_unlink_sigs
  ecryptfs_key_bytes=16
  ecryptfs_cipher=aes
  ecryptfs_sig=bd28c38da9fc938b
WARNING: Based on the contents of [/root/.ecryptfs/sig-cache.txt],
it looks like you have never mounted with this key
before. This could mean that you have typed your
passphrase wrong.

Would you like to proceed with the mount (yes/no)? : yes
Would you like to append sig [bd28c38da9fc938b] to
[/root/.ecryptfs/sig-cache.txt]
in order to avoid this warning in the future (yes/no)? : yes
Successfully appended new sig to user sig cache file
Mounted eCryptfs
```

Теперь разберемся, какие опции мы указали. Мы согласились на использование алгоритма по умолчанию: `AES`. Если вы считаете, что другой алгоритм лучше, можете выбрать другой. Мы отказались от шифрования имен файлов: `Enable filename encryption` — если что-то случится с зашифрованным каталогом, то разобраться, где и какой файл, будет сложно.

Итак, на текущий момент каталог **/home/user** зашифрован. Восстановим и удалим наш бэкап (чтобы никто не смог его прочитать):

```
sudo cp -pfr /tmp/user /home/
sudo rm -fr /tmp/user
```

Осталось самое главное — проверить, зашифрован ли на самом деле каталог? Попробуем скопировать в него любой файл из незашифрованной файловой системы:

```
cp /etc/motd /home/user
```

Размонтируем зашифрованный каталог:

```
sudo umount /home/user
```

Теперь пробуем прочитать файл **/home/user/motd**:

```
cat /home/user/motd
```

Если вы увидите всякого рода иероглифы и абракадабру, значит, шифрование работает.

Шифрование работает, но каждый день (точнее, после каждой перезагрузки/загрузки системы) вам надоест вводить секретную фразу. Нужно позаботиться об

автоматическом монтировании этого каталога. Но где же будет храниться пароль? На жестком диске? Но тогда нет смысла в самом шифровании. Это все равно что установленный пароль написать на желтой бумажке, приклеенной к монитору.

Мы, как обычно, найдем рациональное решение и станем хранить секретную фразу на флешке. Но флешка несет файловую систему FAT32, и секретная фраза будет храниться на ней в незашифрованном виде, — поэтому постарайтесь, чтобы флешка эта не попала к врагу. Двойное шифрование (т. е. и домашнего каталога, и флешки) возможно, но его описание выходит за рамки этой книги.

Первым делом нужно подмонтировать флешку:

```
sudo mkdir /mnt/usb
sudo mount /dev/sdb1 /mnt/usb
```

Затем — заглянуть в файл /root/.ecryptfs/sig-cache.txt. Там будет храниться кеш подписи, он выглядит примерно так: `da51c78bc1fc726d` — запишите это значение.

Откройте файл /root/.ecryptfsrc и добавьте в него следующие строки:

```
key=passphrase:passphrase_passwd_file=/mnt/usb/secret.txt
ecryptfs_sig=da51c78bc1fc726d
ecryptfs_cipher=aes
ecryptfs_key_bytes=16
ecryptfs_passthrough=n
ecryptfs_enable_filename_crypto=n
```

Параметр `key` задает имя файла с паролем, второй параметр — подпись из файла sig-cache.txt. Остальные параметры задают тип шифрования, размер ключа и устанавливают прочие режимы ecryptfs.

Создайте файл /mnt/usb/secret.txt и добавьте в него строку:

```
passphrase_passwd=<секретная фраза>
```

Осталось совсем немного — обеспечить автоматическое монтирование флешки и зашифрованной файловой системы. Откройте файл /etc/fstab и добавьте в него строки:

```
/dev/sdb1           /mnt/usb      vfat          ro           0 0
/home/user          /home/user    ecryptfs      defaults     0 0
```

Первая строка монтирует флешку к /mnt/usb, а вторая — зашифрованную файловую систему. Понятно, что флешка должна быть смонтирована до монтирования зашифрованной файловой системы.

Перезагружаемся: `reboot`. В идеале все должно работать нормально — после перезагрузки автоматически подмонтируется зашифрованная файловая система. Но в нашем Debian все пошло не так — флешка не была автоматически подмонтирована, в результате не смонтировалась и eCryptfs. «Вылечить» ситуацию удалось редактированием файла /etc/rc.local, в который мы перед строкой `exit 0` добавили строку: `/bin/mount -a`:

```
...
/bin/mount -a
exit 0
```

Вот теперь использовать eCryptfs стало комфортно.

Шифрование файловой системы Windows

Начиная с версии Windows 2000, шифровать файлы позволяет и Windows. Для этого диск компьютера должен быть отформатирован в файловой системе NTFS, а сам способ носит название *шифрованная файловая система* (Encrypted File System, EFS).

> ***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.

Зашифровать файл (или папку с файлами) можно следующим образом: выделите его в Проводнике (или в любом окне просмотра папок диска) и откройте меню **Свойства**. Затем на вкладке **Общие** нажмите кнопку **Дополнительно** и в окне **Дополнительные атрибуты** установите флажок **Шифровать содержимое для защиты данных**. После подтверждения операции данные будут зашифрованы. Если вы сохранили настройку параметров интерфейса в значениях по умолчанию, то шифрованные файлы и папки будут отображены в окне Проводника светло-зеленым цветом.

Зашифрованный файл открыть может только тот пользователь, который осуществил шифрование. Он же может и расширить число пользователей, имеющих возможность чтения зашифрованных 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 (рис. 9.18) со списком пользователей, которым разрешен доступ к зашифрованному файлу.

Чтобы добавить нового пользователя, достаточно нажать кнопку **Добавить** и выбрать пользователей, которые *имеют на этом компьютере сертификат*. Если папка зашифрована администратором, то никто не сможет ее расшифровать, поэтому кнопки **Добавить** в этом окне не будет, как и показано на рис. 9.18.

> ***Совет***
>
> Самый простой способ получения сертификата — попытаться зашифровать файл. Во время операции будет создан сертификат, если он отсутствовал.

Если вы работаете в составе домена, то учитывайте, что в корпоративных политиках предусматривается 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 включением дополнительного сертификата восстановления (пользователя) в свойства файла. Кроме того, администратор может настроить опции так, чтобы при создании пары ключей пользователя его закрытый ключ хранился в виде копии в службе каталогов. В результате специально назначенный администратор сможет при необходимости восстановить этот ключ и получить доступ к файлу (фактически от имени пользователя).

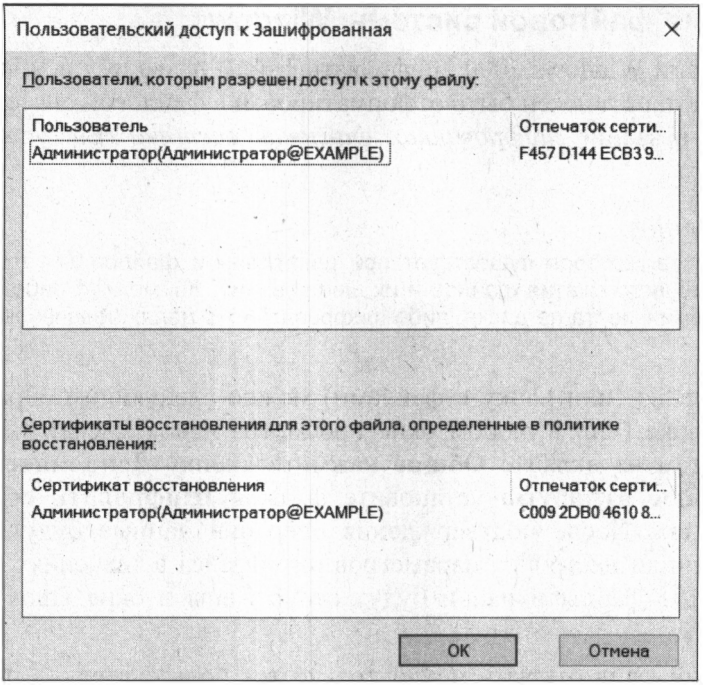


Рис. 9.18. Список пользователей, которым разрешено расшифровать данные файла

При шифровании файлов следует учитывать также и то, что параметры операции привязаны к параметрам безопасности учетной записи. Если получить доступ к ее паролю, то можно расшифровать и этот файл. Так, в Интернете сегодня можно найти несколько утилит, с помощью которых восстанавливается информация из зашифрованных таким способом файлов.

Шифрованную файловую систему EFS можно использовать и для сменных носителей, но для этого их нужно сначала отформатировать в файловой системе NTFS.

Стоит отметить, что EFS — далеко не самое удачное средство шифрования. Начнем с того, что если пользователь задал простой пароль (например, словарное слово или просто некое число), расшифровать файлы, зашифрованные EFS, очень просто. Для этого разработано несколько приложений, и одно из них (на наш взгляд, самое удачное) — Advanced EFS Data Recovery[1] (рис. 9.19). Заинтересовавшимся можем порекомендовать статью, в которой показано, с какой легкостью поддаются расшифровке зашифрованные с помощью EFS файлы[2].

Еще раз хотим обратить ваше внимание, что этот недостаток проявляется только тогда, если пользователь установил простой пароль. При установке сложного пароля, состоящего хотя бы из 10 символов, взломать EFS уже не так легко.

---

[1] См. **https://www.elcomsoft.ru/aefsdr.html**.

[2] См. **http://habrahabr.ru/company/cybersafe/blog/251041/**.

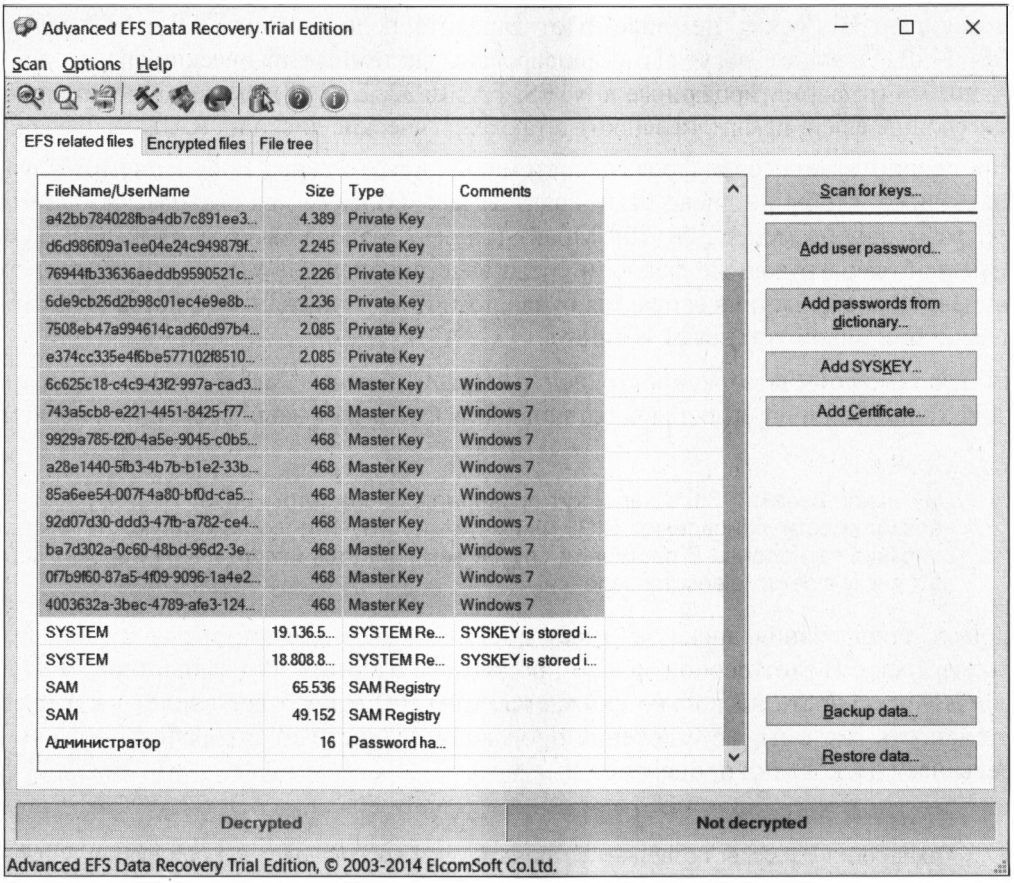


Рис. 9.19. Программа Advanced EFS Data Recovery обнаружила файл, который можно расшифровать

Шифрование диска при помощи BitLocker

В старшие версии Windows (начиная с Windows Vista) включена возможность шифрования данных на диске по технологии BitLocker. Помимо требований к версии ОС, для использования BitLocker необходим компьютер с совместимой версией BIOS и наличием модуля TPM[1] версии 1.2 (один из ключей, используемых при шифровании данных, хранится в этом модуле, что обеспечивает самый высокий уровень его защиты).

> ***Примечание***
>
> Разработчики упомянутой ранее программы шифрования TrueCrypt всегда критиковали проприетарные решения наподобие BitLocker. Однако после прекращения поддержки TrueCrypt они почему-то сами порекомендовали переходить именно на BitLocker (см. **http://truecrypt.sourceforge.net/**). Только нам одним это кажется странным?

[1] TPM (Trusted Platform Module) — специальная микросхема на материнской плате компьютера, обеспечивающая работу системы шифрования.

С помощью BitLocker, независимо от варианта подключения (IDE, ATA, SATA, SCSI, USB, Fireware), могут быть зашифрованы системные логические диски и диски с данными (отформатированные в NTFS, FAT16/32, ExFAT), сменные носители, использующие флеш-память (флешки), а также логические диски на RAID-массивах.

Если предполагается зашифровать системный диск, то перед включением BitLocker необходимо, чтобы на диске были созданы как минимум два раздела: на одном из них, размером не менее 100–300 Мбайт (размер раздела зависит от выпуска ОС), размещаются загрузочные файлы и среда восстановления (Windows PE). Этот раздел невидим, ему не присваивается буква логического диска и создается он автоматически при новой установке Windows.

BitLocker может быть распространен централизованно. Так же централизованно могут храниться и данные для восстановления (доступа к зашифрованным дискам).

> ***Совет***
>
> При использовании BitLocker могут проверяться параметры BIOS. Поэтому в случае необходимости обновления BIOS внимательно изучите соответствующие разделы описания технологии. В противном случае вам придется использовать вариант доступа к диску в режиме восстановления.

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. Сам BitLocker тоже влияет на производительность системы, но снижение производительности от его работы обычно не превышает нескольких процентов.

> ***Совет***
>
> Технология BitLocker позволяет создавать ключ *восстановления* при любом варианте шифрования. Не пренебрегайте этой возможностью. Иначе, например, в случае аппаратных проблем вы потеряете все свои данные.

Использование BitLocker на компьютерах без TPM

Технология BitLocker может быть применена и на компьютерах, *не имеющих TPM-модуля*. С ее помощью можно зашифровать диск, используя для хранения ключа сменный USB-носитель. Такая возможность включается *только* через настройки групповой политики. Для открытия редактора групповой политики наберите в командной строке `mmc` и добавьте в оснастку консоли **Редактор групповой политики**. При запросе объекта редактирования выберите **Локальный компьютер**.

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 | Диски операционной системы** | параметр **Обязательная дополнительная проверка подлинности при запуске**[1] (рис. 9.20). В свойствах параметра необходимо **Разрешить использование BitLocker без совместимого TPM**.

[1] В Windows 10 параметр называется «Этот параметр политики позволяет настроить требование дополнительной проверки подлинности при запуске».

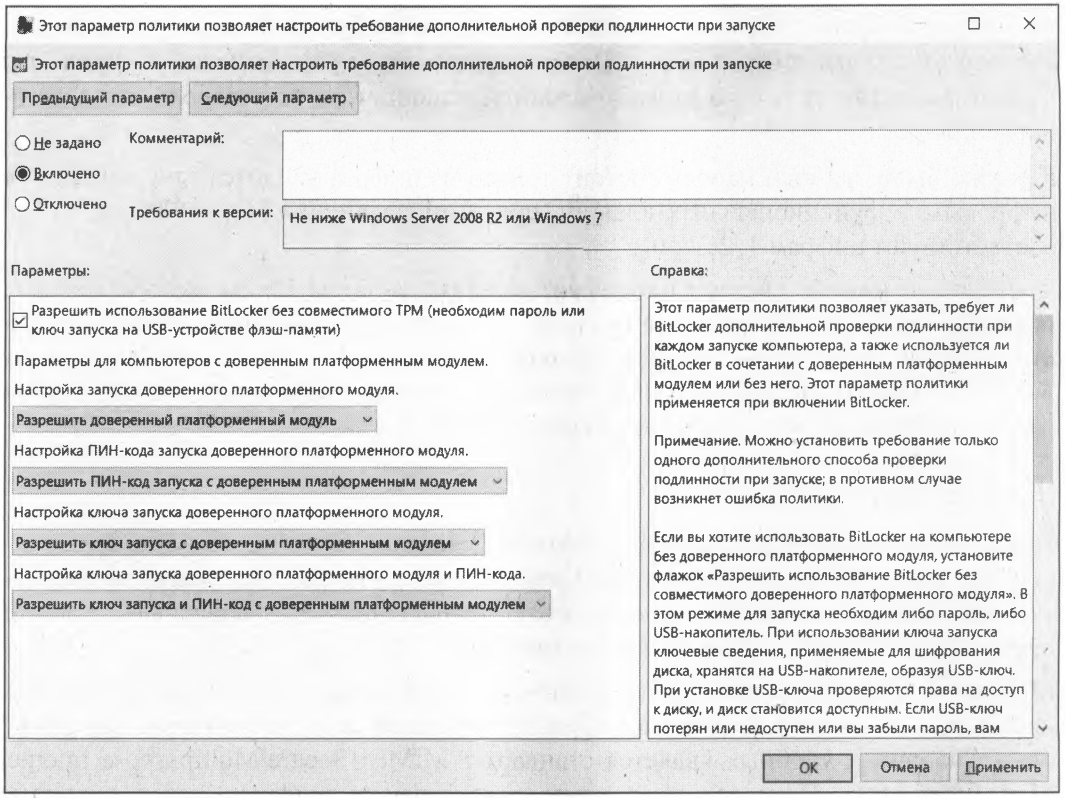


Рис. 9.20. Настройка параметров для включения BitLocker на компьютерах без TPM

Обратите внимание, что в этом случае BIOS должна поддерживать чтение с USB в режиме старта.

Включение шифрования

Включение шифрования BitLocker осуществляется с помощью команды **Панель управления | Шифрование диска BitLocker**. Если все необходимые для шифрования условия выполнены, то в окне появляется опция **Включить шифрование**. После ее выбора запускается мастер операций, и вам нужно просто следовать указаниям программы.

Режим восстановления

В случае выхода из строя оборудования (модуля TPM или всей материнской платы) или изменения загрузочных файлов (например, при 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 отличать 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 этот 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 сможете отключить режим шифрования. Обратите внимание, что есть две возможности его отключения. Первая предполагает полное дешифрование диска — это весьма длительная операция. Вторая только временно отключает режим шифрования, если вы собираетесь, например, заменить на компьютере BIOS.

Шифрование почты

Электронная почта передается по открытым каналам связи, поэтому не исключен риск ее перехвата или модификации. Гарантировать, что текст сообщения никем не изменен, можно с помощью *электронной подписи* письма, а шифрование делает просмотр письма недоступным для посторонних.

Можно использовать различные варианты шифрования сообщений (например, вкладывать в письмо заранее зашифрованный какой-либо программой текст), но одним из самых удобных является стандарт S/MIME (Secure/Multipurpose Internet Mail Extensions). Почтовая программа автоматически шифрует 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.

Работа с подписанными или шифрованными сообщениями не представляет сложности. Система автоматически обрабатывает сообщение, пользователю достаточно лишь включить соответствующую опцию в свойствах письма. О том, что письмо зашифровано, сообщают только значки в панели инструментов сообщения: на рис. 9.21 левый значок в прямоугольнике внизу справа означает, что сообщение зашифровано, правый — что сообщение подписано. Сам текст автоматически расшифровывается в момент открытия сообщения. Щелчок на том или ином значке покажет информацию о сертификате, использованном при составлении письма (рис. 9.22).

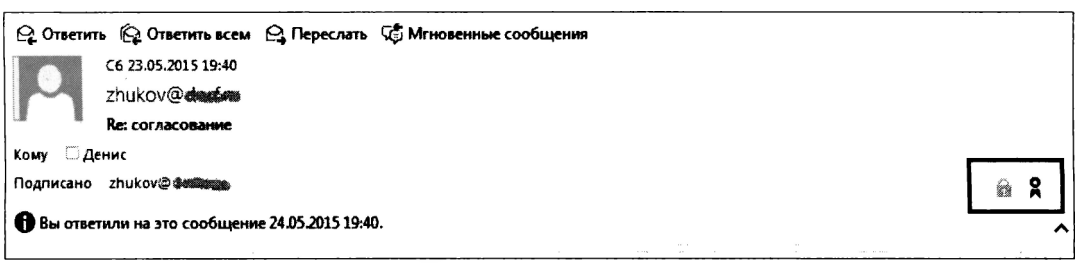


Рис. 9.21. Образец почтового сообщения с электронной подписью и шифрованием текста

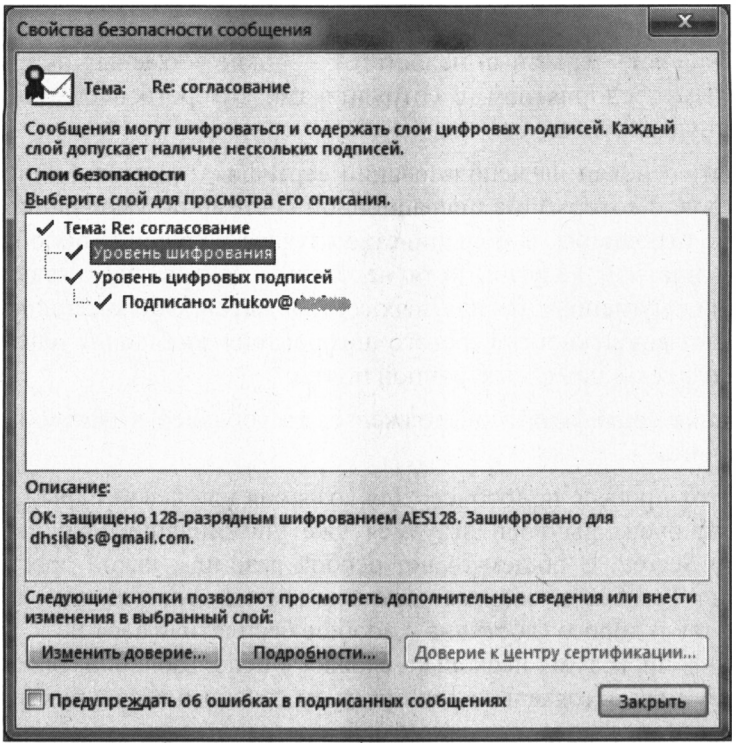


Рис. 9.22. Информация о шифровании

Получение открытого ключа для защищенной переписки

Шифрование сообщения по стандарту S/MIME производится отправителем с помощью открытого ключа получателя письма. Поэтому расшифровано оно может быть только тем пользователем, у которого имеется закрытый ключ, соответствующий использованному открытому ключу.

Поскольку для шифрования требуется знать открытый ключ получателя, то его необходимо получить *до отправки письма*. В рамках предприятия (домена Windows) открытые ключи пользователей доступны через службу каталогов. Если же вы хотите написать письмо внешнему адресату, то предварительно следует получить его открытый ключ, запросив, например, у него письмо с электронной подписью.

Получение цифрового сертификата для защищенной переписки

Используемые для защищенной переписки пары ключей должны быть заверены удостоверяющим центром, которому доверяют как отправитель, так и получатель сообщения. Цифровые удостоверения, выданные серверами предприятия, не вызовут доверия у внешних пользователей, и получатель сообщения увидит предупреждение о нарушении электронной защиты. Хотя сам текст сообщения поврежден не будет, большинство адресатов просто не станут открывать такие письма.

Для обеспечения защищенной переписки между двумя предприятиями существуют два варианта решения. Первый — обменяться сертификатами удостоверяющих

центров своих предприятий и установить к ним доверие в каждом предприятии. У этого решения есть серьезный недостаток — такие «обмены» придется осуществлять с *каждым* предприятием, с сотрудниками которого необходимо осуществлять защищенную переписку.

Второй вариант основан на использовании сертификатов от публичных удостоверяющих центров, с которыми в операционной системе по умолчанию установлены доверительные отношения. В большинстве случаев получение подобного сертификата является платной услугой, хотя некоторые центры предоставляют возможность получения временных бесплатных сертификатов. Обычно такие сертификаты не предполагают возможности строгого шифрования сообщения и фактически удостоверяют только сам адрес электронной почты.

После получения сертификата он должен быть добавлен в настройки программы почтового клиента.

Рассмотрим этот процесс подробнее. Для создания ключевой пары, т. е. открытого и закрытого ключей, мы воспользуемся уже упоминавшейся ранее программой CyberSafe Top Secret[1]. В общем-то нет особой разницы, какой программой создавать ключи, но Top Secret обладает встроенным удостоверяющим центром и при этом стоит не так и дорого (доступна и вообще бесплатная версия). Сразу хотим вас предупредить — программа несколько сложна в использовании, особенно с непривычки, поэтому мы настоятельно рекомендуем ознакомиться с руководством по ее эксплуатации, которое можно скачать с сайта разработчика.

При первом запуске программы надо обязательно принять сертификат от CyberSoft CA. Да, это предлагает и руководство по программе, но лучше лишний раз об этом вспомнить, чем не принять сертификат.

Затем нужно перейти в раздел **Ключи и сертификаты | Личные ключи**, нажать кнопку **Создать** и в открывшемся окне ввести адрес электронной почты и пароль, а также свои имя и фамилию, чтобы вашим друзьям и коллегам сразу стало ясно, кому принадлежит сертификат (рис. 9.23).

Выберите срок действия сертификата и длину ключа. Для мощных компьютеров лучше выбрать максимальную длину ключа, для не очень мощных — 4096 битов. Помните, чем длиннее ключ, тем надежнее защита.

Обязательно установите флажок **Опубликовать, после создания** — ваш сертификат будет автоматически опубликован на сервере CyberSafe, и ваши коллеги смогут легко его найти. Если вы не собираетесь создавать собственный сервер сертификатов или использовать какой-то внешний сервер, то публикация сертификата на сервере CyberSafe — оптимальное решение. Если вы поспешили и не установили этот флажок, не беда — после создания сертификата выделите его и нажмите кнопку **Публик**.

Ну и в завершение нажмите кнопку **Готово**, после чего программа попросит вас подтвердить ваш e-mail. На него будет выслан код подтверждения, который нужно ввести в открывшееся окно (рис. 9.24).

---

[1] См. **http://cybersafesoft.com/product.php?id=1**.

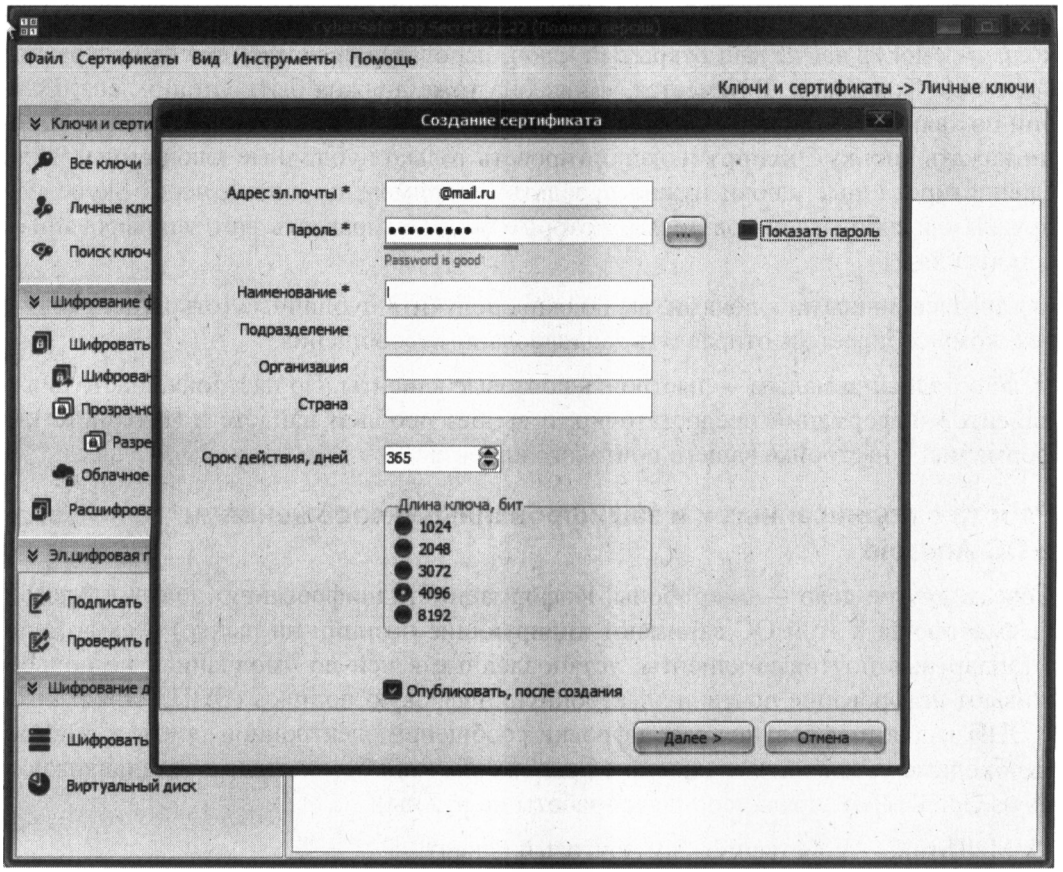


Рис. 9.23. Создание сертификата в программе CyberSafe Top Secret

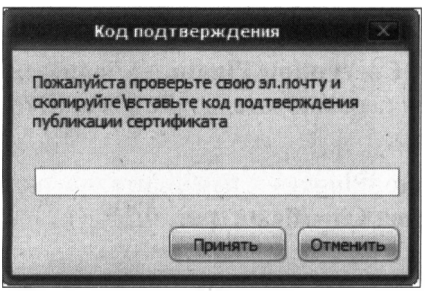


Рис. 9.24. Вводим код подтверждения для публикации сертификата

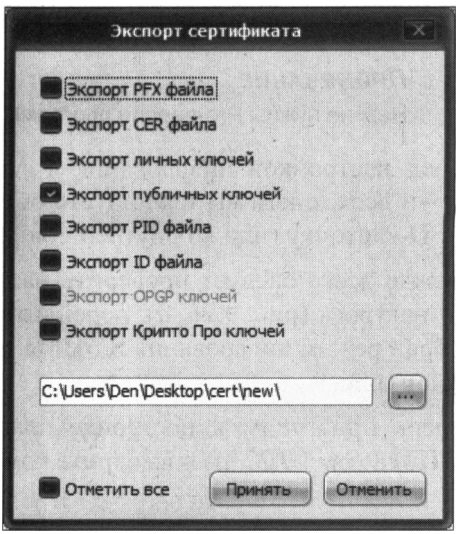


Рис. 9.25. Экспорт публичных ключей

В результате вы получите сообщение, что сертификат успешно опубликован. Ваши коллеги смогут найти ваш открытый ключ, используя средства поиска программы CyberSafe Top Secret. Разумеется, у них она тоже должна быть установлена. Если они по каким-либо причинам этого не сделали, вы можете в разделе **Личные ключи** нажать кнопку **Экспорт** и экспортировать только публичные ключи (рис. 9.25). Экспортированные ключи нужно передать (например, по e-mail, через Skype или другим способом) пользователям, которые будут отправлять вам зашифрованные сообщения.

Обзаведясь личными ключами, вы должны получить публичные (открытые) ключи тех, кому собираетесь отправлять зашифрованные сообщения.

Дело осталось за малым — настроить почтовые клиенты. По настройке настольных клиентов информации предостаточно, и вы без проблем найдете в Интернете информацию о настройке вашего почтового клиента[1].

Работа с подписанными и зашифрованными сообщениями в ОС Android

Совсем другое дело — смартфоны. Информации по шифрованию почты в Android (а смартфоны с этой ОС занимают лидирующие позиции на рынке) весьма мало. Стандартные почтовые клиенты, установленные в ней по умолчанию, не поддерживают шифрование почты и электронную цифровую подпись (ЭЦП). Для работы с ЭЦП и для шифрования/расшифровки сообщений электронной почты в Android необходимо установить следующие приложения (они бесплатные и устанавливаются из Google Play, права root для их работы не нужны):

- MailDroid — собственно, сам почтовый клиент: **https://play.google.com/store/apps/details?id=com.maildroid**;
- Crypto Plugin — плагин, поддерживающий работу с сертификатами: **https://play.google.com/store/apps/details?id=com.flipdog.crypto.plugin**.

> ***Примечание***
>
> Нам не нужны Pro-версии программных продуктов, достаточно обычных (бесплатных).

Перед настройкой шифрования в Android нужно экспортировать ваши ключи и ключи всех, с кем вы планируете обмениваться корреспонденцией, и загрузить их на SD-карточку (или во внутреннюю память) вашего устройства.

Прежде всего следует проверить настройки программы MailDroid — откройте экран настроек (рис. 9.26, *а*), перейдите в раздел **Encryption Plugin** и убедитесь, что выбран режим шифрования **S/MIME** и включен переключатель **Allow MailDroid to decide** (рис. 9.26, *б*).

Теперь приступим к настройке плагина Crypto Plugin — перейдите на вкладку **S/MIME** (рис. 9.27, *а*) и выберите команду **Import Certificate** (рис. 9.27, *б*).

---

[1] Например, о том, как настроить почтовый агент Outlook, подробно рассказано в статье по адресу: **http://habrahabr.ru/company/cybersafe/blog/209642/**.

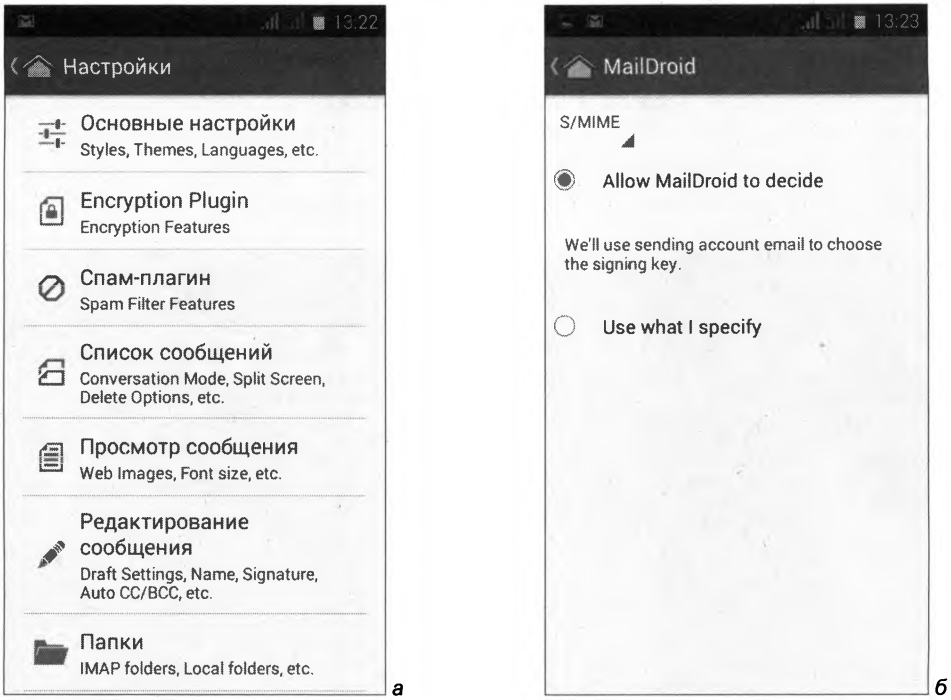


Рис. 9.26. *а* — настройки программы MailDroid; *б* — режим шифрования

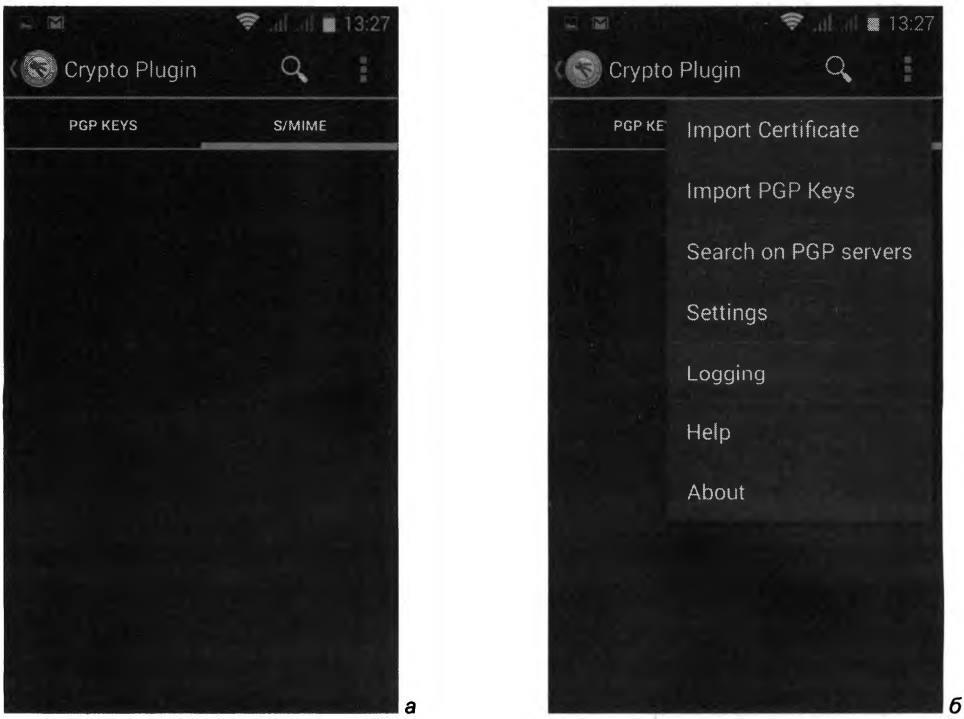


Рис. 9.27. *а* — вкладка **S/MIME**; *б* — выберите команду **Import Certificate**

Далее нужно импортировать корневой сертификат — его файл называется **Root Certificate** (рис. 9.28).

Откройте файловый менеджер, который вам удобно использовать, чтобы указать путь к сертификату (рис. 9.29), перейдите к каталогу, в который вы поместили сертификат, и выберите **Root Certificate.cer** (рис. 9.30). Программа спросит, как открыть файл — выберите вариант **Стандартный** (рис. 9.31).

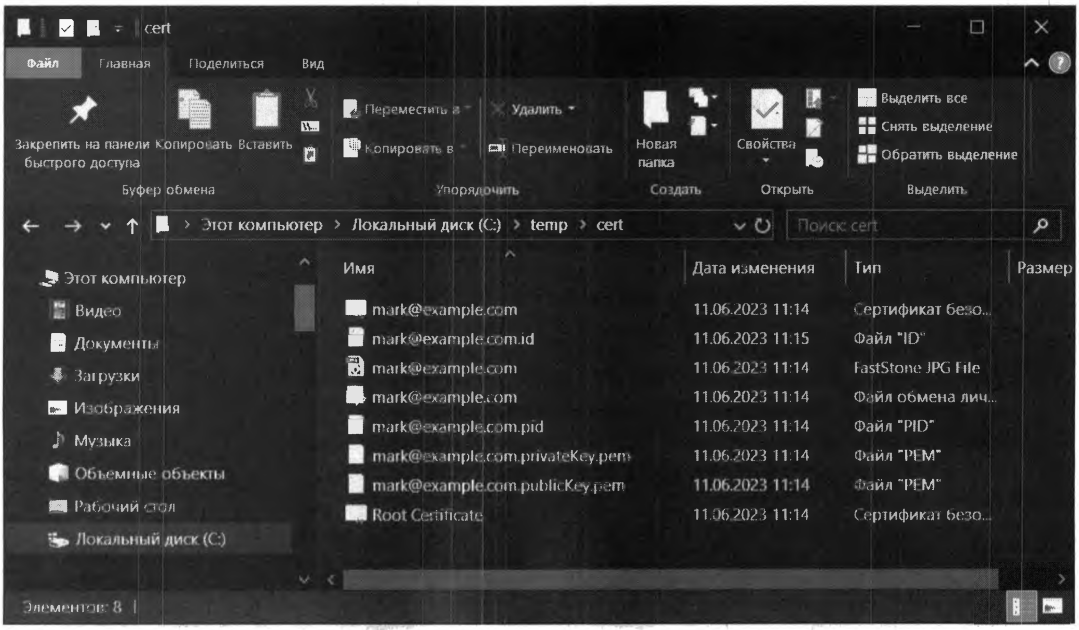


Рис. 9.28. Содержимое каталога с сертификатами

Рис. 9.29. Выбор файлового менеджера

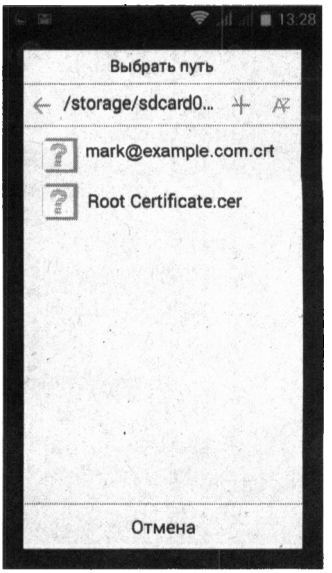


Рис. 9.30. Выбор сертификата

В результате импортированный сертификат появится в списке сертификатов (рис. 9.32). Далее операцию импорта нужно повторить для вашего личного сертификата (*.pfx) и сертификатов всех, с кем вы планируете обмениваться зашифрованными сообщениями и ЭЦП. При импорте личного сертификата будет запрошен пароль. Обратите внимание — ваш личный сертификат помечен в списке как **PRIVATE**.

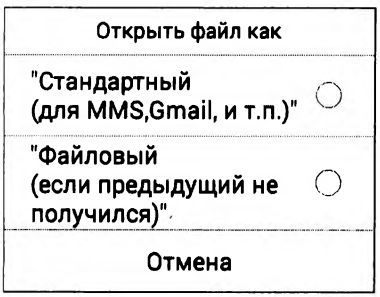


Рис. 9.31. Выберите **Стандартный**

Рис. 9.32. Корневой сертификат импортирован

Импортировав сертификаты, можно приступить к обмену зашифрованными/подписанными сообщениями. Так, при создании нового сообщения в MailDroid вы можете его подписать и зашифровать. Если нужно только подписать сообщение, установите флажок **Sign** (рис. 9.33). Если же надо не только подписать его, но и зашифровать, установите еще и флажок **Encrypt**.

Подписывая сообщение, следует выбрать, какой сертификат будет использоваться. Выбор сертификата осуществляется в области **SIGNERS**. Скорее всего, у вас будет всего один сертификат (см. рис. 9.33).

При шифровании письма сертификаты всех получателей программа добавляет автоматически (если, конечно, вы их импортировали с помощью Crypto Plugin). Посмотрите на рис. 9.34 — программа автоматически добавила в список сертификаты получателей. Выполняет она и проверку сертификатов получателей — обратите внимание на результат проверки сертификата: **CERTIFICATE IS OK** (рис. 9.35).

Итак, отправку подписанных и зашифрованных сообщений мы освоили. Теперь посмотрим, как читать зашифрованные и подписанные сообщения.

Рис. 9.33. Электронная подпись письма и выбор сертификата

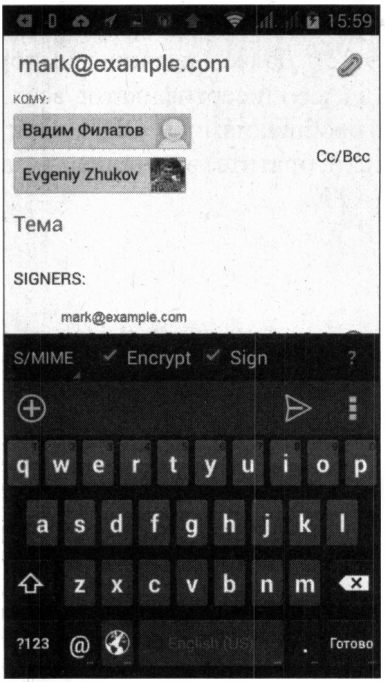


Рис. 9.34. Выбраны получатели сообщения

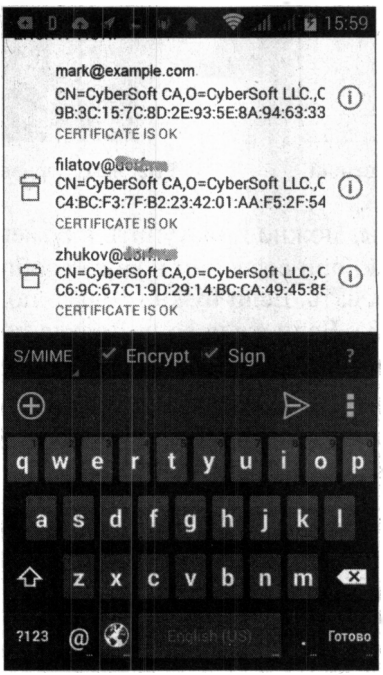
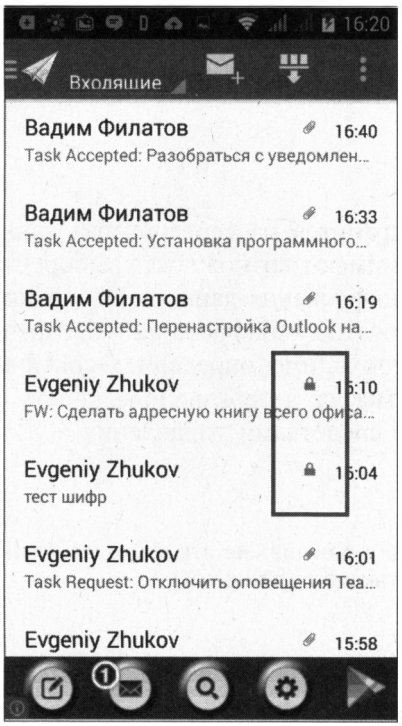
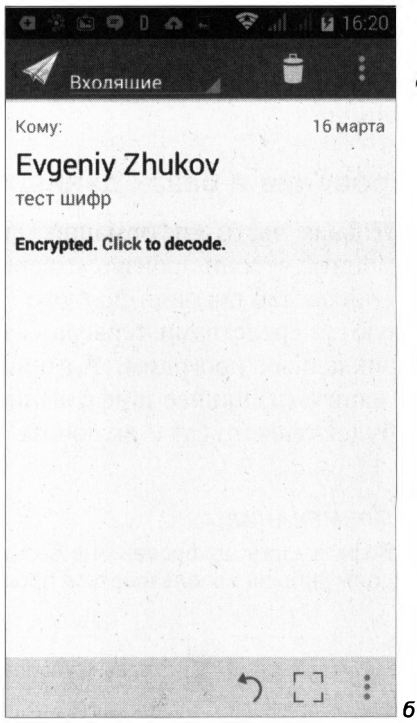


Рис. 9.35. Сертификаты

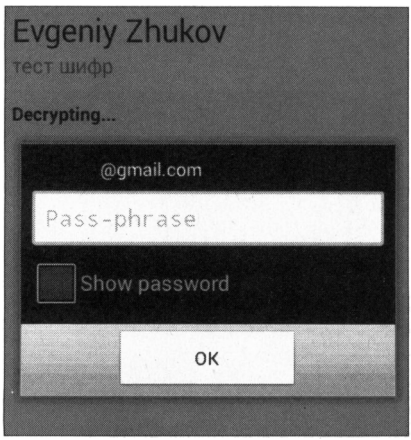
Пришедшее к вам зашифрованное сообщение будет отмечено значком замка (рис. 9.36, *а*). Откройте зашифрованное сообщение — программа сообщит, что оно зашифровано: **Encrypted** (рис. 9.36, *б*). Нажмите ссылку **Click** для расшифровки сообщения и введите пароль своего сертификата (рис. 9.36, *в*) — если пароль введен правильно, сообщение будет расшифровано.



а



б



в

Рис. 9.36. *а* **— зашифрованные сообщения в списке;** *б* **— зашифрованное сообщение;** *в* **— введите пароль**

После установки и настройки MailDroid нужно отключить стандартный почтовый клиент Gmail, чтобы не получать уведомления о новой почте из двух программ. Для этого выполните следующие действия:

1. Откройте **Настройки** Android.
2. Выберите **Приложения**.
3. Перейдите на вкладку **Все**.
4. Выберите **Gmail**.
5. Нажмите кнопку **Остановить**.
6. Нажмите кнопку **Отключить**.

После этого приложение Gmail будет перемещено с вкладки **Все** на вкладку **Отключенные**.

Шифрование в базах данных

Значительная часть информации предприятия хранится на серверах баз данных. Современные версии производственных серверов имеют возможность выборочного (по столбцам таблиц) или полного (всей базы) шифрования данных. Эти функции реализуются средствами сервера баз данных, и поэтому шифрование «прозрачно» для прикладных программ. Администратору необходимо определить критичную информацию (излишнее шифрование не имеет смысла, а производительность системы будет снижаться) и включить шифрование средствами управления SQL-сервера.

Примечание

Возможность шифрования в базах данных была и раньше. Но эта функциональность должна была использоваться программой, работающей с данными.

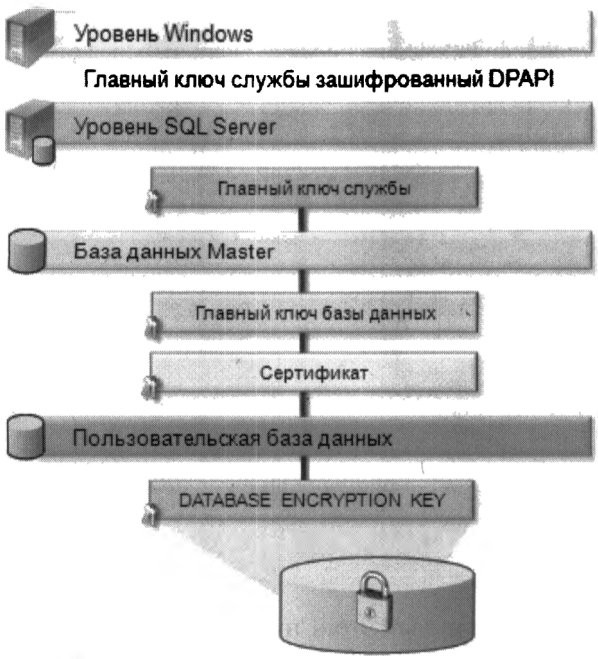


Рис. 9.37. Архитектура шифрования данных в SQL Server 2008/2022

Архитектура решения для Microsoft SQL Server 2008/2022 представлена на рис. 9.37 — каждая база данных шифруется собственным ключом. Для этого используется сертификат, зашифрованный мастер-ключом базы **Master**, который, в свою очередь, шифруется ключом службы сервера базы данных, создаваемым при установке сервера.

Обратите внимание, что прозрачное шифрование данных предотвращает доступ к информации в резервных копиях и на остановленных серверах (выключенных системах). Но если злоумышленник попытается получить доступ через работающий SQL-сервер (например, раздобыв параметры доступа пользовательской учетной записи), то такая попытка завершится успехом. В этом случае должны срабатывать средства контроля доступа SQL-сервера.

Стеганография

Лучший способ защиты информации — не показать злоумышленнику, что такая информация есть. Технология *стеганографии* предполагает маскировку данных среди ничего не значащей информации.

Самый простой способ — это добавить в конец файла изображения еще один архив («склеить» его с изображением). Изображение будет нормально просматриваться в графических программах, но при открытии его в архиваторе вы сможете извлечь скрытые данные.

Анализ поведения пользователей

По результатам некоторых западных исследований, примерно две трети высокотехнологичных корпораций постоянно сталкиваются с внутренними угрозами безопасности информации.

Традиционные способы защиты: ограничение доступа к информации, контроль периметра (почты, различных мессенджеров, сменных носителей и т. д.) по ключевым словам (сигнатурам) и т. д. — становятся малоэффективными.

Во-первых, информация часто похищается теми, кто имеет доступ к соответствующему классу данных. Кроме того, получить доступ к желаемой информации не представляет труда и для злоумышленника, использующего методы социальной инженерии. Во-вторых, пользователи становятся более опытными и подготовленными. Они могут легко узнать, какие продукты используются для защиты данных, какие сигнатуры анализируются, и даже поставить себе для изучения пробную версию такого продукта. В результате злоумышленник сможет вынести с предприятия серьезные объемы информации, имеющей коммерческую ценность.

Для исключения подобных ситуаций стали появляться продукты, анализирующие модель поведения пользователя. Простейший пример: поведение сотрудника, в текущей работе на своем рабочем месте столько-то раз открывающего документы из такой-то папки, производящего поиск по таким-то ключевым словам и т. д., может быть описано соответствующей моделью. Но если он начинает готовиться к уходу с предприятия и собирает кажущуюся ему полезной информацию, то такие допол-

нительные операции будут восприняты программой как отклонения от профиля и специалисты службы безопасности получат предупреждение.

Подобные продукты являются коммерческими решениями. Здесь мы не станем описывать конкретные приложения, поскольку они специфичны для различных типов информации.

DLP-технологии

Защищаемая информация может покинуть предприятие различными путями: через каналы связи и сменные носители, электронную почту, различные мессенджеры, Skype, флешки и т. п. Причем это может быть сделано как умышленно, так и случайно (например, если при создании письма перепутан адрес получателя).

На рынке сегодня имеется несколько продуктов, позволяющих контролировать периметр предприятия и блокировать возможную утечку данных. Такие решения называются *предотвращением утечек* (от *англ.* Data Loss Prevention, DLP). Основная задача DLP — обнаружить и заблокировать запрещенную передачу конфиденциальных данных по любым каналам связи и устройствам.

Большинство таких продуктов работают уже «по факту», т. е. сообщают о наличии подозрительного трафика и утечке данных. Кроме того, методы анализа данных не позволяют говорить о надежности распознавания конфиденциальной информации, тем более что каждой категории данных требуется своя адаптированная технология анализа.

Для анализа документов применяется *теория отпечатков*. Каждому документу ставится в соответствие цифровой отпечаток, который сравнивается с хранимыми цифровыми отпечатками документов, которые эксперты отнесли к конфиденциальной информации. На основе такого анализа определяется вероятность присутствия в документе конфиденциальных данных. Кроме того, проводится морфологический и грамматический разбор текста для обнаружения искомых данных.

DLP-решения являются недешевыми продуктами. О целесообразности их внедрения с экономической точки зрения имеет смысл говорить при числе контролируемых рабочих мест порядка нескольких сотен и более. Кроме того, решение, выносимое такой системой, является вероятностным (хотя и с достаточно высокой степенью правильной идентификации). Поэтому подобные технологии сегодня пока применяются в крупных организациях, где очень высока стоимость утечки данных (финансовый сектор и т. п.).

Далее мы попробуем разобраться, какая система подойдет конкретно в вашем случае. Какой-либо продукт рекомендовать не станем, поскольку выбор DLP-системы — это сугубо индивидуальный процесс, и нет единственного рецепта, покрывающего потребности всех предприятий.

При выборе DLP-системы необходимо учитывать следующие факторы:

- количество контролируемых каналов;
- функции самой DLP-системы;
- надежность и скорость работы системы;

- наличие и качество службы технической поддержки;
- надежность разработчика;
- стоимость покупки и стоимость владения системой.

Помните, что основная задача системы — предотвратить утечку конфиденциальных данных по любому из каналов, которые используются в компании. Что делать, если по всем критериям система пригодна, но один из каналов она не контролирует. Здесь нужно выбирать из следующих вариантов:

- отказаться от использования неконтролируемого канала, если это возможно;
- выбрать другую DLP-систему.

Третьего не дано. Помните, что в большинстве случаев вы не сможете контролировать все каналы. Например, пользователь может сфотографировать важные документы и отправить их фото со своего смартфона — не через корпоративный Wi-Fi, а через сеть мобильного оператора. Сотовую сеть вы не контролируете, соответственно, предотвратить такую утечку не сможете. Отобрать у всех смартфоны на входе? Все зависит от степени секретности вашего предприятия — можно сотрудников и домой не отпускать. Шутка. Самый действенный способ — наличие видеокамер в операционном зале, чтобы пользователи знали, что за ними наблюдают. В этом случае предотвратить слив информации, скорее всего, тоже не получится, но зато вы хотя бы узнаете, кто это сделал.

По своему типу все DLP-системы делятся на две группы: активные и пассивные. Первые способны блокировать передачу конфиденциальных данных при обнаружении нарушения. Вторые только наблюдают за потоками данных, но не вмешиваются в сами процессы. Существуют и решения «два в одном», когда система может не только наблюдать, но и предпринимать какие-то действия.

По типу архитектурной реализации DLP-системы опять-таки делятся на два типа: хостовые и шлюзовые. В первом случае на все компьютеры устанавливается DLP-агент — программа, которая контролирует действия пользователя (здесь наверняка есть возможность записи экрана активности пользователя, создания скриншотов, наблюдения в реальном времени за действиями пользователя). DLP-агент затем передает все это на сервер DLP-системы. Шлюзовые системы устанавливаются на шлюзе и контролируют только передаваемую за пределы компании информацию. Учитывая, что данные в большинстве случаев сегодня зашифрованы, не всегда от таких систем есть толк. А хостовые системы предусматривают возможность перехватить данные еще до их шифрования при передаче по сети — как правило, они содержат встроенный клавиатурный шпион, позволяющий перехватить ввод пользователя с клавиатуры, а также они могут анализировать передаваемые файлы еще до самой передачи — при обращении к ним. Основное преимущество хостовых решений заключается в более полном контроле каналов передачи информации и действий пользователя на рабочем месте. Агенты фиксируют все операции за компьютером, плюс DLP-решения нового поколения позволяют записывать переговоры сотрудников или, например, подключаться к веб-камере их ноутбука.

Недостаток DLP-систем хостового типа — они могут контролировать только устройства, на которые установлен DLP-агент. Однако для выбранной операционной

системы может не оказаться DLP-агента. Например, вам понравилась какая-либо система, но агенты DLP поддерживают только Windows и Linux. Так что если в вашей сети есть несколько макбуков, они останутся неконтролируемыми.

Вот несколько примеров DLP-систем: Symantec DLP, Forcepoint DLP, McAfee DLP, Sophos Endpoint Protection — и это не единственные системы, примеров можно привести еще с десяток. То есть подобных систем очень много, и, как правило, все они платные, причем стоят такие решения недешево. Это основной их недостаток, и для некоторых из них нет даже trial-версий. Другими словами: купите и наслаждайтесь. Если что-то пойдет не так, покупайте любую другую.

Если все же хочется попробовать систему до ее приобретения, обратите внимание на решение MyDLP от Comodo (**https://www.mydlp.com/**). Не будем утверждать, что оно лучшее, однако у него есть хотя бы trial-версия, что позволяет ознакомиться с системой перед ее покупкой.

Из бесплатных систем можно порекомендовать только Open DLP[1] от Google. Однако вы можете испытать сложности при внедрении этой системы в свою инфраструктуру. В первую очередь сложности связаны с отсутствием нормальной документации — даже на главной странице проекта при попытке перейти по ссылке с инструкциями по установке получаешь ошибку 404.

Использовать взломанные DLP-системы, которые можно скачать на торрентах, нет смысла — думаем, вы понимаете почему.

Данные, приведенные в табл. 9.1, помогут вам выбрать DLP-систему. В ней мы приводим свои личные впечатления от различных DLP-систем, с которыми приходилось сталкиваться по роду своей деятельности. Таблица не претендует на истинность, поэтому воспринимайте ее просто как личное мнение.

***Таблица 9.1.** Краткий обзор DLP-систем*

Система	Впечатления	Достоинства	Недостатки
McAfee DLP	Очень тяжелая во внедрении система. Сначала нужно развернуть McAfee ePolicy Orchestrator как собственную платформу управления. Хорошо подойдет для предприятий, где вся инфраструктура основана на продуктах McAfee, но если это не так, придется туго	Возможность задать условные приоритеты для правил, а потом использовать эти приоритеты как параметры фильтрации событий в журнале. Сама фильтрация сделана весьма приятно и удобно. Имеется возможность пересылки запрещенного к пересылке файла при условии ввода пояснения от пользователя	Необходимость установки собственной платформы управления, во многом дублирующей AD. Нет встроенного OCR-модуля: контроль сканированных документов — мимо. Ряд ограничений вроде контроля почты — только в Outlook (переписка через The Bat! пролетела мимо агентского контроля), зависимость от конкретных версий браузеров, отсутствие контроля переписки в Skype (перехватываются только файлы)

[1] См. **https://code.google.com/archive/p/opendlp/**.

Таблица 9.1 (окончание)

Система	Впечатления	Достоинства	Недостатки
Sophos Endpoint Protection	Не очень удачное решение. По сути, это надстройка над антивирусом, а не полноценная DLP-система	Особых нет, разве что возможность пересылки запрещенного к пересылке файла (пользователь может дать пояснение, зачем он это делает, потом служба безопасности проверит все такие моменты)	Нет никаких сложностей в обходе контроля устройств агентом: остановить антивирус от Sophos, затем включить драйвер устройства в Device Manager — и вы получаете полный доступ к запрещенной флешке. Так быть не должно. Нет модуля OCR, перечень контролируемых устройств беден, почта контролируется через встраивание в почтовые клиенты, плохо реализованы правила анализа содержимого
InfoWatch Traffic Monitor	На фоне двух предыдущих систем выглядит весьма приятно. Но все же есть достаточно неприятные нюансы — смотрите достоинства и недостатки	Хороший интерфейс, неплохой набор виджетов, отличный набор отчетов. Хорошо работает с архивами, имеет инструменты анализа содержимого архивов, позволяет создавать скриншоты с рабочих станций	По сути, это не один продукт, а связка Infowatch Traffic Monitor и Infowatch Device Monitor, причем работающая на двух ОС (Windows и Red Hat Linux), поэтому установка и настройка для запуска сложноваты. Добавьте сюда еще и отсутствие хорошей документации, что снижает вероятность самостоятельной настройки

Инструменты анализа безопасности Windows Server

В случае с безопасностью нет предела совершенству — ведь постоянно появляются новые угрозы, нужно держать руку на пульсе, поддерживать систему в актуальном состоянии. В этом разделе будут рассмотрены средства проверки уровня защищенности настольных и серверных версий Windows. Периодическое использование этих инструментов позволит предотвратить различного рода угрозы — найдите уязвимости в своей системе прежде, чем это сделает кто-то другой.

MBSA, Microsoft Baseline Security Alalyzer

Начинать проверку уровня защищенности нужно с базового анализатора Microsoft. Это старейшая утилита, первые версии которой были ориентированы еще на Windows Server 2003. Но и спустя много лет утилита все еще на плаву и поддерживает последние версии Windows: Windows 10/11 и Windows Server 2016/2019/2022.

Утилита предлагает ряд проверок (рис. 9.38): проверку на административные уязвимости, проверку на слабые пароли. Также она позволяет проверить, установ-

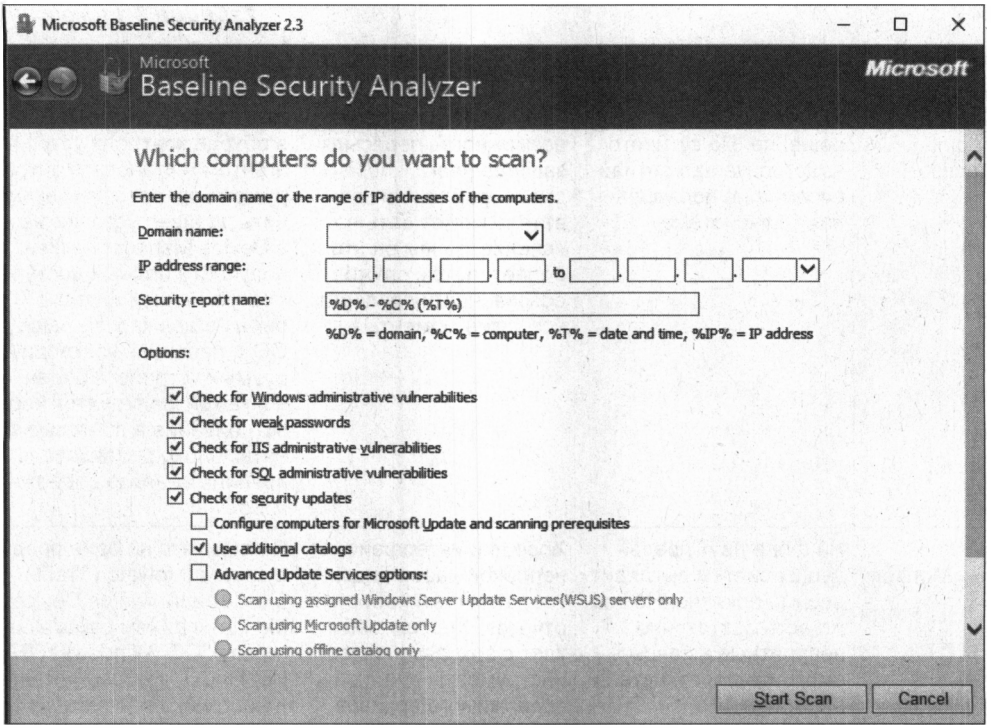


Рис. 9.38. Сканер MBSA

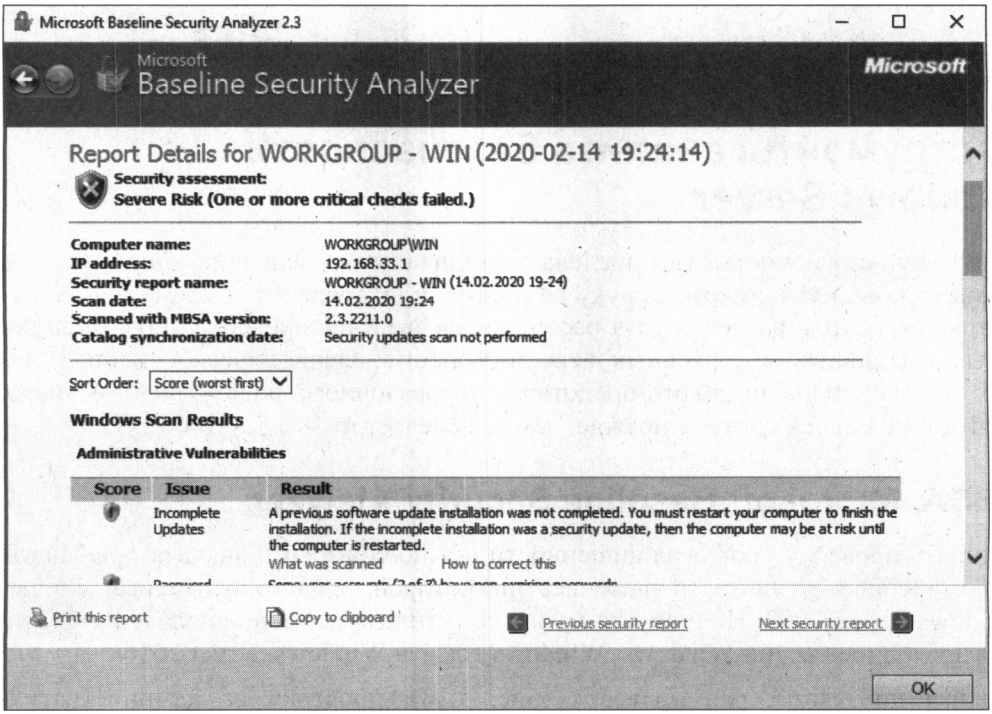


Рис. 9.39. Результат сканирования утилитой Microsoft Baseline Security Alalyzer

лены ли актуальные обновления безопасности. В общем, начинать проверку системы нужно с этой утилиты. Причем проверять не только сервер, но и рабочие станции под управлением Windows. Первым делом надо убедиться, что все системы соответствуют базовым представлениям о безопасности, а потом уже переходить к более сложным сканерам. В результате сканирования вы получите отчет о сканировании узла, в котором будет приведен список проблем и рекомендации относительно того, как эти проблемы исправить (рис. 9.39).

Microsoft Windows Server Best Practice Analyzer

Начиная с версии Windows Server 2012, в серверных операционках от Microsoft появились встроенные инструменты для анализа установленных компонентов на соответствие рекомендациям по информационной безопасности. Как правило, эти средства доступны из Диспетчера серверов.

Просмотреть результаты сканирования можно в самом Диспетчере серверов — на главной странице (**Dashboard**) утилиты прокрутите экран до списка **Роли и группы серверов**, где вы увидите плитки с ролями сервера — например, AD DS, DHCP и т. д. В каждой плитке будет ссылка **Результаты BPA** (рис. 9.40). Первая выводит результаты сканирования, если оно уже было выполнено, вторая — запускает сканирование.

Дополнительную информацию об этом инструменте можно получить на сайте Microsoft по адресу: **https://docs.microsoft.com/en-us/windows-server/administration/server-manager/run-best-practices-analyzer-scans-and-manage-scan-results**.

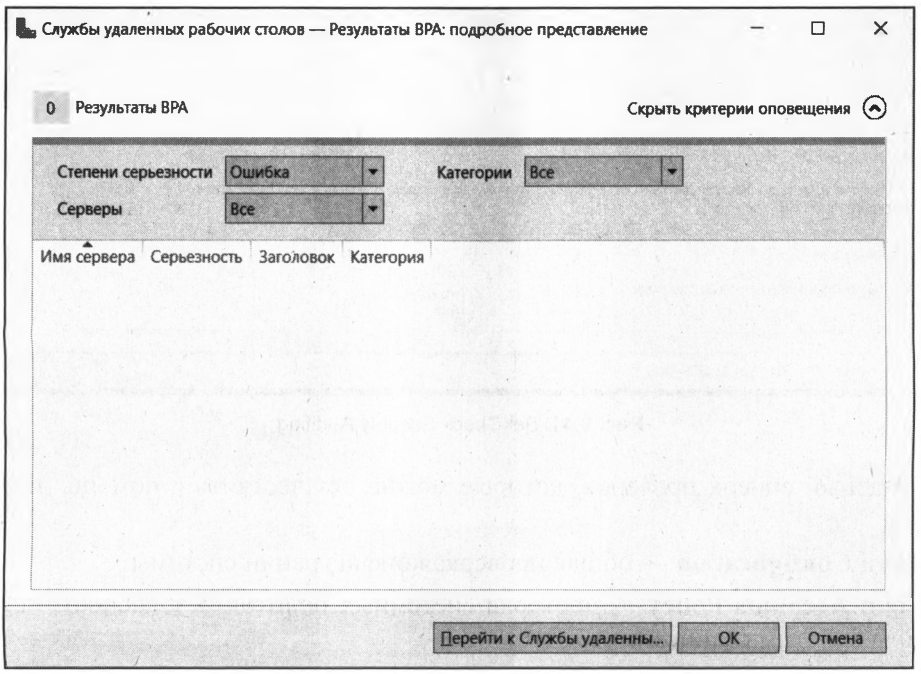


Рис. 9.40. Результаты BPA

SekCheck Security Auditing

Ясное дело, кроме анализаторов безопасности от Microsoft есть и сторонние решения. Одно из таких решений — SekCheck Security Auditing, получить которое можно по ссылке: **https://www.sekchek.com/sekchek-classic-software.htm**.

Несмотря на свой размер, эта утилита является очень мощным средством анализа защищенности и предоставляет отчеты в формате MS Word и Excel. Утилита вычисляет общий рейтинг безопасности и выдает описание найденных проблем безопасности и рекомендации по их устранению. Изюминка утилиты в том, что кроме Windows она поддерживает и другие операционные системы: UNIX, Linux, Novel Netware, IBM iSeries (рис. 9.41). Другими словами, она позволяет произвести комплексный аудит информационной безопасности на предприятии.

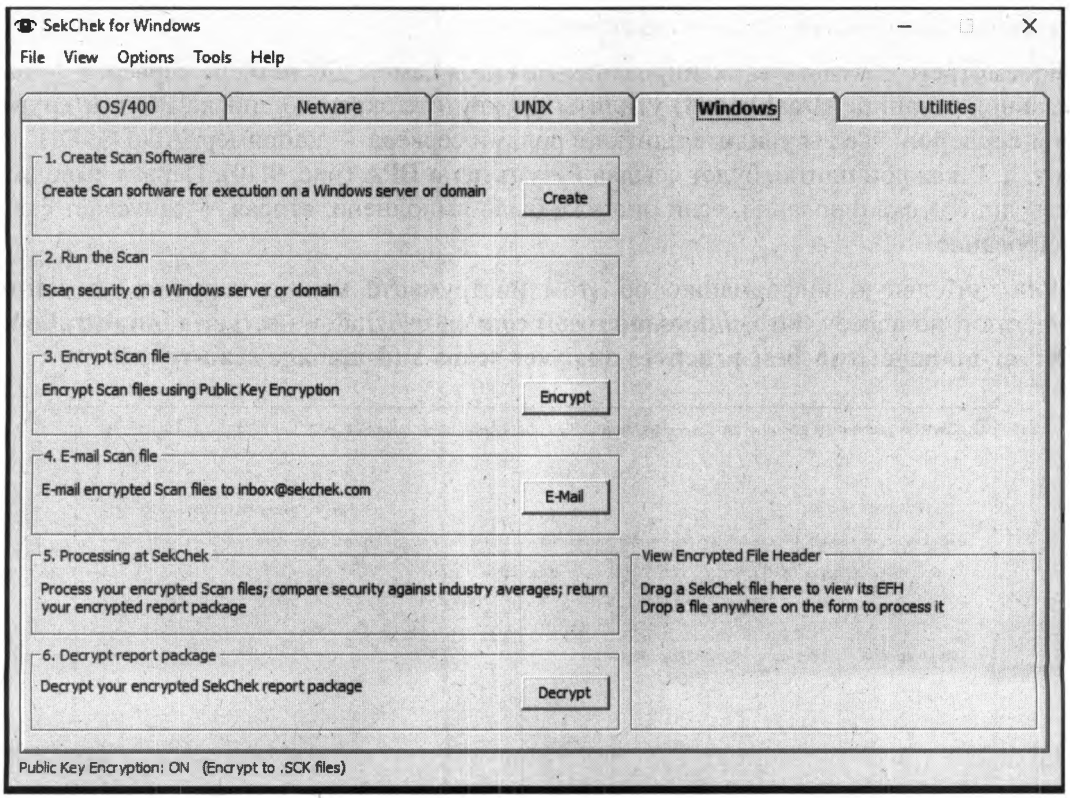


Рис. 9.41. SekCheck Security Auditing

Вот неполный список проверок, которые можно осуществить с помощь этой утилиты:

- **System Configuration** — общая проверка конфигурации системы;
- **System Accounts Policy** — проверка системных политик безопасности для системных учетных записей;
- **Audit Policy Settings** — проверка политик аудита;

- **Registry Key Values** — проверка значений реестра;
- **User Accounts Defined On Your System** — проверка учетных записей пользователя;
- **Local Groups and their Members** — проверка локальных групп и их членов;
- **Global Groups and their Members** — проверка глобальных групп и их членов;
- **Last Logons, 30 Days and Older** — последние попытки входа в систему, в том числе старые для обнаружения неактивных учетных записей;
- **Passwords, 30 Days and Older** — проверка паролей, в том числе тех, которые давно не меняли;
- **Passwords that Never Expire** — отчет по паролям, срок действия которых никогда не истекает;
- **Invalid Logon Attempts Greater than 3** — отчет по неудачным попыткам входа в систему (с числом попыток более 3);
- **Users not Allowed to Change Passwords** — отчет по пользователям, пароль которых изменять запрещено;
- **Disabled Accounts** — отчет по отключенным учетным записям;
- **Network Shares** — проверка общих ресурсов;
- **File Permissions and Auditing** — проверка разрешений файлов.

Скрипт Windows SEC-Audit

PowerShell-скрипт SEC-Audit позволяет проверить настройки безопасности Windows Server. Скрипт абсолютно бесплатен и его можно скачать с GitHub-репозитория по адресу: **https://github.com/Sikkandar-Sha/SEC-AUDIT**.

Сценарий проверяет элементы управления, политики, используемые на отдельной машине или же на контроллере домена, а также параметры безопасности. Работает он просто — содержит список рекомендуемых значений параметров тех или иных политик, и если на ваших системах есть параметры, значения которых отличаются от рекомендуемых, скрипт «бьет тревогу».

В отличие от того же SekCheck, этот скрипт легко использовать для автоматизации проверки уровня защищенности.

Анонимность работы в глобальной сети

В последнее время Интернет становится все менее анонимным. С одной стороны, всевозможные ресурсы и вредоносные программы, собирающие различную информацию о пользователе: IP-адрес, имя, пол, возраст, место жительства, номер телефона. Такая информация может собираться как явно (вы ее сами указываете, заполняя на посещаемых сайтах различные формы-вопросники), так и неявно, когда она определяется на основании косвенных данных (например, ваше местонахождение

при посещении того или иного сайта легко вычисляется по IP-адресу компьютера, с которого вы зашли в Интернет). Вся эта информация может собираться различными сайтами — например, для показа вам рекламных объявлений, привязанных к вашему месту жительства, или в любых других целях. С другой стороны, вас «изучают» силовые органы с помощью оборудования СОРМ (система оперативно-разыскных мероприятий), которое внедряется уже много лет.

Зачем нужна анонимность в Интернете обычному законопослушному пользователю?

Примечание

В побуждения незаконопослушных мы здесь углубляться не станем...

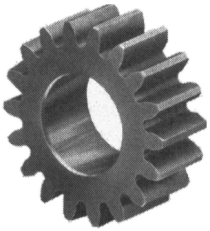
Причины у всех свои, но от них зависят способы достижения цели. В табл. 9.2 приводится несколько типичных задач, которые рано или поздно приходится решать каждому интернет-пользователю.

Таблица 9.2. *Причины сохранения анонимности в Интернете*

Задача	Зачем?	Способы решения
Нужно разово скрыть свой IP-адрес	Вы просто не хотите, чтобы ваш IP-адрес был «записан» сайтом, который вы собираетесь посетить. Вторая причина — ради эксперимента. Например, вы создали свой сайт, установили на нем счетчик и теперь хотите проверить, работает он или нет. Если на сайт вы заходите со скрытого IP-адреса, значение счетчика останется неизменным. Когда же вы зайдете с использованием IP-адреса открытого, значение счетчика будет увеличено	Анонимные прокси-серверы Анонимайзеры
«Смена жительства»	Некоторые сайты разрешают доступ только в том случае, если ваш IP-адрес относится к определенной стране. Пользователям других стран доступ на сайт запрещен	Анонимные прокси-серверы Распределенная сеть Tor
Постоянное анонимное посещение сайтов	Вероятно, вы или скрывающийся блогер (в последнее время — это популярный род деятельности), или же просто не хотите, чтобы администратор (вашей офисной сети или сети провайдера) узнал, какие сайты вы посещаете	Распределенная сеть Tor Проект I2P
Нужно скрыть посещенные сайты от глаз коллег и родственников	У вас нет паранойи, и вам все равно, следит ли за вами администратор, но вы просто не хотите, чтобы ваши родственники или коллеги узнали, на каких сайтах вы бываете	Не нужно никаких специальных средств, достаточно правильно очистить историю браузера или использовать режим приватного просмотра браузера Firefox или Chrome

Таблица 9.2 *(окончание)*

Задача	Зачем?	Способы решения
Нужно посетить заблокированный администратором сайт	«Злой» администратор закрыл доступ к «Одноклассникам» или «ВКонтáкте»? Решение, как всегда, есть!	Распределенная сеть Tor
Зашифровать всю передаваемую вами информацию	Иногда анонимного посещения сайтов мало — важно, чтобы никто не узнал, какую информацию вы передавали этим сайтам (например, какие анкетные данные указывали)	Распределенная сеть Tor



ГЛАВА 10

Отказоустойчивая информационная система

В этой главе речь пойдет о создании отказоустойчивой и надежной информационной системы. Сразу хотим предупредить, что построение такой информационной системы — удовольствие недешевое. И прежде чем приступить к ее созданию, нужно подсчитать стоимость отказа в обслуживании — сколько потеряет предприятие за час, за день, за неделю простоя? Возможно, именно в вашем случае такая система и не нужна, поскольку финансовые потери из-за утраты данных окажутся значительно меньше стоимости создания и обслуживания отказоустойчивой информационной системы.

Уточним для начала, что мы подразумеваем под надежной системой. В свете современных представлений надежной считается система, не имеющая единственной точки отказа. Что произойдет с типичным предприятием, имеющим один сервер, выполняющий функции службы каталогов (Active Directory) и сервера баз данных для «1С:Предприятие», если этот сервер выйдет из строя? Это будет настоящий коллапс. Не нужно долго объяснять, чем обернется для него потеря финансовой информации («1С:Предприятие») или хотя бы остановка работы бухгалтерии на один день. Кроме того, не смогут работать даже те пользователи, которым «1С» и не нужна, — из-за недоступности сервера Active Directory им просто не удастся войти в свои системы. И даже при использовании локальных учетных записей все равно работа сети будет парализована: станут недоступны и сетевые диски, и сетевые принтеры.

Территориальная распределенность

Построение отказоустойчивой системы начнем с *территориальной распределенности*. Зачем она нужна? Смерчи, торнадо, ураганы и извержения вулканов — все это может уничтожить ваше единственное расположение, единственный офис. Но не будем думать о подобного рода катастрофах, а просто представим себе, что у вас исчезло соединение с Интернетом.

И даже если у вас есть резервный канал, то зачастую линии связи проходят по одному и тому же участку. Следовательно, повреждение этого участка каким-нибудь

стихийным бедствием или элементарным пожаром приведет к повреждению и резервного канала связи тоже.

Это же касается и размещения технических средств. Если сетевое хранилище данных, используемое для резервного копирования, находится в одном помещении с сервером, то тот же пожар выведет из строя и сервер, и его резервную копию.

Так что при разработке информационной системы нужно учитывать особенности размещения ее элементов и заранее предусматривать меры, позволяющие восстановить работоспособность системы в любых ситуациях.

Центры обработки данных (дата-центры)

Оптимальный вариант — размещение вычислительных мощностей информационной системы (попросту говоря, серверов) в *центрах обработки данных* (ЦОД) или, как их еще называют, дата-центрах.

ЦОД — это специально подготовленные помещения, обеспечивающие оптимальный режим работы оборудования. И самые серьезные из них — третьего уровня надежности — предусматривают полное дублирование всех систем. Другими словами, дата-центр будет продолжать работать при выходе из строя или выключении для обслуживания любого его узла. Это очень серьезное требование, которое реализуется путем тщательного проектирования. Поэтому построить такой ЦОД очень и очень дорого. В среднем стоимость хорошего ЦОД (а это не только строительные работы, но и оборудование систем электропитания, кондиционирования и аварийного освещения) обходится в 25–30 тыс. долларов США за один квадратный метр его площади.

Понятно, что подобную роскошь может позволить себе не каждая компания, да и стоимость размещения своих серверов в таком ЦОД тоже будет доступна не всем.

С другой стороны, практически каждая компания может позволить себе арендовать облачный ЦОД. Да, имеется в виду виртуализация. И даже если вы против полной виртуализации и еще не можете совсем отрешиться от настоящего «железа», можно развернуть в «облаке» хотя бы резервную площадку, работающую по принципу «теплого» резерва. И если что-то случится с основной площадкой, автоматически начнет работать резервная площадка из «облака».

Далее мы поговорим о требованиях к ЦОД — даже если ваше предприятие не планирует создавать свой собственный дата-центр, вы узнаете, как все там должно быть обустроено.

Требования к помещениям

В Интернете можно найти подробные требования к ЦОД, и нет смысла все их сюда переписывать. Коротко говоря, ЦОД должен размещаться на первом этаже здания, в помещении без окон, трубопроводов и т. п. Нужно избегать и соседства с сооружениями, которые потенциально могут нанести вред его помещению, — с трубопроводами или складами с горючими веществами.

В ЦОД устанавливается весьма дорогостоящее оборудование, поэтому его помещение должно быть стойким ко взлому и оснащено системами контроля доступа.

Материалы внутренней отделки дата-центра должны исключать выделение пыли. Часто для обеспечения чистоты в ЦОД реализуется наддув очищенного воздуха — в этом случае помещение герметизируется и оборудуется входным тамбуром.

Размеры помещения зависят от количества устанавливаемого оборудования (попросту говоря, от количества стоек с серверами) с учетом резерва, который составляет 30–50% от расчетного размера.

Поддержание в помещении постоянной температуры

Одно из основных требований к дата-центру — поддержание температуры. Обычно в ЦОД весьма прохладно — температура устанавливается на уровне 18–20°C (18°C — предпочтительнее). Влажность также не должна быть повышенной, чтобы исключить возможность выпадения росы. В помещении ЦОД обычно не предусмотрена работа персонала — так что не волнуйтесь, что вы и ваши коллеги простудитесь. Но и именно из-за этого нет требований и по воздухообмену. Главное, чтобы воздух был, а его температура не превышала установленных значений.

На поддержание температуры в дата-центре расходуется большая часть потребляемой электроэнергии. Поэтому при проектировании ЦОД надо уделить внимание решениям, позволяющим снизить затраты на электропитание. Решения могут быть разными: от альтернативных источников энергии (хотя, учитывая их стоимость и низкий КПД, они обойдутся очень дорого) до подачи внешнего холодного воздуха зимой для поддержания внутри дата-центра необходимой температуры.

Резервное электроснабжение

Все оборудование ЦОД: серверы, коммутаторы, сетевые хранилища данных и пр. — следует оснащать двумя блоками питания, запитанными от разных линий: основной и резервной. Однако часто реализовать подключение ЦОД к двум независимым вводам от подстанций или выбрать более высокий уровень надежности внешнего электроснабжения невозможно. Поэтому необходимые требования по отказоустойчивости ЦОД нужно реализовывать только путем наращивания мощностей системы резервного электропитания.

Основной параметр такой системы — максимальное время ее автономной работы. Как его рассчитать? Как предугадать, насколько быстро будет возобновлено электроснабжение? Очень часто это время берется «с потолка» — вот представим, что электричество отключат на четыре часа... А что будет, когда это время выйдет? ЦОД потребляет десятки киловатт в час, поэтому система его резервного электроснабжения — устройство весьма дорогостоящее, и даже незначительное увеличение времени автономной работы ведет к ее дополнительному серьезному удорожанию.

При этом — в плане резервного электроснабжения ЦОД — никакие ИБП не помогут, поскольку их мощности окажется недостаточно. Серверы серверами, но есть

еще система кондиционирования, которая потребляет электроэнергии гораздо больше, чем все серверы, вместе взятые.

Минимально необходимое время автономной работы рассчитывается как утроенное время штатного выключения всей информационной системы с сохранением данных. При этом емкость источников аварийного питания следует выбирать с запасом 30%. Однако во многих случаях проще, дешевле и эффективнее использовать дизель-генераторы с автоматическим запуском в случае отключения основного электропитания (если есть такая возможность).

Некоторые разработчики ЦОД на время отключения электропитания предлагают останавливать кондиционеры. Поскольку ЦОД — это полностью закрытое помещение, то сработает эффект «термоса» и некоторое время температура не поднимется выше 20°С (при условии, что исходно она не превышала 18°С). Иногда предлагается, отключив кондиционеры, оставить в работе только вентиляторы. Так можно значительно снизить потребление электроэнергии и в случае ее отключения продлить время автономной работы системы резервного электроснабжения.

Системы пожаротушения

Если площадь дата-центра превышает 20 кв. метров, по правилам пожарной безопасности должны применяться системы газового пожаротушения. При этом желательно, чтобы используемая газовая смесь допускала бы ее вдыхание человеком. Такая система не представляет особой сложности, и ее установку может выполнить любая сертифицированная организация.

Сетевая инфраструктура

Очень важной для дата-центра является и надежность сетевой инфраструктуры. Обычно эта задача решается дублированием каналов связи и активного оборудования (коммутаторов).

Поскольку построение такой инфраструктуры существенно увеличивает стоимость самого дата-центра, то она создается только в том случае, если простои в работе информационной системы недопустимы и могут привести к финансовым потерям.

Выбор правильной топологии сети передачи данных

Топология сети весьма проста — все линии связи должны дублироваться, а дублирующие каналы передачи данных не проходить по тем же участкам, что и основные. Как минимум следует организовать подключение к Интернету через разных провайдеров, причем сами подключения должны быть разных типов — так уменьшается вероятность прохождения каналов связи по одним и тем же участкам. При этом имеет смысл предварительно выяснить у предполагаемых провайдеров, где проложены их линии связи.

Активное сетевое оборудование также должно резервироваться. Это вдвое удорожает инфраструктуру, поэтому резервирование реализуют на уровнях распределе-

ния, ядра и подключения серверной фермы, а оконечные устройства — пользовательские станции — подключают к коммутатору нерезервированной линией связи.

Чтобы не попасть впросак, нужно со всей ответственностью подойти к выбору оборудования и его настройке, не говоря уже о том, что построение отказозащищенной инфраструктуры требует тщательного планирования.

Существуют два варианта построения отказоустойчивой сети с дублированными каналами. Первый вариант использует протоколы, работающие на втором уровне модели OSI. Второй — основан на протоколах маршрутизации третьего уровня модели OSI. Оба эти варианта мы сейчас и рассмотрим.

Построение отказоустойчивой сети на основе протоколов второго уровня модели OSI

Конфигурация на основе протоколов второго уровня модели OSI обеспечивает в случае аварии более быстрое восстановление по сравнению с протоколами третьего уровня. Сеть может восстановиться за 1–2 секунды или даже еще быстрее, если использовать проприетарные[1] протоколы.

Протокол STP

Протоколы STP (Spanning Tree Protocol, стандарт 802.1d) и RSTP (Rapid sTP, 802.1w) обеспечивают автоматическое построение связей сетевой структуры. Суть их работы в том, что коммутаторы пытаются вычислить оптимальные маршруты между всеми устройствами по определенным алгоритмам. При этом для определения маршрутов и контроля соединений по специальным алгоритмам постоянно рассылаются служебные пакеты (Bridge Protocol Data Units, BPDU), и на их основе коммутаторы анализируют и определяют, где подключено активное оборудование, а где — конечные станции. При изменении топологии сети перенастройка ее структуры осуществляется автоматически. При работе по протоколу STP этот процесс, в зависимости от размера сети, занимает от 30 секунд до нескольких минут. Для протокола RSTP это время уменьшено до нескольких секунд.

Протоколы STP/RSTP могут обеспечить связность сети без каких-либо ручных настроек. При построении структуры их алгоритмы учитывают скорость соединения и количество коммутаторов на дублированных линиях связи между точками подключения — администратору нужно лишь включить эти протоколы на портах (часто это предусмотрено настройками по умолчанию для коммутаторов уровня доступа). На основании анализа рассылки пакетов BPDU коммутаторы определяют существующие связи и автоматически отключают порты, к которым подключены вторые, резервные каналы.

Алгоритм изменения конфигурации сети в протоколах STP и RSTP в логический центр сети ставит коммутатор с самым малым весом (Bridge Priority). Для оптимизации процесса настройки сети администратор может вручную эти приоритеты

[1] Проприетарным называется протокол, не являющийся открытым стандартом, а представляющий собой уникальную технологию какого-либо поставщика оборудования.

переназначить. Коммутатор в центре должен иметь самый малый вес. Чем дальше коммутатор находится от логического центра, тем выше его значение Bridge Priority.

Желательно настроить и опцию быстрого старта (Fast Start) для тех портов, к которым подключены конечные устройства. Это исключит их из процедуры определения маршрутов и ускорит процесс перенастройки сети. Однако такая опция возможна только для протокола RSTP.

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

Протоколы STP/RSTP могут использоваться не только при наличии избыточных каналов связи. Включение этих протоколов может сохранить функционирование сети в случае умышленного создания петель, которые без этих протоколов приведут к широковещательному шторму и прекращению функционирования сегмента сети.

Протокол MSTP

Протокол MSTP (Multi Spanning Tree Protocol, стандарт 802.1s) является расширением протокола RSTP на сеть с VLAN.

В отличие от RSTP, протокол 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. Но у этого протокола есть и недостаток — сложность настройки такой структуры. Администратор должен четко представлять разбиение системы на VLAN, оценить потоки данных в каждом сегменте и путем ручной настройки добиться относительно равномерного использования всех каналов связи. К тому же далеко не все коммутаторы поддерживают протокол MSTP.

Отказоустойчивая сеть на основе протоколов третьего уровня модели OSI

Протокол VRRP

Для построения отказоустойчивой сети на основе протоколов третьего уровня используются решения, основанные на протоколах автоматической маршрутизации. Эти протоколы имеют несколько худшие показатели времени перестроения сети, чем протоколы второго уровня, однако трудоемкость настройки структуры сети у них существенно ниже, чем при использовании, например, протокола второго уровня MSTP.

Сеть с резервными каналами связи представляет собой отдельные подсети с несколькими возможными путями передачи данных из одной подсети в другую. Обычно администратору достаточно лишь 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. Недостаток такого решения уже был описан ранее — данные передаются только по одному каналу, а резервный вообще никак не задействован.

Обычно к коммутаторам уровней распределения и ядра подходят несколько каналов связи. В случае отказа одного из них работа продолжается на исправном канале. Однако для рабочих станций существует только одна точка доступа к другим сетям — шлюз по умолчанию. В случае выхода из строя шлюза компьютеры потеряют связь с другими сетями.

Обойти подобную ситуацию можно с помощью протокола VRRP (Virtual Routing Reduntance Protocol). Конечно, лучше использовать другие технологии — например, агрегированные каналы (см. далее), но в случае невозможности их применения подойдет и VRRP.

Недостаток решения на основе протокола VRRP в том, что он поддерживается далеко не всеми моделями маршрутизаторов, — его обычно не поддерживают бюджетные маршрутизаторы.

Принцип создания отказоустойчивого шлюза следующий: в сети устанавливаются два коммутатора с поддержкой VRRP. На каждом из них настраиваются сетевые интерфейсы и включается протокол VRRP. После этого проводится 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 все идет штатно, то по настроенному адресу шлюза работает только главный коммутатор. В случае его выхода из строя данные начинает передавать резервный коммутатор.

Протокол VRRP принят в качестве стандарта, однако некоторые вендоры уже представили свои модификации этого протокола. Например, в реализации VRRP от Nortel оба коммутатора могут работать в качестве шлюзов и передавать данные в другие сети. Мы не станем подробно описывать подобные решения — при наличии заинтересованности нужную информацию вы всегда сможете найти в Интернете.

Агрегированные каналы

Агрегированные каналы описаны в стандарте 802.3ad. Такие каналы позволяют объединить несколько линий связи между коммутаторами в один общий канал передачи данных. Соответственно агрегированный канал имеет пропускную способность, равную сумме пропускных способностей объединяемых каналов. Если все идет штатно, то используется общая пропускная способность всех объединенных каналов. В случае отказа одного из каналов все данные будут передаваться через оставшиеся каналы.

Стандарт 802.3ad позволяет эффективно использовать резервные каналы связи. Дело в том, что провайдеры часто предоставляют клиентам каналы связи с неограниченным трафиком. Следовательно, если не использовать 802.3ad, а отвести

одному из каналов связи роль классического резервного канала, то большую часть времени он будет простаивать, а вы будете за него платить.

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.

Но все имеет свои недостатки, есть они и у этого стандарта — он не поддерживает многоточечное подключение, т. е. соединение может осуществляться только между двумя устройствами. Однако многие поставщики оборудования создали решения, позволяющие обойти такое ограничение. Имеются решения, позволяющие создать агрегированный канал из двух и более линий, соединяющих объединенные в один стек коммутаторы. При этом настройка такого решения выполняется аналогично созданию агрегированного канала в пределах одного коммутатора.

Подобные решения можно найти у различных вендоров: HP, Nortel, Cisco, вот только называются они у каждого из них по-разному. Например, в Cisco интересующая нас технология называется EtherChannel, у Nortel — MLT.

Проприетарные технологии восстановления структуры сети

Произошла авария. Как быстро будет восстановлена структура сети? На основе открытых стандартов реально добиться восстановления работоспособности сети за 3–5 секунд. Это очень хорошие показатели, учитывая, что даже при работе по протоколу STP время восстановления составляет от 30 секунд, что кажется вечностью.

Однако 3–5 секунд — тоже не самый лучший результат. При использовании проприетарных технологий этот период можно сократить до менее чем одной секунды. Некоторые вендоры обещают крайне малые периоды восстановления: 20–30 мс. Конечно, они не рассказывают, в каких условиях были получены такие результаты, поэтому к подобным маркетинговым предложениям следует относиться с осторожностью, особое внимание уделяя не только показателям, но и условиям проведения теста. И перед тем, как сделать выбор в пользу того или иного вендора, ознакомьтесь с результатами, полученными независимыми лабораториями — например, лабораторией Tolly Group (**www.tolly.com**).

Фермы серверов

Ферма серверов — это несколько совместно работающих серверов. Основная задача ферм — балансировка нагрузки, но их можно рассматривать и с точки зрения повышения отказоустойчивости.

Для распределения нагрузки между серверами используются различные решения. Есть аппаратные балансировщики, распределяющие нагрузку на основе учета сете-

вого трафика, есть программные решения, учитывающие загрузку сервера и направляющие новые запросы на менее загруженную систему, и т. п. Самый простой способ — использовать балансировку сетевой нагрузки на основе решения, реализуемого стандартными средствами Windows-серверов.

Как уже было отмечено, существуют различные решения, адаптированные под тот или иной случай использования. Например, в статье по адресу: **https://technet.microsoft.com/ru-ru/library/cc732370.aspx** рассказано, как создать ферму серверов шлюзов удаленных рабочих столов.

Отказоустойчивые решения для приложений

Разработчики программного обеспечения предусмотрели собственные механизмы обеспечения высокой доступности. Такие механизмы реализованы для различных приложений; DHCP-серверов, DNS-серверов, веб-серверов и пр. На практике подобные решения очень эффективны.

DNS-серверы

DNS-серверы служат для разрешения доменных имен в IP-адреса и обратно. При недоступности DNS-сервера работать с информационной системой станет неудобно, а то и вообще невозможно, — это зависит от ее настроек.

Для обеспечения отказоустойчивости в технологиях DNS предусмотрено создание нескольких серверов: *основного* (primary) и одного или нескольких *вторичных* (secondary). При этом клиент получает (например, с помощью DHCP-сервера или при ручной настройке) IP-адреса всех серверов DNS. Если недоступен первый DNS-сервер, задействуется второй и т. д. Обычно поддерживается до четырех серверов DNS.

Как правило, изменения вносятся в основной DNS-сервер, а потом реплицируются на вторичные DNS-серверы. Если основной сервер DNS недоступен, внести изменения в зону невозможно, однако информационная система остается в рабочем состоянии, поскольку работают вторичные серверы, на которых имеется вся нужная информация о зоне.

В домене Windows серверы DNS реализованы на распределенной базе службы каталогов. Этот вариант не только обеспечивает отказоустойчивость, но и позволяет распределять нагрузку — каждый сервер может выступать в роли первичного и вносить изменения в данные зоны. Однако при использовании Windows есть одна большая проблема: при выходе из строя DNS-сервера, IP-адрес которого указан первым в настройках рабочей станции, эта станция не может просто взять и использовать второй IP-адрес (адрес вторичного DNS-сервера), — требуется ее перезагрузка. Вообще-то, обычно это не очень большая проблема, но подобное решение недопустимо для систем, требующих непрерывной работы.

DHCP-сервер

DHCP-сервер обеспечивает автоматическую настройку узлов сети. При его выходе из строя сеть станет неработоспособной. Поэтому при построении отказоустойчивых информационных систем важно обеспечить стабильную работу сетевых служб, в том числе и надежную работу DHCP-сервера.

Ранее в реализации DHCP на основе сервера Microsoft был очень серьезный недостаток, связанный с невозможностью организации его отказоустойчивости. Однако с появлением Windows Server 2012 такая возможность появилась, и реализована она посредством создания отказоустойчивых областей. Подробнее о них вы можете прочитать в *главе 8* книги У. Станека «Microsoft Windows Server 2012 R2: хранение, безопасность, сетевые компоненты. Справочник администратора» издательства «БХВ-Петербург»[1].

В Linux проблема обеспечения отказоустойчивости DHCP-сервера решается довольно просто — вы можете объединить два или более DHCP-сервера в отказоустойчивый пул. Для этого достаточно внести в конфигурацию DHCP-демона следующий блок настроек:

```
pool {

    failover peer "foo";

    <параметры пула>
};
```

Пул использует один диапазон выделяемых адресов для всех серверов, серверы постоянно обмениваются информацией между собой и учитывают адреса, выданные каждым участником пула.

Кластер Oracle RAC

Кластер Oracle RAC (Oracle Real Application Cluster) обеспечивает высокую доступность и распределение нагрузки приложений, работающих с сервером баз данных Oracle.

Oracle RAC — это кластерное решение для сервера баз данных с архитектурой общего кеша. В состав кластера, как правило, входит большое число серверов, а средства управления Oracle обеспечивают равномерное распределение нагрузки и перемещение вычислений в случае отказа одного из пулов.

Это решение загружает все серверы, и чем больше серверов, тем мощнее распределенная база данных.

---

[1] См. **https://bhv.ru/product/microsoft-windows-server-2012-spravochnik-administratora-windows-server-2012-pocket-consultant/**.

Распределенная информационная база программы «1С:Предприятие»

Механизм распределенных информационных баз предназначен для создания территориально распределенных систем на основе идентичных конфигураций программы «1С:Предприятие». Это решение позволяет использовать программу «1С:Предприятие» как в центральном офисе, так и в филиалах. Основано оно на периодической синхронизации данных — изменения, внесенные на сервере, записываются в файл и передаются на другое рабочее место. Принятый файл автоматически обрабатывается, а содержащиеся в нем данные вносятся в локальную копию.

Конечно, у этого решения есть и недостатки: синхронизация требует времени, следовательно, данные обновляются не мгновенно. Некоторые компании отошли от такого подхода в пользу размещения сервера «1С:Предприятие» в «облаке» и предоставления к нему терминального доступа. В этом случае программа «1С:Предприятие» работает в обычном режиме, а пользователи подключаются к ней по RDP. Поскольку в «1С:Предприятие» обрабатываются персональные данные, то должно обеспечиваться шифрование канала.

Дублирование данных

Использование технологий дублирования данных — один из способов обеспечения надежной работы информационных систем. В этом разделе мы рассмотрим различные технологии дублирования данных. Часто такие решения не требуют дополнительных затрат.

Зеркалирование серверов баз данных

Большинство приложений, работающих с систематизированными данными, хранят их на серверах баз данных или SQL-серверах. В связи с распространенностью SQL-серверов для них разработаны решения, обеспечивающие дублирование данных одного сервера на другом.

Зеркалирование (репликация) данных SQL-серверов

Очень часто репликацию данных называют *зеркалированием* базы данных. Вы можете использовать или кластерную систему, или же собственные методы зеркалирования SQL-серверов. В последнем случае можно выделить следующие преимущества:

- зеркалирование можно настроить отдельно для каждой базы данных (в кластере же резервируются все базы данных сервера);
- нет никаких ограничений по оборудованию, которые могут быть актуальными для других вариантов;
- нет необходимости покупать дополнительное оборудование — дублирование производится по обычной сети передачи данных;

- зеркалирование можно настроить в разных режимах. Так, в режиме *активный/пассивный* изменения могут вноситься только на первом сервере, а на втором содержится лишь копия данных. В режиме *активный/активный* изменения можно вносить на каждом сервере.

Основной сервер пересылает на вспомогательный сервер *журнал транзакций* — журнал, в который вносятся изменения в данных. Второй сервер обрабатывает журнал и вносит изменения в свою копию данных. Поэтому можно говорить об асинхронном характере передачи данных.

Операции по изменению данных могут накапливаться по мере изменения базы данных и не вноситься на второй сервер, например из-за сбоя сети. В итоге второй сервер может гарантировать идентичность данных только при нормальном функционировании обоих серверов и сети передачи данных. Именно поэтому администратор обязан постоянно контролировать состояние репликации данных.

Ранее было отмечено, что репликация может быть настроена в двух вариантах: активный/активный и активный/пассивный. Вариант активный/пассивный — это простейший случай, когда данные могут меняться только на одном сервере. Обычно с таким способом репликации никаких проблем нет.

Но если нужно настроить репликацию в обе стороны, и изменения возможны на обоих серверах, неизбежны конфликты. Например, изменения на одном сервере могут противоречить изменениям на другом: пусть на одном сервере значение A равно 100, а на другом — 200. Какое из этих двух значений считать правильным и включить в окончательный вариант БД? Именно поэтому настройку двухсторонней репликации должен выполнять подготовленный администратор баз данных, который хорошо понимает внутреннюю структуру системы и обрабатываемых данных.

Сама настройка зеркалирования не представляет сложности — вам нужно предварительно сделать полную копию данных и включить режим восстановления **Full**. После этого один из серверов назначается *издателем* (publisher) — это главный сервер. А все остальные, которые будут копировать с него данные, будут называться *подписчиками* (subscribers). После настройки репликации надо обязательно проверить ход ее выполнения в системных журналах.

Снимки баз данных

Многие серверы SQL позволяют создавать *снимки данных* (snapshot) — они часто используются при первичном копировании данных на второй сервер. Эта операция выполняется средствами администрирования сервера, и мы не будем на ней акцентировать ваше внимание.

Настройка клиентских подключений

Обычно прикладные программы настраиваются на подключение к одному серверу баз данных. Поэтому в случае отказа основного сервера БД приложение не может автоматически переключиться на второй сервер, где размещена копия БД, и пользователь получит сообщение об ошибке, исправить которую можно лишь отредактировав строку с именем сервера в настройках программы. Конечно, это выход, но

хотелось бы выполнить перенастройку программы без привлечения лишнего внимания пользователя.

Чтобы программа могла автоматически переключаться на другой сервер, она должна быть соответствующим образом настроена. Если программа для доступа к данным использует клиенты Native client или ADO.NET, то задать сервер с копией данных можно так:

```
"Server=server1; Failover_Partner=server2; Database=office"
```

Распределенная файловая система

В Windows для подключения к общим сетевым ресурсам используется следующий формат адреса: **//имя_сервера/имя_ресурса**. Понятно, что при выходе из строя сервера сетевой ресурс, заданный с помощью такого адреса, станет недоступным. Исключить одну такую точку отказа позволяет *распределенная файловая система* (Distributed File System, DFS), реализованная на серверах Windows 2000 и старше.

Распределенная файловая система также упрощает и администрирование — вы можете прозрачно для пользователей перемещать совместно используемые файловые ресурсы с одного компьютера на другой без прекращения обслуживания и перенастройки рабочих станций.

Для Linux-систем на сегодняшний день, к сожалению, нет выделенного стандартного решения. Что-то наподобие DFS можно реализовать средствами NFS, automount и LDAP/NDIS, но все это сложно и не очень гибко. Можно использовать также файловые системы XtreemFS, GlusterFS, GFS (Google File System), GPFS (General Parallel File System), Lustre и др. — это неплохие решения, но все равно немного не то, хотя и лучше, чем вообще ничего. Информацию о настройке этих файловых систем вы с легкостью найдете в Интернете.

Создание DFS

Структура распределенной файловой системы чем-то похожа на дерево каталогов. В корне дерева расположена точка входа, называемая *корнем DFS*. Структура DFS-домена хранится в службе каталогов (AD). А сам корень DFS — это набор ссылок на совместно используемые ресурсы, которые находятся на разных компьютерах сети.

Создается корень DFS средствами Windows Server 20*xx*. В одном домене может поддерживаться несколько корней DFS, на обычных же серверах допускается наличие только одного DFS-корня. В роли корня DFS может выступать любая совместно используемая папка. В этой папке не должны храниться файлы, а только ссылки на сетевые ресурсы.

После создания корня нужно собрать структуру папок DFS. Для этого используется оснастка управления **Управление DFS**, или DFSGUI.MSC (рис. 10.1), вызвать которую можно через меню **Средства** Диспетчера серверов.

Если администратору сети нужно переместить ресурс из DFS-структуры на другой сервер, можно просто скопировать файлы по новому пути и заменить ссылку со

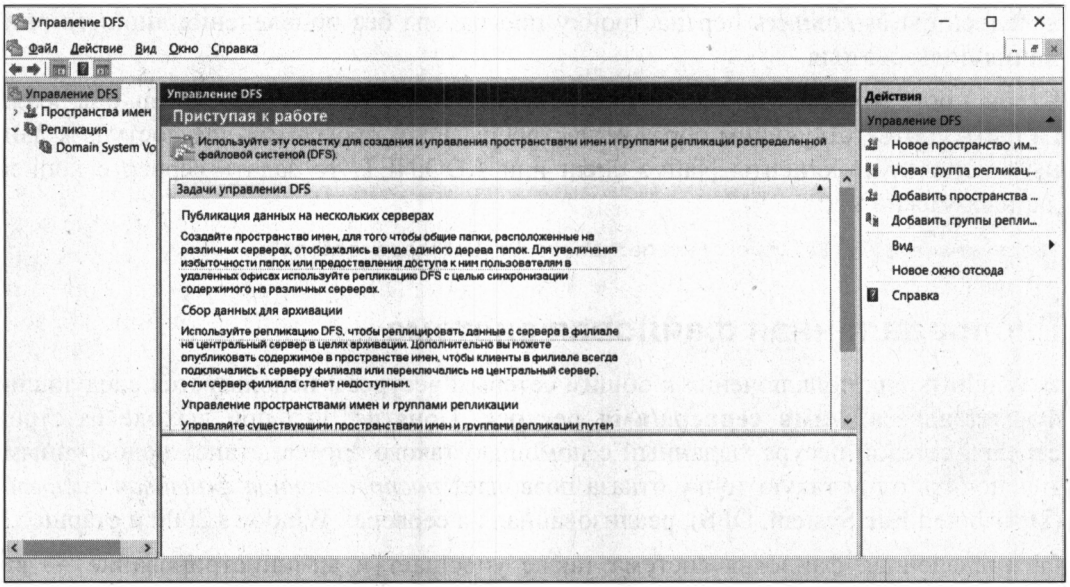


Рис. 10.1. Оснастка управления DFS

старой сетевой папки на новую — для рабочих станций все используемые сетевые пути останутся неизменными.

Репликация DFS

Структуру DFS также можно сделать *отказоустойчивой*. Для этого каждую ссылку нужно продублировать путем создания второй ссылки на аналогичный сетевой ресурс на другом компьютере. В результате, если один ресурс окажется недоступен, клиенты будут перенаправлены на работающий компьютер. Система также будет автоматически синхронизировать имеющиеся ресурсы — если данные будут изменены по одной ссылке, то они продублируются и по другой.

Реплицируемые ресурсы должны находиться на носителях, отформатированных в файловую систему NTFS 5.0. Эта версия файловой системы использует систему протоколирования 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 выключена. Для ее включения нужно выделить соответствующие ссылки на ресурсы и выбрать команду **Синхронизовать**. При создании репликации требуется указать, какой ресурс будет являться *основным* (мастером). По завершении репликации все ссылки станут равнозначными — при изменении данных по одной ссылке они будут также доступны и по второй.

Надо отметить, что автоматически синхронизируются не все файлы. Так, не реплицируются временные файлы. А остальные файлы реплицируются после того, как

с ними завершена работа пользователя. Если с файлом одновременно работают два пользователя или более, да еще и 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 разнесенных площадках. Тем более что в последних версиях серверов используется механизм пересылки только измененных блоков, а не всего документа, что снижает трафик между узлами. Тем не менее 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.

Для настройки графика репликации выполните следующие действия:

1. Запустите оснастку **Пользователи и компьютеры Active Directory** (оснастка DSA.MSC).
2. В меню **Вид** выберите пункт **Дополнительные компоненты**.
3. В левой области последовательно щелкните двойными щелчками на значках **Система** (System) | **Службы репликации файлов** (File Replication Services) | **Тома DFS** | **Контейнер корня DFS**. Объекты подключения DFS отображаются в правой области для каждого уровня пространства имен DFS, где включена репликация DFS в распределенной системе диспетчера файлов (оснастка DFSGUI.MSC).
4. Щелкните правой кнопкой мыши на объекте подключения и нажмите кнопку **Изменить расписание** (рис. 10.2).

Рис. 10.2. Настройка графика репликаций DFS

Примечание

Существуют и другие способы изменения расписания — через оснастку *DFSGUI.MSC*, например. Для этого нужно перейти в группу **Репликация**, щелкнуть правой кнопкой мыши на нужной группе репликации, выбрать команду **Свойства**, а затем нажать

кнопку **Изменить расписание**. Также расписание можно изменить при создании новой группы репликации в оснастке **Управление DFS**. Подробное описание настройки процесса репликации доступно по ссылке: **https://www.vembu.com/blog/distributed-file-system-dfs-windows-server-2016-brief-overview/** или на сайте Microsoft: **https://docs.microsoft.com/ru-ru/windows-server/storage/dfs-replication/dfsr-overview**.

Поддержка DFS в Linux-системах

Хотя для Linux и нет аналога DFS, полностью соответствующего всему функционалу DFS в Windows, на Linux-системах также могут быть размещены корни DFS. Обеспечивает эту функциональность пакет Samba.

Для размещения корня DFS достаточно в глобальной секции конфигурации Samba указать строку: `host msdfs = yes`, а в определение совместно используемого ресурса добавить строку: `msdfs root = yes`.

Поскольку корни DFS включают ссылки на другие совместно используемые ресурсы, то для их создания используется команда `ln` с указанием типа ресурса (`msdfs`):

```
# ln -s msdfs:storage1\\share1 link1
# ln -s msdfs:server1\\share,server2\\share link2
```

Указание двух ссылок на один ресурс означает включение балансировки ресурсов.

В результате конфигурация корня DFS в конфигурации демона Samba будет выглядеть примерно так:

```
...
    [global]
        host msdfs = yes
...
    [dfs]
        path = /dfs
        msdfs root = yes
...
```

Корни DFS на Samba-сервере работают со всеми DFS-клиентами Windows. Обратите внимание, что имена DFS-корням в Samba нужно указывать только в нижнем регистре. Администратору также следует назначить необходимые права доступа на папки с ресурсами и проконтролировать, чтобы на момент создания состав предполагаемых к балансировке папок был идентичным.

Кластеры

Кластер — это приложение, работающее на нескольких серверах и мигрирующее с одного сервера на другой при возникновении отказа оборудования. О кластерах слышали многие администраторы, но относительно мало кто использовал их на практике. Однако все мы знаем, что кластеры — это одно из лучших решений обеспечения отказоустойчивых вычислений.

Кластерные решения предлагают многие производители. Одни из самых известных: IBM HACMP, HP ServiceGuard, IBM Tivoli System Automation for Multiplatforms (SA MP), Linux-HA, Microsoft Cluster Server (MSCS), NEC ExpressCluster, Red Hat Cluster Suite, SteelEye LifeKeeper и Oracle Cluster. Кластер можно создать и собственными силами на базе Linux (чуть позже, в *разд. «Кластер openMosix»*, мы вкратце коснемся того, как это сделать).

Сейчас же мы рассмотрим решение от Microsoft как наиболее легко интегрируемое в существующую информационную систему на базе Windows.

Кластер Microsoft

Кластер Microsoft можно создать на базе старших версий Windows Server: Enterprise Edition или Datacenter. Для создания кластера необходимы два физических сервера (желательно одинаковых) и система хранения, позволяющая осуществить одновременное подключение диска к двум серверам.

Система хранения обычно подключается с использованием технологий iSCSI или Fibre Channel. Системные требования к оборудованию, на котором будет развертываться кластер, работающий под управлением Windows Server 2016/2019, можно найти по ссылке: **https://docs.microsoft.com/en-us/windows-server/failover-clustering/clustering-requirements**.

Для системы хранения — чтобы она не стала единственной точкой отказа — нужно использовать дублированные подключения. При этом вам понадобятся специальные драйверы вроде multipath-драйверов, а для собственно подключения должны использоваться несколько сетевых адаптеров. На рис. 10.3 приводится одна из возможных конфигураций кластера.

Серверы, объединяемые в кластер, должны иметь по два сетевых интерфейса: первый будет использоваться для внутренней сети синхронизации управления, а второй — для передачи обрабатываемых данных. Конечно, можно сэкономить и создать «бюджетный» вариант кластера, вот только если вам действительно нужен кластер, мы не уверены, что стоимость нескольких сетевых адаптеров уж как-то повлияет на общую картину.

Для организации кластера требуется создать *кворумный* диск (от слова Quorum) — ему достаточно выделить 150–200 Мбайт дискового пространства. Обычно кворумному диску назначают букву Q:.

После подключения кворумного диска к обоим серверам и настройки сетевых интерфейсов можно начать создание кластера, запустив соответствующий мастер. Обычно создание кластера с помощью мастера проблем не вызывает — все просто и понятно: на серверах будут созданы службы кластеров, появятся оснастки управления, кластеру будет присвоено новое имя и новый сетевой адрес.

По умолчанию кластер от Microsoft используется для резервирования основных служб: файловых, сертификатов и пр. Чтобы в кластере работали приложения (с использованием всех преимуществ отказоустойчивости), они должны быть разработаны специально для кластера. Если приложение не поддерживает кластер,

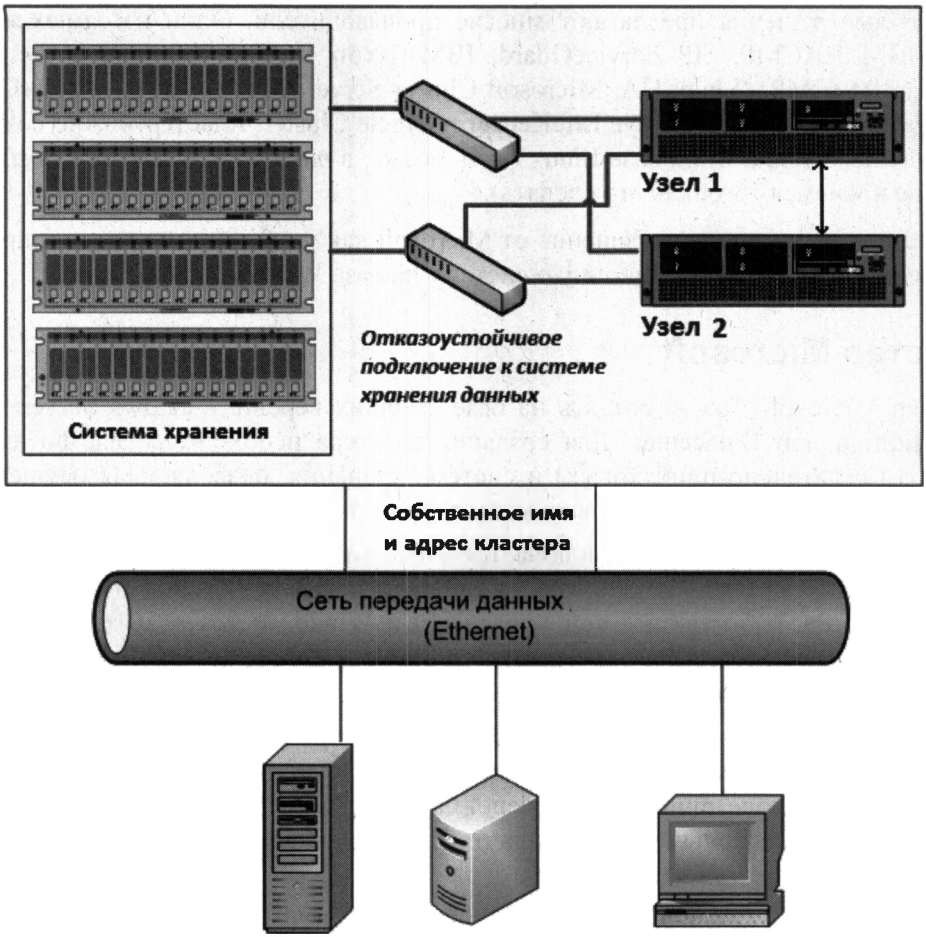


Рис. 10.3. Вариант построения кластера от Microsoft

раскрыть его потенциал в кластере не получится. В случае с Microsoft в кластере могут работать сервер баз данных и почтовый сервер.

При установке приложения в кластер используется специальный вариант запуска программы установки, который создает новый экземпляр сервера (новое имя, новый адрес) и прописывает в настройках службы кластеров параметры резервированных компонентов.

На рис. 10.4 показано окно администратора кластеров с отображением ресурсов программы Symantec NetBackup. При установке этой программы были добавлены ресурсы системы резервного копирования. А в администраторе кластеров вы можете увидеть состояние этих ресурсов, уточнить узел, где в настоящий момент работает программа, добавить или удалить ресурсы и т. п.

В случае отказа узла, к которому подключены ресурсы кластера и где выполняется какая-либо программа, она запускается на другом узле и все ресурсы мигрируют на него (например, осуществляется переподключение дисков системы хранения).

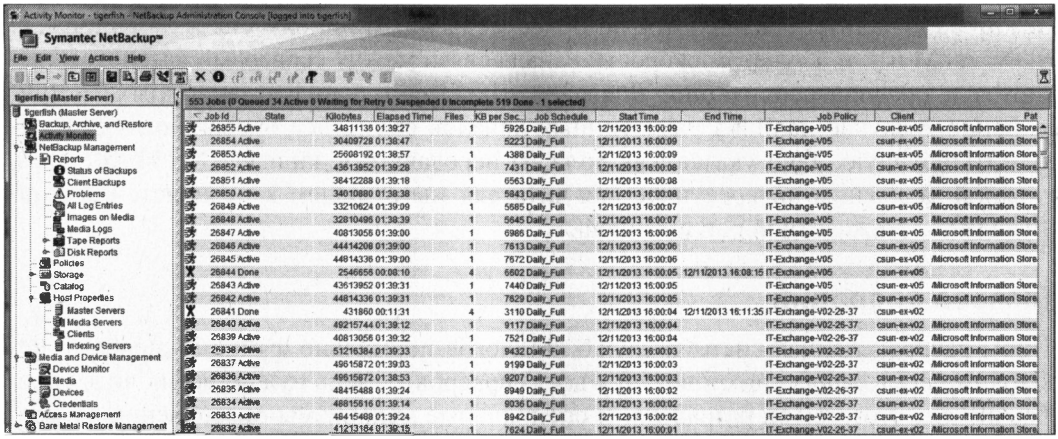


Рис. 10.4. Администратор кластеров для ресурсов NetBackup

Понятно, что такое переключение не происходит мгновенно и что обслуживание потребителей информационной системы на время этого периода прерывается. Но переключение происходит достаточно быстро (от нескольких секунд до десятков секунд — в зависимости от числа ресурсов и сложности приложений), и пользователю обычно достаточно просто повторить операцию, во время которой произошла ошибка.

> ***Совет***
>
> После установки кластера необходимо проверить журналы системы на отсутствие ошибок, проконтролировать состояние ресурсов в консоли администратора и в обязательном порядке протестировать непрерывность обслуживания путем симулирования отказа активного узла кластера.

Распределенные каталоги

Все мы знаем, что для централизованного управления сетевыми ресурсами (серверы, общие папки, принтеры, пользователи и пр.) созданы специализированные средства — *каталоги* — и стандартизованы протоколы работы с ними (X500, LDAP и т. п.). Эти каталоги изначально проектировались с учетом обеспечения распределения нагрузки и исключения единой точки отказа.

Самый яркий и известный пример такого каталога — Active Directory (AD) от Microsoft. В среде Linux часто используется каталог OpenLDAP — это бесплатный аналог AD.

Репликация данных каталогов

Для обеспечения отказоустойчивости в системе обычно устанавливается несколько серверов каталогов, при этом между ними настраивается репликация данных.

В службе каталогов Microsoft для сопоставления физической и логической структур данных введено понятие *сайта*. Сайт объединяет серверы (и пользовательские системы) в пределах локальной сети (где быстрые каналы связи).

Между собой сайты соединяются по более медленным линиям связи — например: ISDN, ATM и т. п. С учетом скорости канала связи между серверами каталогов создаются и правила репликации. Для сложных структур информационных систем, особенно в случае наличия разнотипных каналов связи, эту операцию лучше выполнить вручную, явно указав, как должны передаваться данные. Это может стать сложной задачей, и интересующегося читателя мы отошлем к первоисточнику по управлению межсайтной репликацией[1].

Хозяева операций

Чтобы распределенная система служб каталогов нормально функционировала, необходима постоянная синхронизация всех серверов — ведь нужно исключить сбои. Именно для этого были разработаны специальные механизмы обеспечения распределенной структуры, называемые *хозяевами операций*.

Хозяин операции — это сервер каталога, являющийся главным (мастер-сервером) по какой-либо функции. Такие функции носят название Flexible Single Master Operation role (FSMO). В доменах Windows 20*xx* их пять:

- **владелец схемы** (Schema master) — контролирует обновления и модификации схемы каталога. Для обновления схемы каталога вы должны получить доступ к владельцу схемы;
- **владелец доменных имен** (Domain naming master) — контролирует добавление или удаление доменов в лесу. Для добавления или удаления доменов вам нужно получить доступ к владельцу доменных имен;
- **владелец относительных идентификаторов** (RID master) — распределяет относительные идентификаторы контроллерам домена. Независимо от того, создаете ли вы объект пользователя, группы или компьютера, контроллеры домена присваивают этому объекту уникальный идентификатор безопасности;
- **эмулятор основного контроллера домена** (PDC emulator) — когда вы используете операции смешанного режима, эмулятор PDC работает как Windows NT PDC. Его задача — аутентификация входов Windows NT, процесс изменения паролей и репликация обновлений на BDC;
- **владелец инфраструктуры домена** (Infrastructure master) — обновляет ссылки объектов путем сравнения данных из каталога с глобальным каталогом. Если данные устарели, владелец инфраструктуры запрашивает обновленные данные из глобального каталога и затем реплицирует изменения на другие контроллеры домена.

При первоначальной установке домена все пять ролей зафиксированы за первым контроллером. Впоследствии, с учетом специфики структуры организации, их можно переносить на другие контроллеры. Важно только, чтобы при исключении контроллера домена администратор проследил, что все эти пять операций не потеряли хозяина.

---

[1] См. **http://technet.microsoft.com/en-us/library/cc961783.aspx**.

Чтобы определить, какой сервер является текущим владельцем схемы в домене, откройте командную строку и введите команду:

```
dsquery server -hasfsmo schema
```

Для определения сервера, являющегося текущим хозяином доменных имен, откройте командную строку и введите команду:

```
dsquery server -hasfsmo name
```

Определить, какой сервер является текущим мастером операций инфраструктуры, можно, открыв командную строку и введя команду:

```
dsquery server -hasfsmo infr
```

Для определения сервера, являющегося текущим владельцем относительных идентификаторов для домена, откройте командную строку и введите команду:

```
dsquery server -hasfsmo rid
```

Чтобы определить, какой сервер является текущим эмулятором PDC, откройте командную строку и введите команду:

```
dsquery server -hasfsmo pdc
```

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 ту или иную роль, и выполнить соответствующую команду в меню.

При корректном исключении сервера каталога (путем снижения его роли командой `dcpromo`) мастер операций отслеживает состояние ролей. В случае аварии система может остаться без хозяина какой-либо роли. В этом состоянии служба каталогов не может находиться долго, и необходимо назначить нового хозяина операции.

Все операции по переносу ролей можно выполнить в командной строке. Для этого используется утилита ntdsutil. Главное, что эту утилиту можно применять 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 ntdsutil 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 команду `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 создаются специальные контроллеры, которые хранят (в режиме «только для чтения») *все объекты леса*, но только не с полным, а с частичным набором атрибутов. Такие контроллеры называются *серверами глобального каталога* (Global catalog, GC).

Сервером глобального каталога может быть назначен любой контроллер домена. Назначение контроллера домена сервером глобального каталога выполняется 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 два раза по сравнению с «полным» вариантом описания объекта. Но если конкретным приложениям необходим частый доступ к нереплицируемым атрибутам, 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, и 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).

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.

Отказоустойчивые решения и виртуальные системы

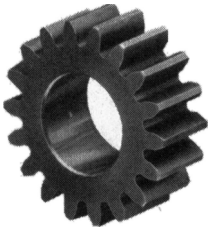
В корпоративных версиях VMware реализованы технологии обеспечения высокой доступности — для обеспечения такой доступности должны быть отдельно приобретены компоненты vSphere.

Высокая доступность реализуется за счет параллельной работы нескольких виртуальных машин. Специальные компоненты обеспечивают синхронизацию оперативной памяти двух машин и переключение расчетов в случае отказа основной виртуальной системы. Соответственно, по этой технологии на виртуальной машине защищаются любые приложения и данные.

Однако у этого решения есть и недостатки. Оно предъявляет к виртуальным машинам определенные требования: идентичность процессоров и наличие аппаратной поддержки виртуализации, необходимость развертывания управляющего центра, наличие нескольких высокоскоростных сетевых адаптеров, наличие системы хранения (диски защищаемых машин автоматически переводятся в «толстый» тип, если они были созданы в режиме «тонких» дисков) и т. п.

Нужно отметить, что такое высокодоступное решение может быть реализовано для любых операционных систем, поддерживающих vSphere.

ГЛАВА 11



Порядок выявления неисправностей и их устранения

В современном мире, когда в электронном виде обрабатывается практически вся информация, а на бумагу переносится лишь небольшая ее часть, отказы информационной системы обходятся очень дорого. Одна из задач администратора заключается в предупреждении отказов и сокращении времени простоя оборудования.

Если отказ уже произошел...

Самое главное — не паниковать. Что случилось, то случилось. Нужно собраться с мыслями и подумать, что можно сделать.

Первым делом надо попытаться получить максимум информации о неисправности. Часть информации об отказе можно почерпнуть из системных журналов, часть — от пользователей. Конечно, иногда отказ бывает такого размаха, что журналы тоже недоступны. Впрочем, это, как правило, следствие халатности администратора, который не обеспечил резервное копирование системных журналов.

Затем администратор должен составить перечень возможных причин отказов и оценить время устранения каждой из них. Не нужно начинать устранение неисправности с самых затратных позиций, если вы не уверены точно, что именно они стали причиной сбоя.

Потом шаг за шагом устраняйте возможные причины сбоя. На каждом шаге проверяйте результат — вдруг причина сбоя обнаружена и сбой устранен. Если не получилось, придется весь процесс начинать заново — составить новый план действий и пройти уже по нему.

Не нужно вносить сразу много изменений в настройки. Внесли одно изменение — попробовали. Внесли второе — опять попробовали и т. д. Записывайте все, что вы делаете, — эти записи помогут вам вернуться в исходную точку, если систему так и не получится восстановить.

Обязательно составьте протокол отказа, в котором опишите причину отказа и способ ее устранения. Такой документ не только послужит вам в качестве отчета перед вышестоящим начальством, но и поможет специалисту, который спустя некоторое

время, возможно, придет на ваше место, — вы сэкономите ему и предприятию много времени и нервов, если аналогичный сбой повторится.

Максимальный аптайм

Некоторые хостеры утверждают, что аптайм[1] их серверов равен 99,999%. На практике этот показатель при круглосуточной работе соответствует примерно пяти минутам простоя за год.

Достичь такого результата — не просто. Здесь нужны большие вложения в виде соответствующего оборудования и обслуживания. Часто подобные затраты нереальны для малых и средних предприятий. Что же по силам небольшим предприятиям? Максимум, что они могут сделать, — это установить источники бесперебойного питания и сетевые хранилища, на которые будет производиться резервное копирование информации.

Задача администратора — создать все условия для оперативного восстановления информации. У него должен быть план на случай возникновения нештатной ситуации — план обеспечения непрерывности функционирования информационной системы.

В этот план надо внести список действий, которые необходимо осуществить в случае отказа оборудования или в различных нештатных ситуациях. В плане должно быть четко указано, что делать в случае возникновения того или иного отказа. Вот примерный список того, что нужно включить в план обеспечения непрерывности:

- место (компьютер, сервер, устройство), куда производится резервное копирование;
- указание, какими средствами производится резервное копирование и как произвести восстановление информации;
- мероприятия на случай выхода из строя жесткого диска;
- описание процедуры подключения другого жесткого диска и ввода его в состав RAID-массива без выключения системы;
- место хранения дистрибутивов программ и операционных систем на случай их переустановки.

Описав все возможные аварийные ситуации и способы их устранения, можно примерно оценить стоимость и время восстановления системы при различных отказах.

Восстановление с нуля, или полное фиаско

Нужно быть готовым к худшей ситуации. Представьте, что сервер «сгорел». Как вы будете его восстанавливать? Перед вами — новый и «голый» компьютер. Где взять

---

[1] Аптайм вычислительной системы (от *англ.* uptime) — время непрерывной работы вычислительной системы или ее части. Измеряется с момента загрузки и до момента прекращения работы (зависания, перезагрузки, выключения, прекращения работы анализируемого приложения).

дистрибутивы? Откуда восстановить данные? Есть ли полные образы уже настроенной системы?

Помочь в такой ситуации может только регулярное резервное копирование всей информации. Кроме копирования баз данных и других реальных данных пользователей нужно создавать и поддерживать образ всей системы для ее максимально быстрого восстановления.

Запасные детали

Не следует забывать и о запасных деталях. Недопустимо, когда простой всей информационной системы вызван, скажем, сгоревшим блоком питания. К сожалению, крупные предприятия — это огромные бюрократические машины, и чтобы купить что-либо нужное, требуется получить несколько подписей, а это все — время простоя. В конечном счете сделают виноватым администратора.

Чтобы не возникало таких неприятных ситуаций, надо заранее обеспечить свои устройства запасными деталями. Такой список уже приводился в этой книге, но лучше его повторить, чтобы вы лишний раз ее не листали:

- блоки питания разных типов;
- если на предприятии используются одинаковые модели ноутбуков (что часто бывает — как правило, закупают оборудование небольшими партиями, а не поштучно), нужно приобрести хотя бы одно зарядное устройство подходящего типа;
- оперативная память разных типов;
- клавиатуры и мыши;
- патч-корды разной длины;
- жесткие диски разных типов.

Как показывает практика, спустя 3–4 года будет трудно купить комплектующие, которые сегодня считаются вполне современными. Например, в 2008 году жесткими дисками ATA (IDE) комплектовалась основная масса компьютеров, а уже в 2010-м их стало найти крайне сложно, да и цена их была выше жестких дисков SATA аналогичного размера. Сейчас ситуация стабилизировалась, и жесткие диски в основном поставляются с интерфейсом SATA (за исключением ноутбуков, где могут быть разъемы M.2, U.2, U.3, но выход из строя накопителя одного пользователя — не так страшен, как выход из строя накопителя сервера, который нужен всем), однако это не освобождает от необходимости их заблаговременной покупки. Присутствующий на предприятиях среднего и большого размера определенный процент «забюрокраченности» делает невозможным быстрое приобретение вышедшего из строя аппаратного обеспечения. А если жесткий диск уже будет в наличии, то это существенно минимизирует время простоя информационной системы.

Формировать фонд запасных частей можно и за счет модернизации компьютеров — например, постепенно производить замену обычных жестких дисков на вы-

сокоскоростные SSD. Снятые жесткие диски при этом выбрасывать не нужно — в крайнем случае их можно будет временно использовать, если из строя выйдет SSD или какой-то другой жесткий диск. Цены на SSD становятся все доступнее, поэтому такая стратегия имеет право на существование.

Также не нужно забывать о времени наработки на отказ. Современные SSD некоторых моделей (например, Evo от Samsung) подсчитывают «мото-часы» — количество часов работы, и, если это время будет превышено, при запуске компьютера встроенная в BIOS утилита S.M.A.R.T. сообщит о наличии такой проблемы. И хотя с диском может быть все прекрасно, но пользователи будут жаловаться, поэтому неплохо бы иметь 1–2 таких накопителя «про запас».

Где получить помощь?

К каким источникам обращаться в случае проблемы? Первый источник — это документация по системе. Справочная система Linux максимально информативна, а в современных дистрибутивах — еще и на русском языке. Справочная система Windows пусть и не столь дружелюбна, но в последнее время наблюдаются существенные сдвиги в лучшую сторону.

Кстати, по продуктам Microsoft можно попытаться получить помощь на портале Microsoft Docs по адресу: **https://docs.microsoft.com/ru-ru/** — здесь очень много полезной и практической информации.

Не нужно забывать и про техническую поддержку производителя. В конце концов вы покупаете лицензионное программное обеспечение, платите огромные деньги за дорогущее оборудование и вправе требовать технической поддержки производителя — разработчика ПО или создателя оборудования. Обычно такая услуга является платной, и лучше оплатить подписку на техническую поддержку заранее — до того, как возникнет неполадка. Впрочем, стоимость подписки малым компаниям может показаться заоблачной. Для средних, скорее всего, стоимость часа простоя тоже не столь высока, чтобы оплачивать подписку на техническую поддержку. А вот для крупных компаний она просто необходима — с ее помощью у вас больше шансов сэкономить время, а значит, и деньги компании.

Если помощь не удалось получить в официальных источниках, попробуйте поискать решение проблемы в Интернете. Вы — не единственный пользователь и, скорее всего, вы не один, кто сталкивался с подобной проблемой. Смело ищите ответ на свой вопрос в Интернете, в различных FAQ и конференциях (форумах) — вы наверняка найдете там подходящее решение.

Сбор информации об отказе

Чтобы успешно решить проблему и предотвратить ее появление в будущем, нужно собрать как можно больше информации об отказе. Собранная информация должна быть качественной, иначе толку от нее будет немного.

Для сбора информации нужно анализировать следующую информацию о системе:

- доступные журналы: журнал событий Windows, syslog для UNIX-систем, журналы приложений;
- время возникновения проблемы;
- операции, которые выполнялись в этот момент;
- проводились ли изменения в настройках системы перед возникновением проблемы, менялось ли оборудование и т. п.;
- встречались ли наблюдаемые симптомы ранее, были ли сходные отказы, которые могли привести к текущей проблеме, и т. п.;
- если ошибка наблюдается у пользователя, поговорите с ним, уточните ситуацию, попытайтесь воспроизвести проблему.

Анализ журналов системы

Практически невозможно определить неисправность без анализа журналов системы. В журналах фиксируются все самые важные события, возникающие в системе. В Windows надо анализировать журналы системы, приложений и безопасности. В UNIX/Linux — журнал syslog и журналы служб.

Ведение журналов требует значительных системных ресурсов, поэтому в журналах фиксируются только основные события и критические оповещения. Если для анализа причин сбоя такой информации недостаточно, приходится настраивать более высокий уровень детализации и заново просматривать журналы.

> ***Примечание***
>
> После устранения неисправности необходимо восстановить исходный уровень детализации журналов, чтобы не использовать нерационально ресурсы системы на запись информации о событиях.

На практике для анализа проблемы часто приходится собирать информацию с нескольких систем. Можно выполнить это штатными средствами — например, просто подключаясь к журналу удаленного компьютера в консоли **Просмотр событий**. Но администратор обычно не ограничивается штатными средствами. Для сбора данных и последующего анализа используются любые доступные утилиты сторонних разработчиков, контролирующие систему в реальном режиме времени.

Например, ранее была очень полезной утилита Insight for Active Directory (от Sysinternals, позже — от Microsoft), позволяющая отслеживать любые запросы к Active Directory. Вот только эта утилита поддерживает лишь 32-разрядные версии Windows Server, и, следовательно, если у вас установлен Windows Server 2008 R2 (который полностью 64-разрядный) или Windows Server 2012/2022, эта утилита работать уже не будет. Вместо нее можно использовать утилиту Tracelog[1] — она не

[1] Подробную информацию об этой утилите можно получить по адресу: **https://docs.microsoft.com/en-us/windows-hardware/drivers/devtest/tracelog**.

такая удобная, как Insight, но зато работает в современных серверных операционных системах.

Средства просмотра журналов системы

Как уже отмечалось ранее, в Windows для просмотра журналов событий используется специальная утилита **Просмотр событий**. В Windows 7 вызвать эту утилиту можно через **Панель управления | Административные задачи | Просмотр событий**. В Windows 10, 11 и Windows Server 2012/2022 эта утилита получила название **Панель мониторинга** (рис. 11.1), и проще всего запустить ее, воспользовавшись средством поиска приложений, — просто на основном экране введите начальные символы названия программы и выберите ее из результатов поиска.

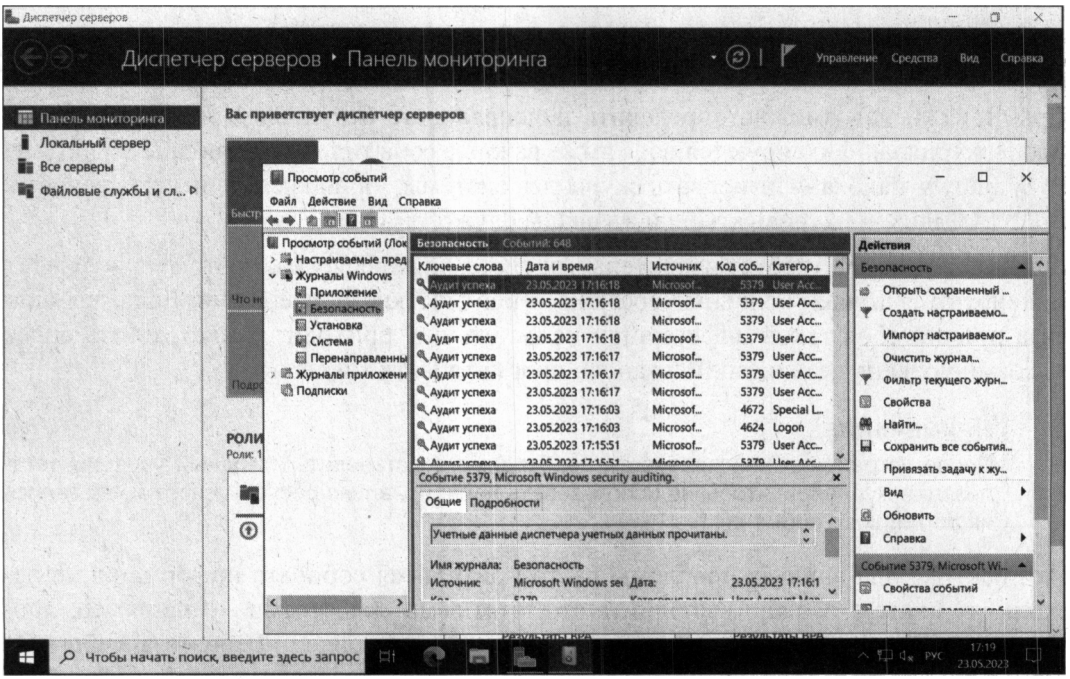


Рис. 11.1. Средство просмотра журнала событий в Windows Server 2022

Примечание

Информация о событиях в программе просмотра Windows не меняется в режиме реального времени. Для ее обновления следует выполнить команду Обновить (нажать клавишу <F5>).

В UNIX-системах события записываются в текстовые файлы. Как правило, для их просмотра служит команда `tail`, которая выводит файл, начиная с конца. Для фильтрации записей обычно используется перенаправление ввода/вывода на команду `grep`, которая и выполняет фильтрацию:

```
# tail /var/log/messages | grep Failed
```

На рис. 11.2 показан результат выполнения команды, позволяющей найти всевозможные сбои (сообщения отфильтровываются по слову «Failed»). Здесь мы просматриваем журнал **syslog.1** (журнал за вчера — так настроена ротация) и ищем всевозможные сбои.

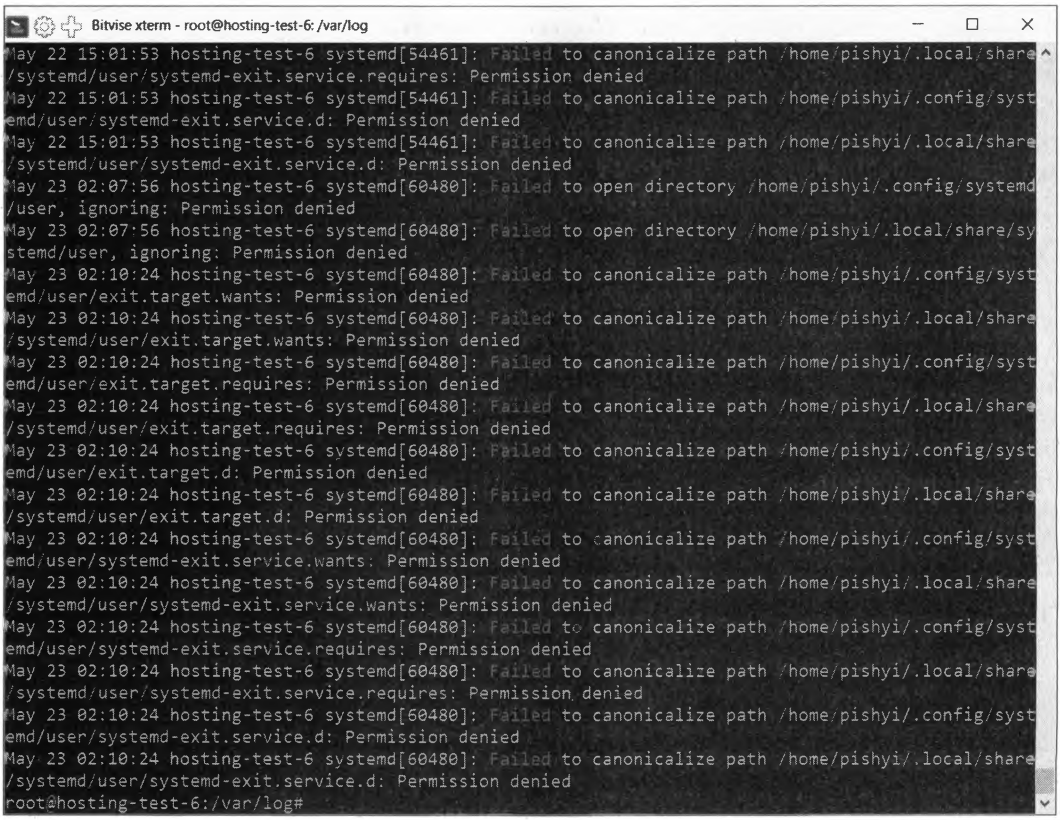


Рис. 11.2. Попытка найти причину сбоя (UNIX-система)

Чтобы одновременно наблюдать за событиями двух или более журналов, в UNIX используется возможность одновременного открытия нескольких консолей: в каждой консоли запускается просмотр одного журнала, а переход к другому реализуется переключением между консолями.

Журналы в Linux: демон syslogd

В любой UNIX-системе, коей является и Linux, имеются *демоны протоколирования* (далее просто «демоны»). Демоны записывают в протоколы (журналы) сообщения, генерируемые ядром, сервисами, пользовательскими программами. В большинстве случаев файлы протоколов размещаются в каталоге /var/log.

Основным демоном протоколирования является syslogd. Он имеется практически на всех UNIX-системах: от самых старых до самых новых. Правда, в современных дистрибутивах применяются модифицированные версии syslogd: rsyslogd или

syslog-ng. Первый из них получил большее распространение, поэтому мы его и рассмотрим. Секрет популярности rsyslogd — в файле конфигурации, синтаксис которого идентичен синтаксису файла настроек демона syslogd. Это очень удобно: во-первых, не нужно изучать новый синтаксис, во-вторых, подобие формата файла упрощает миграцию на rsyslogd — достаточно просто переименовать файл конфигурации и запустить новый демон протоколирования.

Иногда пользователи отключают сервис syslogd (или rsyslogd). Настоятельно рекомендуем не делать этого. Ведь у Linux весьма сильно развита функция самодиагностики, и в случае возникновения сбоя по содержимому журналов вы сможете понять, в чем причина сбоя, и устранить ее. Во всяком случае с записями в журнале это будет проще сделать, чем без них.

Основным файлом конфигурации демона syslogd является файл /etc/syslog.conf, а демона rsyslogd — файл rsyslog.conf. Формат этих двух файлов следующий:

```
селектор[;селектор]   действие
```

В некоторых системах, например в Ubuntu, файл /etc/rsyslog.conf является общим, а конкретные настройки, относящиеся к протоколированию, находятся в отдельных файлах в каталоге /etc/rsyslog.d. Формат всех этих файлов аналогичен формату файла rsyslog.conf. Кстати, в openSUSE вам понадобятся права root даже для того, чтобы лишь прочитать файл /etc/rsyslog.conf.

Итак, рассмотрим параметры основного файла конфигурации демона syslogd:

- параметр `селектор` определяет, какие сообщения должны быть запротоколированы. Вот список наиболее часто использующихся селекторов:
  - `auth`, `security` — все, что связано с регистрацией пользователя в системе;
  - `authpriv` — отслеживает программы, изменяющие привилегии пользователей, например программу su;
  - `cron` — сообщения планировщиков заданий;
  - `kern` — сообщения ядра;
  - `mail` — сообщения почтовых программ;
  - `news` — сообщения новостного демона;
  - `uucp` — сообщения службы Unix-to-Unix-CoPy. Параметр уже давно не используется, но файл конфигурации демона все еще содержит упоминание об этой службе;
  - `syslog` — сообщения самого демона syslogd;
  - `user` — сообщения пользовательских программ;
  - `daemon` — сообщения различных сервисов;
  - `*` — все сообщения.

  При указании селектора можно определить, какие сообщения нужно протоколировать:

- `debug` — отладочные сообщения;
- `info` — информационные сообщения;
- `err` — ошибки;
- `warning` — предупреждения (некритические ошибки);
- `crit` — критические ошибки;
- `alert` — тревожные сообщения, требующие вмешательства администратора;
- `emerg` — очень важные сообщения (произошло что-то такое, что мешает нормальной работе системы);
- `notice` — замечания.

Впрочем, обычно селекторы указываются так:

```
название_селектора.*
```

Это означает, что будут протоколироваться все сообщения селектора. Вот еще несколько примеров:

- `daemon.*` — протоколируются все сообщения сервисов;
- `daemon.err` — регистрировать только сообщения об ошибках сервисов.

❐ теперь перейдем к параметру `действие` — это второе поле файла конфигурации. В большинстве случаев `действие` — это имя файла журнала, в который нужно записать сообщение селектора. Если перед именем файла стоит знак «минус» (-), то после каждой записи в журнал демон не будет выполнять синхронизацию файла, т. е. осуществлять системный вызов `fsync()`. Это повышает производительность системы, поскольку сообщений обычно много, и если после каждого выполнять синхронизацию журнала, система будет работать медленно.

Фрагмент конфигурационного файла rsyslog.conf (syslog.conf) приведен в листинге 11.1.

Листинг 11.1. Фрагмент файла конфигурации /etc/rsyslog.conf

```
# Сообщения ядра протоколируются на консоль
#kern.*                                         /dev/console

# Протоколировать все сообщения (кроме почты) в /var/log/messages
*.info;mail.none;authpriv.none;cron.none        /var/log/messages

# Сообщения селектора authpriv записываются в файл /var/log/secure
authpriv.*                                      /var/log/secure

# Сообщения почты (их будет много, если запущен агент MTA вроде postfix)
# записываются в файл maillog
mail.*                                          -/var/log/maillog

# Сообщения планировщиков заданий записываются в cron
cron.*                                          /var/log/cron
```

```
# Особо критичные сообщения выводятся на экран всех работающих в данный момент
пользователей (вместо имени файла указана звездочка)
*.emerg                                                    *

# Сообщения UUCP и сообщения сервера новостей записываются в /var/log/spooler
uucp,news.crit                                        /var/log/spooler

# Загрузочные сообщения записываются в boot.log
local7.*                                              /var/log/boot.log
```

Исследовав файл конфигурации rsyslog.conf, можно понять, для чего используется тот или иной журнал. Но некоторые сервисы, например Apache, ведут свои собственные журналы, минуя демон протоколирования, — все они тоже хранятся в каталоге /var/log. Именно этим объясняется, что в каталоге /var/log содержатся дополнительные файлы и каталоги, не упомянутые в rsyslog.conf. Вот примеры некоторых файлов (каталогов) журналов:

- /httpd/ — журналы веб-сервера Apache;
- /cups/ — журналы системы CUPS (в вашей системе может быть установлена одна из этих систем печати);
- auth.log — журнал аутентификации: кто и когда входил в систему. В некоторых дистрибутивах такого файла нет, а сообщения системы аутентификации записываются в файл messages;
- boot.log — журнал загрузки системы. В некоторых дистрибутивах сообщения загрузки системы также записываются в файл messages;
- dmesg — загрузочные сообщения ядра (до запуска системы инициализации). Такой файл имеется не во всех дистрибутивах, но вы всегда сможете просмотреть загрузочные сообщения ядра с помощью команды `dmesg`. Если файл /proc/sys/kernel/dmesg_restrict содержит 0, то команду `dmesg` может выполнить непривилегированный пользователь, если же в этом файле единица, команду `dmesg` может выполнить только пользователь root или пользователь с правами `CAP_SYS_ADMIN`;
- messages — основной журнал системы;
- secure — сообщения системы безопасности. Сюда, например, помещаются сообщения при входе пользователя через GDM;
- syslog — журнал демона syslog;
- Xorg.0.log — журнал системы X.Org;
- zypper.log, yum.log, dpkg.log — журналы менеджеров пакетов (в openSUSE, Fedora и Ubuntu/Debian соответственно).

В каком же журнале искать ошибку? Тут нужно исходить из принципа взаимоисключения: если у вас не работает веб-сервер Apache, то искать причину надо в каталоге /var/log/httpd/, но никак не в файле /var/log/mail.

В UNIX-системах для повышения детализации протоколирования той или иной службы нужно редактировать ее конфигурационный файл. Дополнительную ин-

формацию об этом можно получить в документации по службе. Например, в конфигурационных файлах часто встречается строка вида `syslog = 0`. Чтобы повысить уровень детализации протоколирования, следует изменить `0` на большее значение (какое именно — можно уточнить в документации). После этого надо или перезапустить службу (командой: `servive <имя службы> restart`), или заставить ее перечитать файл конфигурации (командой: `service <имя службы> reload`).

К слову сказать, изменение детализации протоколирования большинства служб Windows осуществляется посредством изменения параметров реестра. Названия этих параметров можно найти в документации по службе или на сайтах разработчиков программного обеспечения.

Централизованное ведение журналов

Системным администраторам приходится анализировать данные журналов нескольких серверов. Удобно, если эта операция будет выполняться из одной консоли.

В этих целях в системах Windows 10/11 и Server 2012/2022 присутствует возможность настройки сбора событий с различных компьютеров. Для этого используется опция **Подписка**.

При создании подписки (рис. 11.3) необходимо указать, с каких систем будут собираться данные, настроить фильтры (указать, какие события копировать), назначить журнал, в который станет осуществляться запись. Также нужно настроить параметры учетной записи, которая будет иметь доступ к журналу на удаленном компью-

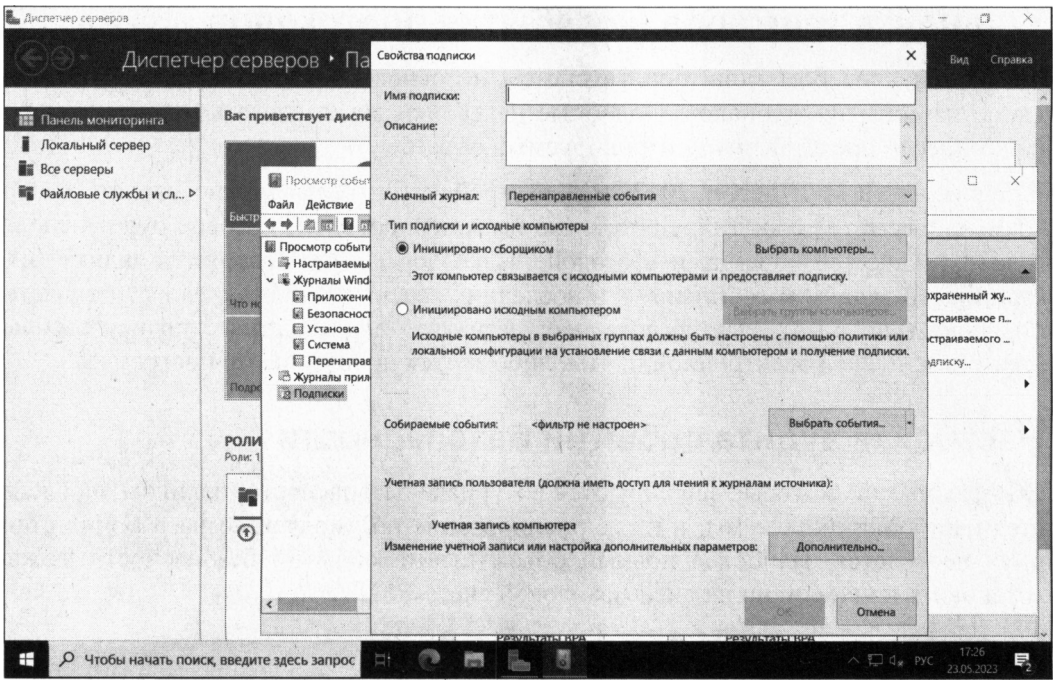


Рис. 11.3. Настройка подписки в Windows Server 2022

тере. Кроме того, надо еще выполнить некоторые настройки на удаленной системе (см. онлайновую справку). Подписку можно оформлять как для компьютеров домена, так и рабочей группы (особенности настройки в этом случае следует уточнить по справочной документации).

При желании использовать для анализа журналов графический интерфейс, можно обратиться к специальной утилите — EventCombMT[1], бесплатно загружаемой с сервера Microsoft.

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.

> ***Примечание***
>
> Существует много коммерческих средств, предназначенных для централизации сбора и анализа событий журналов нескольких систем. При желании найти эти решения не составит особого труда.

События журналов важны и в случае разбора инцидентов. Поскольку злоумышленник будет пытаться очистить журналы атакуемой системы, то при предъявлении повышенных требований к хранению событий последние необходимо копировать на выделенный сервер.

Установка триггеров на события протоколов

Основным способом мониторинга систем на основе Windows является реагирование на события журналов. Подобные настройки легко сделать и собственными силами, если представлять контролируемый объем.

В Windows 10/11 и Server 2012/2022 настройку триггеров можно сделать в программе просмотра событий. Достаточно выделить событие, которое будет использовано в качестве образца, и в столбце задач по ссылке **Назначить задачу** (или **Привязать задачу к событию** — в последних версиях Windows) запустить мастер операций (рис. 11.4). Мастер позволяет назначить для события отправку сообщения, в том числе и электронной почты, либо запуск произвольной программы.

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.

---

[1] См. **https://learn.microsoft.com/ru-RU/troubleshoot/windows-server/windows-security/use-eventcombmt-to-search-logs-for-account-lockout**.

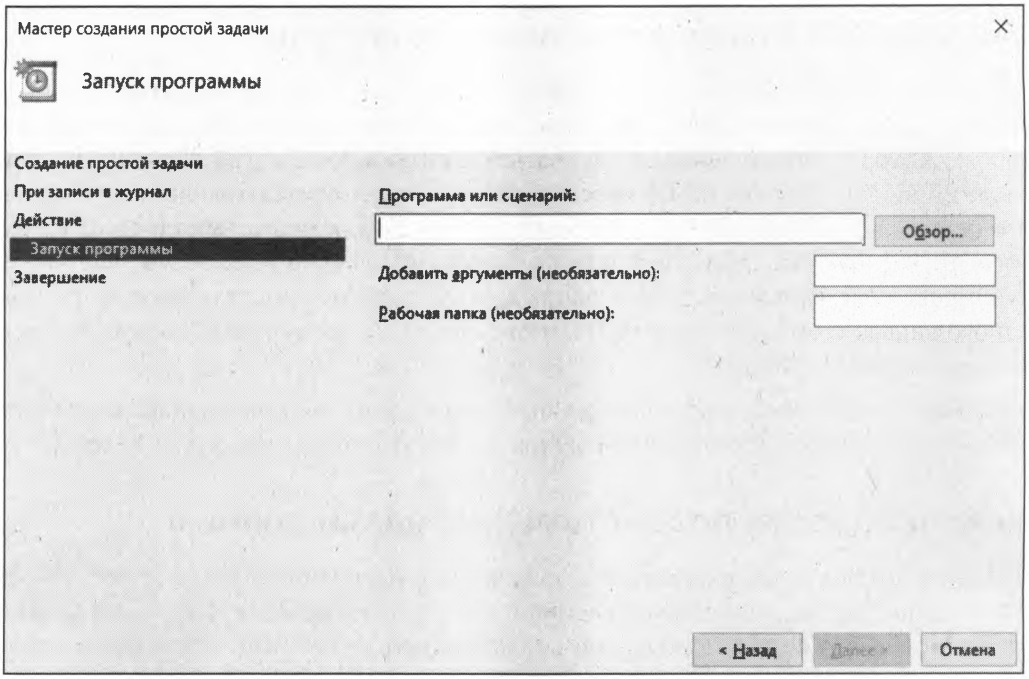


Рис. 11.4. Мастер создания простой задачи на возникновение события в журнале

Чтобы начать протоколирование событий безопасности, необходимо сначала *разрешить аудит* событий безопасности в политике безопасности. Это может быть сделано как локально — в локальной политике безопасности, так и централизованно — путем задания соответствующих параметров в групповой политике. 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.

Если необходимо вести протокол работы с файлами, то следует включить аудит доступа к объектам, после чего в свойствах объекта на вкладке **Безопасность** нажать кнопку **Дополнительно** и выбрать вкладку **Аудит**. Затем нужно добавить сведения о том, какие действия и от каких пользователей должны фиксироваться в журнале.

Особенности отказов различных компонентов

Отказ в обслуживании может возникнуть вследствие отказа любого элемента информационной системы: повреждения кабелей, неполадок в работе коммутирующих устройств, выхода из строя узлов компьютера, зависания операционной системы, ошибок программного обеспечения бизнес-уровня и уровня приложений и т. п.

Мониторинг отказоустойчивой структуры

Если в вашей организации реализованы те или иные технологии дублирования, то следует постоянно проверять состояние каждого элемента любым доступным способом. Авторам приходилось сталкиваться с ситуациями, когда выходил из строя жесткий диск из состава RAID-массива, сервер пищал длительное время, но его никто не слышал, и неисправность не была выявлена до момента выхода из строя второго диска, что уже привело к потере данных. Аналогично если вы используете дублированные каналы передачи данных, то можете не заметить выхода из строя одного канала и столкнуться с полным отказом, будучи уверенным в том, что ваша система отказоустойчива.

Поэтому следует обеспечить постоянный мониторинг состояния информационной системы. Некоторые возможные решения по мониторингу изложены в *главе* 7.

Неисправности подсистемы передачи данных

С одной стороны, неисправность подсистемы передачи данных легко обнаружить — достаточно попытаться скопировать по сети большой файл, — например, в 100 Мбайт. По сети с пропускной способностью 100 Мбит/с такой файл должен передаться менее чем за 20 секунд, для гигабитной сети — менее чем за 5 секунд. Если время копирования больше, следует искать источник проблемы.

С другой стороны, такие отказы часто бывает сложно локализовать. Например, авторы встречались с ситуациями, когда пересохший кабель вызывал исчезающие проблемы при незначительном его перемещении, или когда неисправность была связана с плохим контактом в разъеме сетевого адаптера, что приводило к нестабильной работе после того, как патч-корд просто задевали, иногда ошибки возникали в работе коммутатора, продолжавшего безмятежно мигать своими индикаторами, и т. п.

Обнаружение неисправностей сетевой инфраструктуры

Неисправность пассивной инфраструктуры можно определить с помощью специальных *устройств*, прогоняющих по сети особые тесты, позволяющие проверить линии связи на соответствие всем требованиям стандарта. Однако такие тестеры весьма дороги, и далеко не каждое, даже крупное предприятие их имеет. В большинстве случаев ограничиваются лишь проверкой наличия соединения (есть контакт — нет контакта), которая выполняется простейшими пробниками. Существуют и кабельные тестеры, которые позволяют обнаружить обрыв линии связи, перепутывание проводников и другие типовые неисправности. Такие тестеры доступны любому администратору (их можно найти по цене менее 1 тыс. рублей).

Косвенным признаком исправности кабеля может служить индикатор на сетевом порту — если он горит, то кабель, скорее всего, исправен. И тогда нужно проверить состояние портов сетевого интерфейса компьютера и коммутатора. Случаи выхода из строя сетевых портов нередки. Особенно часто это происходит на длинных (близких к максимальному значению длины) медных линиях связи после гроз.

Примечание

Существуют специальные модули защиты от грозовых разрядов. Но, как показывает практика, они не обеспечивают гарантированной защиты сетевых портов. Поэтому, с учетом стоимости оборудования, часто предпочитают просто заменять сожженный порт на исправный (с последующей заменой всего коммутатора при выходе из строя всех портов).

Если порты исправны, то между ними должны передаваться пакеты данных. Сегодня в большинстве систем применяется протокол TCP/IP, поэтому опишем последовательность проверки соединения для такого случая.

Диагностика IP-протокола

Для диагностики соединения с использованием протокола TCP/IP рекомендуется следующая последовательность операций:

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

Примечание

В Windows существует специальный мастер диагностики сетевого подключения, который выполняет операции, аналогичные описанным, 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

Отобразить параметры IP-протокола можно с помощью следующих утилит: ipconfig (Windows 10/11 и Windows Server) и ifconfig (*NIX-системы). Обе утилиты выполняются в режиме командной строки.

Представим, что у нас в Linux не работает PPPoE/DSL-соединение, и попробуем разобраться, в чем же причина.

Проверить, «поднят» ли сетевой интерфейс, можно с помощью команды `ifconfig`, выполнение которой показано на рис. 11.5. Здесь видно, что сначала мы предприняли попытку установить соединение (ввели команду: `sudo pon dsl-provider`), а затем вызвали `ifconfig`, чтобы убедиться, что соединение установлено. Если бы соединение не было установлено, интерфейс `ppp0` в списке бы отсутствовал. Интерфейс `eth0` относится к первой сетевой плате (вторая называется `eth1`, третья — `eth2` и т. д.), а интерфейс `lo` — это интерфейс обратной петли, который используется для тестирования программного обеспечения (у вас он всегда будет «поднят»).

Итак, наличие в выводе команды `ifconfig` интерфейса `ppp0` подтверждает установку соединения. Если же этот интерфейс оказался не «поднят», нам нужно просмотреть файл **/var/log/messages** сразу после попытки установки соединения:

```
tail -n 10 /var/log/messages
```

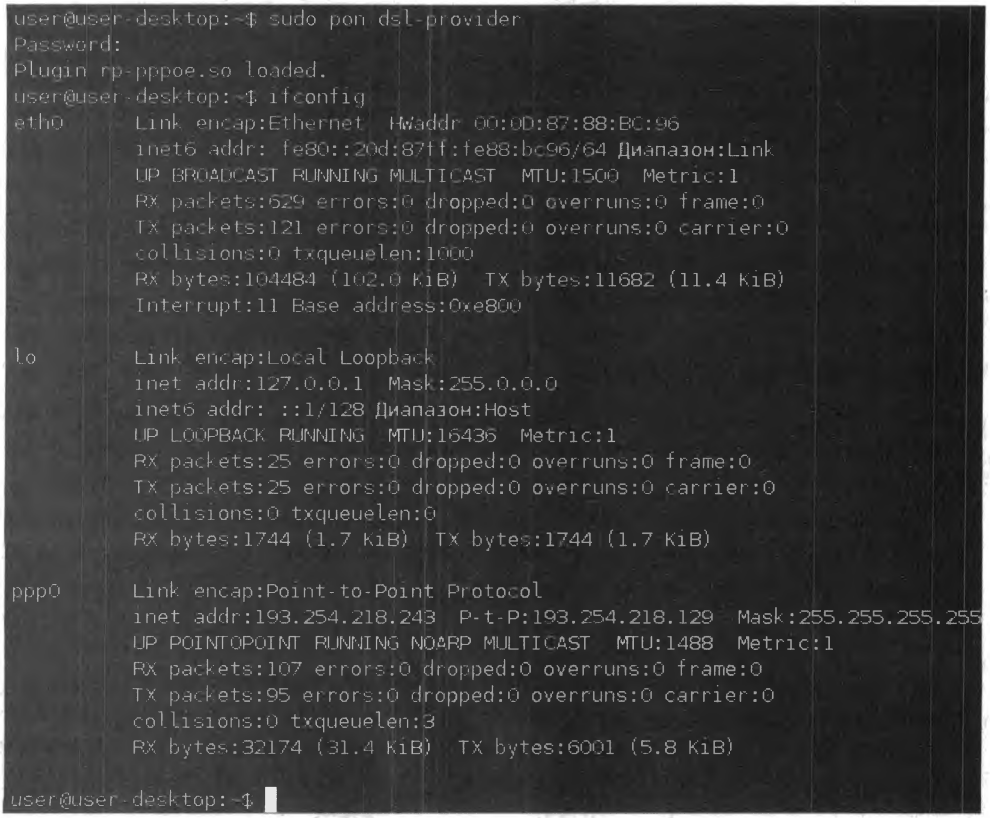


Рис. 11.5. Программа ifconfig

Примечание

В современных дистрибутивах файл */var/log/messages* может отсутствовать, а сообщения, которые ранее помещались в журнал *messages*, теперь можно прочитать в файле */var/log/syslog*.

Приведенная команда просматривает «хвост» файла протокола (выводит его последние 10 сообщений). В случае удачной установки соединения сообщения в файле протокола будут примерно следующими:

```
Feb  6 14:28:33 user-desktop pppd[5176]: Plugin rp-pppoe.so loaded.
Feb  6 14:28:33 user-desktop kernel: [17179852.932000] CSLIP: code copyright
                                198 9 Regents of the University of California
Feb  6 14:28:33 user-desktop kernel: [17179852.944000] PPP generic driver
                                                        versio n 2.4.2
Feb  6 14:28:33 user-desktop pppd[5183]: pppd 2.4.4b1 started by root, uid 0
Feb  6 14:28:33 user-desktop pppd[5183]: PPP session is 2838
Feb  6 14:28:33 user-desktop kernel: [17179852.984000] NET: Registered protocol
                                                        family 24
Feb  6 14:28:33 user-desktop pppd[5183]: Using interface ppp0
Feb  6 14:28:33 user-desktop pppd[5183]: Connect: ppp0 <--> eth0
Feb  6 14:28:33 user-desktop pppd[5183]: Remote message: Login ok
```

```
Feb  6 14:28:33 user-desktop pppd[5183]: PAP authentication succeeded
Feb  6 14:28:33 user-desktop pppd[5183]: peer from calling number
                                                00:15:F2:60:28 :97 authorized
Feb  6 14:28:33 user-desktop pppd[5183]: local  IP address 193.254.218.243
Feb  6 14:28:33 user-desktop pppd[5183]: remote IP address 193.254.218.129
Feb  6 14:28:33 user-desktop pppd[5183]: primary DNS address 193.254.218.1
Feb  6 14:28:33 user-desktop pppd[5183]: secondary DNS address 193.254.218.27
```

Первая строчка — сообщение о том, что загружен модуль поддержки PPPoE. Следующие два сообщения информируют о поддержке нашим компьютером протоколов CSLIP и PPP. Затем сообщается, что демон `pppd` запущен, указывается, от чьего имени он запущен (`root`), и версия самого `pppd`. Далее приводятся имена используемого (`ppp0`) и вспомогательного (`eth0`) интерфейсов (помните, что протокол PPPoE подразумевает передачу кадров PPP по Ethernet). Следующие два сообщения свидетельствуют об удачной регистрации:

```
Feb  6 14:28:33 user-desktop pppd[5183]: Remote message: Login ok
Feb  6 14:28:33 user-desktop pppd[5183]: PAP authentication succeeded
```

Затем система сообщает нам наш IP-адрес, адрес удаленного компьютера, который произвел аутентификацию, а также IP-адреса серверов DNS.

А вот пример неудачной попытки соединения:

```
Feb  6 09:23:48 user-desktop pppd[6667]: PPP session is 2336
Feb  6 09:23:48 user-desktop pppd[6667]: Using interface ppp1
Feb  6 09:23:48 user-desktop pppd[6667]: Connect: ppp1 <--> eth0
Feb  6 09:23:48 user-desktop pppd[6667]: Remote message: Login incorrect
Feb  6 09:23:48 user-desktop pppd[6667]: Connection terminated.
```

Причина неудачи понятна: имя пользователя или пароль неправильные, о чем красноречиво свидетельствует сообщение `Login incorrect`. Для того чтобы изменить имя пользователя или пароль, можно запустить конфигуратор `pppoeconf`. Но не спешите пока это делать — если в предыдущий раз соединение было установлено (а настройки соединения вы не изменяли), возможно, нужно обратиться к провайдеру. Такая ситуация — это явный признак неправильной работы оборудования на стороне провайдера.

Вот еще один пример, характерный для PPPoE:

```
Feb  6 09:23:48 user-desktop pppd[6667]: PPP session is 2336
Feb  6 09:23:48 user-desktop pppd[6667]: Using interface ppp1
Feb  6 09:23:48 user-desktop pppd[6667]: Connect: ppp1 <--> eth0
Feb  6 09:23:48 user-desktop pppd[6667]: Connection terminated.
```

Здесь показан еще один случай неправильной работы оборудования провайдера. Возможно, вам следует перезагрузить точку доступа (access point) — просто выключите и снова включите ее. Если это не поможет, обращайтесь к провайдеру.

Наиболее простая ситуация, когда сеть вообще не работает. В этом случае очень легко обнаружить причину неисправности — если работает устройство, значит, повреждена среда передачи данных (сетевой кабель). В случае с модемной линией надо проверить, нет ли ее обрыва. В случае с витой парой обрыв маловероятен

(хотя возможен), поэтому нужно проверить, правильно ли обжат кабель (возможно, придется обжать витую пару заново).

Проверка достижимости ближайших компьютеров сети

Намного сложнее ситуация, когда сеть то работает, то нет. Например, вы не можете получить доступ к какому-нибудь узлу, хотя пять минут назад все работало отлично. Если исключить неправильную работу удаленного узла, к которому вы подключаетесь, следует поискать решение в маршруте, по которому пакеты добираются от вашего компьютера до удаленного узла.

Сначала пропингуем удаленный узел с помощью команды `ping` (прервать ее выполнение можно с помощью комбинации клавиш <Ctrl>+<C>):

```
ping example.com
```

```
PING example.com (93.184.216.34) 56(84) bytes of data.
64 bytes from example.com (93.184.216.34): icmp_seq=1 ttl=58 time=30.7 ms
64 bytes from example.com (93.184.216.34): icmp_seq=2 ttl=58 time=24.8 ms
64 bytes from example.com (93.184.216.34): icmp_seq=5 ttl=58 time=12.2 ms
64 bytes from example.com (93.184.216.34): icmp_seq=6 ttl=58 time=159 ms
64 bytes from example.com (93.184.216.34): icmp_seq=7 ttl=58 time=19.3 ms
64 bytes from example.com (93.184.216.34): icmp_seq=9 ttl=58 time=29.0 ms
...
```

> ***Примечание***
>
> Команда `ping` имеется как в Linux, так и в Windows, но ее вывод в Windows немного отличается от приведенного здесь.

Тут, как можно видеть, все нормально. Но иногда ответы от удаленного сервера то приходят, то не приходят. Чтобы узнать, в чем причина (где именно теряются пакеты), нужно выполнить трассировку узла:

```
tracepath example.com
```

В некоторых дистрибутивах Linux вместо команды `tracepath` используется команда `traceroute`, а в Windows — `tracert`. На рис. 11.6 показано выполнение команды `tracepath`. Здесь сразу видно, что с прохождением пакетов до удаленного узла есть определенные проблемы — по пути пакеты теряются. Для того чтобы выяснить причину, вам нужно обратиться к администратору того маршрутизатора, который не пропускает пакеты дальше. Причина именно в нем. В нашем случае пакеты доходят до маршрутизатора `ae-66.core1.nyb.edgecastcdn.net`, а после него движение пакетов прекращается.

Проверка функционирования серверов имен

Если соединение установлено (о чем свидетельствует наличие «поднятого» интерфейса в выводе `ifconfig`), а веб-страницы не открываются, попробуйте пропинговать любой удаленный узел по IP-адресу. Если вы не знаете, какой узел пинговать (т. е. не помните ни одного IP-адреса), пропингуйте узел 8.8.8.8. Если вы получите ответ, а страницы по-прежнему не открываются, когда вы вводите символьное имя, значит, у вас проблемы с DNS — сервер провайдера почему-то не передал вашему

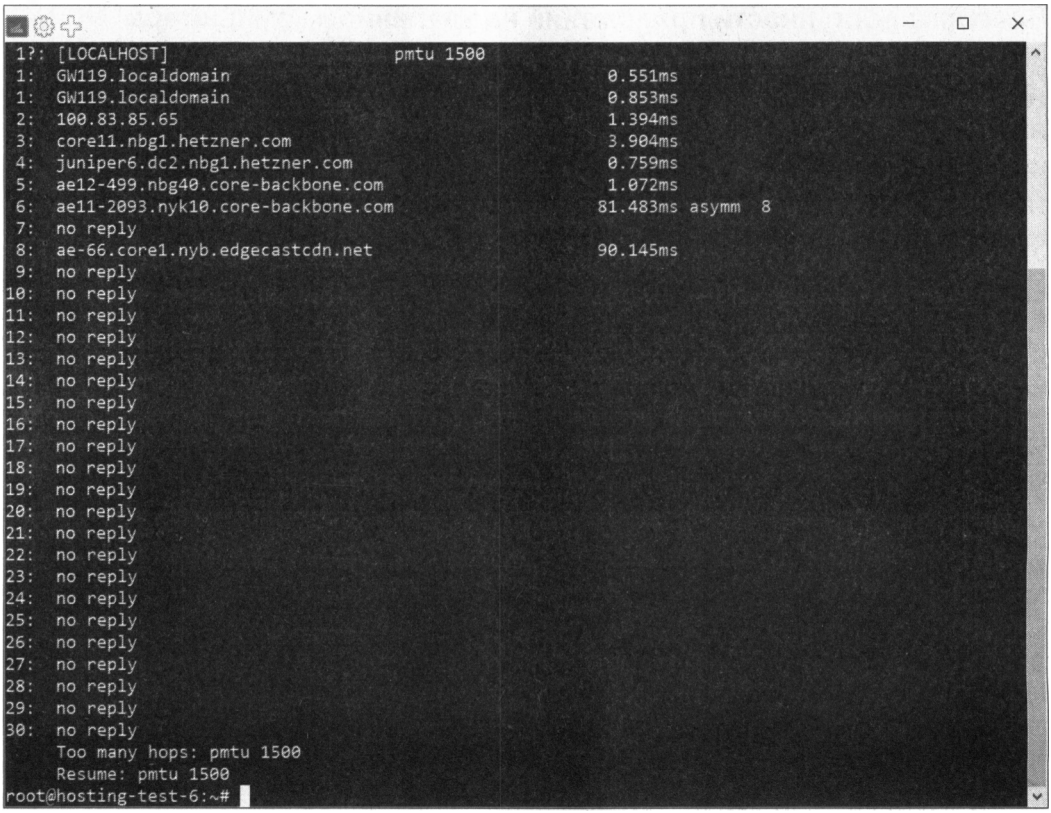


Рис. 11.6. Проблема с прохождением пакетов

компьютеру IP-адреса DNS-серверов. Позвоните провайдеру и выясните причину, а еще лучше — уточните IP-адреса серверов DNS и укажите их в файле /etc/resolv.conf.

Формат этого файла прост:

```
nameserver IP-адрес
```

Например:

```
nameserver 8.8.8.8
nameserver 8.8.4.4
```

Всего можно указать до четырех серверов DNS.

Если же не открывается какая-то конкретная страница, а все остальные работают нормально, тогда понятно, что причина в самóм удаленном сервере, а не в ваших настройках.

В более сложных случаях бывает полезно просмотреть трафик, проходящий по определенному порту. Для этого нужно выполнить команду `tcpdump` — например:

```
tcpdump tcp port 80
```

Эта команда отобразит весь трафик, поступающий на TCP-порт 80.

Проверка доступности приложений на удаленном компьютере

Администраторы часто запрещают в межсетевых экранах прохождение ping-пакетов, открывая только порты, используемые установленными приложениями. В этом случае убедиться в доступности удаленного компьютера можно, если вы знаете порт, на котором работает соответствующая программа. Например, в практике авторов был случай, когда администраторами провайдера были закрыты порты, необходимые для создания безопасного подключения.

Существуют различные возможности проверить удаленные системы. Во-первых, в Support Tools 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 server -e 21
```

Результатом будет, например, такой вывод:

```
Querying target system called:
server
Attempting to resolve name to IP address...
Name resolved to 192.168.0.1
TCP port 21 (ftp service): LISTENING
Data returned from port:
220 server.example.com 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 `server`).

Сходные утилиты, позволяющие получить ответ на запрос, отправленный на конкретный порт, легко найти в Интернете. Но проще использовать программу Telnet, которая входит в состав всех операционных систем. Для систем Windows NT 6.0 и старше ее надо добавить в число установленных компонентов (она называется *клиент Telnet*), в предыдущих же версиях эта утилита доступна по умолчанию.

Запуская утилиту Telnet с параметрами в виде имени удаленной системы и номером порта, вы осуществляете попытку подключения к соответствующему порту. Если попытка подключения удалась, то либо на экране появится ответ, либо экран на некоторое время «зависнет», после чего соединение разорвется по тайм-ауту. Если порт не отвечает, то вы увидите на экране сообщение о невозможности подключения. Далее приведен вывод команды `telnet` при проверке доступности порта 25 (порт почтового сервера, попытка неудачна) и 80 (порт сервера WWW — видно, что порт ответил на запрос).

```
>telnet 192.168.29.1 25
Подключение к 192.168.29.1... Не удалось открыть подключение к этому узлу на
порт 25: Сбой подключения

>telnet 192.168.29.1 80
HTTP/1.1 400 Bad Request
```

```
Server: nginx
Date: Thu, 08 Jun 2023 16:11:22 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 150
Connection: close

<html>
<head><title>400 Bad Request</title></head>
<body>
<center><h1>400 Bad Request</h1></center>
<hr><center>nginx</center>
</body>
</html>
```

Проверка качества канала связи

Даже если связь существует, это не означает, что она высокого качества. В некоторых случаях данные передаются слишком медленно, или же приложения периодически завершают работу с ошибками.

Часто такие неприятные ситуации связаны с перегрузкой канала — когда пропускная способность магистральной линии меньше суммы пропускных способностей подключенных к ней каналов связи. На практике такие ситуации случаются редко. В обычной офисной сети 100 Мбит/с редко какой канал связи может занять всю пропускную способность. Но это верно лишь до того момента, пока вы не надумали внедрить систему видеонаблюдения. Такая система, состоящая всего из пяти камер, при передаче кадров высокого разрешения может с успехом исчерпать полосу пропускания сети 100 Мбит/с.

Что делать? Конкретно в этом случае можно понизить качество видео, что существенно снизит нагрузку на сеть. Можно, конечно, и модернизировать оборудование — до гигабитной сети. Учитывая, что все современные компьютеры имеют «на борту» сетевые адаптеры, позволяющие передавать данные со скоростью 1 Гбит/с, это не обойдется вам слишком дорого — придется заменить лишь коммутаторы и, возможно, кабели.

Объективные показатели качества канала связи

На практике получить показатели качества сигнала связи можно при использовании активного сетевого оборудования с поддержкой протокола SNMP. Многие характеристики меняются на протяжении дня, поэтому желательно собирать и хранить эти показания — они понадобятся вам для последующего анализа в будущем.

> ***Примечание***
>
> Качество линии связи должно проверяться между каждым активным портом сети. Иными словами, снимаемые показатели должны анализироваться на каждом порту коммутаторов и маршрутизаторов локальной сети. Счетчики производительности, значения которых можно оценить в операционных системах компьютеров, характеризуют только качество линии «компьютер — коммутатор».

Для объективного анализа состояния линии связи можно использовать следующие основные показатели:

- *коэффициент использования пропускной способности сети* — для сети Ethernet значение этого показателя, превышающее примерно 70%, уже свидетельствует о критической ситуации;
- *число ошибочных пакетов* — при нормальной работе число ошибочных пакетов не должно превышать десятых долей процента передаваемой информации. Обычно большой процент ошибок контрольной суммы свидетельствует о низком качестве сети (плохие 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. Бóльшая величина — это признак низкого качества сети (локальные коллизии), наличия ошибок адаптеров или неверного проектирования сети (так называемая late collision — коллизия, обнаруживаемая после передачи первых 64 байтов). Причиной late collision часто бывает большое количество повторителей в локальной сети;
- *загрузка процессора активного оборудования* — активное сетевое оборудование не только коммутирует пакеты, но может осуществлять и различную их обработку — например, шифровать информацию между двумя точками или фильтровать данные по каким-либо правилам. Большое количество таких настроек приводит к исчерпыванию мощностей процессора и замедлению обработки информации. Ситуация пока достаточно редкая, поскольку на практике администраторы предприятий нечасто используют подобные возможности оборудования на полную мощность.

Программа Observer

На рис. 11.7 представлен фрагмент окна программы Observer, отображающего 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).

> ***Примечание***
>
> Программа Observer, представленная на рис. 11.7, — коммерческий продукт, 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), отображающую данные статистики маршрутизатора. Изначально программа предназначалась для Linux, но имеется также ее бесплатная версия для Windows, работающая на Perl.

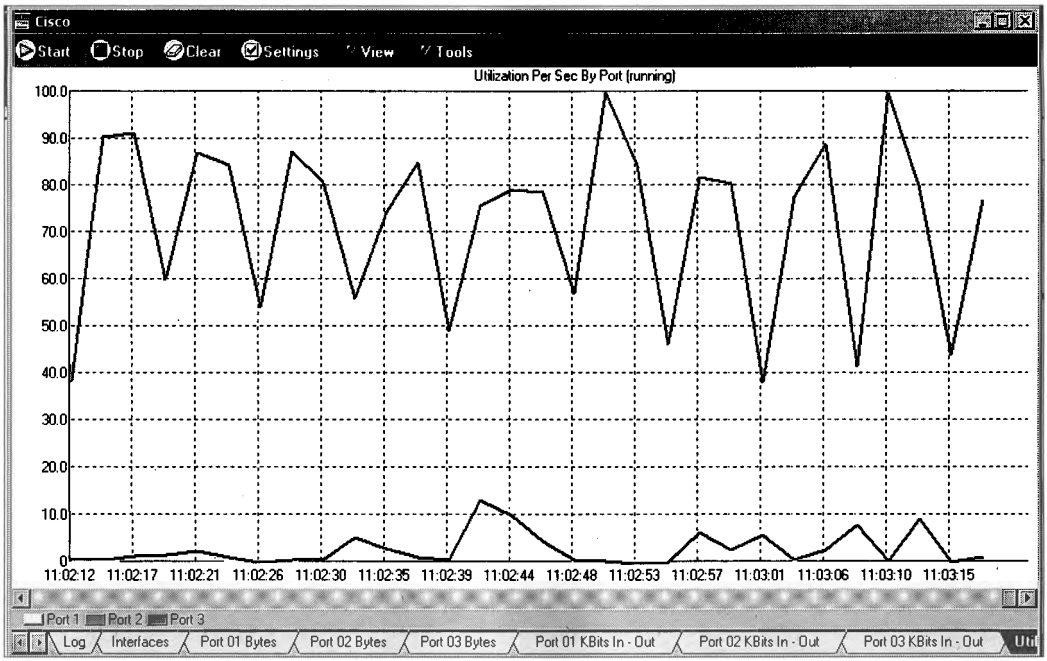


Рис. 11.7. Мониторинг состояния сети по протоколу SNMP

Утилита pathping

В Windows есть одна малоизвестная утилита, которая позволяет быстро оценить качество связи до любого хоста. Это утилита pathping. Она определяет цепочку, по которой передается информация между двумя хостами, и посылает на каждую систему серию проверочных пакетов (по 100 штук). По сути, она объединяет в себе две утилиты: tracert и ping. В итоге на экран выводится информация о количестве откликов и среднем времени ответа. Параметры программы и пример ее вывода приведены далее:

```
C:\Users\Dm>pathping

Использование:
    pathping [-g <список_узлов>] [-h <число_прыжков>] [-i <адрес>] [-n]
             [-p <пауза>] [-q <число_запросов>] [-w <тайм-аут>]
             [-4] [-6] <конечный_узел>

Параметры:
    -g <список_узлов>     Свободный выбор маршрута по списку узлов.
    -h <число_прыжков>    Максимальное число прыжков при поиске узла.
    -i <адрес>            Использовать указанный адрес источника.
    -n                    Не определять имена узлов по адресам.
    -p <пауза>            Пауза между отправками пакетов (мс).
    -q <число_запросов>   Число запросов при каждом прыжке.
    -w <тайм-аут>         Время ожидания каждого ответа (мс).
    -4                    Обязательное использование протокола IPv4.
    -6                    Обязательное использование протокола IPv6.
```

```
C:\Users\Dm>pathping example.com

Трассировка маршрута к example.com [93.184.216.34]
с максимальным числом переходов 30:
  0  DESKTOP [10.3.18.64]
  1  10.3.18.1
  2  188.213.34.65
  3  172.30.254.109
  4  172.30.245.85
  5     *        *        *
Подсчет статистики за: 100 сек. ...
           Исходный узел     Маршрутный узел
Прыжок  RTT   Утер./Отпр.   %  Утер./Отпр.  %  Адрес
  0                                           DESKTOP [10.3.18.64]
                                 0/ 100 =  0%   |
  1   42мс     0/ 100 =  0%     0/ 100 =  0%  10.3.18.1
                                 0/ 100 =  0%   |
  2   42мс     0/ 100 =  0%     0/ 100 =  0%  188.213.34.65
                                 0/ 100 =  0%   |
  3   40мс     0/ 100 =  0%     0/ 100 =  0%  172.30.254.109
                                 9/ 100 =  9%   |
  4   40мс     9/ 100 =  9%     0/ 100 =  0%  172.30.245.85

Трассировка завершена.
```

Утилита pathping выводит статистические данные о достижимости каждого промежуточного хоста, причем время усреднения выбирается исходя из конкретной ситуации (в примере подсчет проводился за период в 100 секунд).

Сначала выводится время доступа к какому-либо узлу, затем показывается количество пакетов, которые были на него отправлены, и число неполученных ответов с процентом успеха. Как видите, в нашем случае не было потеряно ни одного пакета.

Неисправности аппаратной части компьютера

При полном отказе какого-либо аппаратного компонента неисправность обнаружить легко. Но когда тот или иной компонент находится еще в стадии «умирания», выяснить непостоянную неисправность бывает весьма сложно. Например, компьютер может зависать лишь в определенных режимах. Вот как-то на одном из ПК часто зависала Windows. При этом оперативная память и жесткий диск нормально проходили все возможные тесты. Запустили Linux с LiveCD — система работала штатно, но при попытке установки обнаружилась ошибка копирования. Жесткий диск? Мы тоже так подумали. Но в итоге неисправной оказалась оперативная память — после извлечения одного из модулей система стала работать нормально. Причем неисправность, как видите, была определена не с помощью диагностических утилит, а, как говорится, методом «научного тыка»...

При подозрении на аппаратную неисправность нужно выполнить следующие операции (именно в такой последовательности):

1. Проверить оперативную память (чуть позже мы расскажем, как это сделать).
2. Попытаться установить самые последние драйверы устройств: материнской платы, видеокарты и пр.
3. Если это не поможет — выполнить чистую установку операционной системы и не устанавливать какие-либо прикладные программы. После этого установить самые последние драйверы и проверить, не исчезла ли неисправность. Не используйте драйверы, прилагающиеся к материнской плате, — они, как правило, устаревшие. Скачайте с сайта производителя оборудования самые последние версии драйверов. Не загружайте драйверы со сторонних сайтов.
4. Обновите BIOS материнской платы. Эта операция требует осторожности, т. к. в случае неправильных действий можно превратить материнскую плату в бесполезную «железку».

Наиболее частая причина нестабильной работы системы — некачественная оперативная память. На следующем месте по выходу из строя — жесткие диски. За ними следуют видеокарты и блоки питания. А вообще, может выйти из строя все, что угодно: и привод CD/DVD, и процессор, и т. д. и т. п. Как правило, сложные устройства, состоящие из механических (и движущихся!) частей, например CD/DVD-приводы и жесткие диски, ломаются чаще.

Контроль жестких дисков

В операционные системы встроены утилиты проверки файловых структур, которые автоматически запускаются во время перезагрузки компьютера в случае обнаружения ошибок (например, ошибочных блоков). В Linux, кроме того, после длительного периода работы или определенного числа перезагрузок. Такими утилитами являются checkdsk для Windows и fsck для Linux (строго говоря, fsck является оболочкой, которая запускает программу проверки, специфичную для используемой в Linux файловой системы).

Программы проверки можно запустить вручную. Обратите внимание, что для исправления ошибок необходимо отключить (размонтировать) логический диск. В Windows эта операция может быть осуществлена самой программой (с запросом подтверждения пользователя) — кроме системного диска, ошибки на котором можно исправить только при старте операционной системы, в Linux размонтировать диск необходимо вручную.

Поскольку в Linux также рекомендуется для проверки перейти в однопользовательский режим, то для упрощения можно воспользоваться следующими двумя способами включения проверки при очередной перезагрузке:

- если планируется перезагрузка в текущий момент, то следует выполнить команду:

  ```
  shutdown -rf now
  ```

  Ключ `f` здесь как раз и заставляет выполнить проверку при старте;
- если необходимо просто настроить запуск проверки при очередной перезагрузке, то следует создать файл forcefsck в корне диска (например, командой `touch /forcefsck`, выполняемой от имени суперпользователя).

Но контроль ошибок файловой системы — это еще не все. Современные жесткие диски поддерживают технологию S.M.A.R.T., которая может предсказать надвигающуюся «кончину» жесткого диска, — это очень удобно, ведь вы сможете заранее заменить жесткий диск, не дожидаясь его отказа.

Существует множество поддерживающих S.M.A.R.T. программ (как платных, так и бесплатных), используя которые вы можете получить информацию о своем жестком диске. Одна из таких программ — CrystalDiskInfo[1] (рис. 11.8). Программа бесплатная, поэтому можете использовать ее безо всяких ограничений. Подобную проверку желательно проводить раз в квартал или чаще, если есть подозрения, что какому-либо жесткому диску «плохо» (подробно технология S.M.A.R.T. описана в *главе 7*).

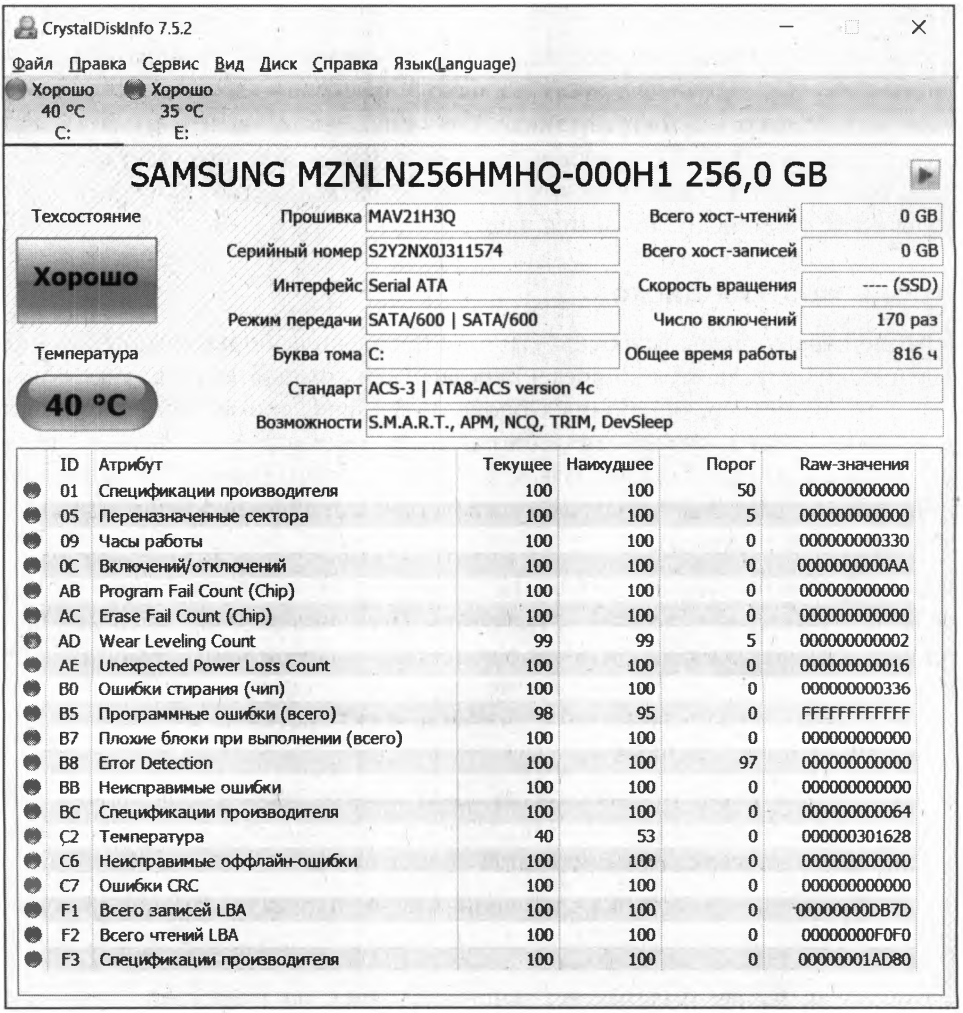


Рис. 11.8. Программа CrystalDiskInfo

[1] См. **https://crystalmark.info/en/software/crystaldiskinfo/**.

Восстановление данных с жестких дисков

В Windows не предусмотрены штатные средства для восстановления удаленных данных, кроме программы Корзина. Поэтому наиболее часто применяемыми средствами для восстановления информации с жестких дисков являются программы Easy Recovery[1] от Ontrack Data Recovery, Inc., NTFS Data Recovery Toolkit[2] и GetDataBack[3] от RunTime Software.

Эти программы позволяют восстановить данные с дисков после их форматирования, и даже с тех дисков, которые не определяются в BIOS компьютера.

Использование указанных программ достаточно очевидно. Сначала проводится 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.

> ***Совет***
>
> Самое лучшее средство от потери данных — это резервная копия. Лучше каждый день создавать резервные копии важных данных, чем потом ломать голову над тем, какой программой восстанавливать утраченное.

Проверка оперативной памяти

В Windows 10/11 и Server 2012/2022 включена программа проверки оперативной памяти. Запуск ее осуществляется выбором соответствующего пункта загрузки при старте системы. Для предыдущих версий Windows можно использовать утилиту memtest, которую легко найти на просторах Интернета. Эту утилиту необходимо запускать, загрузившись в режиме командной строки (без подключенных драйверов памяти) с флешки или компакт-диска (образы загрузочных дисков для различных версий ОС Windows можно загрузить, например, с сайта **http://www.allbootdisks.com/**).

В Linux-системах утилиты проверки памяти часто включаются в комплект установочных дисков. Например, запуск теста памяти в Ubuntu осуществляется при загрузке компьютера с установочного компакт-диска из главного меню (на первом экране). В других дистрибутивах такое приложение нужно установить. Например, в CentOS — это пакет memtest86+:

```
# yum install memtest86+
```

После чего выполнить программу настройки пакета memtest, которая добавит в меню загрузчика Linux запись:

```
# memtest-setup
```

---

[1] См. **www.ontrack.com**.

[2] См. **http://www.ntfs.com/recovery-toolkit.htm**.

[3] См. **www.runtime.org**.

Теперь можно перезагрузить компьютер и в меню загрузчика выбрать команду запуска теста памяти (рис. 11.9). Будет запущена утилита memtest — делать ничего не требуется, просто дождитесь результата тестирования памяти (рис. 11.10).

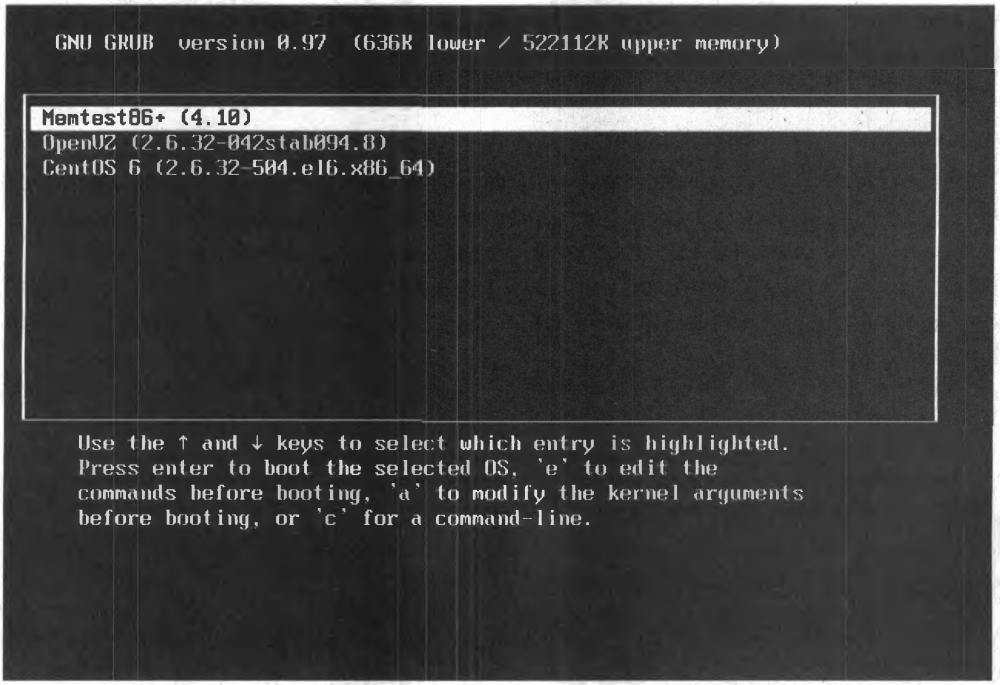


Рис. 11.9. Загрузчик Linux

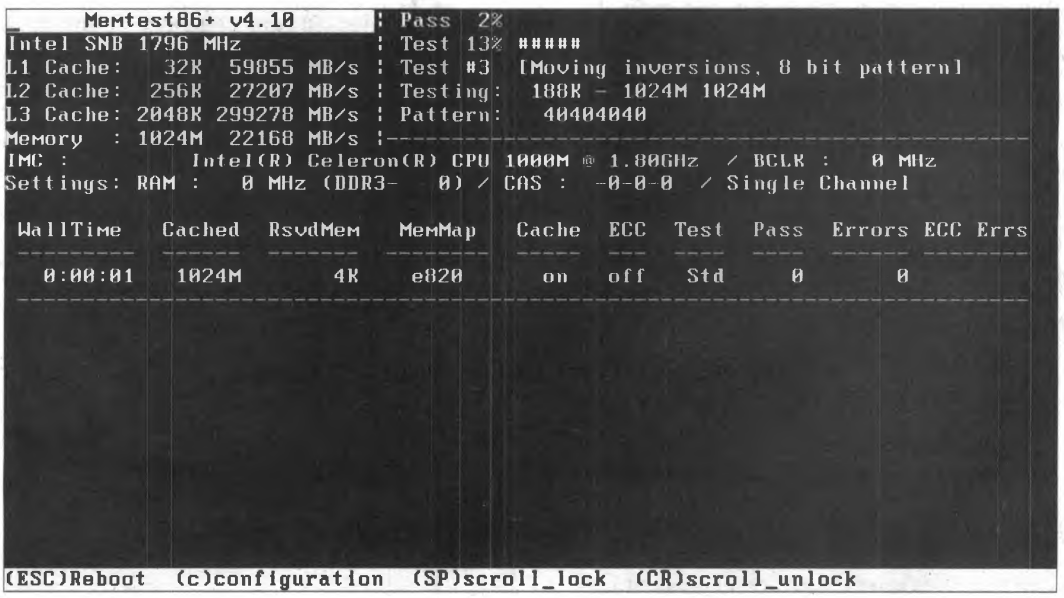


Рис. 11.10. Программа memtest86+

По умолчанию запускается самый простой тест. Если ошибка не обнаружена, увеличьте число проходов и/или выберите более сложный тест (из меню **Configuration**).

Помните, что полное тестирование модуля памяти может занять несколько часов. Если такой простой недопустим, то подозрительные модули памяти нужно заменить на запасные и провести их тестирование в более свободное время.

Контроль теплового режима работы системы

Одна из распространенных причин нестабильной работы компьютера — неудовлетворительный тепловой режим в системном блоке. Работа процессора при повышенной температуре может стать причиной отключения системного блока. Понятно, что такое отключение производится на аппаратном уровне, и пользователь теряет все несохраненные данные.

Прежде всего нужно очистить систему охлаждения от пыли — она забивает радиатор процессора и эффективность вентиляции снижается. Как правило, чистка системы охлаждения в 90% случаев решает проблему. Если проблема не решена и компьютер продолжает выключаться, надо заменить термопасту в месте контакта процессора и радиатора, причем термопасту следует наносить и на сам процессор, и на радиатор.

Конечно, нужно проверить и эффективность работы самого вентилятора, охлаждающего радиатор процессора. Вентилятор — не очень надежное устройство, и лучше, если у вас есть несколько запасных.

Дешевые вентиляторы уже через год начинают крутиться медленнее, что отрицательно сказывается на охлаждении процессора. Сюда же нужно добавить и слой пыли, которой за год успеет обрасти радиатор (учитывая, что обычно корпус компьютера опечатан, в течение гарантийного срока никто чистить радиаторы не станет — чтобы не лишиться гарантии на весь системный блок).

Кроме радиатора процессора вентиляторы работают также и на видеокарте, внутри блока питания, на материнской плате, а иногда и на стенке корпуса компьютера, обеспечивая дополнительную вытяжку. Количество вентиляторов в системном блоке зависит от конфигурации компьютера и используемых аппаратных средств.

Спустя некоторое время вентиляторы начинают издавать не очень приятный шум. Да, можно смазывать оси вентиляторов специальной смазкой, однако такой операции хватает ненадолго, и месяца через три вентиляторы снова «берутся за свое». Отсюда рекомендация — смазать вентиляторы и в течение трех месяцев заменить их новыми.

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.

Температура внутри корпуса компьютера может повыситься не только из-за ухудшения качества вентиляторов. Причиной перегрева могут стать и 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, к возникновению сбоев в его работе или даже полному выходу из строя. Учтите, что 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.

Ошибки программного обеспечения

Описать все возможные ошибки программного обеспечения, сами понимаете, невозможно. Ни в этой книге, ни в какой-либо еще. Хотя бы по той причине, что программное обеспечение регулярно обновляется, старые ошибки исправляются и новые добавляются.

Какие-либо рекомендации дать тоже невозможно, поскольку никто не может предугадать, с какой проблемой столкнетесь именно вы. Единственное, что можно посоветовать, — попробуйте поискать описание ошибки в Интернете. Полагаем, вы не единственный, кто с ней сталкивался, и решение, скорее всего, уже есть. Не нужно забывать и о службе технической поддержки разработчика, если вы на ее услуги подписаны.

Восстановление «упавших» систем

Если сервер не загружается, то у администратора есть несколько способов восстановить его работоспособность:

- восстановить загрузчик системы (если проблема в нем);
- восстановить всю систему из ранее созданного образа (не всегда эффективно, но практически всегда восстанавливает весь функционал системы);
- загрузка в специальных режимах, позволяющих устранить неисправности;
- использование последней удачной конфигурации из контрольных точек восстановления — возврат к предыдущему состоянию;
- переустановка сервера с нуля.

Восстановление из резервной копии

Начнем с этого способа, поскольку восстановление из резервной копии — самый простой и быстрый способ решения проблемы. Быстрый, потому что вы уже знаете все необходимые шаги. Простой, потому что никаких проблем решать не нужно, достаточно действовать по заранее подготовленному сценарию. Главное, чтобы вы имели актуальную копию данных.

Восстановление из резервной копии хорошо еще тем, что оно позволяет возобновить работу системы на новом оборудовании (в случае физического выхода сервера из строя). Подготовка к восстановлению является достаточно простой операцией и подробно описана в соответствующих руководствах. К сожалению, такой функциональностью обладают коммерческие программы резервного копирования, но это один из тех случаев, когда экономия может обойтись дороже.

Восстановление загрузчика системы

В современных системах ситуация с невозможностью начала загрузки является весьма редкой. На производственных системах она возникает в случае катастрофического выхода из строя загрузочного диска. Ситуация чаще встречается в условиях тренировочных полигонов и возникает вследствие ошибок администратора — например, при установке нескольких операционных систем.

Восстановление загрузчика — только первый шаг, обычно за ним следуют операции по восстановлению загрузки в полном объеме (успешного старта всех служб сервера).

Восстановление загрузки Windows 8

О том, как восстановить загрузку Windows 7, рассказывать не станем — о клавише <F8> знают все. Но что делать, если не загружается рабочая станция, работающая под управлением Windows 8? Меню, да и сама процедура восстановления этой системы существенно отличаются от того, что мы видели в Windows 7, — именно поэтому меню предыдущей ОС было переименовано в *среду восстановления* — так солиднее.

Итак, несколько нововведений, о которых вам нужно знать, особенно если вы работали с предыдущими версиями Windows:

- теперь клавиша <F8> не работает. А мы-то все пытались ее нажимать... Среда восстановления запускается иначе — более хитро. А как именно — будет сказано чуть далее;
- средство автоматического восстановления системы (рис. 11.11) запускается теперь при малейшем намеке на сбой (чтобы получить этот снимок с экрана, нам пришлось отключить питание при загрузке системы. Способ весьма жестокий, зато мы проверили работу средства в «боевых» условиях). Автоматическое восстановление можно запустить и через среду восстановления. Честно говоря, лучше бы при сбое запускалась среда восстановления. Было бы проще до нее добраться;
- можно вернуть старое загрузочное меню, если новое вам не по душе (информацию вы можете найти в Интернете);
- в разделе **Общие** средства изменения параметров компьютера (новой панели управления) имеется кнопка **Перезагрузить сейчас**. После ее нажатия компьютер перезагрузится и будет запущена среда восстановления. Но ведь сначала нужно вызвать эту панель, а потом перейти в раздел **Общие**. Одним словом, нам предлагается бродить по дебрям меню...

Рис. 11.11. Автоматическое восстановление

Да, похоже, что в Microsoft кто-то ночей не спал — все думал, как бы сделать запуск среды восстановления менее удобным. И придумал воистину извращенное решение — вместо привычной всем пользователям клавиши <F8> теперь нужно выполнить следующие действия:

- нажать клавиатурную комбинацию <Windows>+<I> — для отображения панели **Параметры** (рис. 11.12);
- нажать кнопку **Выключение**, затем клавишу <Shift> и, удерживая ее, выбрать из меню пункт **Перезагрузка**. То есть команду **Перезагрузка** для запуска среды восстановления следует выполнять только при нажатой клавише <Shift> (если клавишу <Shift> не удерживать, будет выполнена простая перезагрузка).

Рис. 11.12. Панель Параметры

После перезагрузки, выполненной таким способом, появится синий экран, содержащий следующие опции (рис. 11.13):

- **Продолжить** — выйти из меню и продолжить нормальную загрузку компьютера;

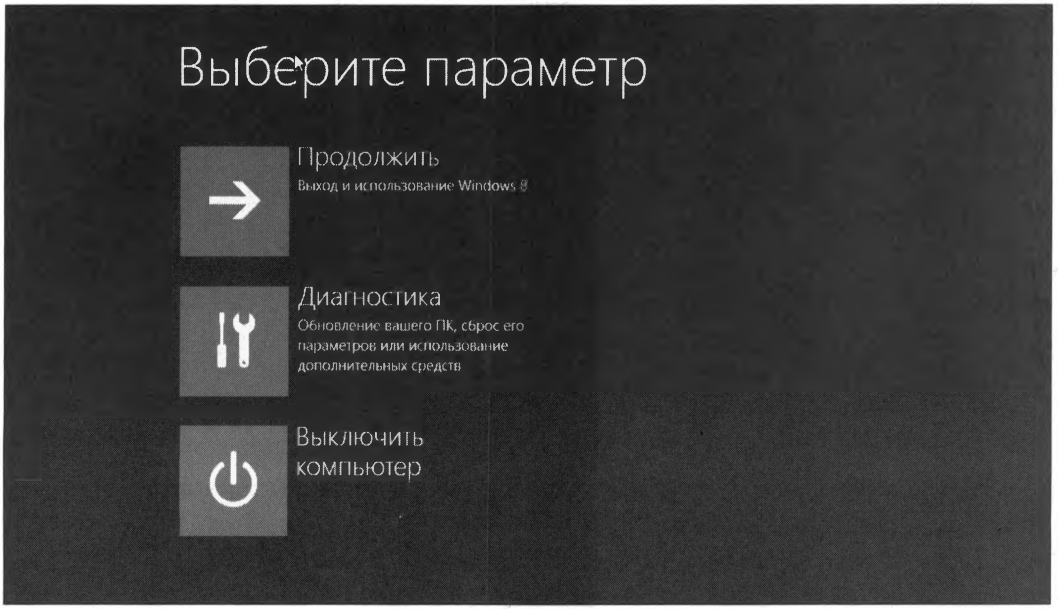


Рис. 11.13. Загрузочное меню Windows 8

- **Диагностика** — здесь вы найдете команды решения проблем. По сути, будет запущена среда восстановления;
- **Выключить компьютер** — соответственно названию.

С первой и третьей командами все предельно ясно, поэтому выбираем команду **Диагностика**. Откроется меню **Диагностика** (рис. 11.14), содержащее команды сброса (**Вернуть в исходное состояние**) и обновления (**Восстановить**) вашего компьютера, а также команда **Дополнительные параметры**, вызывающая меню с дополнительными опциями.

В меню **Дополнительные параметры** (рис. 11.15) содержатся следующие команды:

- **Восстановление системы** — восстановление системы из ранее созданной точки восстановления. Точку восстановления можно создать вручную, но система периодически (например, перед установкой программы или драйвера) сама создает контрольные точки восстановления. При выборе этого варианта система предложит выбрать одну из таких точек;
- **Восстановление образа системы** — восстанавливает Windows по предварительно созданному образу. При выполнении этой команды система предложит выбрать файл образа системы — можно указать файл образа с винчестера или с диска CD/DVD;

Рис. 11.14. Меню Диагностика

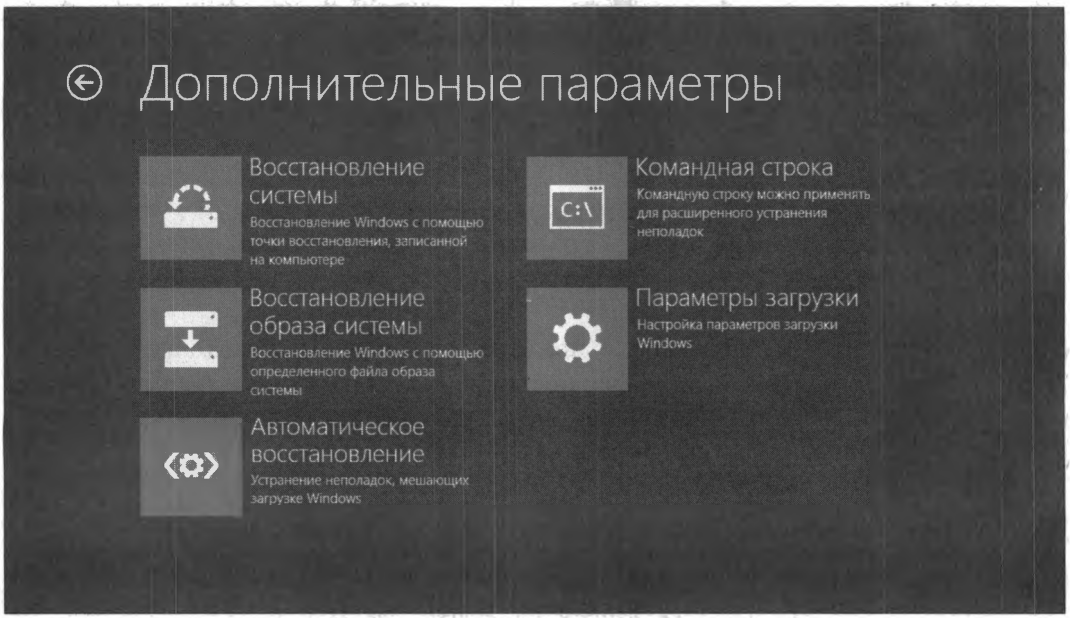


Рис. 11.15. Меню Дополнительные параметры

- **Автоматическое восстановление** — автоматическое исправление некоторых проблем, мешающих загрузке Windows (инструмент, показанный на рис. 11.11);
- **Командная строка** — вызов командной строки для ручного ввода команд;
- **Параметры загрузки** — открывает экран **Параметры загрузки** (рис. 11.16), в котором для доступа к этим параметрам нужно нажать кнопку **Перезагрузить**.

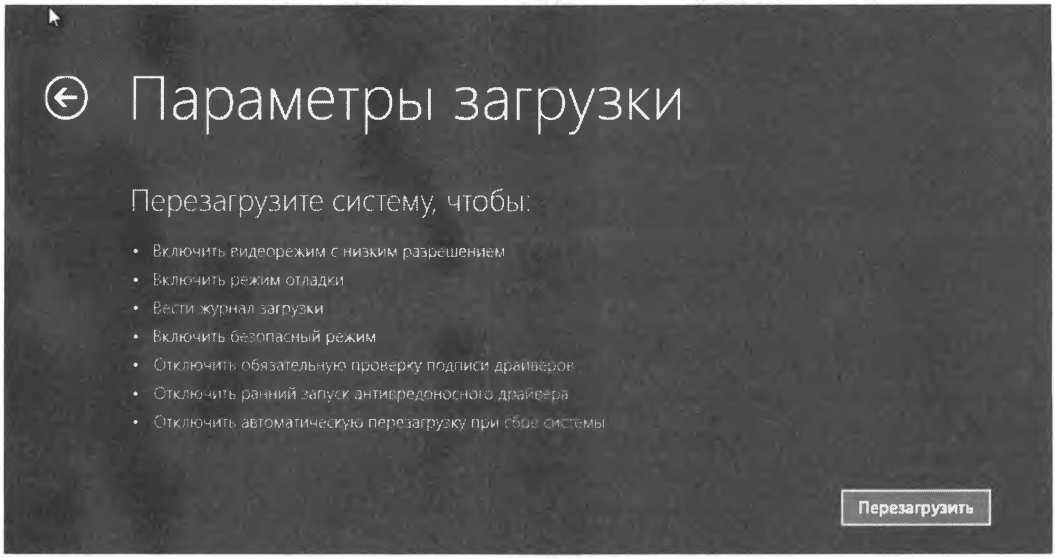


Рис. 11.16. Нажмите кнопку **Перезагрузить**

А после перезагрузки вы увидите экран параметров загрузки (рис. 11.17), которые раньше находились в меню, вызываемом при загрузке компьютера по нажатии клавиши <F8>. В этом меню вы найдете команды загрузки в безопасном режиме, команды отключения антивредоносной защиты, включения видеорежима с низким разрешением и т. д.

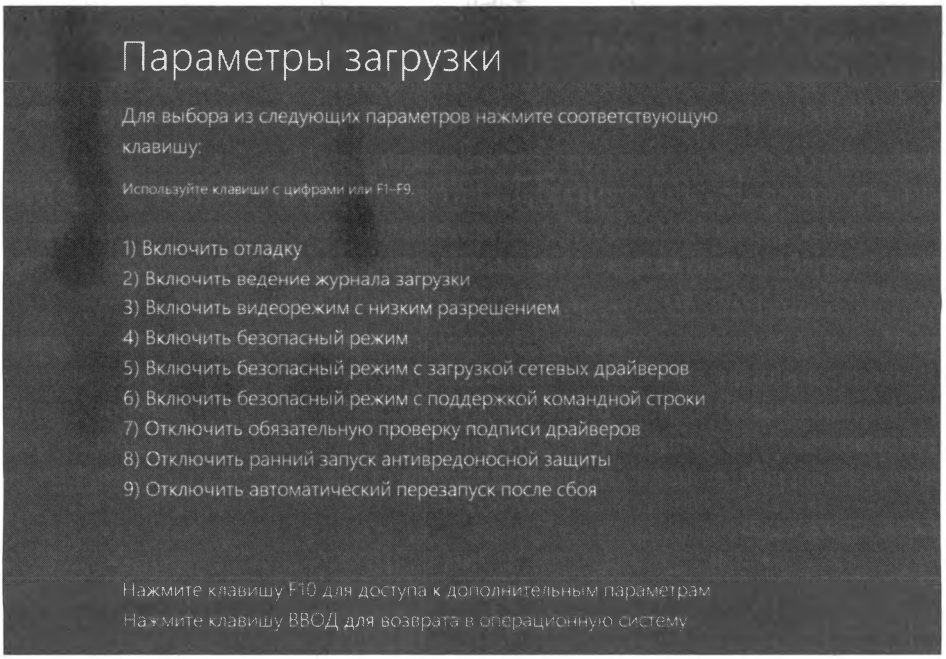


Рис. 11.17. Параметры загрузки

Зачем нужно было так далеко прятать это полезнейшее меню, мы не знаем...

Выбор команд здесь осуществляется или цифровыми клавишами, или клавишами <F1>–<F9>. Клавиша <F10> отображает меню (рис. 11.18), в котором можно или загрузить среду восстановления, т. е. вернуться к меню дополнительных параметров (см. рис. 11.15), или загрузить операционную систему, нажав клавишу <Enter>.

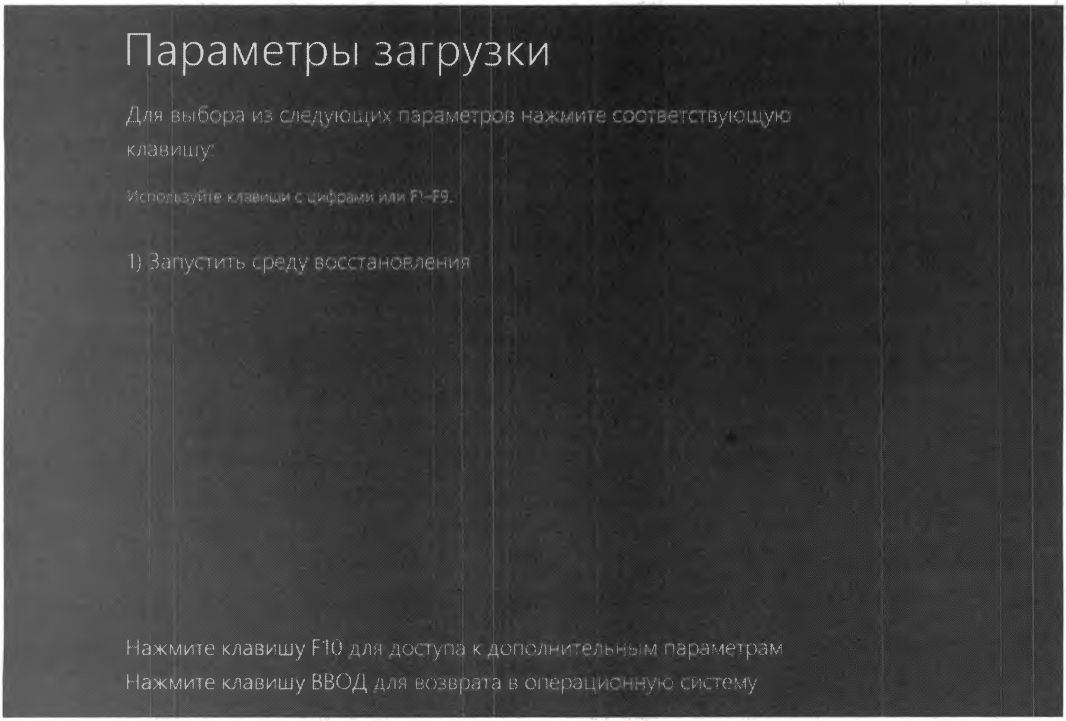


Рис. 11.18. Дополнительные параметры загрузки

Восстановление загрузки Windows 10/11

Чтобы *открыть* среду восстановления Windows 8, нужно было выполнить немало манипуляций, недалеко ушедших от пресловутой пляски вокруг компьютера с бубном (см. предыдущий раздел). В Windows 10/11 все достаточно просто: откройте окно **Параметры**, перейдите в раздел **Обновление и безопасность | Восстановление** и нажмите кнопку **Перезагрузить сейчас** (рис. 11.19).

> ***Примечание***
>
> Конечно, среда восстановления запустится и автоматически — после сбоя.

После перезагрузки вы увидите меню со следующими опциями (рис. 11.20):

- **Продолжить** — выйти из меню и продолжить нормальную загрузку компьютера;
- **Диагностика** — здесь вы найдете команды решения проблем;
- **Выключить компьютер** — выключить компьютер.

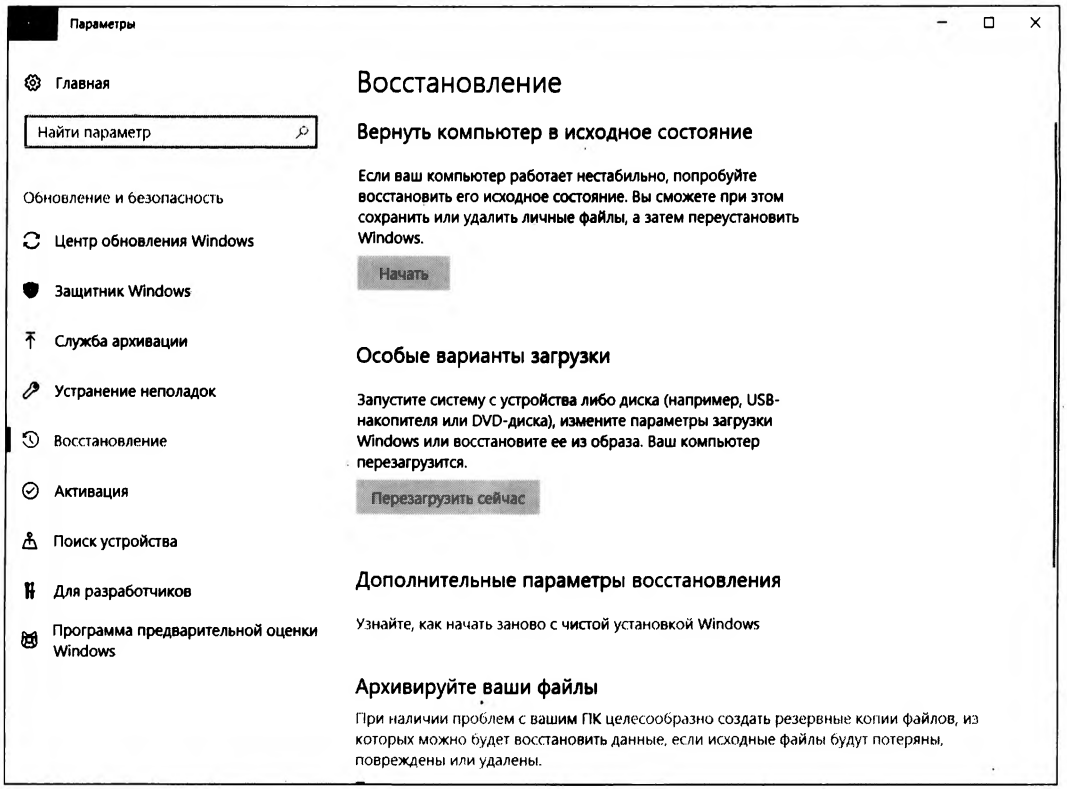


Рис. 11.19. Раздел **Восстановление**

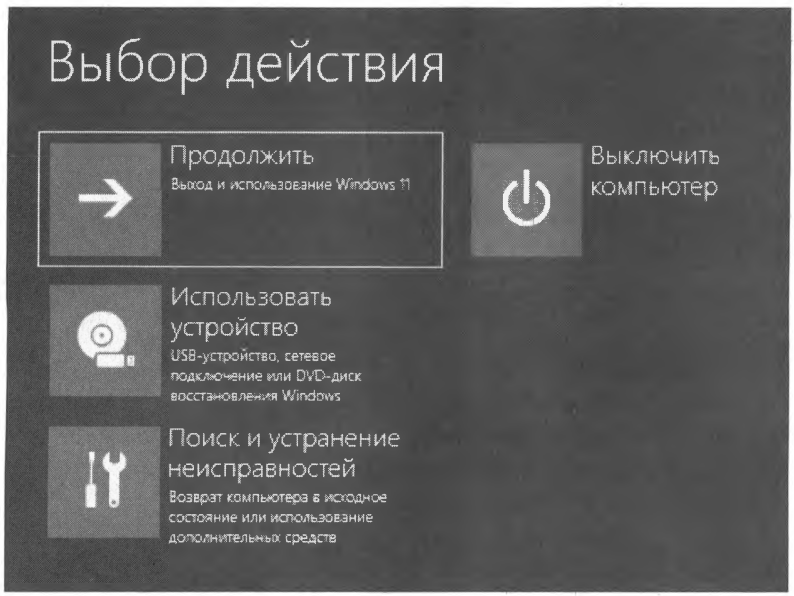


Рис. 11.20. Среда восстановления Windows 11

Первая и третья команды здесь также вопросов не вызывают, поэтому выбираем команду **Диагностика**. Откроется меню **Диагностика** (рис. 11.21), содержащее команды сброса и обновления вашего компьютера, а также команду **Дополнительные параметры**, вызывающую меню с дополнительными опциями (рис. 11.22).

В меню **Дополнительные параметры** содержатся команды, аналогичные командам такого же меню Windows 8 (см. *разд. «Восстановление загрузки Windows 8»*).

Рис. 11.21. Меню Диагностика

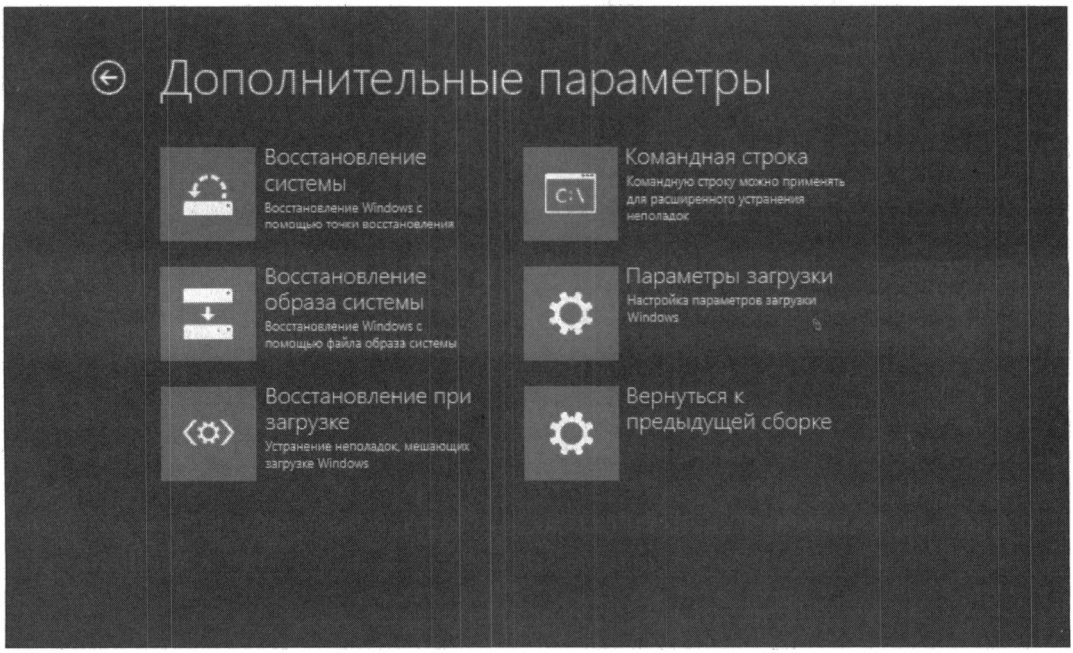


Рис. 11.22. Меню Дополнительные параметры

Восстановление загрузки Linux-систем

Что делать, если загрузчик Linux (GRUB2 или его более старая версия — GRUB) поврежден? Восстановить его, для чего загрузиться с LiveCD (подойдет любой LiveCD с любым дистрибутивом Linux) и ввести следующие команды:

```
mkdir /old
mkdir /old/dev
mount /dev/sdaN /old
```

> ***Примечание***
>
> Все команды должны выполняться от имени root, поэтому командам восстановления следует предпослать команды `su` или `sudo`.
>
> В частности, в LiveCD Ubuntu нужно вводить все команды с использованием команды `sudo` — например, так:
>
> ```
> sudo mkdir /old
> sudo mkdir /old/dev
> ...
> ```

Разберемся, что означают эти команды:

- первая из них создает каталог /old, который будет использоваться в качестве точки монтирования;
- вторая — создает в этом каталоге подкаталог dev, который пригодится для монтирования devfs — псевдофайловой системы;
- третья — используется для монтирования корневой файловой системы дистрибутива Linux, установленного на жестком диске в разделе /dev/sdaN (где *N* — номер раздела), к каталогу /old.

  Предположим, что на вашем компьютере дистрибутив Linux был установлен в раздел /dev/sda5. Тогда вам нужно ввести следующую команду:

  ```
  mount /dev/sda5 /old
  ```

После этого надо подмонтировать каталог /dev к каталогу /old/dev. Это делается с помощью все той же команды `mount`, но с параметром `--bind`:

```
mount --bind /dev /old/dev
chroot /old
```

Команда `chroot` заменяет корневую систему нашего LiveCD на корневую систему дистрибутива, установленного на винчестере. Вам остается лишь ввести команду:

```
/sbin/grub-install /dev/sda
```

Эта команда установит загрузчик GRUB так, как он был установлен изначально. После установки GRUB нужно перезагрузить компьютер командой `reboot`.

Если опции восстановления недоступны...

Описанные ранее способы восстановления загрузки работают, если не нарушена структура жесткого диска. А если, например, повреждена таблица разбиения диска или он был по ошибке отформатирован, то сначала нужно вылечить сам диск.

В Сети можно найти много различных программ, собранных на загрузочные компакт-диски. Загрузившись с такого компакт-диска, можно вызвать соответствующую программу и попытаться восстановить структуру диска. Мы не приводим конкретных ссылок, поскольку ссылки подвержены изменениям, но найти их не представляет труда. Отметим только, что такую сборку желательно подготовить заблаговременно.

Понятно, что это все требует существенных затрат времени и должно использоваться только в том случае, если нет другого варианта.

Загрузка в специальных режимах

Выбор специального варианта загрузки осуществляется при старте системы — меню выбора показывается на небольшое время, в течение которого администратору необходимо выбрать желаемый вариант.

Загрузка Windows 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.

Если вам удается загрузиться в безопасном режиме, то далее уже можно приступить к лечению: заблокировать устройства, перевести сбойные службы в отключенный режим и т. п.

> ***Примечание***
>
> Если настройками отключен вывод меню загрузки, то перейти в безопасный режим можно, удерживая при включении компьютера нажатой клавишу <Shift> (или нажимая клавишу <F8> — с учетом ограничений, описанных в *разд. «Восстановление загрузки Windows 8»*).

Загрузка *NIX-систем в однопользовательском режиме

В Linux можно загрузиться в так называемом *однопользовательском* режиме. Это аварийный режим, который используется для восстановления системы в самых сложных случаях.

Для перехода в этот режим нужно через загрузчик GRUB2 передать ядру параметр `single`. В зависимости от настроек системы для входа в однопользовательский режим может понадобиться ввести пароль root.

Графический режим в этом режиме не запускается — вам придется работать в командной строке. Администраторы, привыкшие к Windows, могут ощущать в этом режиме некоторый дискомфорт.

Все команды в однопользовательском режиме выполняются с правами root, поэтому при работе в нем нужно быть особенно осторожными.

Откат к предыдущим состояниям системы

Загрузка последней удачной конфигурации Windows

В случае установки некорректного драйвера или других ошибок конфигурации может понадобиться запуск системы в режиме загрузки последней удачной конфигурации.

Режим загрузки последней удачной конфигурации подойдет, если после перезагрузки системы выяснилось, что она не загружается. Но поможет он только в тех случаях, если пользователь в систему не заходил, поскольку конфигурация после входа пользователя в систему сохраняется заново. То есть если вы вошли в систему и уже там обнаружили, что что-то не так, то загрузка последней удачной конфигурации вам не поможет, поскольку конфигурация окажется перезаписана. В таком случае вам придется обратиться к восстановлению из контрольной точки.

Загрузка конфигурации из точек восстановления Windows

Начиная с Windows Vista, в Windows появились опции создания точек восстановления, позволяющих «откатить» систему на предыдущее состояние после какого-либо системного действия — например, установки программы, обновления драйвера и пр. Обычно точки восстановления создаются системой автоматически, но вы можете создать их и вручную. Например, отладили вы систему и видите, что она работает стабильно, — в этом случае можно создать точку восстановления.

Обычно администраторы забывают создавать точки восстановления вручную, поэтому остается полагаться лишь на систему. Утилита **Восстановление системы** позволяет выбрать, какую точку восстановления задействовать. Получить доступ к этой утилите можно из окна **Дополнительные параметры** (см. пункт слева вверху в меню на рис. 11.22). Как можно видеть на рис. 11.23, в системе имеются сейчас четыре точки восстановления.

Значения реестра системы сохраняются в папках точек контрольного восстановления системы (папки System Volume Information). При работе операционной системы эти папки доступны только системной учетной записи, но администратор может настроить для себя права доступа к ним. В режиме консоли восстановления контроль прав доступа не действует, и данные из этих папок будут доступны без дополнительных операций. Их параметры обычно более точно соответствуют последним настройкам системы, чем копии реестра, хранящиеся, например, в папке \Windows\Repair (здесь и далее в примерах этого раздела считается, что система установлена в папку C:\Windows, — иначе следует заменить название каталога).

Данные точек контрольного восстановления системы хранятся в каталогах с именами типа: _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 RPномер и зайти в папку snapshot. В ней сохранены файлы реестра, правда, под именами, отличающимися от тех, которые используются в папке конфигурации. Поэтому для замены файлов реестра администратору необходимо скопировать файлы, указанные левом столбце табл. 11.1,

в папку \Windows\System32\Config и переименовать их так, как указано в правом ее 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

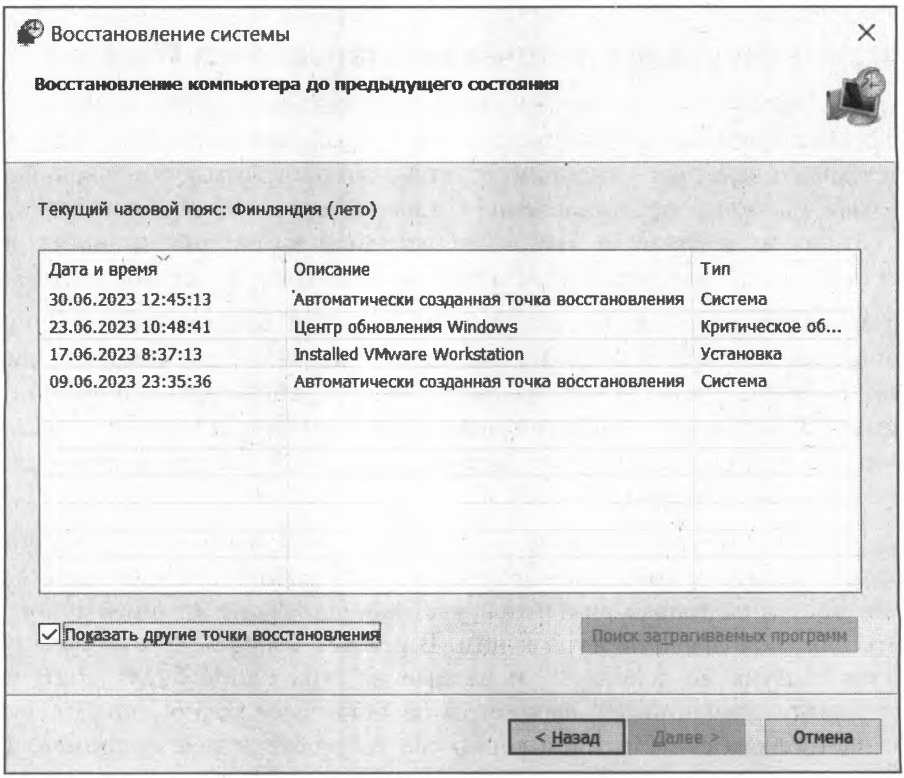


Рис. 11.23. Восстановление системы

Восстановление Windows путем переустановки

В Windows существует возможность восстановления работоспособности системы путем восстановления к настройкам установки (при этом данные пользователя и установленные программы сохраняются). Часто этот способ является самым простым для неподготовленного пользователя.

Если система перестала запускаться, загрузите ее с установочного компакт-диска и начните установку. Когда вы укажете для установки диск, на котором операционная система была установлена ранее, программа обнаружит ее и предложит провести *восстановление*. При подтверждении выбора этого 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, разрушение файловой структуры, в результате чего программа не может обнаружить папки установленной системы).

Учтите, что система восстанавливается к состоянию обновлений, соответствующему установочному пакету. Поэтому после такого восстановления необходимо сразу же установить все обновления, имевшиеся в исходной системе, поскольку в противном случае возможно возникновение ошибок в работе. Чтобы минимизировать операции после такого восстановления, желательно интегрировать в установочный пакет последний сервис-пак и необходимые обновления.

В Windows 10/11 включены режимы быстрой переустановки системы: **Сохранить мои файлы** и **Удалить все** (рис. 11.24). Получить доступ к этим режимам можно из окна **Диагностика** (см. верхний пункт меню на рис. 11.21).

- В режиме **Сохранить мои файлы** будут восстановлены параметры компьютера по умолчанию, ваши параметры персонализации не изменятся, все созданные

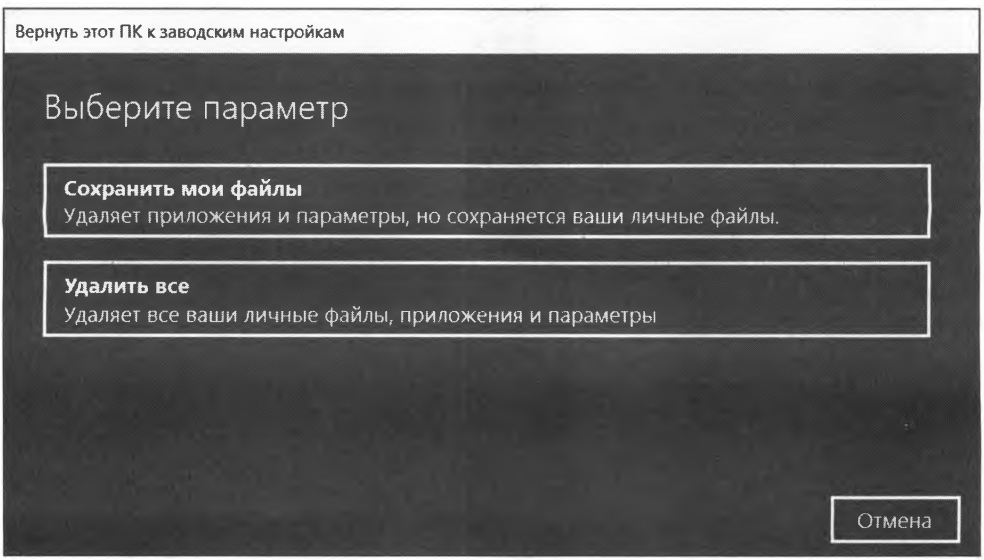


Рис. 11.24. Варианты быстрой переустановки Windows 10/11

вами файлы останутся в целости и сохранности, а вот все установленные приложения будут удалены (кроме приложений, загруженных из Магазина Windows). Список удаленных приложений будет сохранен на рабочем столе.

Этот способ можно порекомендовать, если компьютер начал подтормаживать или работать «неправильно». Причина может быть в неправильно установленных параметрах компьютера, кроме того, негативно повлиять на работу компьютера могли и сторонние приложения.

- В режиме **Удалить все** Windows будет полностью переустановлена с «чистого листа». Ваши приложения, файлы и настройки персонализации будут удалены.

  Обратите внимание — при такой переустановке иногда может потребоваться заново ввести ключ продукта, так что убедитесь, что он у вас есть. Впрочем, если лицензионная система устанавливалась на компьютер штатно, то после переустановки ее активация будет автоматически подтверждена сервером авторизации Microsoft.

Восстановление удаленных данных

Администратору часто приходится восстанавливать один или несколько файлов, случайно удаленных пользователем. К сожалению, большой объем информации не доступен к восстановлению штатными средствами системы.

Оптимально, если на предприятии настроена система резервного копирования и пользователь сможет сам восстанавливать удаленные данные.

Корзины

«Штатная» Корзина Windows малоэффективна, прежде всего, из-за наличия лимита по объему — если удалено файлов больше, чем настроен лимит в свойствах Корзины, то данные уже не будут доступны к восстановлению. Кроме того, Корзина не защищает файлы, удаляемые по сети, в режиме DOS и т. п.

Обеспечить такую защиту могут коммерческие решения, имеющие вид специализированных корзин (например, Norton Protected Recycle Bin) или специализированных серверных решений — таких как Executive Undelete от Executive Software International, Inc. или аналогичных. Подобные программы могут быть централизованно развернуты администратором на рабочие станции и позволяют выполнять операции восстановления как непосредственно пользователем, так и администратором при подключении по сети.

Восстановление из теневых копий

В Windows 10/11 и Server 2008/2022 реализована технология *теневого копирования* для локальных дисков (в Windows 2003 эта возможность присутствует только для сетевых ресурсов и носит название *восстановление предыдущей версии документа.* По умолчанию эта опция не настроена).

Технология теневого копирования (shadow copy) состоит в создании по определяемому администратором графику копий информации. По умолчанию она включена,

администратор может изменить график создания копий или вообще отключить эту функциональность.

Предел количества хранимых копий за различные моменты времени определяется только размером дискового пространства, отведенного для этой операции (рис. 11.25). При этом сама технология очень экономно использует это пространство — десяти процентов объема диска может хватить для хранения промежуточных копий за несколько месяцев интенсивной работы.

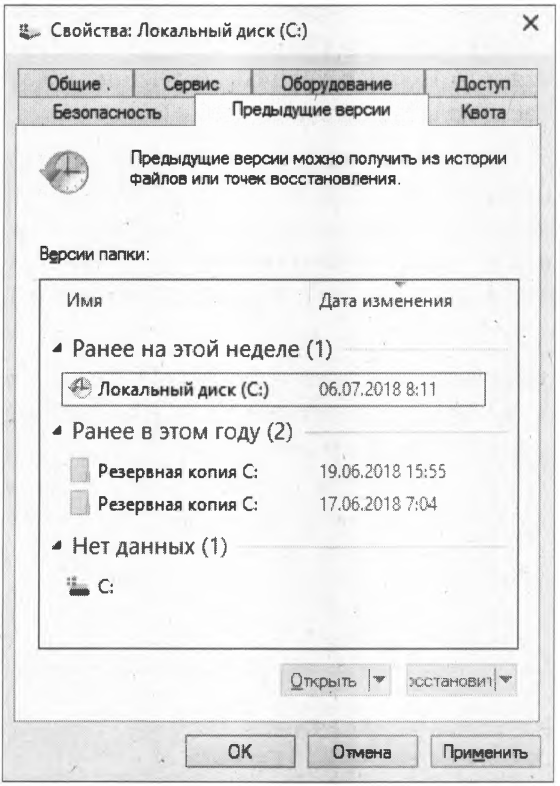


Рис. 11.25. Просмотр предыдущих версий файла (Windows 11)

Технология теневого копирования позволяет, во-первых, осуществлять резервное копирование *всех* данных, в том числе и открытых на момент операции. Во-вторых, у пользователей появилась прекрасная возможность безо всяких дополнительных затрат иметь *несколько версий* документа. Например, после внесения в документ очередных правок вы поняли, что более правильным решением был его предыдущий вариант. Если он не был сохранен в качестве отдельного документа, то вернуться к прежним формулировкам ранее было затруднительно. При использовании же технологии теневого копирования достаточно посмотреть перечень предыдущих версий документа и восстановить необходимую (в другую папку, чтобы не затереть текущую версию).

История файлов

В Windows 8/10/11 есть аналог машины времени (Time Machine) из macOS — функция **История файлов** (ранее History Vault). В Windows 7 уже имелась функция теневого копирования файлов, позволяющая восстановить содержимое файла, скажем, по состоянию на вчера или позавчера, что весьма удобно, ведь ошибочное удаление файла — явление довольно редкое, а вот внесение некорректных изменений в файл встречается гораздо чаще.

В Windows 8/10/11 эта функция усовершенствована. Теперь вы можете выбрать, из каких каталогов файлы не требуется резервировать, где следует хранить резервные копии (предполагается, что их надо хранить на внешнем жестком диске или хотя бы на сетевом), как часто делать резервные копии.

Перед настройкой функции **История файлов** подключите внешний жесткий диск. Впрочем, можно и не внешний, но он обязательно должен быть отдельным — нет смысла хранить резервную копию на другом разделе того же жесткого диска — в случае сбоя все данные, в том числе и резервная копия, будут утеряны. Затем откройте панель управления и перейдите в раздел **Система и безопасность | История файлов**.

По умолчанию **История файлов** выключена (рис. 11.26). Для ее включения нажмите кнопку **Включить**. Если же у вас нет подходящего для истории файлов жесткого диска, вы увидите соответствующее сообщение (рис. 11.27).

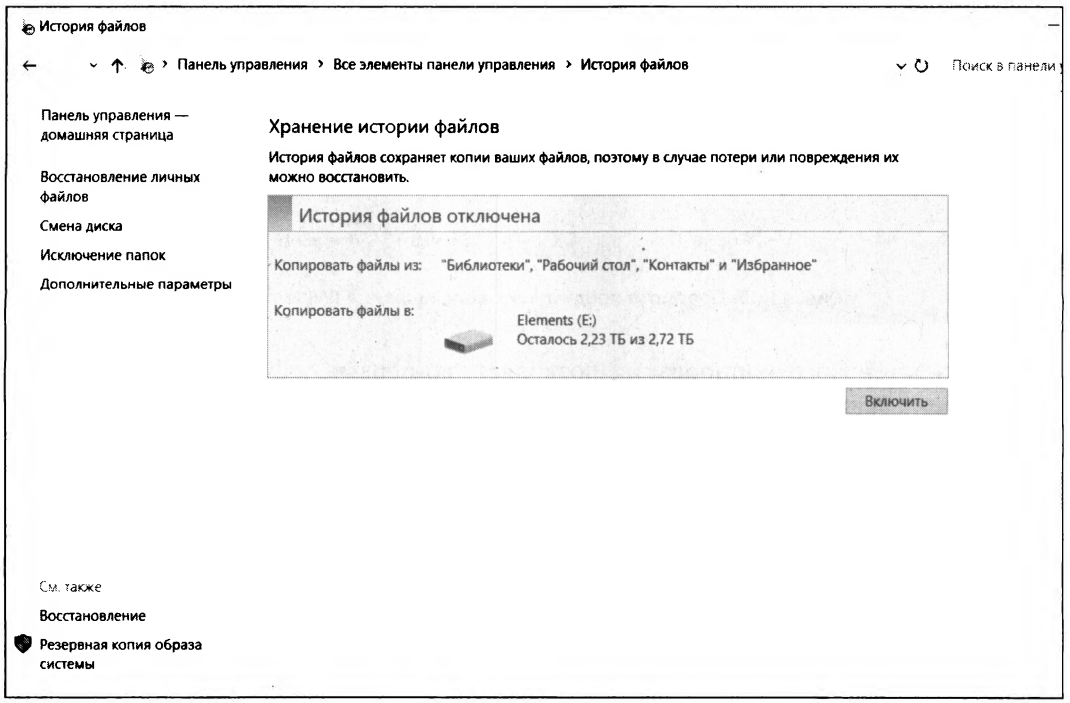


Рис. 11.26. История файлов выключена

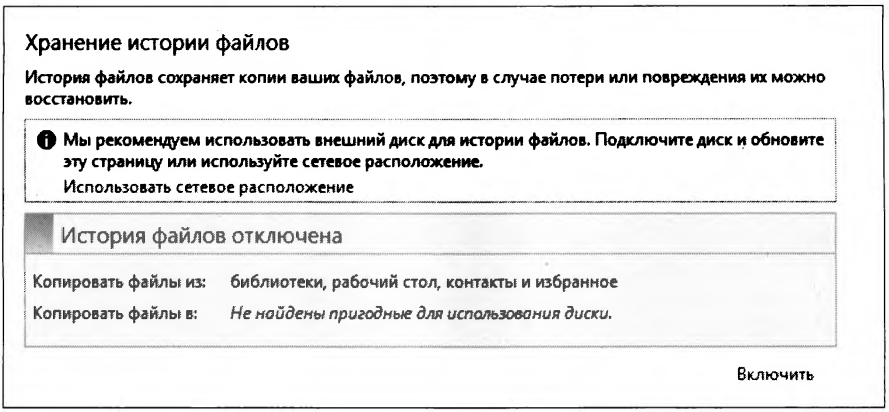


Рис. 11.27. Нет подходящего жесткого диска

При включении функции **История файлов** система спросит вас, хотите ли вы рекомендовать этот жесткий диск для резервного копирования другим членам вашей домашней группы (если вы подключены к домашней группе, разумеется). Это очень полезно, когда есть всего один внешний жесткий диск, а компьютеров в доме — несколько. Понятно, что все остальные компьютеры должны работать под управлением той же версии Windows.

Затем **История файлов** сообщит вам, что она включена, и по умолчанию на внешний диск скопируются все ваши библиотеки, содержимое рабочего стола, контакты и избранное (рис. 11.28).

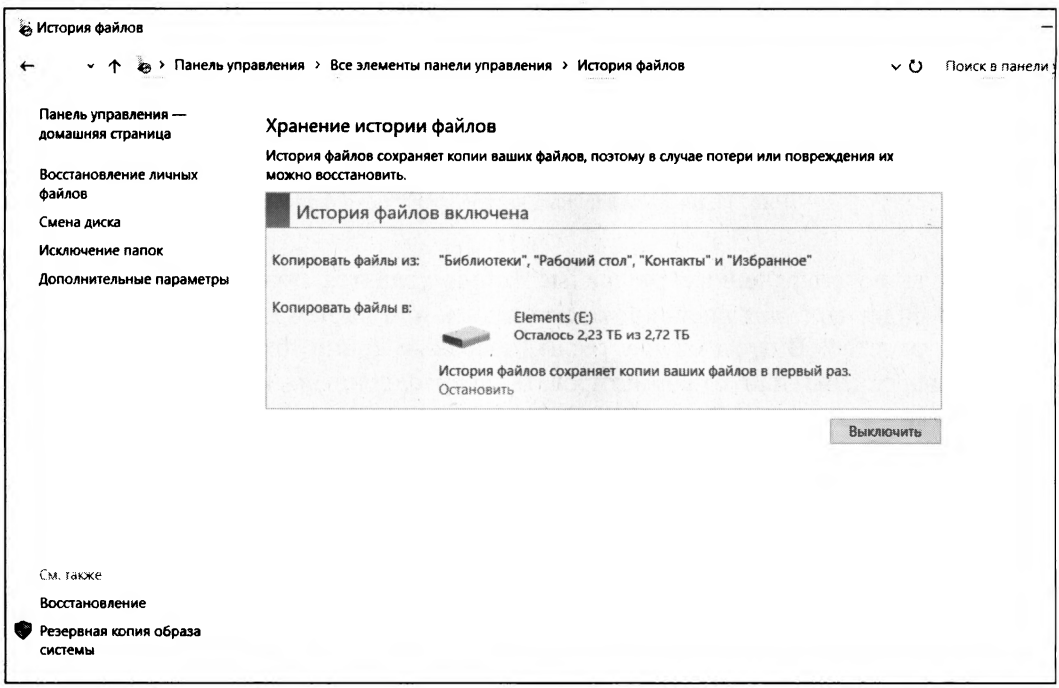


Рис. 11.28. История файлов включена

Теперь следует настроить функцию **История файлов**, чтобы она работала в соответствии с вашими предпочтениями. Выберите команду **Дополнительные параметры** в левой области окна функции (см. рис. 11.28) — откроется окно ее расширенных настроек (рис. 11.29). Здесь вы можете указать, как долго нужно хранить сохраненные резервные копии (**Хранить сохраненные версии**), как часто следует делать резервные копии (**Сохранять копии файлов**) и надо ли рекомендовать этот внешний диск другим членам домашней группы (**Домашняя группа**).

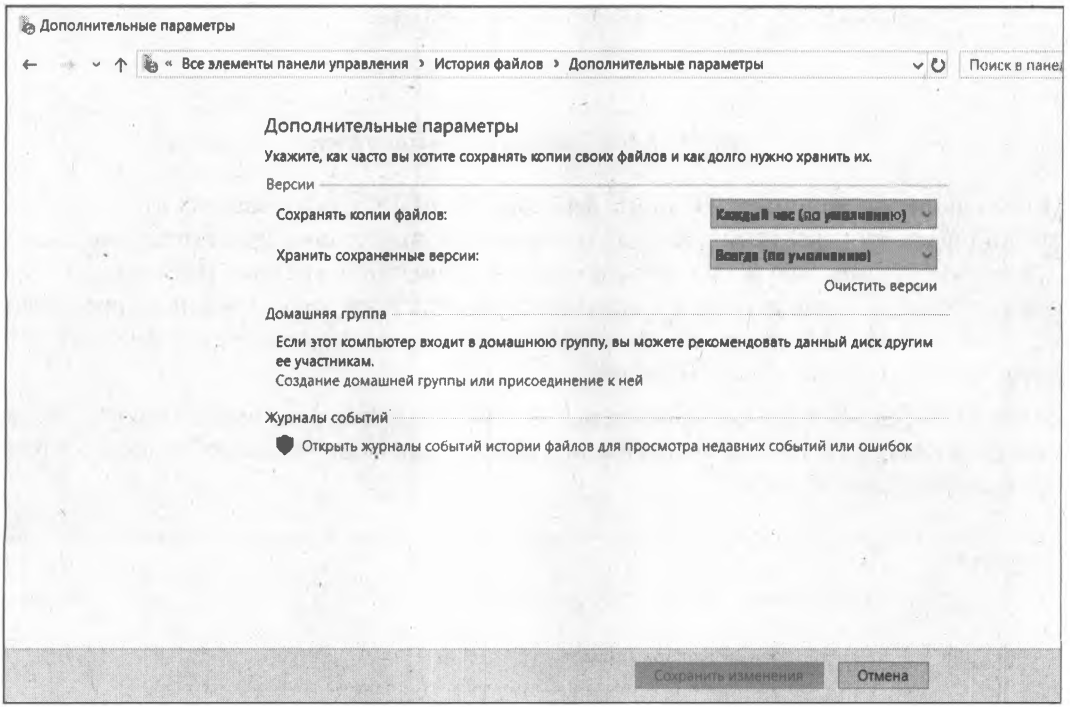


Рис. 11.29. Расширенные настройки истории файлов

По умолчанию сохраненные резервные копии хранятся пожизненно (**Всегда**) — пока не выйдет из строя внешний жесткий диск или на нем не закончится свободное пространство. В этом случае (если резервные копии для вас так важны) вы будете вынуждены или отформатировать переполненный носитель, или купить новый взамен испорченного.

Создаются резервные копии по умолчанию каждый час. Это значение рекомендуется не менять. Если же вы обеспокоены местом на внешнем диске, следует или уменьшить срок хранения копий (установить, например, срок хранения один месяц), или же исключить некоторые папки из резервного копирования. Для этого в левой области окна функции (см. рис. 11.28) выберите команду **Исключение папок** и в открывшемся окне (рис. 11.30) нажмите кнопку **Добавить** для выбора и внесения папки в черный список. Мы исключили папку **Видео**, т. к. в ней хранятся видеофайлы, занимающие на диске много места.

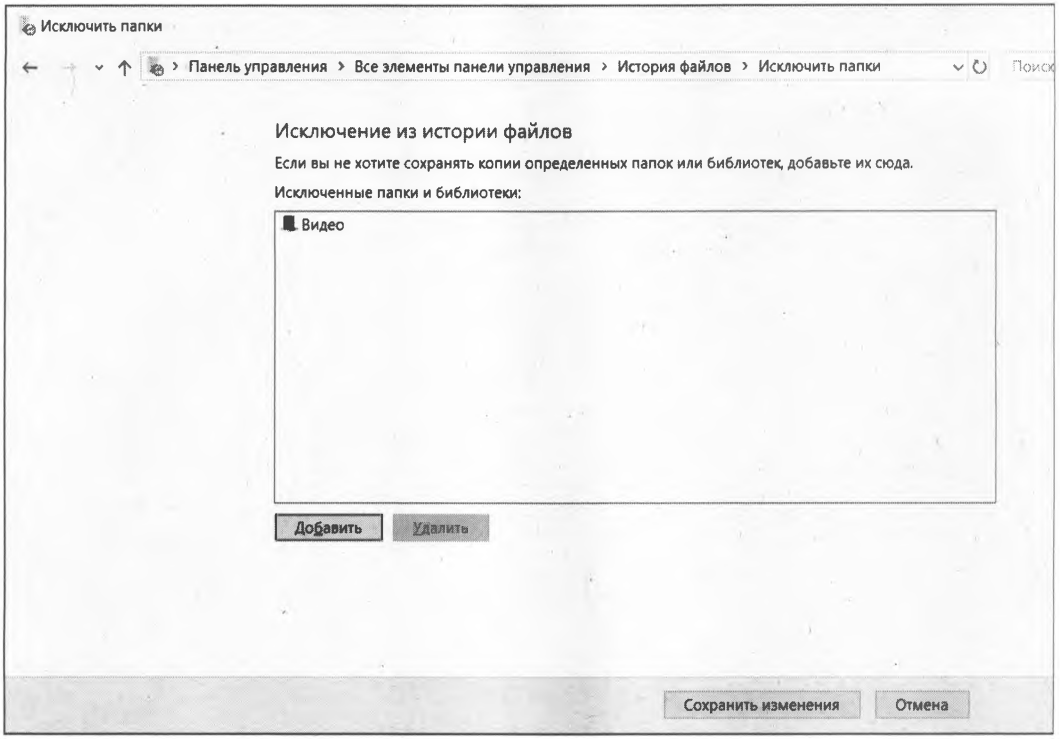


Рис. 11.30. Список исключений

Совет

Какие папки стоит исключить? Понятное дело: видео (библиотека **Видео**) и музыку (библиотека **Музыка**). Видео и музыка занимают на диске слишком много места, да и в случае сбоя вы всегда сможете снова загрузить и видео, и музыку из Интернета. Если же композиции вам столь дороги, создайте их резервную копию на DVD и запрячьте ее куда-нибудь в сейф, а загромождать ими резервный диск не следует. Копировать музыку и видео на внешний диск стоит лишь в одном случае — если вы их автор, и файлы эти могут у вас время от времени модифицироваться.

Осталось рассмотреть одну опцию функции **История файлов — Смена диска** (см. рис. 11.28). С ее помощью вы можете изменить диск, использующийся для резервного копирования (рис. 11.31). Нажав кнопку **Добавить сетевое расположение**, можно добавить сетевой диск.

Небольшой трюк

Чуть ранее было сказано, что можно хранить резервные копии на отдельном разделе жесткого диска, но система позволяет выбрать только или съемный, или сетевой диск. Все правильно — **История файлов** не позволяет выбрать локальный диск для хранения копий файлов. Но можно ее обмануть. Скажем, у вас есть два раздела: C: и D:, и второй раздел (D:) вы хотите использовать в качестве диска для резервных копий. Предоставьте к нему общий сетевой доступ, а в настройках истории файлов укажите его как сетевой диск. **История файлов** будет «думать», что сохраняет данные по сети, а на самом деле они будут физически храниться на соседнем разделе вашего единственного жесткого диска.

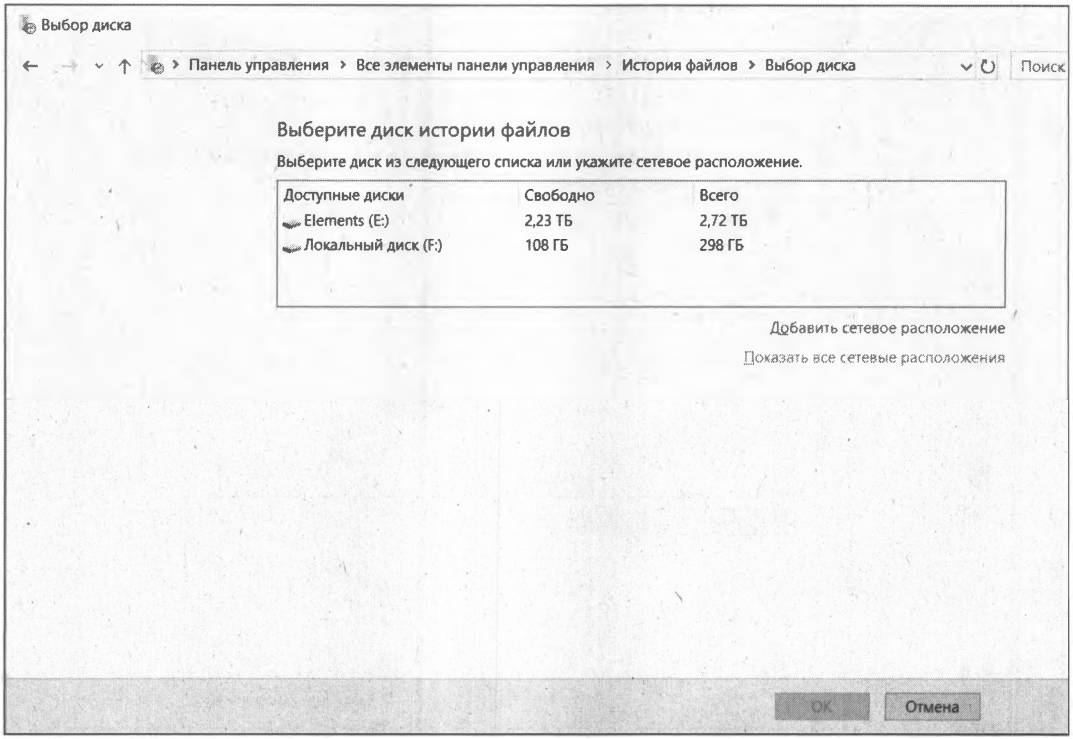


Рис. 11.31. Выбор диска для размещения резервных копий

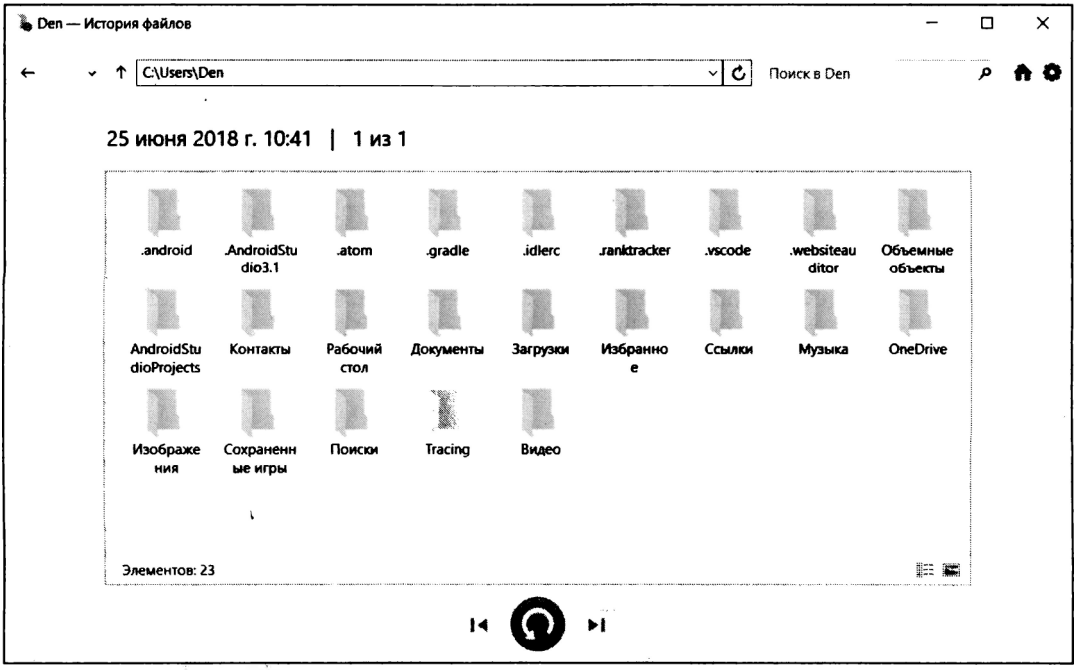


Рис. 11.32. Восстановление личных файлов

Теперь о самом главном — о восстановлении данных из резервной копии. Мало ее создать — еще нужно знать, как восстановить файлы. Для этого выполните команду **Восстановление личных файлов** (рис. 11.32).

Затем выберите дату резервной копии (с помощью кнопок **Назад** и **Вперед** внизу окна) и каталоги, которые следует восстановить. Остается только нажать кнопку **Восстановление в исходном расположении** — большую синюю кнопку по центру окна под областью выбора папок и библиотек.

Иногда требуется восстановить предыдущее содержимое папки, но не в исходное местоположение, а в другой каталог, чтобы сравнить две версии файлов: текущую и предыдущую. Для этого нажмите значок шестеренки (в правом верхнем углу окна), выберите команду меню **Восстановить в** (рис. 11.33) и укажите папку, в которую следует восстановить резервную копию.

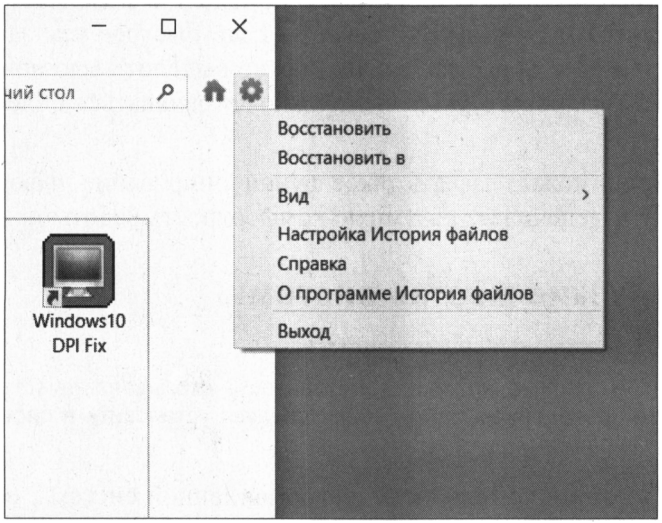


Рис. 11.33. Восстановление резервной копии в определенный каталог

Оптимизация настроек компьютера

Зачастую на администратора компьютерной сети небольшого предприятия ложится выбор моделей приобретаемых компьютеров. В большинстве случаев покупается типовая на текущий момент конфигурация у того поставщика, с которым предприятие (администратора) связывают длительные отношения. Многие предприятия подчас не могут позволить себе приобретение компьютерных брендов, поэтому большинство эксплуатируемых у них моделей собрано специалистами региональных фирм из отдельных блоков. На сбалансированность таких конструкций часто обращается немного внимания, поскольку производительность современных моделей обычно существенно превосходит требования, предъявляемые на индивидуальных рабочих местах, и если производительность компьютера перестает удовлетворять потребности пользователя, то взамен ему 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 покупка нового сервера. Кроме того, правильная конфигурация сможет сэкономить существенные средства.

Что такое «медленно»?

Удовлетворенность производительностью системы — субъективная оценка. Если для пользовательского интерфейса время реакции не должно составлять более 0,6 секунды (например, после щелчка мышью на команде диалоговое окно с параметрами должно появиться за указанный промежуток), то длительность обработки данных зависит от многих параметров: объема данных, сложности вычислений и т. п. Так, в зависимости от условий одно вычисление может считаться быстрым, если оно завершится за 5 минут, а другое — если быстрее чем за 8 часов. Например, для квартального «закрытия» склада можно выделить всю ночь, но для открытия типовых форм кадрового учета не должно затрачиваться более нескольких секунд.

Поэтому медленной можно назвать такое функционирование информационной системы, которое не обеспечивает разумную комфортность работы пользователей.

Основные «узкие места» системы

> ***Совет***
>
> Существенное влияние на производительность оказывает качество драйверов. Поэтому перед проведением оптимизации следует установить в систему их последние имеющиеся версии.

«Узким местом» производительности информационной системы обычно становится один из следующих компонентов:

- процессор;
- оперативная память;
- дисковая подсистема;
- сетевой адаптер (сетевая инфраструктура).

В идеальном случае каждый компонент должен не только не простаивать, но и не сдерживать работу других частей. Для того чтобы проанализировать показатели использования того или иного компонента системы, используются *счетчики производительности*.

В счетчиках постоянно обновляются показатели. Это обновление можно отключить, но особого смысла такая операция не имеет — на производительность системы счетчики практически не оказывают влияния. В операционных системах на базе ядра Windows NT для отображения состояния счетчиков служит программа **Производительность** (Performance Monitor). Для *NIX-операционных систем можно найти большое количество утилит, но наиболее популярными являются: top (отобра-

жает загрузку процессора, использование памяти и данные по наиболее загруженным процессам), iostat (показывает загрузку процессора и параметры использования дисков), nmon (отображает основные параметры нагрузки и позволяет записывать их с заданной периодичностью в файл с последующей обработкой и формированием отчетов) и др.

Число счетчиков непостоянно и может меняться в зависимости от установленного программного обеспечения и подключенного оборудования. Хотя суммарное число доступных для наблюдения и анализа показателей весьма велико (для Windows-системы оно составляет несколько сотен параметров), однако для качественной оценки информационной системы достаточно упомянутых далее. Полный спектр параметров доступен для анализа только квалифицированным специалистам в целях тонкой настройки приложений.

Администраторы сейчас могут найти не одну программу, которая соберет данные производительности системы и сформирует общие рекомендации. Например, Server Performance Advisor от Microsoft (бесплатное ПО) позволяет в течение нескольких минут составить отчет по параметрам системы и представить его руководителю. Но, на взгляд авторов, системный администратор сам должен владеть основами оценки параметров системы.

В табл. 11.2 приведены значения параметров производительности, по которым можно судить о состоянии системы.

Таблица 11.2. *Показатели производительности*

Параметр	Состояние компьютера	
	оптимальное	перегруженное
Процент загрузки процессора	< 40%	> 80+90%
Средняя длина очереди заданий процессора	< 2	>4
Процент загрузки процессора обслуживанием системы	< 4%	> 10%
Обмен страниц памяти в секунду	< 500	> 1000
Среднее время операции записи/чтения на логический диск	< 15 мс	> 25 мс
Средняя длина очереди операций записи/чтения на диск	< 0,2	> 0,6
Процент использования полосы пропускания сетевого адаптера	< 40%	> 60%
Очередь на передачу пакетов в сетевом адаптере	0 пакетов	> 2 пакетов

Оценка производительности процессора

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.

В современные серверы, как правило, устанавливают не по одному многоядерному процессору. И в условиях среднего предприятия увидеть загрузку процессоров компьютера, близкую к 100%, маловероятно. При этом именно процессор может оказаться «узким местом».

Связано это с тем, что показатель производительности подсчитывается усредненно по всем процессорам, а многие расчеты в приложениях не могут быть распараллелены: сначала нужно вычислить одну величину, потом она будет использована в других расчетах, и т. д. Поэтому если какой-либо прикладной процесс (например, процесс сервера базы данных) выполняется в одну нить (поток), то соответствующая загрузка процессора будет показываться как 100%/(число процессоров) и распределится (в программе **Производительность**) между всеми ядрами/процессорами.

Поэтому более информативным будет анализ непроизводительных расходов процессора. В случае Windows-систем это будет счетчик **Processor\% Privileged Time**, а для Linux-компьютеров нужно оценивать время, затрачиваемое процессором на системные операции и ожидание готовности других устройств.

На рис. 11.34 приведен листинг утилиты iostat. В строке `avg-cpu` показаны характеристики загрузки процессора: параметр `%system` отображает загрузку системными операциями, `%iowait` — время, затрачиваемое на ожидание завершения операций ввода/вывода на диски.

Если процент времени, затраченного процессором на служебные цели, составляет 5% и более (примерно), то необходимо принять меры к минимизации этой нагрузки. Возможными причинами могут быть избыточное количество одновременно запущенных программ (время тратится на переключение между процессами), проблемы с оборудованием (увеличенное число прерываний от устройств) и т. д.

```
admin@test:~$ iostat
Linux 2.6.32-34-generic-pae (test)     04.11.2011      _i686_  (1 CPU)
avg-cpu:  %user   %nice %system %iowait  %steal   %idle
           8,10    0,00    1,50    0,96    0,00   89,44
Device:            tps   Blk_read/s   Blk_wrtn/s   Blk_read   Blk_wrtn
sda               2,08        15,09       109,64    1257276    9133150
sdb               0,03         0,87         0,00      72700          0
sdc               0,09         2,74         0,00     228062          0
dm-0             14,34        15,05       109,61    1254018    9131104

                  dm-1         0,01         0,02         0,02       1488       2032
```

Рис. 11.34. Листинг утилиты iostat

Заменить процессор в реальной системе маловероятно. Хорошо, если анализируемая система является виртуальной машиной. В этом случае можно добавить еще один виртуальный процессор. Для физических же серверов практически единственным способом разрешения проблем излишней нагрузки на процессор является уменьшение числа решаемых задач.

Итак, познакомимся с некоторыми показателями оценки производительности процессоров.

- **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. При этом очень часто средний процент загрузки процессора остается сравнительно небольшим.

  Когда процессор не успевает выполнять задания от различных процессов, то эти задания становятся в очередь, процент полезного использования процессора снижается (основное время тратится на переключения между заданиями), а 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).

- **Processor\Interrupts/sec** — счетчик показывает количество запросов к процессору на обработку. Максимальное число прерываний, которое может обработать процессор, зависит от его типа. Для разных процессоров эта величина колеблется от 500 до 2000 прерываний в секунду.

  Поскольку высокое значение этого 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

Установка дополнительной памяти часто является самым простым способом повышения быстродействия системы. Поэтому важно уметь оценить, действительно ли компьютер нуждается в таком обновлении.

- **Объем свободной памяти** — современные операционные системы и приложения весьма агрессивно используют оперативную память компьютера, захватывая весь свободный объем. При этом если другим приложениям потребуется дополнительный объем оперативной памяти, то система выполняет ее перераспределение. Поэтому судить о достаточности или нехватке оперативной памяти по ее свободному объему не имеет смысла.

Более продуктивным является анализ показателей, отображающих использование файла подкачки.

- **Memory\Pages/sec** — одним из самых интегральных показателей использования оперативной памяти является счетчик, демонстрирующий количество запросов страниц памяти из файла подкачки на диске. Такие операции проводятся в случае нехватки физической памяти, поэтому большое значение этого показателя свидетельствует о необходимости установки в систему дополнительной памяти. Для современных серверов приемлемым значением считается величина до 200 страниц в секунду. Критическое значение — порядка 1000 страниц в секунду.

> ***Совет***
>
> Обратите внимание, что на некоторых материнских платах частота, на которой работает оперативная память, зависит от конфигурации устанавливаемых модулей. В этом случае добавление новых модулей памяти может привести к снижению скорости работы с ней. Поэтому при необходимости добавления новых модулей надо предварительно изучить рекомендации вендора по оптимальной конфигурации оперативной памяти системы.

Оценка дисковой подсистемы

Дисковая подсистема может существенно снижать производительность компьютера, поскольку она является самым медленным компонентом. Интегральным же показателем оптимальности используемой дисковой подсистемы можно считать длину очереди заданий (см. далее).

Показатели производительности дисков

- **LogicalDisk (PhysicalDisk)\Avg. Disk Queue Length** — счетчик показывает среднюю очередь заданий (операций записи или чтения) для соответствующего диска. Интерпретация этого параметра достаточно проста — если существует очередь на дисковые операции, то это означает, что диски не справляются с записью/чтением информации. Поскольку дисковая подсистема обычно является самым медленным компонентом, а этот счетчик отображает среднее значение, то уже само наличие очереди (значение счетчика, большее примерно 0,5) существенно замедляет скорость вычислений. Поэтому оптимально добиваться минимально возможных значений для этого счетчика.

- **% 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.

- **Определение источника дисковой активности** — в реальных системах часто причиной повышенной дисковой активности бывают не только полезные программы, но и те или иные сервисные процессы. Поэтому при оптимизации работы системы с дисками следует проанализировать процессы, инициирующие операции обмена с дисками, составить перечень файлов, работа с которыми ведется наиболее активно, и т. п.

Определить наиболее активные процессы и узнать, в какие файлы пишутся (читаются) данные, поможет программа **Монитор ресурсов**. Администратор может отсортировать процессы по желаемому типу активности, отфильтровать информацию и т. п. (рис. 11.35).

Для Linux-систем аналогичной функциональностью обладает, например, утилита iotop, позволяющая вывести на экран названия процессов с наибольшей дисковой активностью и отобразить соответствующие файлы.

Нелишне убедиться, что фактическая производительность дисковой подсистемы соответствует характеристикам оборудования. Диски различных вендоров отличаются по своим параметрам весьма незначительно. Так, для дисков с частотой вращения 7200 об/мин среднее время записи/чтения (без учета кеширования) составляет не более 15 мс. Оно должно быть соответственно меньше с учетом объединения дисков в RAID-массив.

Существует несколько утилит, предназначенных для проверки параметров скорости работы устройств хранения, но наиболее известным и практически профессиональным инструментом является Iometer[1] — пакет, первоначально разработанный Intel и впоследствии переданный сообществу Open Source.

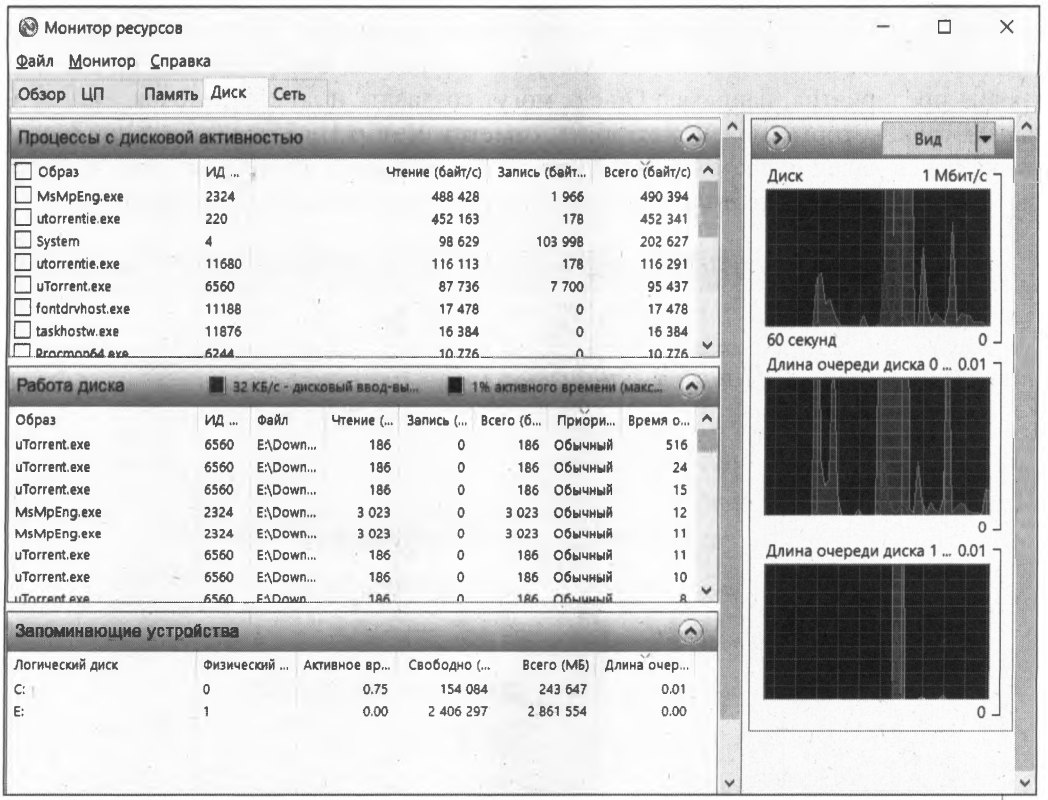


Рис. 11.35. Окно программы **Монитор ресурсов** с отфильтрованными данными дисковой активности

[1] См. **http://sourceforge.net/projects/iometer/files/**.

Программа позволяет замерить реальные параметры работы устройств хранения, однако для получения результата необходимо сначала внимательно ознакомиться с документацией (на что часто не хватает желания у системных администраторов). Причина в том, что в настройках программы необходимо указать большое количество параметров, влияющих на оценку производительности. Например, размер блоков хранения, процент операций записи/чтения и пр. Причем эти значения будут различны для отличающихся вариантов использования дисков: одни значения необходимо указать для проверки дисков, предназначенных для работы с базами данных, другие — для файловых серверов и т. п.

Комплект поставки включает два файла: Dinamo используется для управления тестированием на нескольких устройствах, iometer — файл, который следует запустить для проверки. После запуска надо импортировать файл конфигурации (как описано ранее), не забыть ограничить размер файла, который создается для тестирования в корне диска (заменить значение Maximum Disk Size на допустимое число секторов в файле теста, иначе файл будет создан на всем свободном пространстве диска), и выбрать на вкладке **Access Specifications** необходимые тесты. По умолчанию в программе создается такое число процессов тестирования (**Worker**), которое соответствует числу процессоров в системе. Но их количество можно изменить, как и сменить количество одновременных потоков ввода/вывода (**# of Outstanding IO**). Простые приложения обычно используют 1–4 потока ввода/вывода, приложения уровня предприятия, например Oracle, могут создавать и до 256 потоков. Из других параметров, которые можно настроить, отметим **Ramp Up Time** (время на разогрев диска перед началом теста) и **Run Time** — максимальное время тестирования (если вы хотите завершить тестирование по истечении заданного периода времени).

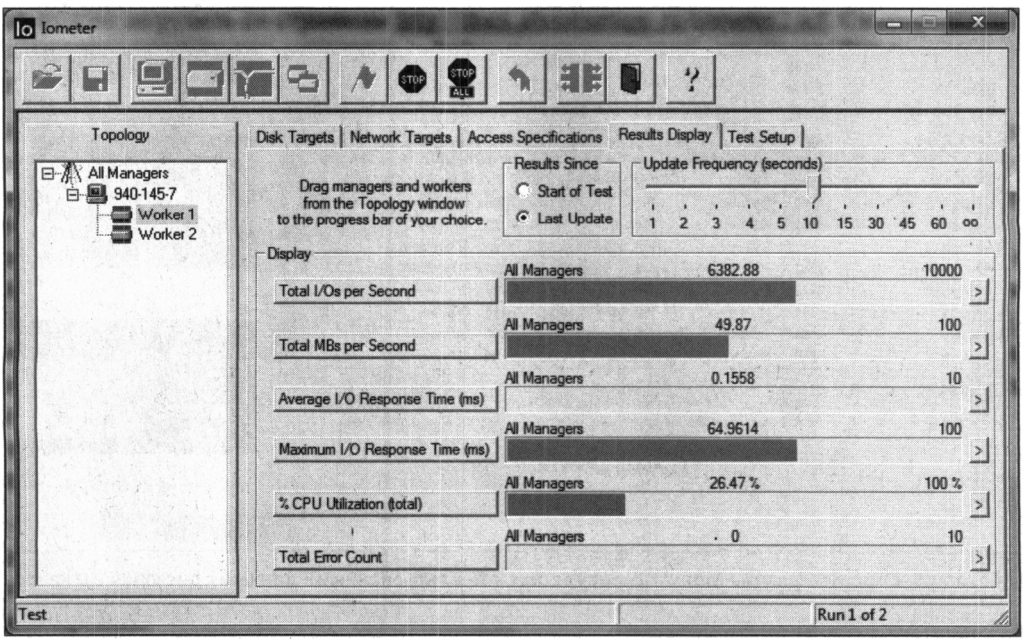


Рис. 11.36. Параметры диска, отображаемые утилитой iometer

После запуска теста на вкладке **Results Display** (рис. 11.36) можно наблюдать за получаемыми значениями (следует только назначить моменты обновления данных). Обратите внимание, что набор отображаемых на диаграмме параметров допускает изменения по желанию оператора. Итоговые значения тестирования будут сохранены в CSV-файле, который можно будет впоследствии проанализировать.

Пути оптимизации дисковой подсистемы

Какие могут быть варианты решения проблемы при обнаружении «узкого места» в дисковой подсистеме?

- Самый эффективный путь — добавление жестких дисков в соответствующий RAID-массив, на базе которого создан логический диск. Чем больше жестких дисков объединены в логический, тем более производительным он будет.
- Кроме того, если позволяет устройство хранения, выберите оптимальные для используемого типа данных варианты RAID-массивов. Не забывайте, что самый популярный тип массива — RAID5 — не является самым быстрым.
- Проанализируйте дисковую активность и отключите необязательные задачи, ведущие запись информации на диск (например, откажитесь от излишнего протоколирования, перенесите фоновые операции дефрагментирования на периоды минимальной активности и т. п.).
- Убедитесь, что в системе установлено достаточно оперативной памяти. Увеличьте ее при нехватке.
- 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. Для NTFS-дисков можно отключить запись имен файлов в формате 8.3 и запись времени последнего доступа к файлу (для чего в ветви реестра:

  `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Filesystem`

  надо установить в значение `1` параметры `NtfsDisable8dot3NameCreation` и `NtfsDisableLastAccess` соответственно).

Если эти операции не приведут к успеху, следует искать возможность приобрести более быструю дисковую подсистему.

> ***Совет***
>
> Если позволяют характеристики системы хранения, то можно выполнить точную настройку таких параметров, как размер кластера и т. п. Обычно подобные настройки необходимо выполнять *до* создания логического диска, поскольку изменение их можно провести только с уничтожением хранимой информации. Поэтому такие настройки необходимо тщательно планировать на этапе ввода системы хранения в эксплуатацию.

Оценка работы сетевого адаптера и пути оптимизации системы передачи данных

Для оценки работы сетевого адаптера используется тот же подход, что и для подсистемы ввода/вывода системы хранения: использование полосы пропускания

должно быть ниже предела скорости передачи и очереди на отправку пакетов не должно быть. Обычно считается допустимым среднее значение очереди, равное 1.

Что касается использования полосы пропускания, то для сети, выполненной по стандарту Ethernet, — а это практически все локальные компьютерные сети, — величина утилизации сети, равная 60%, уже считается критической. На практике следует внимательно проанализировать работу сети при достижении порога утилизации порядка 30–40%. Администраторы обычно используют для оценки состояния сети различные SNMP- и RMON-мониторы, которые имеют возможность автоматически высылать предупреждения при достижении установленных пороговых значений.

> ***Примечание***
>
> Счетчики отображают объемы передаваемой и принимаемой информации в *байтах*, тогда как скорость сети указывается в *битах* (100 Мбит/с, 1 Гбит/с и т. д.). Поэтому показания счетчика надо умножить на 8, чтобы сравнивать с максимально возможной скоростью передачи данных.

С помощью счетчиков также можно выяснить, какое приложение генерирует максимальный трафик. Хотя на практике это имеет несущественное значение — обычно администраторам это приложение известно.

Улучшить работу сетевого адаптера крайне сложно. Можно порекомендовать обновить его драйвер. Кроме того, иногда бывает, что параметры подключения, которые по умолчанию выставляются в режим **авто**, настроены не на максимальную производительность. Например, вместо полного дуплекса будет использован режим полудуплекса или даже установлена более низкая скорость работы. Выяснить такие отклонения можно, если посмотреть состояние сетевого порта коммутатора, к которому подключен тот или иной сетевой адаптер. Если состояние порта не оптимальное, то необходимо вручную сменить настройку и зафиксировать ее в требуемом значении.

Если настройки оптимальны и большой трафик свойствен нормальным условиям работы системы, то необходимо либо добавить еще один сетевой адаптер, либо перейти на сеть с большей скоростью передачи данных.

После установки дополнительного сетевого адаптера данные будут передаваться одновременно по нескольким каналам, в результате чего нагрузка на отдельный канал снизится (примерно пропорционально числу каналов) и будет находиться в приемлемых диапазонах. Такое объединение (*агрегирование*) сетевых адаптеров на серверной стороне канала передачи реализуется программным обеспечением сетевых адаптеров наиболее известных вендоров (например, ProSet для адаптеров изготовления фирмы Intel). Поэтому лучше всего при установке дополнительного адаптера выбирать модель, идентичную уже установленной в сервере. Соответствующие возможности нужно уточнить по документации.

> ***Примечание***
>
> 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 под-

твердение получения данных). Как правило, эти параметры автоматически настраиваются системой, и устанавливать их вручную имеет смысл только при большом числе сетевых подключений (при массовом обслуживании). Соответствующие настройки следует уточнить по описанию операционной системы.

Аналогично если не хватает полосы пропускания между двумя коммутаторами локальной сети, то следует создать вторую, параллельную линию связи и объединить их (агрегирование каналов средствами коммутационного оборудования). Для регулировки (чтобы минимизировать влияние сетевого трафика одних программ на другие) следует ввести настройки качества обслуживания (установить приоритеты трафика) и ограничения используемой полосы пропускания (так называемый shaping).

Некоторые советы по анализу показаний производительности

Чтобы снятие показаний счетчиков меньше сказывалось на загрузке проверяемой системы, лучше всего эту операцию делать удаленно — например, подключая задачу **Производительность** к удаленному серверу. Если вы хотите, чтобы работа самой программы при отображении данных вносила минимальные искажения в параметры производительности, то запускайте ее для Windows-систем с низким приоритетом:

```
start /low
```

Для объективной оценки производительности системы необходимо использовать усредненные за некоторый период показания счетчиков. Чем за больший период времени будут сняты показания, тем более объективные выводы оценки производительности системы можно будет выполнить. Например, кратковременная загрузка процессора, близкая к 100%, при выполнении расчета вполне допустима. Но если процессор загружен более 70% в течение длительного периода времени, то этот факт свидетельствует о необходимости расшивки такого «узкого места».

Как правило, программы мониторинга производительности имеют возможность записи показаний счетчиков в файл в реальном режиме времени. Администратору необходимо только задать периодичность снятия показаний и указать длительность записи. В качестве примера на рис. 11.37 приведен один из графиков отчетов, сформированных программой nmon (бесплатное ПО для мониторинга производительности *NIX-систем) реального компьютера. Часто такие отчеты снабжаются указаниями на параметры, значения которых зафиксированы в неоптимальных коридорах.

Кроме того, в период замеров следует выполнять обычные для того или иного 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.

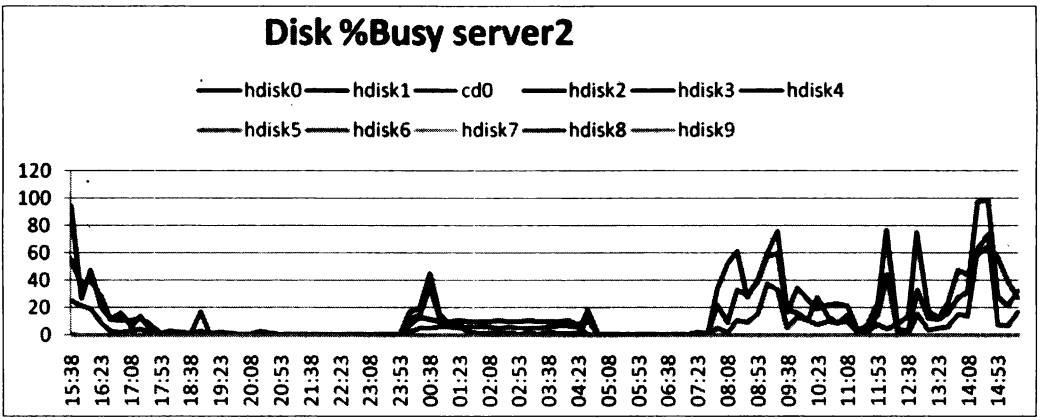


Рис. 11.37. Один из графиков отчета по данным мониторинга AIX-системы программой nmon

Оптимизация приложений

Пользователь может сказать, что компьютер работает медленно, что ему хотелось бы, чтобы расчеты выполнялись не более чем за некоторый, заранее определенный промежуток времени. Задача администратора — определить причины недостаточной производительности, понять, какой параметр вносит наибольшее замедление в работу информационной системы, и попытаться устранить проблему.

Еще раз отметим, что невозможно добиться ускорения вычислений сразу по всем параметрам. Следует выделить операции, наиболее существенно замедляющие работу, попытаться оптимизировать их и затем повторять эти шаги снова и снова, пока не будет достигнут требуемый эффект. Обязательно следует выбрать типовые операции, зафиксировать время их выполнения до начала оптимизации и контролировать эффект каждого шага.

Современные коммерческие приложения обычно имеют много «тонких» внутренних настроек, позволяющих оптимизировать вычисления под конкретную конфигурацию заказчика. Поэтому наряду с устранением узких мест аппаратной составляющей (так, как это описано ранее) следует ознакомиться с подобными руководствами по оптимизации и реализовать изложенные в них настройки.

Однако все эти меры не всегда могут уменьшить время обработки данных до приемлемых величин. Поэтому администратору обычно необходимо также разбираться и в том, как осуществляются расчеты в приложении. Часто наибольший эффект может дать изменение алгоритма расчетов. Например, расчет заработной платы для всего предприятия можно провести за меньшее время, если одновременно запустить несколько процессов — параллельно по нескольким подразделениям. А формирование отчета за длительный период можно ускорить, если предварительно сформировать отчеты за промежуточные периоды, и т. д.

Задача администратора в подобной ситуации — выяснить причины проблемы и подсказать возможные пути их разрешения.

Диагностика службы каталогов и обнаружение ее неисправностей

Следствием неисправностей функционирования службы каталогов (Active Directory, AD) неизбежно являются отказы информационной системы.

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.

Системному администратору следует предпринять 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, отмеченным 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, 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, необходимо использовать любую систему мониторинга реального времени.

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. В частности, это dcdiag, специально предназначенная для тестирования AD. Кроме того, для тестирования инфраструктуры можно воспользоваться утилитами, указанными в табл. 11.4.

Таблица 11.4. *Утилиты для тестирования инфраструктуры*

Утилита	Используется для
netdiag.exe	Проверки сетевой инфраструктуры
netdom.exe	Проверки и управления доверительными отношениями
nltest.exe	Проверки состояния secure channel
ntfrsutl.exe	Управления службой репликации файлов
dsastat.exe	Анализа состояний AD на различных контроллерах
repadmin.exe	Проверки репликации данных AD, возможности инициировать частичную или полную репликацию заданного контекста
replmon.exe	Контроля репликации данных и запуска 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	Используется для
ADSI Edit	Просмотра и редактирования объектов AD, установки списков доступа (Access Control Lists, ACLs)
ldp.exe	Взаимодействия с AD по протоколу LDAP

Для проверки сетевых соединений и их качества можно применять любые утилиты из состава операционной системы (см. *разд. «Диагностика IP-протокола» ранее в этой главе*). 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.

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. Необходимо 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 команды `nslookup`, выполнить попытку разрешения имен, приведенных в табл. 11.6. Для разрешения имен служб (записи типа SRV) в `nslookup` предварительно следует 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.

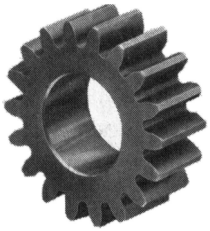
Обратите внимание и на весьма простую операцию, удачное выполнение которой зависит от правильности настройки системы разрешения имен и от функционирования контроллера домена, — попробуйте открыть следующий сетевой ресурс:

```
//<DNS_имя_домена>/SYSVOL
```

Если попытка неудачна, то либо на предприятии неверно настроено разрешение имен, либо контроллер домена неработоспособен.

Таблица 11.6. *Перечень имен, проверяемых в процессе теста*

Имя	Тип записи	Соответствует
_ldap._tcp.dc._msdcs.<*DNS_имя_домена*>	SRV	Контроллеру домена
_ldap._tcp.pdc._msdcs.<*DNS_имя_домена*>	SRV	Эмулятору первичного контроллера
_ldap._tcp.gc._msdcs.<*DNS_имя_леса*>	SRV	Серверу глобального каталога
_kerberos._tcp.dc._msdcs.<*DNS_имя_домена*>	SRV	Расположению службы KDC



ГЛАВА 12

Плановые задачи обслуживания

К сожалению, в обязанности администратора помимо творческого решения возникающих проблем входит и выполнение довольно-таки рутинной работы. О ней мы и поговорим в этой главе. В чем она заключается? А в том, что периодически администратору приходится выполнять ряд плановых операций. Какие именно? Все зависит от специфики предприятия. И мы здесь попытаемся сформировать некий набор мероприятий, который вы можете взять за основу при разработке собственного плана обслуживания.

Конечно, вам придется внести существенные коррективы в этот набор, но у вас хотя бы будет, от чего отталкиваться.

Ежедневные задачи

Основная ежедневная задача — это мониторинг, контроль текущего состояния информационной системы. Задача мониторинга состоит из серии операций, которые вам предстоит выполнять каждый день.

- **Оценка показаний датчиков аппаратного контроля** — нет ничего хуже жесткого диска, который вышел из строя, а если еще учесть, что он предупреждал за месяц до этого... Современное оборудование позволяет контролировать температурный режим, скорость вращения вентиляторов, параметры электропитания и даже предсказывать скорый выход из строя жестких дисков на основе технологии S.M.A.R.T. (Self-Monitoring, Analysis and Reporting technology).
- **Проверка результатов выполнения резервного копирования** — практически все утилиты резервного копирования предоставляют отчет о выполнении резервного копирования. Мало просто настроить резервное копирование по определенному сценарию и забыть о нем — нужно ежедневно проверять, создалась ли резервная копия? Мог выйти из строя жесткий диск сетевого хранилища, используемого для резервного копирования. Во время резервного копирования могло произойти отключение электричества, обрыв сетевого соединения... В результате резервная копия не была создана, а вы об этом узнаете только тогда, когда она понадобится.

- **Проверка журналов серверов** — администратору нужно регулярно проверять журналы работы серверов (особенно если у вас их несколько), обращая особое внимание на журналы безопасности и ошибок. В них можно найти много интересного — например, сведения о неудачных попытках входа в систему. Если таких попыток одна-две, пользователь просто ошибся с паролем, а вот если их много, то, возможно, кто-то пытался подобрать пароль.
- **Проверка свободного пространства на носителях** — правильнее всего настроить автоматический мониторинг дискового пространства. Типичный пример: на сетевом хранилище осталось 5 Гбайт свободного пространства. Вы еще не получили сообщения о том, что свободное пространство закончилось, но если вы знаете, что резервная копия, которая будет создана вечером, занимает, скажем, 7 Гбайт, то не стоит дожидаться того самого сообщения — нужно принять меры по ликвидации дефицита дискового пространства. Меры могут быть самыми разными: от удаления неактуальной информации до приобретения еще одного жесткого диска.
- **Проверка функционирования основных служб** — следует регулярно проверять работоспособность основных служб системы: соединения с Интернетом, службы каталогов, службы электронной почты и пр.
- **Проверка обновлений программного обеспечения** — возможно, вышли обновления используемого ПО. Администратору нужно ознакомиться с сутью каждого обновления, а не слепо устанавливать все полученные обновления.
- **Проверка антивирусных баз** — обычно антивирусные базы обновляются автоматически. Но администратор должен убедиться, что обновление произошло.
- **Оценка внешних факторов** — администратор должен контролировать температуру вокруг серверов, проверять отсутствие внешних признаков вскрытия корпусов серверов и АРМ[1].

Еженедельные задачи

Некоторые задачи администратору нужно выполнять каждую неделю или каждые две недели — все зависит от специфики предприятия.

- **Проверка системы охлаждения серверов** — система охлаждения серверов имеет свойство забиваться пылью, и ее надо периодически чистить, но раз в неделю нужно хотя бы внешне оценивать необходимость такой чистки. Следует также контролировать состояние вентиляторов — иногда они выходят из строя. Если вентиляторы гудят, замените их. Если замена по тем или иным причинам,

[1] АРМ (автоматизированное рабочее место) — индивидуальный комплекс технических и программных средств, предназначенный для автоматизации профессионального труда специалиста и обеспечивающий подготовку, редактирование, поиск и выдачу на экран и печать необходимых ему документов и данных. Автоматизированное рабочее место обеспечивает оператора всеми средствами, необходимыми для выполнения определенных функций.

в том числе финансовым, невозможна, смажьте подшипники гудящих вентиляторов.

- **Проверка системы кондиционирования** — серьезные серверные комнаты оснащаются системами кондиционирования и фильтрации воздуха. Хотя бы раз в две недели нужно оценивать состояние фильтров системы кондиционирования и при необходимости производить их чистку или замену.
- **Проверка производительности серверов** — необходимо производить проверку производительности серверов и анализировать изменения в ней по сравнению с прошлыми периодами. Если производительность понизилась, следует принять меры по поддержанию привычного уровня обслуживания пользователей.
- **Формирование отчета** — в конце каждой недели администратору желательно составлять отчет о проделанной работе. Это дисциплинирует самого администратора и позволяет держать руководителя предприятия в курсе всего происходящего в информационной системе.

Прочие плановые операции

Некоторые операции администратору нужно производить относительно редко, но о них не стоит забывать. Следующие операции можно выполнять раз в квартал.

- **Очистка оборудования от пыли** — в предыдущем разделе речь шла о контроле состояния системы охлаждения серверов и фильтрующих элементов системы кондиционирования. Но не надо забывать, что кроме серверов у вас есть еще и парк прочей компьютерной техники. Понятно, что парк этот весьма объемный, и раз в неделю проверить состояние системы охлаждения каждого рабочего места не получится. Следовательно, такую проверку нужно производить раз в квартал и при необходимости чистить систему охлаждения. Эту процедуру требуется производить с выключением питания компьютера, поэтому следует заранее ее планировать и предупреждать о ее проведении сотрудников предприятия. Почему проверку системы охлаждения серверов нужно производить раз в неделю (или раз в две недели), а обычных рабочих станций — раз в квартал? Обычная рабочая станция, как правило, никогда не работает на полную мощность, и небольшое загрязнение охлаждающей системы никак не повлияет на ее работу. С сервером все гораздо сложнее — обычно к нему обращаются все компьютеры предприятия, поэтому он весьма часто бывает загружен на все 100%. Отсюда повышенное тепловыделение от процессора и жестких дисков, и в результате перегрева компьютер может просто выключиться. И если выключение одного компьютера и потерю несохраненных данных его пользователя (впрочем, смотря какого пользователя) еще пережить можно, то о выключении сервера с потерей данных всех пользователей и подумать страшно.
- **Удаление старых объектов службы каталогов** — состав объектов в службе каталогов часто не соответствует реальному положению дел. Поэтому периодически нужно удалять из AD старые записи — например, учетные записи уволенных сотрудников, замененных компьютеров и т. п.

- **Учебное восстановление системы** следует производить ежеквартально — администратор должен в случае сбоя оперативно восстановить работу системы. Именно для этого и нужны периодические тренировки. Администратор должен знать, как произвести замену вышедшего из строя накопителя в составе RAID, как восстановить работу сети, как в случае необходимости восстановить всю «упавшую» систему. Если у вас нет сервера для экспериментов, тренируйтесь в виртуальных машинах.
- **Планирование развития** — администратор должен оценивать текущее положение дел информационной системы. Возможно, пора модернизировать сервер или рабочие станции, заменить некоторые компьютеры на новые, приобрести дополнительные жесткие диски. Все это следует производить планово — вряд ли руководителю понравится, если администратор вдруг заявит: «Нам нужен новый сервер», хотя вчера еще и старый всех устраивал. Поэтому нужно составлять план развития на следующий квартал, в котором предусматривать необходимость покупки/модернизации оборудования. В план развития также надо включать и прочие расходы, связанные с выполнением обязанностей ИТ-отдела: оплату услуг хостинга и регистрации доменного имени, стоимость обновления программного обеспечения или продления лицензий. Руководитель предприятия или финансовый директор должен знать, что, например, в следующем месяце нужно будет оплатить услуги хостинга, а через два месяца истечет срок лицензии антивируса.
- **Актуализация организационно-распорядительной документации** — раз в год нужно актуализировать схемы сетей, помещений и пересматривать руководящие документы, касающиеся работы ИТ-отдела (например, должностные инструкции его сотрудников, политику безопасности и резервного копирования и т. п.).
- **Периодическая проверка серверов инструментами анализа безопасности** — существует ряд инструментов для анализа безопасности Windows Server (например, Microsoft Baseline Security Analyzer (MBSA), Microsoft Windows Server Best Practice Analyzer и др.). В процессе эксплуатации сервера, ясное дело, в его конфигурацию вносятся изменения. Не всегда внесенные изменения являются безопасными. С помощью подобного рода инструментов можно заблаговременно определить слабые места вашего сервера, пока это не сделал кто-то другой. Если нет прямых предпосылок (например, обнаружен несанкционированный доступ или его попытка), такую проверку необходимо проводить раз в квартал.

Предметный указатель

7

7Zip 51

8

802.1x 441
802.3ad 509

A

Access control list (ACL) 111
Account Lockout and Management Tools 173, 174
Active Directory (AD) 19, 22, 36, 153, 589
◊ восстановление данных 169
ADSL-модем 90, 143
APIPA 112
ARP 114
Avast! 52

B

Babiloo 52
bash-сценарий 218
BitLocker 477
◊ включение без TPM 478
◊ режим восстановления 479
Bitvise SSH Client 237
Boot threshold 127
Bridge Protocol Data Units (BPDU) 507
Browser Helper Object (BHO) 463

C

Callback 235
Clonezilla 290
Clonezilla Server Edition 297
Collabtive 52
Common Information Model (CIM) 278
COMODO Internet Security 52

D

DEB-пакеты 64
Default gateway 107
Demilitarized zone (DMZ) 205
Destination NAT 213
DFS (Linux) 518
DHCP 111
◊ отказоустойчивая конфигурация 512
◊ порядок получения IP-адреса 127
◊ фиксированные IP-адреса 123
DHCP Relay Agent 126
DHCP-сервер 111, 114, 118, 120–128, 143, 203, 511, 512
DirectAccess 241
Distinguished Name (DN) 156
Distributed File System (DFS) 515
DLP-система 24, 492
DNS split 136
DNS-имя 115
DNS-сервер 511
Domain Name System (DNS) 129, 155
◊ зона 130
◊ отказоустойчивая конфигурация 511
◊ сервер 118
dotProject 52
Dynamic Host Configuration Protocol (DHCP) 104

E

Easy Recovery 553
ERD Commander 434
ERP-система 45

F

Firewall 205
Flexible Single Master Operation role (FSMO) 522
FQDN (полное имя узла) 116
FreeCommander 51
Fully qualified domain name (полное имя узла) 116

G

Gateway 106
GetDataBack 553
Global catalog (GC) 524
GoldenDict 52

H

HAL (hardware abstraction layer) 286
Hop-count threshold 127
hot fix 450
Hyena 284

I

Ideal Administrator 284
IDS 439
ImageBurn 51
Integrated Script Environment (ISE) 281
Internet Information Server (IIS) 189
Intrusion Detection Systems (IDS) 208, 439
Intrusion Prevention Systems (IPS) 208, 440
IoMeter 583
iostat 580
iotop 583
IP-порт 113
IP Multicast Addressing 103
iptables 214
IPv4-forwardin 214
IPv6 (Internet Protocol version 6) 196, 198
IP-адрес 103, 195
IP-протокол
◊ диагностика 541
◊ проверка доступности портов 546

L

late collision 548
LDAP Interchange Format (LDIF) 167
LDIF-файл 167
Lightweight Directory Access Protocol (LDAP) 164
◊ escape-последовательности 166
◊ синтаксис запросов 165
Link Aggregation Control Protocol (LASP) 510
Linux Live 290
LiveUSB 290
Local System 172

M

MAC-адрес 114, 440, 441, 457
◊ программная смена 440
◊ устройства 98
Management Information Base (MIB) 313
MIB-файл 313
MSTP 508
Multi Router Traffic Grapher 548
Multi Spanning Tree Protocol 508
MySQL-клиент 340
MySQL-сервер 339

N

NanoCAD 51
NAT 199
NetBIOS-имя 115
Network Access Protection (NAP) 447
nobody 39, *См.* Гость
NRPE 328
NSClient++ 324

O

Offline NT Password Editor 434
OID 312
OpenLDAP 36
OpenSSH-сервер 238
Oracle RAC 512
Organization Unit (OU) 155

P

PackageForTheWeb-дистрибутивы (PFTW) 301
Performance Monitor 578
Power over Ethernet 79
PowerShell 281
◊ Integrated Script Environment 281
◊ Script Repository 276
◊ центр технологий 276
Provider 278
Public Key Infrastructure (PKI) 98
Рагрузчик GRUB2 67

R

Radius
◊ клиент 445
◊ ключ 445
RADIUS-сервер 444
RAID-массивы 585
Rainbow-таблица 433
RAS 235
RAW-диски 362
Read-only DNS (RODNS) 162
Read-Only Domain Controller 240
Relative Distinguished Names (RDN) 156
Relative ID (RID) 172
Repackages 301
Resource records 133
RJ-45, расшивка разъема 76
RODC 162, *См.* Read-Only Domain Controller
rootkit 457
Routing and Remote Access Server (RRAS) 126
Routing table 107
RPM-пакеты 64
rsyslogd 533

S

S/MIME 480
Script Center 276
Security Configuration Manager (SCM) 449
Service pack 450
SFP-модули для подключения оптического канала 74, 75
SID 172
SNMP Nagios 328
SOHO-сети 143
Source NAT 214
Squid SSL bump 234
ssh-клиент 237
ssh-сервер 237, 238
Stub-зона 132
Sysinternals 282
syslog 317
syslogd 533
syslog-ng 534
sysprep 287

T

TCP, стек протоколов 101
telnet 546
telnet-клиент 236
Traffic shaping 89

U

UNIX-подобные операционные системы 21, 52
UPS 35

V

VDI 369
Virtual Machine Manager (VMM) 356
Virtual Private Network (VPN) 235
Virtual Routing Reduntance Protocol 509
VLAN, автоматическая настройка клиентов 445
VPN-маршрутизатор 239
VPN-подключения 209
VPN-сервер 239
VRRP 509

W

Web-based Enterprise Management (WBEM) 278
Windows Server 2022 36
Windows Software Update Services (WSUS) 455
Wireless Access Point (AP) 93
WMI Query Language (WQL) 279
WMI-фильтр 267

X, Z

X-терминалы 236
ZoneAlarm 52

А

Автоматизированное управление кабельной инфраструктурой 257
Авторизация DHCP-сервера в Active Directory 121
Агент
◊ мониторинга
▫ NC_NET 324
▫ NSClient++ 324–328
▫ OpMonAgent 324
◊ резервного копирования 365
◊ ретрансляции DHCP 126
Агрегированные каналы 509
Адаптер
◊ Wi-Fi 69, 90, 204
◊ Wi-Fi Intellinet Wireless 150N 90, 91
Административная установка 303
Администратор терминального сервера 247
Адрес
◊ динамический 104
◊ обратной петли 197
◊ самостоятельное назначение 112
◊ сервера DNS 118
Адреса
◊ Anycast 198
◊ Multicast 199
◊ Unicast 198
Алгоритм
◊ 3DES 237
◊ BlowFish 237
◊ IDEA 237
◊ RSA 237
◊ Strict Priority Queuing (SPQ) 89
◊ Weighted Round Robin (WRR) 89
Анализатор протоколов loganalyzer 330
Антивирусная защита служб 461
Аппаратный брандмауэр 209
Аппаратный маршрутизатор Wi-Fi 143
Аппаратный шлюз 106
Атрибут 165
Аудитор 151
Аутентификация 320
◊ на основе смарт-карты 432

Б

Безопасность
◊ беспроводной сети 71, 97
◊ клиента 98
◊ паролей 430
Белый список MAC-адресов 225
Бесплатное программное обеспечение 21
Бесплатные офисные пакеты 46
◊ Apache OpenOffice 47
◊ LibreOffice 47, 51
Бесплатные почтовые системы 48
Бесплатные программные продукты 206

Бесплатные программы для Windows 51, 52
Беспроводные сети 69, 90
Билет Kerberos 37
Брандмауэр 113, 203–206, 208, 209, 211–214, 216, 428, 438
◊ iptables 106, 204, 206, 208, 211–219, 221, 222, 227, 228
◊ UFW 222
◊ Windows 98, 206, 209
Браузер
◊ Firefox 42, 51
◊ Google Chrome 42, 48, 51
◊ Internet Explorer 42
◊ Microsoft Edge 42
◊ Opera 42
Быстрая переустановка Windows 10 569

В

Веб-доступ к терминальному серверу 250
Веб-сервер Apache 233, 318, 339
Версионность документов 571
Виртуализация 504
Виртуальная локальная сеть (VLAN) 351, 379–382, 384, 385
Виртуальная машина 351, 357, 359, 368, 369, 372, 393
◊ KVM (Kernel Virtual Machine) 353, 373
◊ Microsoft Hyper-V 353
◊ OpenVZ 353, 373
◊ Oracle VirtualBox 67, 353, 354
◊ VirtualBox 65, 352, 360
◊ VMware 107, 353, 358, 360, 525
◊ VMware vSphere 353
◊ VMware Workstation 67, 352, 354, 359
◊ Xen 352
Виртуальная частная сеть 395
Виртуальное ядро (vCPU) 393
Виртуальный жесткий диск 360–363, 367
Виртуальный сервер 351, 387–389, 397, 398, 404, 405
Виртуальный сетевой адаптер 357
Вирус
◊ лечение 460
◊ троянский конь 462
◊ червь 208
Включение
◊ защиты имен 129
◊ компьютера в домен 145
Владелец объекта 179
Волоконно-оптические кабели 74
Волоконно-оптические линии связи 74
Восстановление
◊ доступа к ресурсам 179
◊ загрузки Linux-систем 565
◊ загрузки Windows 10 562
◊ загрузки Windows 8 557
◊ загрузчика 557
◊ из резервной копии 556
◊ параметров безопасности 185
◊ пароля root 435
Восстановление данных
◊ корзины 570
◊ теневые копии 570
◊ из резервной копии 577
Встроенные учетные записи 187
Вторичная зона DNS 130
Вторичный DNS-сервер 511
Выбор
◊ аппаратных и программных средств 25
◊ материнской платы 31
◊ оперативной памяти 33
Выделенный кеш 252

Г

Гарантийный срок 27
Гипервизор 352–355, 357, 358, 362, 365
◊ ESX 363
◊ Hyper-V 353, 358, 378
◊ Hyper-V 2016 354
◊ VMware ESXi vSphere 358
◊ VMware ESXi vSphere 6.5 354
◊ Xen 352
◊ XenServer 353
Гость 39, *См.* nobody
Графическая среда
◊ GNOME 58
◊ KDE 58
Графический режим Linux 58
Группа пользователей
◊ DHCP Administrators 191
◊ DHCP Users 191
◊ HeplSevicesGroup 191
◊ Network Configuration Operators 191
◊ Print Operators 191
◊ Remote Desktop Users 191
◊ WINS Users 191
◊ Администраторы (Administrators) 190
◊ Все (Everyone) 191
◊ Гости (Guests) 191
◊ Операторы резервного копирования (Backup Operators) 190
◊ Опытные пользователи (Power Users) 190
◊ Пользователи (Users) 190
◊ специальная 191
Групповая рассылка 103, 104
Групповые политики 86, 150, 152, 157, 227, 241, 258–260, 262, 266, 432, 444, 446, 450, 455, 456, 462, 463, 467, 478
Группы
◊ безопасности 174
◊ встроенные локальные 175
◊ глобальные 175

◊ локальные, домена 175
◊ пользователей 174, 175
  ▫ ролевое управление 176
◊ рассылки 175
◊ универсальные 175

Д

Дата-центр (ДЦ) 386, 389, 404, 504–506
◊ надежность сетевой инфраструктуры 506
◊ системы газового пожаротушения 506
Двойное выключение виртуальной машины 369
Дедупликация 46
Делегирование прав 168
Демилитаризованная зона 205
Демон
◊ rsyslogd 331, 333, 335
◊ syslogd 317, 331, 335
◊ протоколирования 533
  ▫ rsyslogd 534
  ▫ syslogd 533
Дерево 155
◊ идентификаторов 312
Динамические IP-адреса 195
Динамический жесткий диск 362
Диспетчер серверов 158, 161, 162, 201, 249, 250, 406
Дистрибутив Astra Linux 67
Дистрибутивы Linux 55
Домен 154
◊ вложенный 155
◊ второго уровня 116
◊ имя 116
◊ первого уровня 116
Домен Windows 154
◊ право добавления рабочих станций 146
◊ удаление устаревших записей 148
Доменные службы Active Directory 158, 160, 162

Ж

Журнал
◊ syslog 531
◊ событий
  ▫ назначение задания 538
  ▫ настройка аудита безопасности 538
◊ транзакций 514

З

Загрузка системы: специальные режимы 566
Загрузочный диск Dr.Web LiveDisk 461
Закрытый ключ
◊ получателя 481
◊ пользователя 475
Занятие имен 129
Запись ресурса 133
Заплатка 450
Запрос 279
Защита имен 129
Зеркалирование базы данных 513

И

Идентификатор безопасности (SID) 172
Изменение MAC-адреса
◊ в Linux 114
◊ в Windows 114
Инженерные пароли 468
Интегрированная среда сценариев ISE 281
Интегрированный продукт
◊ Avast Premium Security 206
◊ Comodo Internet Security 206
◊ ESET NOD32 Smart Security 206
◊ Kaspersky Internet Security 206
◊ Outpost Security Suite 206
◊ Symantec Endpoint Protection 206
Интернет
◊ блокировка рекламы 230
◊ оптимизация доступа 224
◊ регурировка полосы пропускания 228
Интерпретатор wmic (WMI Command-line tool) 279
Интерфейс
◊ PATA (ATA/IDE/EIDE) 33
◊ Windows Management Interface (WMI) 278
Интерференция сигналов Wi-Fi 69
Исключение компьютера из домена 149
Использование групповых политик 152
Источники бесперебойного питания 528
Итеративный запрос 132

К

Кабели
◊ витой пары 73
◊ оптические
  ▫ многомодовые 74
  ▫ одномодовые 74
Калькулятор эффективности Oracle Desktop Virtualization TCO Calculator 370
Каталог 153
◊ Active Directory 521
◊ OpenLDAP 521
◊ признак каталога 56
◊ схема 153
Качество
◊ каналов связи 547
◊ обслуживания классов пакетов 85–87
Кворумный диск 519
Кеширующий прокси-сервер 225
Класс обслуживания пакетов 85
Классификация трафика 88
Классы сетей 196
Кластер 519
◊ Oracle RAC 512

Кластерные решения 519
Клиент Kerberos 36
Клонирование
◊ виртуальной машины 359
◊ рабочих станций 285
Ключевая пара 482
Колокация 389
Команда
◊ arp 114
◊ chmod 56
◊ dcdiag 590, 591
◊ dnsdiag 140
◊ dsquery 523
◊ gpupdate 261
◊ ifconfig 541
◊ ipconfig 112
◊ ldifde 167
◊ MSTSC 247
◊ netdom 146
◊ netsh 191
◊ netstat 107, 113
◊ nslookup 136, 138, 591
◊ ntdsutil 523
◊ pathping 549
◊ ping 114, 544
◊ portqry 546
◊ route 107
◊ SHADOW 247
◊ ssh 237
◊ su 63
◊ sudo 63
◊ tail 541
◊ tcpdump 545
◊ tracepath 544
◊ traceroute 544
◊ tracert 110
◊ winipcfg 112
Командлет 281
Командный интерпретатор 257, 276
◊ WMIC 257
Коммутатор управляемый 255
Коммутаторы D-Link 384
Коммутационное оборудование 34
Комплект средств развертывания Windows ADK 285
Компонент AppLocker 269, 270
Коннекторы RJ-45 76
Консоли управления AD 590
Консоль
◊ редактирования групповой политики 262
◊ сервера 246
Контроллер домена 154
◊ «только для чтения» 162, 240
Конфигуратор pppoeconf 543
Концентратор 80
Копирование учетной записи 184
Корзина 570
◊ Active Directory 161, 169
Коррекция ошибок (ECC) 33
Криптографический токен 432, 433

Л

Лес 156
Лицензия
◊ ФСБ 404
◊ ФСТЭК 404
Локальные групповые политики 259
Локальные группы 174

М

Маркированные порты 381
Маркированный трафик 381
Маркировка
◊ (tagging) кадров 380
◊ пакетов 88
Маршрутизатор
◊ Cisco 25
◊ D-Link 25
◊ TP-Link 25
◊ TP-LINK Archer AX1500 26
◊ TP-LINK TL-WR740N 71
◊ Wi-Fi 25, 69, 90, 92, 93, 106, 143, 199, 203, 206, 226
▫ Cisco 819 92
◊ ZyXEL 25
Маска
◊ адреса 105
◊ сети 196
Мастер
◊ делегирования управления 169
◊ настройки доменных служб Active Directory 158
Межсетевой экран (МСЭ, брандмауэр) 204, 205, 438
Метод авторитетного восстановления 170
Механизм распределенных информационных баз 513
Миграция виртуальных машин 367
Многовариантная загрузка 67
Многомодовые оптические волокна 74
Множественные групповые политики 259
Модель
◊ OSI 100
◊ угроз 425
Модуль
◊ CheckWMI.dll 327
◊ TPM 477–479
Мониторинг
◊ информационной системы 309
◊ сети 318
◊ трафика 337, 339
Монтирование файловой системы Linux 57

Н

Набор утилит Ideal Administrator 284
Назначение прав доступа 182
Наследуемые разрешения 178
Настройка
◊ NAT 199
◊ SOHO-сетей 144
◊ VPN-сервера 236
◊ брандмауэра 195
◊ групповой политики брандмауэра Windows 209
Начальные объекты групповой политики (GPO) 265
Немаркированные порты 381

О

Обеспечение безопасности информации 425
«Облачный» ЦОД 504
Обратное разрешение имени 130
Обход перекрестной проверки 180
Оверселлинг 373
Ограничение полосы пропускания 89
Ограничения доступа к станциям 437
Одномодовые оптические волокна 74
Однопользовательский режим Linux 566
Операции
◊ копирования 180, 181
◊ перемещения 181
Операционные системы 20
Оптимизация настроек 577
Организационное подразделение 155
Организация виртуальных частных сетей (VPN) 195
ОС
◊ *ALT Linux* 21
◊ Android 39
◊ Astra Linux 21
◊ Astra Linux Special Edition 21
◊ CentOS 21
◊ Debian Linux 21
◊ FreeBSD 20, 21, 63, 236
◊ Linux 20, 21, 53, 106, 239
◊ macOS 20, 22
◊ openSUSE 21
◊ SLED (SUSE Linux Enterprise Desktop) 21
◊ SUSE Linux 21
◊ Ubuntu Linux 21
◊ UNIX 59
◊ Windows 20–22
  ▫ Windows 10 22, 42
  ▫ Windows 11 22
  ▫ Windows 7 23
Оснастка
◊ Анализ и настройка безопасности 185
◊ Локальная политика безопасности 184
◊ Управление групповой политикой 263
◊ Управление компьютером 151
◊ управления AD 146, 174
Основной DNS-сервер 511
Основной файл конфигурации демона syslogd 534
Отказ в обслуживании 539
Отказоустойчивость DHCP-сервера 125
Отказоустойчивый пул DHCP-серверов 512
Открытый ключ получателя 481, 484
Офисный пакет MS Office 2021 47
Очередь приоритизации 88
Очистка кеша 131

П

Пакет 64
◊ memtest86+ 553, 554
◊ openssh 237
◊ openssh-clients 237
◊ Samba 40
◊ администрирования Hyena 284
Панель управления
◊ VestaCP 394, 398, 399, 402
◊ Xelent Cloud 387, 404
◊ виртуальным сервером 398
Параметр IOPS 32
Параметры политик 262
Пароль доступа к Wi-Fi 144
Патч openMosix 519
Патч-корд 78
Первичная зона DNS 130, 138
Переименование домена AD 164
Перекрестная обжимка кабеля (crossover) 77
Перемаркировка трафика 88
Переупаковка 301
Перехват управления клавиатурой и мышью 274
Песочница (Windows Sandbox) 421
Плагин NRPE 328
План обеспечения непрерывности функционирования информационной системы 430
Планировщик заданий 315
Подключение волоконно-оптических линий 74
Подмена MAC-адреса 339
Подписка на события 316, 537
Подсеть 105
Показатели производительности 579
Поле ToS 86
Политика
◊ Kerberos 186
◊ административный шаблон 272
◊ безопасности 539
◊ восстановление значений по умолчанию 264
◊ групповая 152, 155, 258, 439
◊ локальная групповая 259
◊ обход параметров пользователя 266
◊ по установке программного обеспечения 270
◊ Предпочтения групповых политик 267
◊ фильтрация 266
Политики
◊ компьютера 261
◊ пользователя 261, 266

Пользователь root 55, 58
Порог ожидания 127
Порт 113
◊ well-known 113
◊ сканирование 114
Постоянные (статические) IP-адреса 195
Построение отказоустойчивой сети 507
Почта Gmail 48
Почтовые протоколы 51
Почтовый клиент Microsoft Outlook 48
Почтовый сервер
Lotus 48
Microsoft Exchange Server 48
◊ MS Exchange 140
◊ клиенты Lotus 48
Права доступа 146, 150, 164, 169, 171, 174, 177, 178, 181
◊ в Linux 55
Права учетной записи 184
Правила
◊ изменения атрибутов 180
◊ приоритизации 88
Практические WMI-сценарии 280
Предопределенные учетные записи 187
Предотвращение утечек (DLP) 492
Приложение phpMyAdmin 330
Приобретение доменного имени 116
Провайдер 278
Проверка памяти 553
Программа
◊ «10-Страйк: Схема Сети» 255
◊ Ad-aware 462
◊ Advanced EFS Data Recovery 430, 476, 477
◊ AdwCleaner 461
◊ AIDA64 344, 346
◊ BitDisk 467
◊ Cain & Abel 433
◊ Crypto Plugin 484, 487
◊ Crystal DiskInfo 344, 345, 552
◊ CyberSafe Top Secret 471, 472, 482–484
◊ DeviceLock 438, 439
◊ Dr.Web CureIt 461
◊ ERD Commander 434
◊ Executive Undelete 570
◊ Filemon 282
◊ GetDataBack 553
◊ Hidden Administrator 275
◊ LAN Flow 255
◊ loganalyzer 330
◊ MailDroid 484, 485, 487, 489
◊ Multi Router Traffic Grapher 548
◊ nmap 114
◊ nmon 587, 588
◊ Norton Protected Recycle Bin 570
◊ NTFS Data Recovery Toolkit 553
◊ Observer 548
◊ Offline NT Password Editor 434
◊ Ontrack Data Recovery 553
◊ OpenVAS 451
◊ Panda 460
◊ PGP Desktop 482
◊ Process Monitor 282
◊ Regmon 282
◊ Remote Administrator (RAdmin) 275
◊ RkHunter 451
◊ robocopy.exe 190
◊ RootkitRevealer 465
◊ Security Configuration Manager (SCM) 449
◊ Server Performance Advisor 579
◊ Symantec Endpoint Protection 43, 447, 457, 458, 467
◊ Symantec EndPoint Protection 439
◊ Symantec Endpoint Protection Manager 457, 458
◊ Symantec NetBackup 520
◊ Symantec Security Check 460
◊ TeamViewer 274, 275
◊ telnet 546
◊ Traffic Control 87
◊ Trend Micro 460
◊ TrueCrypt 468–470, 477
◊ UltraViewer 43
◊ VeraCrypt 468
◊ Virtual Network Computing (VNC) 275
◊ WBEMTest.exe 279
◊ Wifi Analyzer 94
◊ WinImage 360
◊ Производительность 578
◊ Редактирование ADSI 164
◊ тихая установка 297
◊ файл трансформации 298
Программный брандмауэр 208
Программный шлюз 106, 143
Программы
◊ опубликованные 271
◊ управления удаленным компьютером 274, 275
Продление аренды IP-адреса 127
Продукты просмотра WMI 278
Проект Samba 39
Прозрачное шифрование данных 491
Прокси-сервер 201, 207, 225–228
◊ прозрачный 227
Прокси-сервер Squid 228, 230
Пространство имен 155
Протокол
◊ 802.1x 441–447
◊ Address Resolution Protocol (ARP) 114
◊ DiffServ 86, 87
◊ Internet Control Message Protocol (ICMP) 102
◊ IPv6 102
◊ Kerberos 36, 40
◊ LACP 510

◊ LDAP 164
◊ MSTP 508
◊ NetBEUI 99
◊ NetBIOS Frame Protocol (NBFP) 99
◊ NRPE 326, 328
◊ NSClient 326
◊ NWLink IPX/SPX 99
◊ RSTP 507, 508
◊ Simple Network Management Protocol (SNMP) 312
◊ SMB 38
◊ SNMP 34, 278, 309, 310, 312, 328, 549
◊ SSH 236
◊ SSL (Secure Socket Layer) 233
◊ STP 507, 508
◊ TCP/IP 100, 118
◊ Telnet 236
◊ Transmission Control Protocol (TCP) 102
◊ User Datagram Protocol (UDP) 102
◊ VRRP 508, 509
◊ Wi-Fi 69
◊ отказа 527
◊ сетевой 99
Процессоры
◊ AMD 28
◊ Core i7/i9 29
◊ Intel 28
◊ Intel Core i9 28
◊ Intel Xeon 28, 29
◊ Intel Xeon E5 2697v 28
◊ Intel Xeon Phi 3120A 28
◊ Intel Xeon W-3275 29
◊ Intel Xeon W-3365 28
◊ Intel Xeon W-3375 28
◊ Intel Xeon X-3275 28
Прямое разрешение имени 130
Пул задержек 228

P

Развертывание
◊ программы 303
◊ сети Wi-Fi 69
Разделение
◊ DNS 136
◊ клиентов по классам 124
Разностный жесткий диск 362
Разрешение имен 119
Разрешения
◊ безопасности 177, 178
◊ общего доступа 177
◊ явно установленные 178
Распределенная файловая система (DFS) 515, 518
Распределенный кеш 252, 253
Расширения VMware Tools 359
Реализация NAT 199
Регистровая память (Registered DIMM, RDIMM) 34
Редактор
◊ ee 63
◊ joe 63
◊ mcedit 63
◊ nano 62
◊ pico 62
◊ групповой политики 86
◊ презентаций LibreOffice Impress 47
◊ рисунков LibreOffice Draw 47
◊ управления групповыми политиками 263
◊ формул LibreOffice Math 47
◊ электронных таблиц LibreOffice Calc 47
Режим
◊ консоли Linux 58
◊ терминального сервера 245
Резервирование клиентов 124
Резервное копирование
◊ виртуальной машины 365
◊ информации 528, 529
Результирующее право 176
◊ пользователя 181
Рекурсивный запрос 132
Репликация
◊ SQL-серверов 513
◊ службы каталогов 521
Репозиторий 64
Ресурс административный 148
Решения VDI 369–372
Ролевое управление 176
Руткит 457

C

Сайт 156
Сервер
◊ Active Directory 503
◊ DHCP 112, 120, 127
◊ DNS 118, 159
◊ NAT 357
◊ RADIUS 442, 445
◊ rsyslog 330
◊ баз данных 503, 512
◊ глобального каталога 524
◊ каталогов AD 203
◊ лицензий 244
◊ лицензирования 411–414, 416, 417
◊ мониторинга 311, 318
◊ сценариев 277
▫ Windows Script Host (WSH) 277
◊ терминалов 396, 397, 404
◊ терминальный 242
◊ удаленного доступа (RAS) 235
Серверная версия Clonezilla Server Edition 297
Серверная ферма 81
Серверные источники бесперебойного питания (ИБП) 389
Серверный корпус 30

Сервис
◊ Google Drive 39
◊ systemd-journald.service 335
Сервис-пак 450
Сертификат
◊ восстановления 475
◊ ФСТЭК 452, 458
Сертификация UTI 390, 391
Сетевой анализатор (сниффер) 283
◊ OmniPeek Network Analysis 284
◊ Only WLAN Analysis and Recorder Appliance 284
Сетевой информационный центр (NIC) 196
Сеть
◊ безопасность 97
◊ виртуальная частная 235
◊ локальная 103
◊ одноранговая 145
Система
◊ iPatch Real Time Infrastructure Management 257
◊ PatchView 257
◊ squidGuard 231
◊ инициализации systemd 335
◊ контроля доступа LIDS 428, 440
◊ контроля доступа SELinux 428
◊ корпоративной работы Zimbra Collaboration Suite (ZCS) 49
◊ неизменность состояния 467
◊ резервного копирования 44
Система мониторинга
◊ Nagios 318, 320, 324, 328, 344
◊ Zabbix 311
◊ трафика darkstat 337, 338
◊ трафика NeTAMS 337, 339, 343
Системный журнал Linux (syslog) 317
Системы
◊ контроля доступа 42
◊ обнаружения вторжений (СОВ) 208
◊ предотвращения вторжений (СПВ) 208
Сквозное подключение физического диска 362
Скрипт Linux Live 290
СКС
◊ категорирование 72
◊ питание по сети Ethernet 79
◊ приоритизация трафика 85
◊ проектирование беспроводных сетей 93
◊ сеть управления 82
◊ стандарты 72
◊ требования к прокладке силовых кабелей 78
◊ требования пожарной безопасности 79
◊ уровень доступа 80
◊ уровень распределения 80
◊ ядро сети 80
Служба
◊ IAS 444, 445
◊ RADIUS 443–445, 447
◊ WINS 118
◊ автоматического обновления (WSUS) 455
◊ каталогов 153, 589
  ▫ Active Directory (AD) 145, 503, 589
  ▫ LDAP 145
◊ терминальная 242
Служебные пакеты BPDU 507
Смарт-карта 432, 433
Снимок данных (snapshot) 514
Сниффер 283
Снятие образа физического сервера 360
Сообщение
◊ DHCPACK 127
◊ DHCPDISCOVER 127
◊ DHCPOFFER 127
◊ DHCPREQUEST 127
Сообщество OpenSource 52
Социальная инженерия 435, 491
Способы управления локальной системой 151
Среда восстановления Windows 557
◊ Windows 10 562
Средства
◊ автоматического восстановления 557
◊ клонирования Linux (Clonezilla) 290
◊ обнаружения вторжений (IDS) 439
◊ предупреждения вторжений (IPS) 440
◊ просмотра журнала событий 532
◊ развертывания Windows 10 285
◊ удаленного администрирования сервера (RSAT) 262
Стандарт
◊ 802.3ad 509
◊ Intelligent Platform Management Interface (IPMI) 278
◊ S/MIME 480, 481
◊ шифрования данных
  ▫ Wi-Fi Protected Access (WPA) 97
  ▫ Wired Equivalent Privacy (WEP) 97
  ▫ WPA2 97
Стандартные учетные записи 172
◊ беспроводных сетей 93
◊ веб-управления предприятием (WBEM) 278
◊ СКС 72
Статический IP-адрес 120, 134
Стек протоколов TCP/IP 101
Структура DFS-домена 515
Структурированные кабельные сети (СКС) 71, 255
Сценарии PowerShell 281
Сценарий входа в систему 151

T

Таблица маршрутизации 107
Твердотельные диски (SSD) 33
Текстовый процессор LibreOffice Writer 47
Текстовый редактор vi 59, 61
Тендер 22
Терминальные системы 242
Терминальный сервер 404
Тестирование СКС 83

Техническая поддержка производителя 530
Технологии
◊ Active Directory 157, 158
◊ BitLocker 477–479
◊ BranchCache 252
◊ DirectAccess 102, 241
◊ Discrete Device Assignment 355
◊ Enternet 100G 76
◊ Enternet 40G 76
◊ Ethernet 10G 75
◊ Itracks 257
◊ KVM 374
◊ NAP 447, 448
◊ NAT 196
◊ Quality of Service (Qos) 85
◊ S.M.A.R.T. 344–346, 349, 552, 593
◊ USB Redirection 355
◊ WMI 278
◊ виртуализации на уровне ядра 373
◊ виртуализации рабочих станций (VDI) 369
◊ передачи данных 75
◊ переупаковки 301
◊ стеганографии 491
◊ теневого копирования 570, 571
◊ трансляции сетевого адреса (NAT) 196, 199
◊ шифрования WPA2 71
Топология сети 80
Точка
◊ восстановления 559, 567
◊ доступа Wi-Fi 93, 94
Трансляция адресов 103
Трансляция сетевых адресов (NAT) 357
Трап 312
Туннель 239

У

Удаление контроллера домена AD 162
Удаленное подключение к рабочему столу 273, 274
Удаленное управление 246
Удаленный помощник 273
Удаленный рабочий стол (RDP) 43
Уровни
◊ RAID 32
◊ надежности (Tier) 390, 391, 404
Установка
◊ Active Directory 158
◊ Linux 66
◊ ПО
  ▫ административная 303
  ▫ переупаковка 301
  ▫ тихая 300
Устойчивый пароль 430
Утилита
◊ ADSI Edit 590
◊ arp 114, 123
◊ checkdsk 551
◊ dcdiag 590, 591
◊ dnsdiag 140
◊ EventCombMT 538
◊ fsck 551
◊ HiliSoft MIB Browser 314
◊ ifconfig 541, 542, 544
◊ ifmember 276
◊ Insight for Active Directory (от Sysinternals) 531
◊ iometer 583, 584
◊ iostat 579, 580
◊ iotop 583
◊ ipconfig 541
◊ iReasoning MIB Browser 314
◊ journalctl 335, 336
◊ LDP.exe 164
◊ ldp.exe 590
◊ memtest 553, 554
◊ Microsoft Security Compliance Manager 450
◊ mklivecd 290
◊ monit 343
◊ Nagios 317
◊ NewSID 359
◊ nmon 579
◊ nslookup 138
◊ ntdsutil 163, 523
◊ ntdsutil.exe 590
◊ OpenNMS 317
◊ pathping 549, 550
◊ portqry.exe 546
◊ sysprep 287, 290
◊ top 578
◊ Tracelog 531
◊ V2V Converter 360
◊ WinAgents MIB Browser 314
◊ WinImage 361
◊ Zabbix 317
◊ Панель мониторинга 532
◊ Просмотр событий 532
◊ просмотра WMI Object Browser 327
Утилиты администрирования 282
Учет компьютеров 257
Учетная запись 144, 146, 148–150, 152, 161, 171–174, 176, 182–184, 187–189, 191, 192
◊ HelpAssisstant 188
◊ IWAM_имя_компьютера 189
◊ Microsoft 173
◊ SUPPORT_номер 188
◊ Администратор (Administrator) 182
◊ доменная 173
◊ локальная 173
◊ пользователя
  ▫ LocalService 187
  ▫ LocalSystem 187
  ▫ NetworkService 187
  ▫ Администратор 188
  ▫ Гость 188

Учетная запись *(прод.)*
◊ результирующие права 181
◊ создание и удаление 182
Уязвимость ARP-spoofing 440

Ф

Файл
◊ /etc/resolv.conf 545
◊ /etc/sudoers 63
◊ Adsutil.vbs 189
◊ gpttmpl.inf 261
◊ hosts 118
◊ lmhosts 119
◊ networks 119
◊ Registry.pol 260
◊ Sysprep.inf 289
◊ образа системы 559
◊ права доступа 55
◊ трансформации 298, 300
Файловая система Linux 55, 59
Ферма серверов 510
Фиксированный жесткий диск 362
Фоновое изменение политики 261
ФСТЭК 21, 206, 207, 209
Функция
◊ File History 251
◊ Squid SSL bump 234
◊ История файлов 251, 572, 575
◊ теневого копирования файлов 251

Х

Хеш-функция 253
Хозяева операций 522
Хост 115

Ц

Центр
◊ администрирования Active Directory 257
◊ выдачи ключей KDC (Key Distribution Center) 36
◊ обработки данных (ЦОД) 390, 504
Цепочка правил брандмауэра 212
Цифровая подпись изготовителя 288
Цифровые удостоверения 481
ЦОД 504, 505, 506
◊ наддув очищенного воздуха 505
◊ поддержание температуры 505
◊ резервное электропитание 505

Ч

Черный список 230

Ш

Шаблон
◊ compatws.inf 186
◊ административный 272
Широковещательные запросы 117, 119, 127
Широковещательный адрес 197
Шифрование 468
◊ EFS 475
◊ данных 97, 430, 468, 472, 474–479, 484, 490
◊ диска 470, 472, 477–480
◊ сообщений 480–482, 484, 485
Шифрованная файловая система
◊ eCryptfs 472–474
◊ EFS 430, 475, 476
Шлюз 106
◊ по умолчанию 107
◊ сети 214
◊ терминалов 250, 251

Э

Эксплойт 451
Электронная подпись письма 480
Электронный замок «Соболь» 438
Эмулятор Wine 66

Я

Язык
◊ WQL 279
◊ запросов для WMI 279