

**АЛЕКСАНДР КЕНИН
ДЕНИС КОЛИСНИЧЕНКО**

САМОУЧИТЕЛЬ СИСТЕМНОГО АДМИНИСТРАТОРА

4-е издание

**Системы высокой доступности
и их построение**

**Оптимизация
производительности**

**Выбор оборудования
и его характеристики**

**Использование облачных
технологий**

**Объединение компьютеров
Windows и Linux**

Контроль и управление

Надежная защита данных

**Информационные системы
на основе Windows 7/8/Server
2012**

Александр Кенин
Денис Колисниченко

**САМОУЧИТЕЛЬ
СИСТЕМНОГО
АДМИНИСТРАТОРА**
4-е издание

Санкт-Петербург
«БХВ-Петербург»

2016

УДК 004
ББК 32.973
К35

Кенин, А. М.

К35 Самоучитель системного администратора / А. М. Кенин,
Д. Н. Колисниченко. — 4-е изд., перераб. и доп. — СПб.: БХВ-Петербург,
2016. — 528 с.: ил. — (Системный администратор)

ISBN 978-5-9775-3629-5

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 распределенных 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 (в том числе Windows 7/8 и Windows Server 2012) и Linux с использованием как проприетарных, так и открытых технологий. Книга написана на основе многолетнего опыта разработки и практического администрирования информационных систем.

Из четвертого издания удален весь неактуальный материал, связанный со старыми технологиями, версиями Windows, старым программным обеспечением. Рассмотрены новейшие технологии, в том числе облачные, существенно возросло количество практических советов, инструкций и рекомендаций.

Для начинающих системных администраторов

УДК 004
ББК 32.973

Группа подготовки издания:

Главный редактор	<i>Екатерина Кондукова</i>
Зам. главного редактора	<i>Евгений Рыбаков</i>
Зав. редакцией	<i>Екатерина Капальгина</i>
Редактор	<i>Григорий Добин</i>
Компьютерная верстка	<i>Ольги Сергиенко</i>
Корректор	<i>Зинаида Дмитриева</i>
Дизайн серии	<i>Инны Тачиной</i>
Оформление обложки	<i>Марины Дамбиевой</i>

Подписано в печать 30.09.15.

Формат 70×100^{1/16}. Печать офсетная. Усл. печ. л. 42,57.

Тираж 1000 экз. Заказ №

"БХВ-Петербург", 191036, Санкт-Петербург, Гончарная ул., 20.

Первая Академическая типография "Наука"
199034, Санкт-Петербург, 9 линия, 12/28

ISBN 978-5-9775-3629-5

© Кенин А. М., Колисниченко Д. Н., 2016
© Оформление, издательство "БХВ-Петербург", 2016

Оглавление

Предисловие	17
Что нового вы найдете в четвертом 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.....	26
Выбор процессора	27
Выбор шасси	29
Выбор материнской платы.....	30
Выбор дисков	31
Выбор памяти.....	32
Дополнительные требования к коммутационному оборудованию.....	33
Дополнительные требования к аварийным источникам питания.....	33
Состав программного обеспечения типовой организации.....	34
Подсистема аутентификации и контроля доступа	34
Подключение Linux к домену: протокол Kerberos.....	35
Настройка конфигурации клиента Kerberos	35
Настройка файла <i>nsswitch.conf</i>	36
Получение билета Kerberos для учетной записи администратора	36
Подключение к домену.....	36
Проверка подключения.....	36
Сервер Linux в качестве контроллера домена	37
Совместно используемые ресурсы	37
Учетная запись для анонимного доступа.....	38
Работа с Windows-ресурсами в Linux.....	38

Установка пакета Samba	38
Настройки Samba	39
Подключение к общим ресурсам	40
Браузеры Интернета	40
Защита узлов сети	41
Средства удаленного администрирования	42
Средства резервного копирования	42
Офисный пакет	44
Электронная почта	46
Свободное программное обеспечение	49
Базовые сведения о работе в *NIX-системах	50
Linux-мифы	51
Надежность Linux и Windows	52
Несколько моментов, о которых следует знать пользователям Linux	52
Ядро и дистрибутивы	52
Файловая система	53
Монтирование файловой системы	55
Консоль и графический режим	56
Пользователь root	56
Структура папок Linux	57
Текстовые редакторы: vi и другие	58
Выполнение команд с правами другого пользователя	61
Прикладные программы в Linux	62
Кроссплатформенный запуск программ	63
Установка Linux	64
Загрузка нескольких операционных систем	64
Тестирование Linux на виртуальной машине	65
Глава 3. Структура сети.....	66
Структурированные кабельные сети	66
Категории СКС	68
Волоконно-оптические сети	70
Сети 10G	71
Схема разъема RJ-45	72
Варианты исполнения СКС	73
Удлинение кабеля	74
Прокладка силовых кабелей	74
Питание по сети Ethernet (PoE)	74
Требования пожарной безопасности	75
Топология сети	76
Размеры сегментов сети на витой паре	76
Уровни ядра, распределения и доступа	76
Топология каналов распределенной сети предприятия	77
Сеть управления	78
Документирование структуры каналов связи	78
Качество сетей связи предприятия	79
Проверка кабельной системы	79
Проверка качества передачи данных	79

Приоритезация трафика	81
Варианты приоритезации: QoS, ToS, DiffServ	81
Классификация, маркировка, приоритезация.....	84
Как работает приоритезация: очереди	84
Ограничение полосы пропускания трафика (Traffic shaping)	85
Беспроводные сети	86
Стандарты беспроводной сети.....	88
Проектирование беспроводной сети предприятия.....	89
Безопасность беспроводной сети	92
Шифрование трафика беспроводной сети.....	92
Аутентификация пользователей и устройств Wi-Fi.....	93
Безопасность клиента	94
Настройка транспортных протоколов.....	95
Протоколы	95
Модель OSI.....	95
Стек протоколов TCP/IP.....	96
Протоколы UDP, TCP, ICMP	97
IPv6.....	97
Параметры TCP/IP-протокола	98
IP-адрес	98
Групповые адреса	99
Распределение IP-адресов сети малого офиса.....	99
Маска адреса	100
Шлюз (Gateway, default gateway)	101
Таблицы маршрутизации	102
Автоматическое присвоение параметров IP-протокола	107
Серверы DHCP	107
Адресация APIPA.....	107
Назначение адресов при совместном использовании подключения к Интернету	108
Порт	108
Протокол ARP	109
Имена компьютеров в сети TCP/IP	111
Доменные имена Интернета.....	111
Соотношение доменных имен и IP-адресов компьютеров	112
Серверы доменных имен (DNS).....	113
WINS	113
Статическое задание имен.....	114
Последовательность разрешения имен	114
Настройка серверов DHCP и DNS.....	115
Настройка DHCP.....	115
Создание и настройка зоны	116
Авторизация DHCP-сервера.....	117
Настройка параметров области.....	118
Фиксированные IP-адреса	119
Подстройка DHCP под группы клиентов.....	119
Отказоустойчивость DHCP-сервера	120
Обслуживание DHCP-сервером других сегментов сети.....	120

Порядок получения IP-адресов клиентами DHCP.....	121
Первичное получение адреса.....	121
Продление аренды.....	122
Диагностика и обслуживание DHCP-сервера.....	122
Интеграция DHCP и DNS.....	123
DNS.....	123
Термины DNS.....	124
Порядок разрешения имен в DNS.....	127
Основные типы записей DNS.....	128
Установка сервера DNS.....	129
Записи домена Windows.....	130
Разделение DNS.....	131
Настройка DNS в удаленных офисах.....	132
Обслуживание и диагностика неисправностей DNS-сервера.....	133
Перенос записей зон.....	135
Глава 4. Информационные системы предприятия.....	136
SOHO-сети.....	136
Одноранговые сети.....	138
Сеть с централизованным управлением.....	138
Управление локальными ресурсами.....	138
Возможность добавлять рабочие станции в домен.....	139
Удаление устаревших записей о компьютерах и пользователях.....	141
Изменения настроек системы при подключении ее к домену.....	141
Локальный администратор против доменного.....	142
Проблема аудитора.....	144
Методы управления локальной системой.....	144
Служба каталогов.....	146
Служба каталогов Windows (Active Directory).....	146
Домены Windows.....	147
Подразделение.....	148
Лес.....	149
Сайты.....	149
DN, RDN.....	150
Управление структурой домена предприятия.....	150
Создание нового домена.....	151
Функциональный уровень домена.....	152
Компоненты Active Directory.....	152
Создание контроллеров домена «только для чтения».....	153
Удаление контроллера домена.....	153
Переименование домена.....	155
LDAP и Active Directory.....	155
Подключаемся к каталогу по протоколу LDAP.....	155
Синтаксис поисковых запросов LDAP.....	156
Команда <i>ldifde</i>	158
Делегирование прав.....	159
Корзина Active Directory. Просмотр и восстановление удаленных объектов каталога.....	160

Учетные записи и права	162
Понятие учетной записи.....	162
Локальные и доменные учетные записи	163
Группы пользователей.....	165
Ролевое управление	166
Результирующее право: разрешить или запретить?	167
Разрешения общего доступа и разрешения безопасности.....	167
Наследуемые разрешения: будьте внимательны.....	168
Восстановление доступа к ресурсам	170
Обход перекрестной проверки.....	170
Изменение атрибутов объектов при операциях копирования и перемещения.....	171
Результирующие права и утилиты	172
Рекомендации по применению разрешений	173
Создание и удаление учетных записей	173
Права учетной записи.....	174
Восстановление параметров безопасности по умолчанию	175
Автоматически создаваемые учетные записи	177
Встроенные учетные записи пользователей.....	177
Предопределенные учетные записи пользователя.....	178
Учетная запись <i>Администратор</i>	178
Учетная запись <i>Гость</i>	179
Другие встроенные учетные записи пользователей	179
Встроенные группы	180
Специальные группы	182
Рекомендации по использованию операции <i>Запуск от имени Администратора</i>	183
Глава 5. Работа в глобальной сети	184
Организация доступа к ресурсам Интернета.....	184
Сетевая адресация.....	184
NAT — трансляция сетевого адреса	187
Реализация NAT средствами службы маршрутизации Windows Server	187
Аппаратный NAT.....	191
Реализация NAT средствами Linux	192
Фильтрация трафика.....	192
Демилитаризованная зона	193
Межсетевой экран (брандмауэр)	194
Выбор межсетевого экрана.....	194
Нужен ли прокси-сервер?.....	195
Системы обнаружения вторжений	196
Варианты межсетевых экранов	196
Аппаратные решения.....	197
Встроенный межсетевой экран Windows 7/8/10/Server 2008/2012	197
«Киберсейф Межсетевой экран»	198
Настройка параметров межсетевого экрана при помощи групповой политики	200
Групповые политики межсетевого экрана.....	200
Межсетевой экран Linux	202
Настройки запуска	202
Цепочки и правила.....	203

Задание правил брандмауэра	205
Пример настройки брандмауэра	208
Оптимизация доступа в Интернет	212
Основные мероприятия оптимизации	212
Прокси-сервер	213
Прозрачный прокси	214
Настройка использования полосы пропускания	216
Блокировка рекламы, порносайтов и т. п.	218
Удаленная работа	221
Виртуальные частные сети	221
Удаленное подключение к Linux	222
Протокол SSH	223
«Тонкие» клиенты	224
Использование графических утилит для подключения к Linux	225
Подключения филиалов	225
Контроллер домена «только для чтения»	226
DirectAccess	227
Терминальный доступ	228
Терминальные серверы от Microsoft	228
Терминальные клиенты	228
Режимы терминальных служб	230
Лицензирование терминальных служб	230
Особенности использования приложений на терминальном сервере	231
Безопасность терминальных сессий	231
Подключение к консоли терминального сервера	232
Подключение администратора к сессии пользователя	233
Публикация приложений в терминале	233
Веб-доступ к терминальному серверу	235
Шлюз терминалов	236
Создание локальных копий данных	236
История файлов	237
Технология BranchCache	238
Доступ из-за межсетевое экрана	239
Глава 6. Управление информационной системой	241
Состав информационной системы	241
Построение топологии существующей СКС	241
Инвентаризация физических каналов связи	242
Учет компьютеров и программ	243
Мониторинг функционирования ПО	244
Управление с помощью групповых политик	244
Порядок применения множественных политик	245
Совместимость версий групповых политик	245
Места хранения и условия применения групповых политик	246
Последствия отключений политик	247
Редактирование групповых политик	248
Начальные объекты групповой политики	251
Расширенное управление групповыми политиками	251

«Обход» параметров пользователя.....	252
Фильтрация объектов при применении групповой политики.....	253
Фильтрация при помощи WMI-запросов.....	253
Настройка параметров безопасности групповых политик.....	254
Предпочтения групповых политик.....	254
Рекомендации по применению политик.....	255
Блокирование запуска нежелательных приложений с помощью компонента AppLocker.....	255
Некоторые особенности политики установки программного обеспечения.....	257
Административные шаблоны.....	258
Утилиты группового управления.....	259
Средства поддержки пользователей.....	259
Удаленный помощник.....	259
Утилиты подключения к рабочему столу.....	261
Средства автоматизации — сценарии.....	262
Использование командной строки.....	263
Сценарии Visual Basic.....	263
Интерфейс IPMI.....	264
Интерфейс WMI.....	265
Язык запросов WMI Query Language.....	265
Варианты применения WMI.....	266
Примеры WMI-сценариев.....	266
PowerShell.....	267
Отдельные утилиты администрирования третьих фирм.....	269
Утилиты от компании Sysinternals.....	269
Снифферы.....	270
Ideal Administrator.....	270
Нуена.....	271
Автоматизация установки программного обеспечения.....	271
Развертывание Windows 7 при помощи WAIK.....	271
Развертывание Windows 8 при помощи Windows ADK.....	272
Клонирование Windows-систем.....	272
Подводные камни процесса клонирования.....	272
Утилита sysprep.....	273
Создание установочного образа системы при помощи утилиты sysprep.....	274
Подготовка диска для существенно отличающейся системы.....	274
Дублирование жесткого диска.....	275
Образы клонируемого диска и их модификация.....	277
Клонирование компьютеров-членов домена.....	277
Клонирование Linux-систем.....	277
Средства клонирования Linux.....	277
Использование Clonezilla.....	278
Подготовка программ для тихой установки.....	285
Файлы ответов (трансформаций).....	285
Использование ключей тихой установки.....	287
Переупаковка.....	288
Административная установка.....	289
Развертывание программы в Active Directory.....	290

Глава 7. Мониторинг информационной системы.....	295
Основные способы мониторинга.....	295
Журналы системы и программ	295
Протокол SNMP	296
Опрос служб	296
Мониторинг с использованием агентов.....	297
Мониторинг на основе протокола SNMP	298
Простейшие варианты мониторинга	300
Контроль журналов Windows	300
Привязка задачи	300
Подписка на события.....	302
Создание собственных событий в журналах Windows	302
Настройка журналирования в syslog	303
Утилиты мониторинга	303
Система мониторинга Nagios	303
Необходимость мониторинга сети	303
Установка Nagios	304
Настройка Nagios	305
Мониторинг в Nagios серверов Windows.....	309
Мониторинг Windows-систем на основе WMI.....	312
Мониторинг в Nagios серверов Linux	313
Мониторинг систем с использованием протокола SNMP	313
Сервер протоколов	315
Постановка задачи	315
Настройка основного (центрального) сервера	316
Настройка остальных серверов сети	318
Системы мониторинга трафика	320
Простейшая система мониторинга трафика: darkstat	320
Система NeTAMS	323
Глава 8. Виртуализация.....	328
Секрет популярности виртуализации.....	328
Глоссарий	329
Вендоры виртуальных решений	329
Решения по распределению ресурсов в *NIX	330
Выбор гипервизора.....	331
Программное обеспечение и виртуальная среда.....	332
Особенности сетевых подключений виртуальных машин	332
Лицензирование программного обеспечения виртуальных машин	333
Создание виртуальных машин.....	333
Создание виртуальной машины путем чистой установки операционной системы.....	333
Клонирование виртуальной машины	334
Снятие образа физического сервера.....	335
Миграция между решениями различных производителей.....	335
Некоторые замечания к устройству виртуальных машин	336
Жесткие диски.....	336
Типы виртуальных дисков	336
Необходимость блочного доступа к виртуальному диску	337
Варианты подключения виртуального диска	337

Обслуживание файлов виртуального диска.....	337
Сохранение состояния виртуальной машины	338
Распределение вычислительных ресурсов.....	338
Оперативная память.....	338
Сервисные операции	339
Резервное копирование и антивирусная защита	339
Обмен данными.....	339
Копирование данных с машины на машину.....	339
Общие папки	340
Миграция виртуальных машин.....	340
Подключения к виртуальным машинам.....	341
Особенности выключения виртуальных машин	342
Виртуальные рабочие станции	343
Сравниваем VDI-решения с терминальными клиентами	343
Немного об экономике VDI	343
Структура VDI-решений	344
Некоторые особенности VDI-решений.....	345
Производительность виртуальных систем	346
KVM и OpenVZ.....	346
Разница между KVM и OpenVZ	346
Установка ядра OpenVZ.....	348
Создание и запуск виртуальной машины.....	348
Советы по оптимизации виртуальных систем.....	350
Виртуализация в сетях передачи данных	351
Виртуальные частные сети.....	351
Зачем нужны виртуальные сети?.....	351
Маркировка кадров.....	352
Порты и VLAN.....	353
Практика настройки VLAN на коммутаторах Cisco	354
Другие производители оборудования	356
Настройка VLAN в Linux	356
Глава 9. Безопасность.....	358
Безопасность и комфорт	358
Попытаемся разложить по полочкам	359
Как будем защищать?.....	360
Три «кита» безопасности.....	361
Организационное обеспечение информационной безопасности.....	362
План обеспечения непрерывности функционирования информационной системы	363
Безопасность паролей.....	363
Токены и смарт-карты	365
Rainbow-таблицы	366
Блокировка учетной записи пользователя	366
Восстановление пароля администратора.....	367
Методы социальной инженерии	368
Меры защиты от внешних угроз	369
Физическая безопасность.....	369
Ограничение доступа к рабочим станциям	369

Межсетевые экраны.....	371
Ограничения подключения нового оборудования.....	371
Обеспечение сетевой безопасности информационной системы.....	371
Контроль проходящего трафика.....	372
Контроль устройств по MAC-адресам.....	372
Протокол 802.1x.....	374
Особенности применения протокола 802.1x.....	375
Настройка протокола 802.1x.....	375
Выдача сертификатов компьютерам.....	376
Настройка службы каталогов.....	376
Настройка службы RADIUS.....	377
Настройка автоматического назначения VLAN для порта коммутатора.....	377
Настройка клиентского компьютера.....	378
Настройка коммутатора.....	379
Технология NAP.....	379
Обнаружение нештатной сетевой активности.....	380
Контроль состояния программной среды серверов и станций.....	381
Индивидуальная настройка серверов.....	381
Security Configuration Manager.....	381
Security Compliance Manager.....	382
Исключение уязвимостей программного обеспечения.....	382
Уязвимости и эксплойты.....	383
Как узнать об обновлениях?.....	383
Проверка системы на наличие уязвимостей.....	383
Тестирование обновлений.....	385
Обновления операционных систем Linux.....	385
Индивидуальные обновления Windows-систем.....	386
Обновление Windows-систем на предприятии.....	387
Установка обновлений через групповые политики.....	389
Защита от вредоносных программ.....	389
График обновления антивирусных баз.....	391
Внимательность пользователя.....	391
Лечение вирусов.....	392
Защита от вторжений.....	393
Программы-шпионы: «тройанские кони».....	394
Редактирование списка автоматически загружаемых программ.....	398
Безопасность приложений.....	398
Основные принципы безопасности приложений.....	398
Единый фонд дистрибутивов и средства контроля запуска программного обеспечения.....	399
Неизменность системы.....	399
Защита от утечки данных.....	400
Шифрование данных.....	400
Шифрование данных на устройствах хранения.....	400
Шифрование архивов.....	400
Бесплатные программы шифрования данных.....	400
Шифрование дисков: коммерческие программы.....	402

Шифрование в Linux.....	404
Шифрование файловой системы Windows	406
Шифрование диска при помощи BitLocker	409
Использование BitLocker на компьютерах без TPM.....	410
Включение шифрования.....	411
Режим восстановления.....	411
Шифрование почты	412
Получение открытого ключа для защищенной переписки.....	413
Получение цифрового сертификата для защищенной переписки.....	413
Работа с подписанными и зашифрованными сообщениями в ОС Android.....	416
Шифрование в базах данных	422
Стеганография.....	423
Анализ поведения пользователей.....	423
DLP-технологии	424
Анонимность работы в глобальной Сети	425
Глава 10. Отказоустойчивая информационная система.....	427
Территориальная распределенность	427
Центры обработки данных (дата-центры)	428
Требования к помещениям.....	428
Поддержание в помещении постоянной температуры	428
Резервное электроснабжение	429
Системы пожаротушения.....	430
Сетевая инфраструктура	430
Выбор правильной топологии сети передачи данных	430
Построение отказоустойчивой сети на основе протоколов второго уровня	
модели OSI	431
Протокол STP.....	431
Протокол MSTP.....	432
Отказоустойчивая сеть на основе протоколов третьего уровня:	
протокол VRRP.....	432
Агрегированные каналы.....	433
Проприетарные технологии восстановления структуры сети.....	434
Фермы серверов.....	434
Отказоустойчивые решения для приложений.....	435
DNS-серверы	435
DHCP-сервер	435
Кластер Oracle RAC.....	436
Распределенная информационная база «1С».....	436
Дублирование данных	436
Зеркалирование серверов баз данных	437
Зеркалирование (репликация) данных SQL-серверов	437
Снимки баз данных.....	438
Настройка клиентских подключений	438
Распределенная файловая система	438
Создание DFS.....	439
Репликация DFS	440
Поддержка DFS в Linux-системах	441

Кластеры.....	442
Кластер Microsoft.....	442
Кластер openMosix.....	445
Распределенные каталоги	445
Репликация данных каталогов	445
Хозяева операций	446
Смена хозяев операций	447
Сервер глобального каталога (GC).....	448
Отказоустойчивые решения и виртуальные системы.....	449
Глава 11. Порядок выявления неисправностей и их устранения	450
Если отказ уже произошел.....	450
Максимальный аптайм	451
Восстановление с нуля, или полное фиаско	451
Запасные детали.....	452
Где получить помощь?.....	452
Сбор информации об отказе	453
Анализ журналов системы	453
Средства просмотра журналов системы	454
Журналы в Linux. Демон syslogd.....	456
Централизованное ведение журналов	459
Установка триггеров на события протоколов	461
Настройка аудита событий безопасности.....	461
Утилиты от Sysinternals	462
Особенности отказов различных компонентов.....	462
Мониторинг отказоустойчивой структуры.....	462
Неисправности подсистемы передачи данных.....	463
Обнаружение неисправностей сетевой инфраструктуры.....	463
Диагностика IP-протокола	464
Проверка параметров настройки IP-протокола	464
Проверка достижимости ближайших компьютеров сети.....	466
Проверка функционирования серверов имен	468
Проверка доступности приложений на удаленном компьютере.....	468
Проверка качества канала связи	470
Объективные показатели качества канала связи.....	470
Коэффициент использования пропускной способности сети.....	470
Число ошибочных пакетов	471
Величина коллизий	471
Загрузка процессора активного оборудования.....	471
Утилита pathping	472
Неисправности аппаратной части компьютера.....	473
Контроль жестких дисков	474
Восстановление данных с жестких дисков.....	476
Проверка оперативной памяти	476
Контроль теплового режима работы системы.....	478
Ошибки программного обеспечения.....	479
Восстановление «упавших» систем.....	479
Восстановление из резервной копии.....	479

Восстановление загрузчика системы	480
Восстановление загрузки Windows 8	480
Восстановление загрузки Windows 10	486
Восстановление загрузки Linux-систем	488
Если опции восстановления недоступны.....	489
Загрузка в специальных режимах.....	489
Загрузка Windows в безопасном режиме	490
Загрузка *NIX-систем в однопользовательском режиме	490
Откат к предыдущим состояниям системы	490
Загрузка последней удачной конфигурации Windows.....	490
Загрузка конфигурации из точек восстановления Windows.....	491
Восстановление Windows путем переустановки	492
Восстановление удаленных данных	494
Корзины	494
Восстановление из теневых копий.....	494
История файлов.....	495
Оптимизация настроек компьютера.....	501
Что такое «медленно»?.....	501
Основные узкие места системы.....	502
Оценка производительности процессора.....	503
Оценка использования оперативной памяти	505
Оценка дисковой подсистемы	506
Показатели производительности дисков.....	506
Пути оптимизации дисковой подсистемы.....	509
Оценка работы сетевого адаптера и пути оптимизации системы передачи данных	510
Некоторые советы по анализу показаний производительности	511
Оптимизация приложений	512
Диагностика службы каталогов и обнаружение ее неисправностей	513
Средства тестирования AD	514
Проверка разрешения имен	515
Глава 12. Плановые задачи обслуживания.....	516
Ежедневные задачи.....	516
Еженедельные задачи	517
Прочие плановые операции	518
Предметный указатель	521

Предисловие

Эта книга пригодится всем, кто занимается созданием и эксплуатацией информационных систем. Главное внимание в ней уделено оценке тех или иных технологий: 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 показывает, что проблемы и вопросы пользователей и специалистов, 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.

Большинство книг тематики, подобной этой, организованы по принципу: задача — решение. Возможно, в них приводится несколько вариантов решения, но в любом случае предлагается точная последовательность действий. Наша книга организована несколько в ином ключе. Последовательность действий описана в технической документации и ознакомиться с ней — не проблема. Здесь же представлено наше видение 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.

В случае возникновения вопросов обращайтесь на форум сайта <http://dkws.org.ua>, где вам будет оказана посильная помощь.

¹ См. <http://www.bhv.ru/books/book.php?id=190774>.

Что нового вы найдете в четвертом издании?

Во-первых, переработан и обновлен весь материал книги — в ходу давно Windows Server 2012, а предыдущее издание опиралось на версию 2008, кроме того, многих описанных в нем утилит и программ уже просто не существует. Так что весь неактуальный и устаревший материал из книги удален.

Во-вторых, предшествующее — третье — издание имело сильный крен в теоретические дебри. Да, то-то и то-то сделать можно и с помощью такого-то средства, а вот как — будьте добры, читайте в соответствующем руководстве. С одной стороны, это подход правильный — книга указывает направление поиска. С другой, прекрасно понимаю читателя, которому не хочется обращаться к другим источникам или лезть в компьютер и «гуглить» дополнительную информацию, — желательно, чтобы все было под рукой. Поэтому теорию здесь мы в достаточной степени дополнили практикой. Конечно, так, чтобы ничего не испортить. Поэтому книга, не утратив в целом теоретической направленности, по некоторым темам содержит развернутые практические советы.

Ну, и в-третьих, если материал предыдущих изданий был в основном ориентирован на Windows-системы и не касался систем на Linux, то в этом издании сей недостаток устранен. И хотя здесь по-прежнему в рассмотрении сохраняется приоритет Windows-систем, однако и Linux теперь нашим вниманием уже не обойден.

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. Сеть создать и настроить, установить/переустановить программу или операционную систему, отремонтировать/модернизировать компьютер, заправить картридж принтера, участвовать в закупке нового оборудования и т. д. 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/программного обеспечения, с которыми заключили партнерские соглашения.

Понятно, что один человек не может знать всё про всё. Поэтому на большом предприятии сотрудники ИТ-службы закреплены 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. д. 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 ИТ-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 того или иного производителя программного обеспечения, предлагающих свое видение вашей системы, которое не всегда верное 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 как раз и входит в обязанности системного администратора. А для его реализации есть 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, Mac OS. 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 местах, где заранее неизвестно, какие программы могут понадобиться. А 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 в организации 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 ФСТЭК¹ дистрибутивов можно упомянуть только ALT Linux 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 или 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: SUSE Linux или ALT Linux. 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. Один из авторов этой книги ранее создавал свою собственную сборку — Denix (denix.dkws.org.ua) — именно на базе Ubuntu. Но потом ему надоело бороться с бесчисленными ее «глюками», и последние две версии Denix сделаны на базе Debian.

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 данный момент на предприятии нет администратора UNIX-системы, придется такового нанять, а это дополнительные расходы. Конечно, любому квалифицированному пользователю не составит особого труда разобраться с основами UNIX, а вот для решения серьезных задач понадобится серьезная подготовка. Не

¹ ФСТЭК — Федеральная служба по техническому и экспортному контролю.

скажем, что найти специалиста по UNIX слишком сложно (на дворе уже далеко не 2000-й год, когда таких специалистов можно было пересчитать по пальцам), но их меньше, чем администраторов Windows-систем.

Участие в тендерах

Периодически возникает необходимость внедрения новых технических решений. Само 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/определенное 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 другой политики. Применять обновления нужно выборочно — если обновление несет в себе необходимый функционал (нужные пользователям функции, исправление «дыр» в безопасности и т. д.). В противном случае обновления применять не следует. Как говорится — не мешайте компьютеру работать. Если все программы функционируют нормально и пользователи ни на что не жалуются, 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 XP на Windows 8¹), то тут нужно оценить экономическую целесообразность такого решения. Переход только ради перехода нерационален. Переход должен быть оправданным. Зачем осуществляется переход?

Предположим, что у вас есть парк компьютеров под управлением Windows XP с установленными последними обновлениями. Как мы уже знаем, поддержка Windows XP прекращена, а это означает, что не будут выходить обновления системы, а также разрабатываться драйверы устройств под нее. Но если сейчас все работает, а пользователей и администраторов устраивает функционал этой ОС, есть ли смысл тратиться и переходить на Windows 8 или на Windows 10? — это будут впустую потрачен-

¹ Упомянув здесь и далее Windows 8, мы имеем в виду все существующие в настоящее время ее варианты, — Windows 8.1 и последующие возможные.

ные деньги. Переход на новую версию Windows нужно производить по мере необходимости. Приведем некоторые примеры:

- необходимо установить какое-то ПО, которое не совместимо с Windows XP и требует более новой версии Windows. Что ж, если нельзя использовать аналог этого ПО, работающий в XP, придется переходить на Windows 8 или Windows 10;
- компонент ПК вышел из строя. Представим, что «сгорела» видеокарта. Вы покупаете новую и обнаруживаете, что для нее нет драйвера под Windows XP. Не мудрено — видеокарта довольно современная, а поддержка XP уже прекращена. Здесь есть два решения проблемы: или обменять видеокарту на более старую, имеющую драйверы под XP, или же обновиться до Windows 8;
- появилась необходимость в использовании каких-либо функций, предоставляемых только новыми версиями Windows.

Совсем другое дело — Windows 7. Поддержка этой ОС также прекращается, но производители оборудования понимают, что еще сколько-то лет эта ОС будет актуальной, и поэтому не спешат отказываться от поставки драйверов оборудования для «семерки».

Если вы сейчас используете Windows 7, то, тем более, пока нет смысла в переходе на более новую версию Windows. Лучше всего немного подождать, и перейти уже на Windows 10. На момент подготовки этой книги Microsoft анонсировала выход финального релиза Windows 10 на 29 июля 2015 года. При этом объявлено, что переход на Windows 10 пользователей легальных версий Windows 8/8.1, а также — внимание! — Windows 7, в течение года после выхода релиза будет осуществляться бесплатно.

Так что, на Windows 8/8.1 смысла переходить нет вовсе — лучше перейти сразу на Windows 10. И дело тут не в гонке за новизной, а в том, что «десятка» действительно лучше и удобнее «восьмерки». Вы, фактически, получите те же функции, что и в «восьмерке», но интерфейс «десятки» гораздо удобнее, — по крайней мере, на наш взгляд.

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. И если вы до обновления использовали Windows XP и Microsoft Office 2003, для чего вполне было достаточно 1–2 Гбайт оперативной памяти, то при переходе на Windows 8/10 и MS Office 2013 вам понадобится как минимум 4 Гбайт.

О моральных качествах администратора

Системный администратор — это пользователь с практически неограниченными правами, благодаря которым он может получить доступ к любой информации на предприятии, — например, выяснить, у кого какая зарплата, может перехватить

передаваемый трафик и даже прочитан почту. В некоторых организациях ведется даже учет паролей — не только к учетным записям, но также и к ключам электронной подписи. Такая практика в корне неправильна, но она существует. Сами понимаете, что имея пароли пользователей, администратор получает неограниченную власть над данными этих пользователей. Да и без паролей пользователей администратор может получить доступ к любому объекту, но система все равно запишет, что доступ получал администратор. А если он воспользуется паролем пользователя, то система запροтоколирует 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 данным, их хищению и т. п.

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 вам помочь сделать такой выбор и попытаемся 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 «иконки»: 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 — вовсе неплохой производитель, не ровня прочим китайским устройствам No-Name.

Впрочем, 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, и т. п. С другой стороны, в топовых моделях вы, как правило, не воспользуетесь и половиной предоставляемого функционала — так зачем платить больше?

Теперь сравним две модели, которые в любом магазине продаются примерно за одни и те же деньги: ZyXEL Keenetic Giga II и TP-LINK TL-WDR3600. Казалось бы, выбор очевиден: ZyXEL — ведь он стоит столько же, сколько и TP-Link. Но взглянем на характеристики. Да, у Keenetic Giga II есть поддержка 3G, что несомненно понравится домашним пользователям: пропал основной канал — можно работать по 3G. Очень удобно.

Однако мы выбрали бы для офиса TL-WDR3600. Почему? Изучив характеристики обоих устройств, мы обнаружили, что у модели от ZyXEL отсутствует поддержка IPsec¹, что представляет собой существенный недостаток. Кроме того, маршрутизатор от TP-LINK является двухдиапазонным, обладает аппаратным NAT² со скоростью до 800 Мбит/с (от WAN к LAN) и может «выжать» максимальную пропускную способность в 600 Мбит/с (при работе в двух диапазонах частот: 300 Мбит/с на 5 ГГц + 300 Мбит/с на 2,4 ГГц). Плюс к этому гарантия 24 месяца, а не 12. Так что, пусть выбор и не очевиден, но есть над чем задуматься.

ПРИМЕЧАНИЕ

При сравнении оборудования пользуйтесь только официальными источниками (сайтами производителей). На сайтах интернет-магазинов информация может оказаться неточной, и использовать ее для сравнения устройств не рекомендуется. Например, в одном из интернет-магазинов было указано, что у TL-WDR3600 несъемные антенны и нет поддержки IPTV. Это не так, и опровержение может быть найдено на официальном сайте производителя.

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 далее) такой удаленный ремонт может занять длительное время — на одну только пересылку оборудования туда-сюда уйдет, как минимум, от 2-х до 4-х 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.

¹ IPsec (сокращение от IP Security) — набор протоколов для обеспечения защиты данных, передаваемых по межсетевому протоколу IP.

² NAT (от англ. Network Address Translation, преобразование сетевых адресов) — механизм в сетях TCP/IP, позволяющий преобразовывать IP-адреса транзитных пакетов.

Почему мы все-таки выбрали оборудование от TP-Link? Потому что представители TP-Link в случае выхода оборудования из строя сразу же (в день обращения) заменяют его на такое же или аналогичное по параметрам. Гарантийного же ремонта устройства от ZyXEL придется ждать две недели. А что делать все это время? — ведь подменное устройство они не предоставляют. Две недели без доступа к Интернету — перспектива неутешительная.

Но 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 сломавшемуся устройству купить хоть самый дешевый. Такой выход, хоть и не очень приятен, но не сильно отразится ни на бюджете конечного пользователя, ни, 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 — под заказ или бывшие в употреблении. Да и цена не порадует. Один модуль DDR SDRAM емкостью 1 Гбайт обойдется вам дороже, чем DDR3 SDRAM емкостью 2 Гбайт. 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 используемого 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. д.). 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 i7. Первые считаются немного устаревшими, но из-за этого они сейчас весьма доступны по цене, дешевле даже, чем Intel Core i7.

При выборе процессора обращайте внимание также и на их модификацию. Например, Intel Core i7-5820K стоит в два раза дороже, чем Intel Core i7-4771, хотя у второго частота выше, чем у первого: 3,5 ГГц против 3,3 ГГц.

Если вы хотите узнать, чем отличаются друг от друга те или иные процессоры, ищите информацию на сайте <http://www.cpu-world.com/>. Например, узнать, почему Intel Core i7-5820K лучше, чем Intel Core i7-4771, можно по адресу:

http://www.cpu-world.com/Compare/514/Intel_Core_i7_i7-4771_vs_Intel_Core_i7_i7-5820K.html

Еще более наглядно сравнение процессоров осуществляется на сайте <http://cpuboss.com>. Так, на странице:

<http://cpuboss.com/cpus/Intel-Core-i7-5820K-vs-Intel-Core-i7-4771>

можно найти сравнительные данные тех же процессоров: Intel Core i7-5820K и Intel Core i7-4771 (рис. 2.1).

Посмотрим, в чем особенности модели Intel Core i7-5820K:

- другой сокет — s2011-3 против s1150 у Intel Core i7-4771 (соответственно, для Intel Core i7-5820K нужна другая материнская плата, и это тоже может отразиться на стоимости всего сервера);

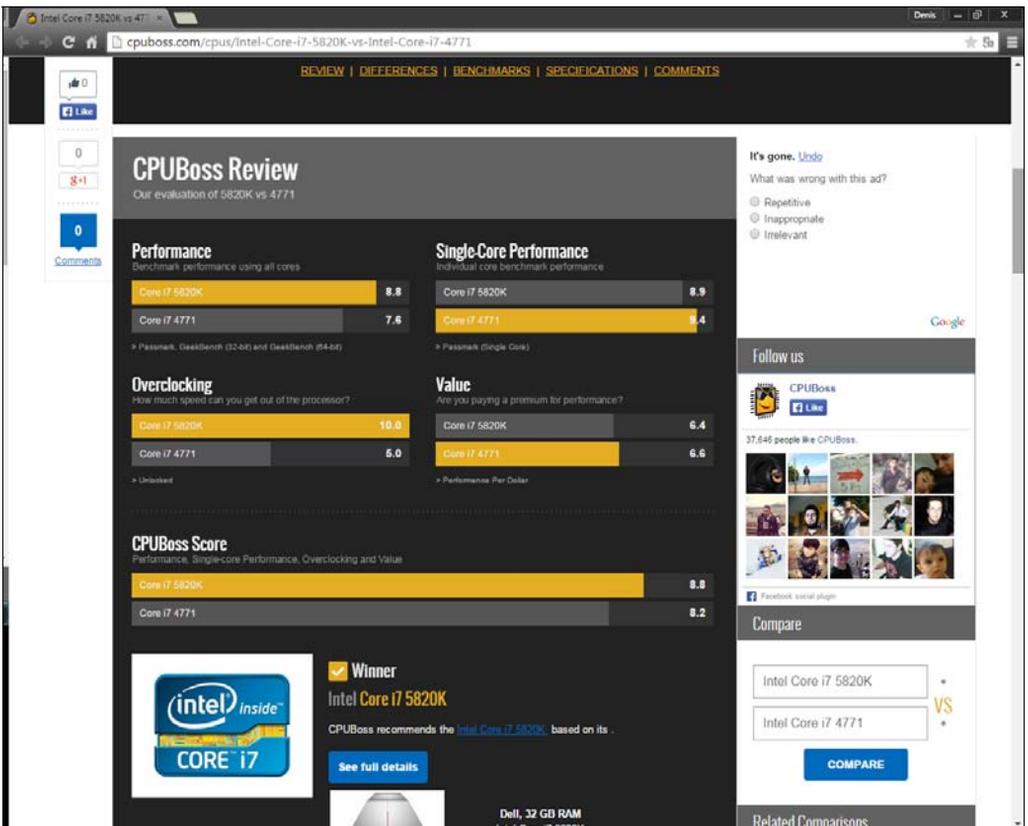


Рис. 2.1. Сравнение процессоров Intel Core i7-5820K и Intel Core i7-4771 на сайте <http://cpuboss.com>

- больше ядер: 6 против 4;
- 15 Мбайт кэша третьего уровня против 8 Мбайт у Intel Core i7-4771;
- разблокированный множитель, что позволяет легко разгонять процессор, т. е. 3,3 ГГц — это не предел. Вы можете легко увеличить его частоту (хотя на сервере мы бы не рекомендовали этого делать).

В табл. 2.1 приводятся основные характеристики актуальных процессоров семейства Intel Core i7.

Таблица 2.1. Основные характеристики процессоров Intel Core i7

Модель	Сокет	Частота, ГГц	Кол-во ядер	Кэш L3, Мбайт	Частота шины, ¹ GT/s	Разблок. множитель
i7-3960X	s2011	3,3	6	15	5	Да
i7-3970X	s2011	3,5	6	15	5	Да
i7-4770	s1150	3,4	4	8	5	Нет
i7-4770K	s1150	3,5	4	8	5	Да
i7-4771	s1150	3,5	4	8	5	Нет
i7-4790	s1150	3,6	4	8	5	Нет
i7-4790K	s1150	4,0	4	8	5	Да
i7-4820K	s2011	3,7	4	10	5	Да
i7-4930K	s2011	3,4	6	12	5	Да
i7-4960X	s2011	3,6	6	15	5	Да
i7-5820K	s2011-3	3,3	6	15	5	Да
i7-5930K	s2011-3	3,5	6	15	5	Да
i7-5960X	s2011-3	3,0	8	20	5	Да
i7-990X	s1366	3,46	6	12	6,4	Да

Впрочем, процессоры Intel — это не панацея. Вполне возможно, что вам придется использовать совсем другие процессоры и даже совсем другую 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 позво-

¹ GT/s — сокращение от Giga-Transfers/second (миллиардов пересылок в секунду). Чаще всего используется как численная характеристика скорости работы с оперативной памятью процессоров Intel, поддерживающих технологию Intel QuickPath.

ляет выдвигать их из стойки для упрощения обслуживания. Шасси должно иметь два блока питания, допускающих их «горячую» замену.

На рис. 2.2 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. 2.2. Типичный серверный корпус

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 32 Гбайт. Конечно, если вы создаете сервер начального уровня, то хватит и 16 Гбайт, но не нужно забывать о возможной последующей модернизации. Память — очень критичный ресурс, и очень скоро вы обнаружите, что вам ее недостаточно. И хорошо, когда есть возможность расширения;
- ❑ **Количество слотов памяти** — на серверной материнской плате должно быть 4 слота под ОЗУ;
- ❑ **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 будут установлены несколько жестких дисков. Например, на

борту материнской платы Asus P9D-X имеется четыре разъема SATA II и два SATA III.

Для упрощения мониторинга 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 понадобятся всего два жестких диска для построения отказоустойчивого массива (зеркала).

Совсем другое дело, если данные предполагается хранить на сервере. Тогда нужно установить в сервер максимальное число дисков, что ограничивается форм-фактором корпуса. Следовательно, при выборе корпуса это следует учитывать. Количество дисков зависит от выбранного уровня RAID. Так, для RAID 5 необходимы три, а для RAID 5E — четыре диска. Общая информация о некоторых уровнях RAID представлена в табл. 2.2.

Таблица 2.2. 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-х дисков). Общий размер массива вычисляется по формуле:

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

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

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

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 больше, 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 только от скорости вращения шпинделя — чем выше скорость, тем больше IOPS. Зависит также IOPS и от размера блока. Понятно, что чем выше 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) 15 000 оборотов в минуту. Если скорость вращения равна 10 000 RPM, то IOPS будет равен 120. Да, именно такие жесткие диски нужны для серверов. Для сравнения — на рабочих станциях обычно используются жесткие диски с частотой вращения шпинделя 7200–7500 RPM. В этом случае IOPS будет равен всего 70.

Соответственно, 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 SSD-дисков. Однако следует учитывать, что время наработки на отказ у них ниже, чем у обычных жестких дисков, и заменять такие диски придется чаще. Учитывая стоимость SSD-дисков большого размера (от 500 Гбайт), это удовольствие не из дешевых.

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 PC3-<число>. Например, стандарт PC3-12800 означает, что эффективная пропускная способность составляет 12 800 Мбайт/с. Все модули должны быть одного стандарта. Если у вас установлены модули PC3-19200, а вы докупите один модуль PC3-12800, то затормозите работу всей системы. Аналогично, если у вас установлены модули PC3-12800, не следует думать, что если вы добавите модули PC-19200, то вырастет производительность подсистемы памяти. Она останется неизменной. Вырастет просто объем ОЗУ;
- **частоту памяти** — она измеряется в мегагерцах, и обычно можно сказать, что чем больше этот параметр, тем лучше, но и это не всегда так. Нужно, чтобы ма-

теринская плата поддерживала выбранную вами частоту. Если, например, вы купите модули памяти, работающие на частоте 3200 МГц, но поспешите на 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. Модули будут работать, но на частоте материнской платы — 2133 МГц;

- **режим работы оперативной памяти** — это характеристика не модулей памяти, а материнской платы. Здесь вам нужно обратиться к руководству по материнской плате. Например, у вас может быть два слота для оперативной памяти, а ее режим работы — двухканальный (Dual-channel architecture). Следовательно, для получения полной отдачи вам нужно установить два одинаковых модуля (одинакового стандарта, емкости и частоты, желательно одного производителя). Если вы установите один модуль емкостью 16 Гбайт, то он будет работать медленнее, чем два по 8 Гбайт.

Аналогично, бывают и трехканальный, и четырехканальный режимы работы. Для работы в трехканальном режиме вам потребуются три одинаковых модуля, которые, возможно, нужно будет установить в определенные слоты (обычно они отмечены разными цветами — обратитесь к документации по материнской плате). 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 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. Оборудование без поддержки SNMP допустимо выбирать в самых простых случаях и для самых малых организаций.

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 зарядки и оставшемся времени автономной работы.

Состав программного обеспечения типовой организации

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 1С, другие — нет. Одним предприятиям требуется CRM¹, 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 организации);
- подсистема электронной почты.

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

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 используется 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 2012. Возможно участие Linux-систем и в домене Active Directory.

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.

Поэтому, если в вашей организации 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 протокола Kerberos. Поскольку в современных версиях Windows используется именно Kerberos, то для подключения Linux-клиентов рекомендуется задействовать именно его.

Здесь мы рассмотрим настройку гипотетического Linux-клиента. В вашем дистрибутиве настройки могут быть несколько иными — например, могут 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 этого 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. Если же вы будете знать, что и в каком конфигурационном файле находится, графические конфигураторы вам вообще не понадобятся.

Файл конфигурации Kerberos обычно называется `/etc/krb5.conf`. В этом файле нужно изменить параметры доменной зоны (`realm`) и службы Kerberos — центра выдачи ключей KDC (Key Distribution Center, Центр распределения ключей):

```
[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 домена¹. 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

После редактирования конфигурации 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
```

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:

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

```
[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, что служба winbind успешно получает пароли с контроллера домена (командой: `getent passwd`) — 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 лицензии 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. По состоянию на сегодня русская версия Windows Server Standard 2012 R2 на 10 клиентов стоит 78 тыс. рублей, которые можно было бы сэкономить. Мы уже молчим о размере экономии, если количество клиентов превышает 10.

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

В любой организации не обходится без общих папок с документами. В Windows для доступа к общим папкам и принтерам служит протокол SMB (Server Message 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, — например, продуктами фирмы CyberSoft (<http://cybersafesoft.com/rus/>).

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

Основной файл конфигурации Samba называется `/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 выбрать 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 поставляется браузер Internet Explorer. Он считается одним из самых популярных, но это не его заслуга — своей популярностью Internet Explorer обязан тому, что поставляется в составе Windows.

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 systems);
- контроль приложений (блокировка запуска нежелательных приложений) и устройств (блокировка доступа к устройству).

В Linux используется ряд систем контроля доступа, такие 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 корпоративной среды можно отметить и сугубо корпоративные решения — например, Symantec Endpoint Protection (рис. 2.3).

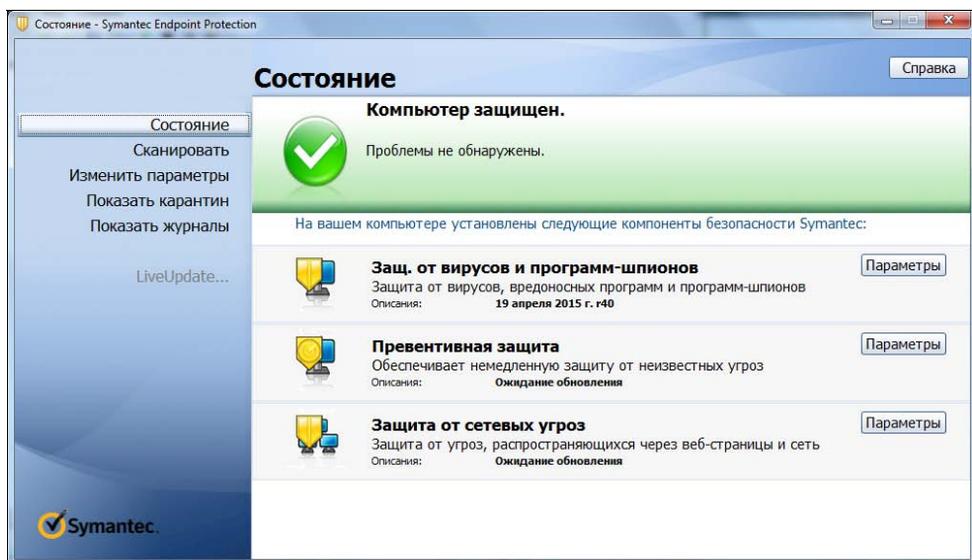


Рис. 2.3. Symantec Endpoint Protection

Средства удаленного администрирования

В компаниях средних и больших размеров администратору гораздо удобнее удаленно настраивать компьютеры пользователей. При этом администратору не требуется лично подходить к компьютеру, что значительно повышает оперативность его работы и оптимизирует использование рабочего времени.

Для удаленного администрирования можно применять различные средства, в том числе RDP (удаленный рабочий стол). Также довольно популярна программа TeamViewer, которая бесплатна для личного пользования (рис. 2.4).

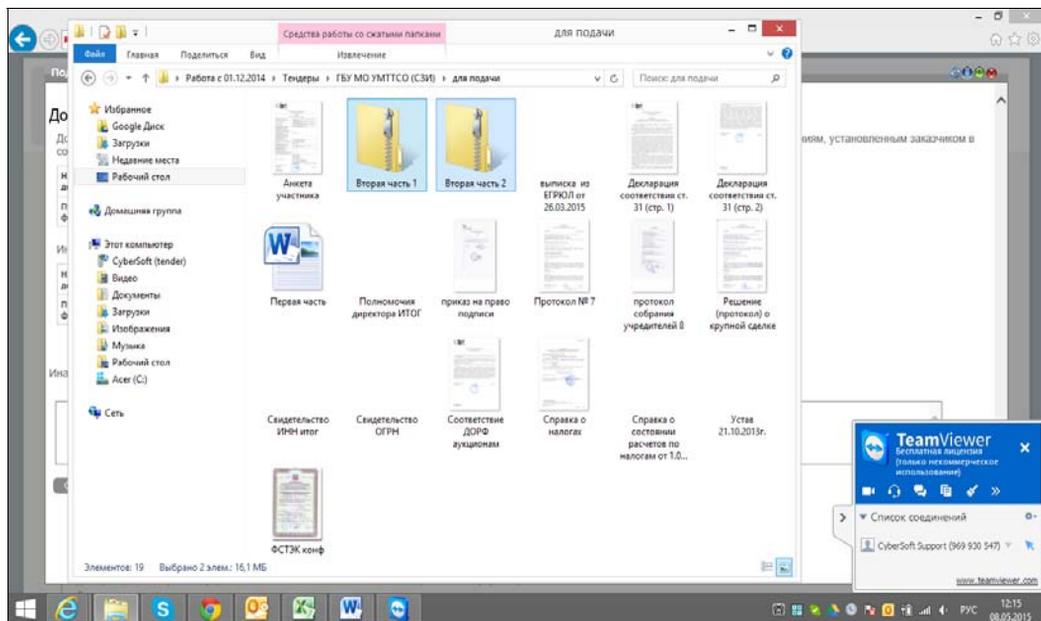


Рис. 2.4. Сеанс подключения по TeamViewer

Средства резервного копирования

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

Именно поэтому важна система резервного копирования, которая копирует 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 (рис. 2.5).

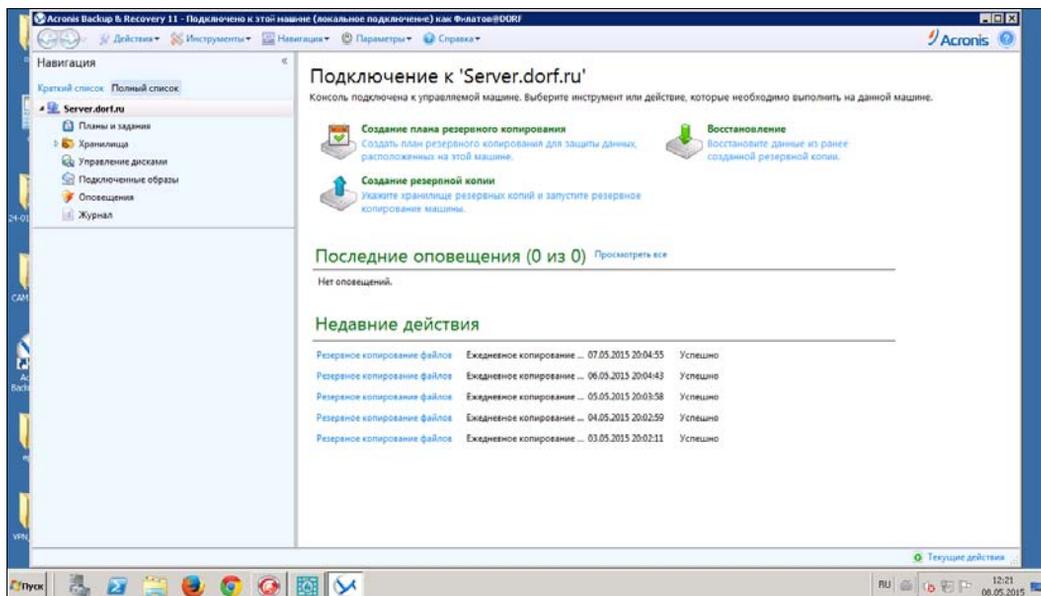


Рис. 2.5. Программа Acronis Backup & Recovery

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

- *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;
- *поддержка прикладных программ, эксплуатируемых в организации*, — корпоративная программа резервного копирования должна выполнять задачу сохранения данных для всех программ, которые используются в организации. Это касается серверов баз данных, почтовых программ различных производителей, ERP-систем¹, 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.

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

- *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 такая функциональность доступна самим пользователям, чтобы они не привлекали администраторов для решения указанных 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)* — в большей части организаций 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 к себе: специальных условий хранения, периодических перемоток и т. п. Поэтому ленточные библиотеки применяются только в крупных организациях или в специализированных целях;

- *дедупликация данных (опционально)* — технология дедупликации подразумевает исключение дублирования хранимых данных. Данные разбиваются на блоки, для них вычисляется хэш-функция. И если выполняется попытка записи нового блока, который уже совпадает с тем, что хранится в системе (совпадают значения хэш-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 организации должно создаваться и храниться много промежуточных копий (например, если требуется сохранять ежедневные копии в течение месяца).

Такие возможности специфичны для каждого продукта.

Офисный пакет

Любой организации нужен пакет офисных приложений: текстовый процессор, электронная таблица, средство для создания презентаций и т. д. Наличие офисного пакета стало стандартом. При покупке ПК уже никто и не задумывается — покупать 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 OS X можно по адресу <https://www.openoffice.org/download/>, и LibreOffice, который для тех же операционных систем предлагает скачать сайт <https://ru.libreoffice.org/>. Надо так-

же отметить, что офисный пакет LibreOffice входит в состав большинства дистрибутивов 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 Apache OpenOffice, в состав которого входят следующие приложения:

- текстовый процессор OpenOffice.org.Writer (аналог Microsoft Word);
- редактор формул OpenOffice.org.Math (в пакете Microsoft Office используется как встроенный объект);
- редактор рисунков OpenOffice.org.Draw;
- редактор электронных таблиц OpenOffice.org.Calc (аналог Microsoft Excel);
- редактор презентаций OpenOffice.org.Impress (аналог Microsoft PowerPoint).

Интерфейс OpenOffice (рис. 2.6) напоминает интерфейс старого доброго Microsoft Office 2003. На наш взгляд, этот интерфейс более удобен и привычен пользователям, чем интерфейс нового Microsoft Office 2013, и эти строки сейчас написаны именно в OpenOffice.

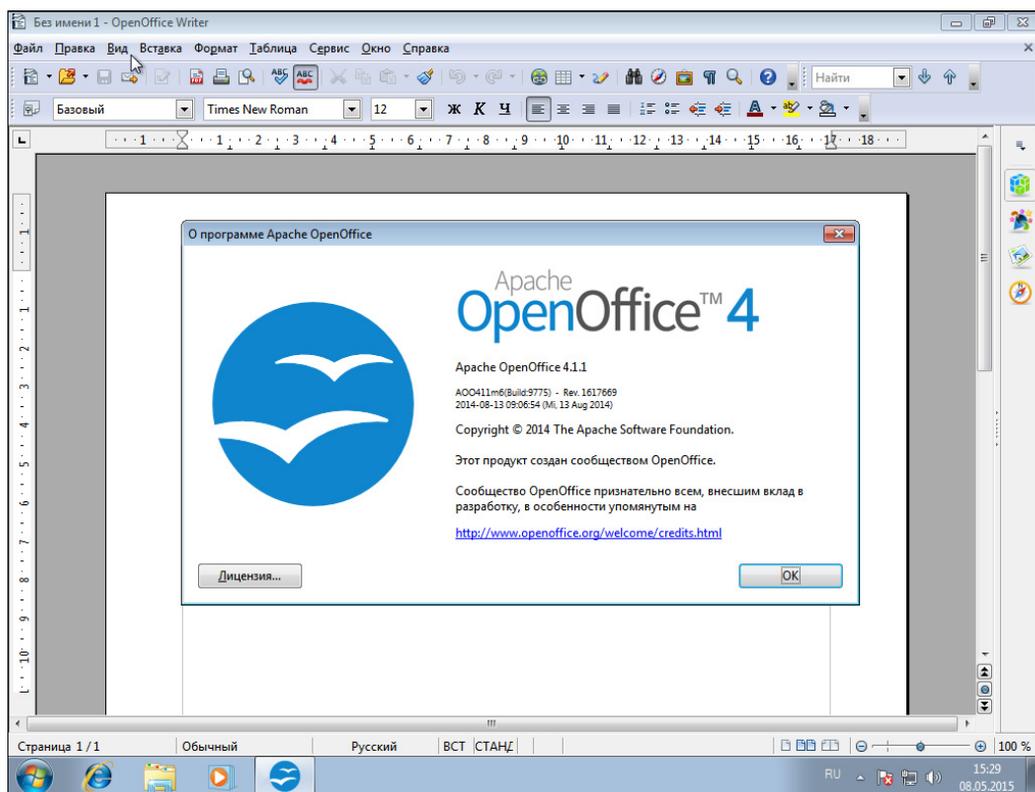


Рис. 2.6. Интерфейс OpenOffice

OpenOffice поддерживает форматы даже самого последнего MS Office 2013. Конечно, не все так гладко — если ваши документы содержат сценарии, написанные на Visual Basic, то вам все же придется установить (купить) MS Office.

Электронная почта

Если для индивидуального пользователя часто достаточно почтового ящика на любом из бесплатных серверов Интернета, то серьезность организации 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.) — что зависит от конкретных условий.

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 можно вести календарь, а если в качестве клиента использовать обозреватель Google Chrome, 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.

ПРИМЕЧАНИЕ

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

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

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 — так же 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 организациям. В то же время существует ряд бесплатных продуктов, поддерживающих возможности групповой работы, — в частности, это:

- 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. 2.7.

В Zimbra Collaboration Suite Open Source Edition реализованы, например, следующие возможности (рис. 2.8):

- 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.

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

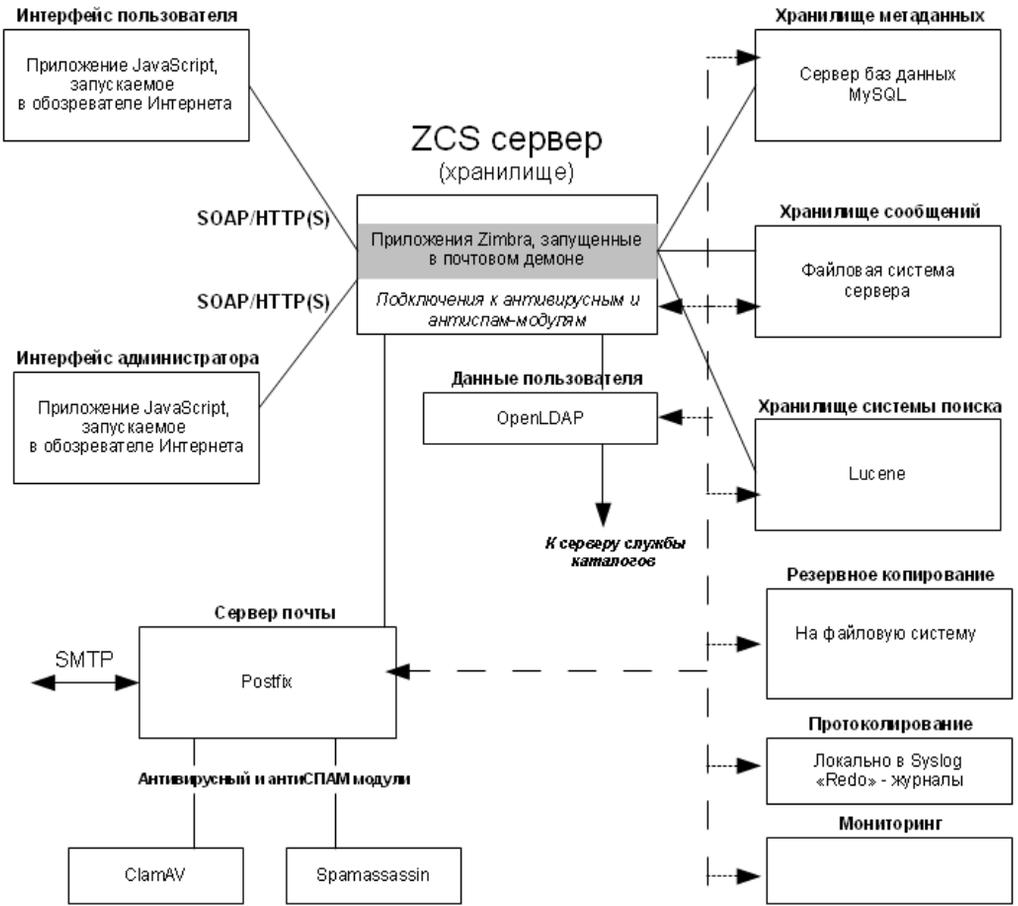


Рис. 2.7. Архитектура ZCS

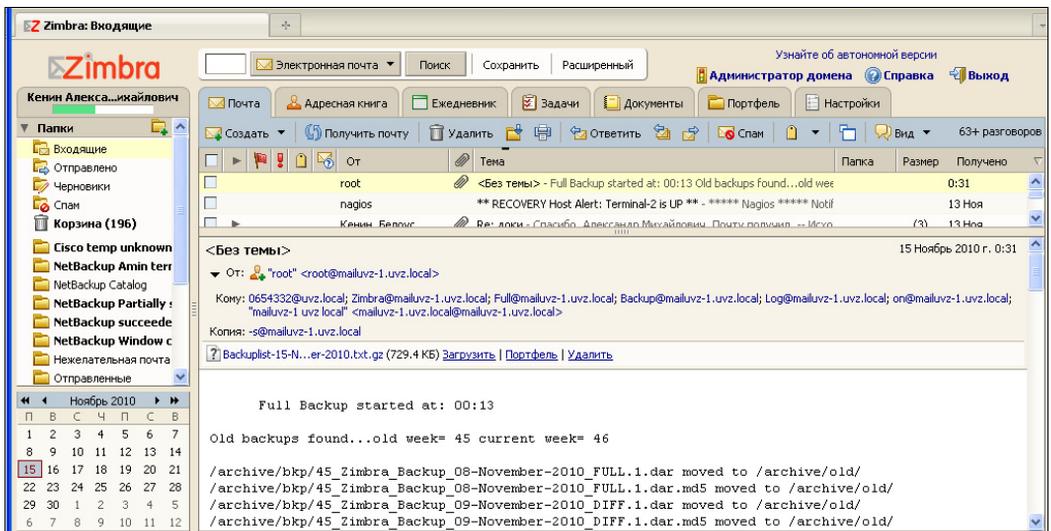


Рис. 2.8. Пример веб-интерфейса ZCS

Работать с ZCS по стандартным почтовым протоколам (POP3, IMAP, HTTP/HTTPS, SMTP/SMTPTS) 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 (если вдруг кому захочется скачать нелегальные программы с пиратских ресурсов).

В табл. 2.3 приведен список некоторых бесплатных программ. В большинстве случаев свободное программное обеспечение является кроссплатформенным, 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 2.3. Перечень некоторых бесплатных программ для Windows

Название и соответствующий сайт	Описание
OpenOffice, http://www.openoffice.org/	Популярный офисный пакет, включающий текстовый процессор, электронную таблицу, средство для создания презентаций и работы с базами данных. Является аналогом Microsoft Office и поддерживает форматы документов Microsoft Office
Firefox, http://www.firefox.com/ Google Chrome, http://www.google.ru/chrome?hl=ru	Бесплатные браузеры — являются самыми популярными браузерами в мире и доступны для разных операционных систем
GIMP, http://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, http://www.freecommander.com/	Двухпанельный файловый менеджер, созданный по образу и подобию широко известного в недавнем прошлом Norton Commander
7Zip, http://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
CCleaner, http://www.ccleaner.com/	Очень мощная программа для чистки реестра