

# ■ ALT Linux 4.0 Server

- Виртуализация
- Удобство настройки и сопровождения
- Поддержка аппаратных платформ x86 и x86-64



**Виртуальный сервер одним нажатием кнопки**

Наличие в комплекте готовых профилей для создания виртуальных серверов позволяет быстро организовать выполнение наиболее распространённых задач.

Благодаря своим возможностям ALT Linux 4.0 Server обеспечит надёжное и безопасное функционирование корпоративных сетей.

Гарантированный срок поддержки дистрибутива: 3 года



[www.altlinux.ru](http://www.altlinux.ru)  
[sales@altlinux.ru](mailto:sales@altlinux.ru)

№6(55) июнь 2007

# системы администратор

№6(55) июнь 2007  
подписной индекс 20780  
[www.samag.ru](http://www.samag.ru)

**Не допустите потери данных!**  
**К вашим услугам**  
**ленточная библиотека**

**Как настроить ATC Samsung:**  
**первые шаги**

**Разворачиваем кластер**  
**Microsoft Exchange**

**Строим сетевую инфраструктуру**  
**для системы 1С:Предприятие**

**Антивирус+Антиспам Dr.Web**  
**для почтовых серверов UNIX**

**Система анализа квот на базе**  
**File Server Resource Manager**

**FreeBSD: особенности**  
**сборки ядра**

**Тестируем дистрибутив**  
**ALT Linux 4.0 Server**





ВОСЕМНАДЦАТАЯ ЕЖЕГОДНАЯ ВЫСТАВКА

# ИНФОРМАЦИОННЫХ И КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ

При поддержке:

Российской Академии Наук, Федерального агентства по науке и инновациям, Федерального агентства по информационным технологиям

# SoftTool

www.softtool.ru

• 2 - 5 октября 2007 года • Москва, ВВЦ •



ИНФОРМАЦИОННАЯ  
БЕЗОПАСНОСТЬ

ТЕХНОЛОГИИ  
УПРАВЛЕНИЯ

DOCFLOWDAY

электронное  
обучение



LinuxLand

8-ая научно-практическая конференция

## "Информационные технологии в России"

**Вам трудно разобраться в современном  
мире информационных технологий?**

# SoftTool – форум профессионалов

**Мы поможем Вам сделать правильный выбор!**

Организатор:  
(495) 624-7072/4556  
softtool@garnet.ru



VELES DATA  
COMPUTER CENTER

Autodesk

ОТКРЫТЫЕ  
СИСТЕМЫ  
Open Systems Publications

РУССКАЯ  
ПРОМЫШЛЕННАЯ  
КОМПАНИЯ

Так видит журнал читатель, который забыл оформить подписку:



Так видит журнал читатель, оформивший подписку:



# ПОДПИШИТЕСЬ И ЧИТАЙТЕ!

Роспечать – 20780, 81655  
Пресса России – 87836  
Интер-почта – тел. (495) 500-00-60



**3 ТЕНДЕНЦИИ****РЕПОРТАЖ****4 Конференция RHPCONF с каждым годом становится успешнее**

Итоги шестой международной конференции «Современные технологии эффективной разработки веб-приложений с использованием PHP».

**Дмитрий Горяинов**  
dmitry.goryainov@gmail.com

**6 Open Source вновь в центре внимания на Interop Moscow**

Во второй раз в Москве прошла международная выставка-конгресс информационных технологий для бизнеса Interop Moscow 2007. Как и в прошлом году, одной из ключевых тем обсуждения стало программное обеспечение с открытым кодом.

**Дмитрий Шурупов**  
osa@samag.ru

**АДМИНИСТРИРОВАНИЕ****8 FreeBSD: некоторые особенности сборки ядра**

Сборка собственного ядра на сервере – это почти обязательный ритуал для каждого системного администратора. Сегодня мы расскажем о том, как это делать быстрее и эффективнее.

**Сергей Супрунов**  
amsand@rambler.ru

**12 Не допустите потери данных! Ленточная библиотека к вашим услугам**

Руководство по созданию системы резервного копирования.

**Виталий Банковский**  
smartcgi@gmail.com

**22 Доступ к Active Directory с помощью прилинкованного SQL-сервера**

Скорость получения данных из AD с помощью штатных средств в сценарии оставляет желать лучшего. Одно из решений проблемы – использовать прилинкованный SQL-сервер.

**Иван Коробко**  
ikorobko@prosv.ru

**28 Разворачиваем кластер Microsoft Exchange**

Один из наиболее распространенных способов обеспечить отказоустойчивость сервиса электронной почты – кластер Microsoft Exchange.

**Андрей Бирюков**  
mex\_inet@rambler.ru

**34 Строим сетевую инфраструктуру для системы 1С:Предприятие**

Предлагаем решение на базе сервера терминалов в Windows Server 2003 с использованием 2X Application Server.

**Сергей Алаев**  
alaev777@mail.ru

**40 Система анализа квот на базе File Server Resource Manager**

В Windows Server 2003 RC2 появился инструмент, позволяющий назначать квоты на использование дискового пространства серверов – File Server Resource Manager.

**Иван Коробко**  
ikorobko@prosv.ru

**46 Vyatta – Linux-дистрибутив для роутеров**

Компания Vyatta анонсировала вторую версию разрабатываемого ею дистрибутива, позволяющего превратить обычный ПК в маршрутизатор.

**Сергей Яремчук**  
grinder@ua.fm

**50 ALT Linux 4.0 Server: что день грядущий нам готовит?**

Тестируем новый серверный дистрибутив от компании ALT Linux.

**Дмитрий Шурупов**  
osa@samag.ru

**ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ****54 Антивирус+Антиспам Dr.Web для почтовых серверов UNIX**

Когда начинаешь тонуть под наплывом спама и вирусов, хватаешься за каждую соломинку... Но зачем полагаться на соломинку, когда к вашим услугам настоящий спасательный круг?

**Сергей Супрунов**  
amsand@rambler.ru

**IP-ТЕЛЕФОНИЯ****56 Развертываем корпоративную телефонную сеть на основе технологии VoIP. Часть 1**

Даже простая настройка ATC Samsung – занятие весьма нетривиальное. Программа-конфигуратор чрезвычайно неудобна и весьма недружественна. Опыт Рашида Ачилова поможет освоиться с основами программирования ATC Samsung немножко быстрее.

**Рашид Ачилов**  
achilov-rn@askd.ru

**ЧЕЛОВЕК НОМЕРА****64 СМИ уровня 2.0**

Благодаря аналитику Михаилу Елашкину я решила стать представителем этого вида средств массовой информации.

**Оксана Родионова**  
rodion@dol.ru

**WEB****68 Система аутентификации веб-пользователей WebAuth**

Как обеспечить надежность аутентификации пользователей.

**Сергей Яремчук**  
grinder@ua.fm

**ПРОГРАММИРОВАНИЕ****76 Организуем доступ к базам данных при разработке кроссплатформенных приложений на C++/wxWidgets**

Написание кроссплатформенных приложений на C++, использующих для своей работы базы данных, не является непосильной задачей.

**Владимир Тряпичко**  
t-rex@mail.zp.ua

**РЕТРОСПЕКТИВА****86 Судебные войны: берегай своё, не посягай на чужое. Часть вторая – программная**

Так уж повелось, что, в отличие от мира аппаратного обеспечения, судебные разбирательства между компаниями, занимающимися разработкой программных продуктов, проходят намного ожесточеннее, да к тому же длятся значительно дольше. А уж суммы результирующих штрафов и вовсе сводят с ума. За примерами далеко ходить не надо.

**Дмитрий Мороз**  
akuji@list.ru

**92 КНИЖНАЯ ПОЛКА****74, 75 BUGTRAQ**



Полное собрание сисадминов!

II

# Всероссийский Слет системных администраторов

Последние выходные июля 2007.  
На том же месте, в тот же час!

Подробности и регистрация — на сайте <http://sysadmin.mail.ru>



Так  
прошел  
◀ слет-2006



## Открыт код Open Sound System

14 июня компания 4Front Technologies, разработчик Open Sound System (OSS), системы поддержки аудио для UNIX и Linux, открыла доступ к исходному коду продукта.

На «информационном сайте для разработчиков» Open Sound System (<http://developer.opensound.com/sources>) появился исходный код OSS под лицензиями GNU GPLv2 (для Linux) и CDDL 1.0 (для Solaris, \*BSD). Такое разделение было сделано специально, поскольку авторы считают, что GPL может оказаться неприемлемой для сообществ сторонников лицензии BSD. Не допускается смешивания файлов из пакетов Open Sound System с разными лицензиями.

Исходный код Open Sound System теперь также доступен и для закрытых операционных систем вроде SCO UnixWare/OpenServer, однако пользователям этих ОС для легального использования OSS необходимо купить коммерческую лицензию от 4Front Technologies.

## Solaris может привести Linux к GPLv3

В своем сообщении в почтовую рассылку для Linux-разработчиков Линус Торвалдс (Linus Torvalds), автор ядра Linux, говорит о том, что ОС Solaris может инициировать переход Linux-ядра на новую готовящуюся версию лицензии на свободное программное обеспечение – GNU GPLv3.

«Если Sun действительно собирается выпустить OpenSolaris под GPLv3, это может стать хорошей причиной» для перехода Linux на новую лицензию, заявил Торвалдс.

«Не думаю, что GPLv3 – такая же хорошая лицензия, как и GPLv2, но, с другой стороны, я прагматик, и если мы можем избежать ситуации с существованием двух ядер, распространяющихся под разными лицензиями, и с вызванными этим разногласиями, я по крайней мере вижу причину для перехода на GPLv3», – пояснил свою позицию главный разработчик Linux-ядра.

До этого Торвалдс уже выражал свое недовольство новой версией лицензии GNU GPL, однако после появления последнего чернового варианта GPLv3 стал лучше относиться к этому проекту. Несмотря на это, сам он до сих пор отдает предпочтение GPLv2.

## Патентные угрозы Microsoft разделили мир Open Source

В середине мая Брэд Смит (Brad Smith) из Microsoft «напомнил», что программное обеспечение с открытым кодом в совокупности нарушает 235 патентов его корпорации. При этом никакой конкретной информации о том, что именно нарушается, не сообщалось.

Вскоре Microsoft, руководствуясь опытом заключения сделки с Novell, удалось достичь договоров о сотрудничестве с другими Open Source-поставщиками, среди которых оказались Xandros и Linspire. При этом основой новых договоров стало обеспечение корпорацией Microsoft своим «союзникам» защиты от возможных патентных проблем.

Другие же производители Linux-дистрибутивов отреагировали обратным образом. Представители Red Hat,

Canonical (Ubuntu) и Mandriva объявили о том, что не желают обсуждать с Microsoft вопросы возможного заключения лицензионных соглашений.

«Полагаясь на то, что нам удалось наблюдать, в договоре мы не заинтересованы. Мы продолжаем верить в то, что Open Source и его инновации не должны быть предметом для необоснованных и непонятных поборов», – сообщила Лэй Дэй (Leigh Day) из компании Red Hat.

Марк Шаттлворт (Mark Shuttleworth), глава компании Canonical Ltd, занимающейся поддержкой Ubuntu Linux, высказал схожую позицию. Он заявил об «отказе от обсуждения любых договоров с Microsoft под угрозой непонятных патентных нарушений», добавив, что не видит никакой необходимости защищать пользователей Ubuntu от подобных сомнительных притязаний Microsoft.

Франсуа Бансильон (Francois Bancelhon), исполнительный директор Mandriva, так прокомментировал происходящее в своем блоге:

«... Не было ни одного конкретного доказательства того, что Linux и приложения с открытым кодом нарушают какие-либо патенты. Поэтому мы считаем, что, как и при любой демократии, люди не виновны, пока их вина не доказана, и мы можем продолжать добросовестно работать.

Так что мы не видим необходимости в том, чтобы получать прикрытие от Microsoft для выполнения работы или платить за подобную защиту кому-либо».

*Составил Дмитрий Шурупов  
по материалам [www.nixp.ru](http://www.nixp.ru)*



**безопасное хранение данных**

### Zserver Suite

Риск несанкционированного физического доступа к серверам и резервным копиям намного выше, чем кажется. Беспечность в этом вопросе приводит к утечке информации и другим нежелательным последствиям.

Шифрование носителей информации – это наиболее гибкий и надежный способ защитить данные и избежать возможных проблем.

Задумайтесь о защите носителей информации!

[www.securit.ru](http://www.securit.ru)  
+7 495 221 2160

# Конференция PHPCONF с каждым годом становится успешнее



**24-25 мая в Москве прошла 6-я международная конференция «Современные технологии эффективной разработки веб-приложений с использованием PHP». В качестве места проведения на этот раз был выбран конференц-зал ММТС-9, известной как «М9».**

**П**о доброй традиции организаторы конференции: международный клуб разработчиков PHPCLUB (<http://phpclub.ru>), специализированный учебный центр в области современных IT и веб-технологий PHPCenter (<http://phpcenter.ru>) и электронный журнал для веб-разработчиков PHP{INSIDE} (<http://phpinside.ru>) в очередной раз постарались превзойти самих себя. В отличие от множества широко рекламируемых конференций, PHPCONF по-прежнему сохраняет атмосферу дружеской компании и определенную непринужденность.

Так, вместе с дежурным комплектом раздаточных материалов каждый из участников в этот раз получил... небольшую подушечку с логотипом конференции.

## Лицом к залу, день первый

Во вступительном слове Александр Смирнов (основатель <http://phpclub.ru> и активный участник движения за качественное веб-программирование и повышение квалификации разработчиков) развил тему непринужденного общения в рамках конференции. Помимо официальной части, организаторы предложили участникам в перерывах между докладами живое общение с экспертами и докладчиками в формате флипчартов. Такой вариант неформального общения оказался очень удачным. Настолько, что иногда организаторы были вынуждены настоятельно просить участников вернуться в зал и послушать, наконец, следующий доклад.

Чем же «потчевали» в официальной до-докладной части? Дмитрий Шей-

ко, ведущий программист Red Graphic Systems, взял на себя нелегкую долю быть первым, выступил с докладом «Практика разработки корпоративных веб-приложений-2007». Несмотря на слегка обобщенный характер поданного материала, выступление Дмитрия получилось довольно живым и энергичным. Он сумел поговорить и о современных тенденциях в интернет-решениях, и об их применении к системам масштаба предприятия.

Павел Шевелев, основатель проекта <http://agiledev.ru>, посвященного методам гибкой разработки ПО, и ведущий разработчик проекта Limb (<http://limb-project.com>), предложил залу в качестве допущения вопрос о том, что было бы, если бы мы с вами жили в идеальном мире, повел речь об аспектно-ориентированном программировании (АОП) в PHP. Боюсь, что этот допуск об «идеальном мире» несколько потерялся из виду. Слушатели так увлеклись, что, кажется, испытали некоторое разочарование от прозвучавших под конец проблемах с практическим использованием. А зря. Стоит пояснить, что концепция АОП применительно к PHP-платформе пока находится ближе к уровню модели, чем к практической применимости. И сама концепция АОП требует несколько иного подхода к разработке проектов с тем, чтобы приложение аспектов было оправданным.

Сергей Антонинко, технический директор Umisoft (<http://umisoft.ru>), одного из спонсоров конференции, прочитал один из самых доходчивых докладов о применении технологии memcache. Части слушателей доклад показался слишком простым, но лично мне эта выбранная докладчиком простота изложения материала показалась достойной всяческого уважения.

Следующего докладчика зал встретил овациями, ибо на сцене появился автор веб-сервера nginx Игорь Сысоев. Доклад Игоря был посвящен разработке модулей под nginx. Послушать советы по этой теме от самого автора сервера удается нечасто и чрезвычайно полезно. Правда, лично меня ждало некоторое разочарование: отловив Игоря после доклада в кулуарах, я не мог удержаться от вопроса о том, можно ли в принципе заставить nginx работать с разными location от разных пользователей? И увы, мне при-



шлось услышать четкое «нет» от автора. А жаль, жаль.

После такого серьезного погружения в серверную часть нам всем предложили взглянуть на интернет-технологии с другой стороны. Андрей Иванников решил оживить вечную тему «PHP & Flash, новая альтернатива для создания Rich Internet Applications». Вообще тема Flash и всего с ним связанного подается как «новая альтернатива» уже лет так пять, и лично мне иногда напоминает старый анекдот, где смеяться надо после слова «лопата». Но именно к докладу Андрея Иванникова это не относится. На этот раз речь шла об Adobe Flex2. Это решение, родственное и основанное на Flash, прежде всего ориентировано на проектирование интерфейсов, способных «прокручиваться» на клиенте при помощи уже традиционного Flash Player и взаимодействовать с приложениями на стороне сервера. Доклад, по-моему, получился вполне конкретным и имеющим практическую ценность не только для поклонников интернет-мультипликации.

Еще один «взгляд с другой стороны» представил главный редактор электронного журнала PHP{INSIDE} Андрей Олищук. Назвав свой доклад «Практика независимой веб-разработки», Андрей постарался втиснуть в отведенные регламентом рамки довольно объемную сагу о том, что же такое и как оно быть автономным freelance? Надо отдать Андрею должное: очень четко оставив в сторону типичную подработку, время от времени он говорил о реалиях работы «частного специалиста fulltime». С чем приходится сталкиваться, какие нюансы учитывать, как организовывать свою работу и свои взаимоотношения с заказчиком?

## День второй, продолжая традиции

Следующий день конференции был в чем-то проверкой организаторов на прочность. Заполучив в прошлом году в качестве гостей и докладчиков самого автора PHP Расмуса Лердорфа (Rasmus Lerdorf) и такую яркую фигуру в PHP Core Team, как Андрей Змиевский (Andrei Zmievski), организаторы в этом году выставили в роли приглашенной знаменитости маститого Дерика Ретанса (Derick Rethans). Помимо того что Дерик – автор Xdebug, он по сути



Представитель компании MySQL ведет демонстрацию работы целого кластера MySQL NDB на одном ноутбуке

является сейчас чуть ли не единственным мантейнером постепенно заменяемой 4-й версии PHP. Доклад «Раскрывая секреты PHP, или Как все работает внутри» прежде был интересен не только оценкой применимости и выгоды использования оптимизаторов, но также затронул механизмы и особенности поведения интерпретатора.

В этом году главным спонсором конференции выступила компания Microsoft. А ее полномочным представителем на конференции стал Дрю Роббинс (Drew Robbins) – эксперт по технологиям разработки программного обеспечения. Успокоив собравшихся заявлением о том, что нет, Microsoft не планирует поглощать Zend Corporation и подменять PHP на какой-нибудь Visual PHPScript, м-р Роббинс в очень изящной манере устроил показательную демонстрацию использования PHP под управлением MS IIS 7. Пишу это без всякой иронии, поскольку конфигурационные возможности и умение подхватывать изменение настроек на лету в новой версии сервера интернет-приложений от Microsoft действительно произвели впечатление.

После такой усиленно-показательной международной части конференция плавно вернулась на круги своя, к обсуждению технологий.

Прозвучал доклад о микроформатах. Да, семантика в разметке должна рано или поздно прийти и проявиться. Но насколько она может найти практическое применение уже сейчас? И глав-

ное, найдется ли ей место не в специфических или ориентированных на IT-специалистов проектах, а в массе?

Два взгляда на традиционное взаимодействие через формы были представлены в докладах Александра Владимировича Анохина, начальника бюро экспертизы интернет-проектов ОАО «АвтоВАЗ», и Дмитрия Котерова, наверное, более всего известного как автора книг «Самоучитель PHP4» и «PHP». Еще одним практичным докладом стал доклад того же Анохина о применении служб LDAP.

## Лучше, чем другие

Что же можно сказать в завершение? PHPCONF продолжает сохранять атмосферу непринужденного клубного общения, выгодно отличаясь от конференций формата «кто есть кто». При этом уровень представительства, формат проведения и уровень докладов каждый раз приятно удивляют. Великолепная идея флипчартов, предложенная и успешно реализованная организаторами, оставила только одно ощущение: да, именно так и надо проводить конференции для разработчиков. Два (а для участников мастер-классов – все пять) дня полного погружения в среду активного обсуждения и обмена мнениями оставили очень позитивные ощущения. Так держать, и до встречи в следующем году! 🌀

Текст: Дмитрий Горяинов,  
фото: Сергей Чеперис

# Open Source вновь в центре внимания на Interop Moscow

30 и 31 мая в Москве, в комплексе «Форум Холл», во второй раз прошла международная выставка-конгресс информационных технологий для бизнеса Interop Moscow 2007. Как и в прошлом году, одной из ключевых тем обсуждения стало программное обеспечение с открытым кодом.

## Open Source Forum @ Interop

Все мероприятия, посвященные программному обеспечению с открытым кодом, были проведены в рамках «Третьего форума по открытому коду» (III Open Source Forum), который проходил в течение первого дня Interop.

Если на Interop 2006 были такие видные мировые деятели Open Source, как Йон Холл (Jon «maddog» Hall), Ян Мердок (Ian Murdock), Виетс Винема (Wietse Venema) и Марк Спенсер (Mark Spencer), то и в этом году состав зарубежных гостей не разочаровал. Среди них были:

- Брайен Белендорф (Brian Behlendorf), один из родоначальников веб-сервера Apache, ныне технический директор CollabNet;
- Льюис Суаре-Поттс (Louis Suarez-Potts), старший менеджер сообщества OpenOffice.org (с 2000 года);
- Эрик Олман (Eric Allman), автор Sendmail.

Из наших соотечественников можно выделить присутствие Алексея Смирнова и Алексея Новодворского из компании ALT Linux, Александра Давыдова из NAUMEN.

## Ключевой доклад Белендорфа

Брайен Белендорф – не только один из авторов самого распространенного веб-сервера, но и заметная фигура в сообществе Open Source ([http://en.wikipedia.org/wiki/Brian\\_Behlendorf](http://en.wikipedia.org/wiki/Brian_Behlendorf)). Поэтому именно он и открыл Open Source Forum @ Interop, выступив с докладом «10 вещей об Open Source, которых вы могли не знать».

Основные моменты, которые докладчик обозначил в сообщении, таковы:

1. Программное обеспечение с открытым кодом появилось раньше проприетарного. Здесь следует разделять Open Source и Free Software: последнее появилось намного позже (организация Ричарда Столлмана Free Software Foundation стартовала лишь в 1985 году).
2. Проекту Apache удалось сохранить свободу глобальной сети Интернет. Потому что на начальных этапах его разработки существовала опасная вероятность, что какому-нибудь одному поставщику удастся стать мировым диктатором в этой области, имея в своем распоряжении доминирующий набор базовых интернет-приложений: веб-браузер и сервер.
3. Проект OpenSSL обеспечил всеобщую доступность криптографии.
4. ПО с открытым кодом помогло сохранить свободу генома человека. Благодаря усилиям одного Perl-программиста был опубликован исходный код скрипта, реализующего сложные математические расчеты над необработанными данными, необходимыми для установления последовательности генов человека. Иначе эта процедура была бы запатентована коммерческим консорциумом Celera.
5. Microsoft любит Open Source. Автор сослался на известный факт о том, что MS заимствовала для Windows код TCP/IP от разработчиков из Беркли, а также на ее сотрудничество с такими Open Source-проектами, как MySQL, SugarCRM и JBoss.
6. Альтруизм не служит единственным мотивирующим фактором для создания Open Source. Хотя бы потому, что многие разработчики ПО с открытым кодом используют его в своей профессиональной деятельности.
7. Online-сообщества действительно могут решать конкретные задачи. Несмотря на то что такое международное сотрудничество бывает склонно к хаосу, этот подход зачастую способствует эффективным разработкам.
8. Самая важная свобода – возможность ответвления (fork), создания собственной версии того или иного Open Source-продукта на базе опубликованного кода.
9. Open Source все еще может изменить мир. В качестве примеров были приведены проект дешевых ноутбуков для детей в развивающихся странах OLPC (One Laptop Per Child) и развернувшаяся борьба с технологиями управления авторскими правами (DRM).
10. Программное обеспечение с открытым кодом нуждается в вашей помощи (и не важно, кто вы). Призыв достаточно всеобъемлющий:



Льюис Суаре-Поттс



используйте Open Source, участвуйте в разработке, сообщайте о найденных ошибках, помогайте с переводом интерфейсов и документации...

## Интервью с зарубежными гостями

За ключевым докладом последовало общение трех иностранных Open Source-гуру с публикой. В качестве ведущего «интервью» выступал Дмитрий Дмитриев из отечественной компании Линукс Инк.

Им и были заданы несколько первых вопросов. В частности, он спросил у гостей, почему Open Source-проекты обычно занимают позицию догоняющего, заимствуя инновации у проприетарных аналогов. Ни один из гуру не смог согласиться с такой позицией. В том числе и Суаре-Поттс – несмотря на настойчивые утверждения Дмитриева, что OpenOffice.org появился после Microsoft Office, вобрав в себя многие его черты.

Среди затронутых общественностью проблем запомнился вопрос о том, как привлечь разработчиков к начинающему Open Source-проекту.

Здесь отличился Белендорф, лаконично ответивший, что подобные инициативы обречены на гибель, поэтому не стоит их даже пытаться начинать. Аргументируя эту позицию, он добавил, что перед тем как создавать Open Source-проект, полезно предварительно ознакомиться с уже существующими и помочь одному из них. В ином случае мир программного обеспечения с открытым кодом будет расти в количественном, но не качественном отношении.

На протяжении всей дискуссии Суаре-Поттс активно призывал публику присоединяться к проектам Open Source, чем наглядно подтверждал не только свой статус в OpenOffice.org, но и десятый пункт ключевого доклада Белендорфа.

## «К барьеру!»

Следующее мероприятие – «К барьеру!», анонсированное как «Сторонники и противники открытого кода встречаются на ринге», – было проведено в формате, близком к тому, что можно наблюдать в одноименном телевизионном шоу. Разве что оно было проведено как «командная игра». С од-



Участники мероприятия «К барьеру!»

ной стороны – Владислав Шершульский, Владимир Мамыкин (Microsoft), Андрей Федоров (Digital Design), с другой – Алексей Смирнов, Алексей Новодворский (ALT Linux) и Александр Давыдов (NAUMEN). Представители каждого «лагеря» поочередно высказывали свое мнение по тому или иному вопросу, что в сумме сформировало объективный взгляд. «Модератором» же был автор этой статьи – Дмитрий Шурупов.

Само обсуждение началось после уточнений в терминологии. Так, участники условились понимать под ПО с открытым кодом его традиционное определение «Open Source Definition». Первой предложенной темой для дискуссии стала обоснованность применения программного обеспечения в государственном секторе. Вместе с тем была затронута и проблема выбора наиболее приемлемых решений для об-

суждению программного обеспечения, используемого в сферах, связанных с национальной безопасностью. Сторонники Open Source выразили мнение, что открытие исходного кода Microsoft для определенных служб само по себе недостаточно, потому что это не позволяет вносить какие-либо модификации в существующий код. Соответственно такая «открытость» не удовлетворяет необходимым условиям обеспечения настоящего уровня безопасности.

Некоторое время было отведено на вопросы из зала, где особенно отметился профессор В. А. Каймин, ныне занимающийся юриспруденцией. Начав с вопросов по проблемам патентования, он в результате изрядно развлекал публику продолжительными и зачастую юмористичными комментариями.

## Open Source в «театре»

После обеда была проведена заключительная секция, посвященная программному обеспечению с открытым кодом: «Open Source-проекты в театре Interop».

С получасовыми докладами выступили все зарубежные гости (Суаре-Поттс, Белендорф, Олман) и Алексей Смирнов.

## Общие впечатления

Interop Moscow вновь примечателен тем, что смог предоставить желающим возможность послушать видных деятелей сообщества Open Source и пообщаться с ними. При этом стоит особенно отметить значительные улучшения в отношении последнего – интерактивности действия. Все это вкупе с традиционно высоким уровнем организации оставило приятные впечатления. Хороший повод ждать продолжения мероприятий, проводимых в рамках Interop, в следующем году. ●

Текст: Дмитрий Шурупов,  
фото: Татьяна Афанасенко



# FreeBSD: некоторые особенности сборки ядра

*Сергей Супрунов*

Сборка собственного ядра на сервере – это почти обязательный ритуал для каждого системного администратора. Сегодня мы поговорим о том, как это делать по возможности быстро и эффективно.



## Плюсы и минусы «стандартного» подхода

Информацию о том, как собирать собственное ядро, можно найти практически в любой книге, посвящённой системе FreeBSD. Естественно, есть она и в официальной документации (в частности, см. Handbook), так что не будем останавливаться на этом вопросе.

В конфигурационном файле ядра в первую очередь по устоявшейся традиции отключают все «лишние» устройства. Действительно, какой смысл собирать в ядре поддержку сетевых карт USB или SCSI-дисков, если их в сервере нет и в ближайшие годы не планируется? Так что, добавляя поддержку пакетного фильтра или квот, практически любой системный администратор заодно пробегает и по стройным рядам device-строк, безжалостно расставляя комментарии перед теми, которые выглядят подозрительно.

Но одной из особенностей сборки ядра во FreeBSD является то, что, даже закомментировав в конфигурационном файле строку, отвечающую за то или иное устройство или опцию, вы всё равно получите их поддержку в виде модуля. То есть драйвер редко используемого устройства не будет постоянно занимать место в оперативной памяти, но при необходимости его всегда можно подгрузить.

Но есть здесь и небольшой недостаток – время на сборку модулей будет всё равно потрачено. И зачастую даже небольшое изменение конфигурации ядра требует нескольких часов на пересборку, особенно на не слишком мощном «железе». Как правило, особых проблем это не создаёт (запустил сборку и пошёл обедать; да и на вопрос начальства «Чем занимаешься?» всегда можно честно ответить: «Ядро собираю»). Однако иногда «жаба душист», когда десятки минут созерцаешь процесс сборки чего-то, что никогда на сервере не понадобится... Попытаемся решить эту проблему.

## Ничего лишнего!

Допустим, вам нужно пересобрать ядро на сервере. А действительно ли необходимы здесь модули поддержки звуковых карт? А как насчёт USB, если из оборудования здесь – четыре сетевых карты в PCI-слотах да CD-привод для аварийно-восстановительных ра-

## Пара советов

Хотя эти советы не оказывают непосредственного влияния на размер или скорость сборки ядра, но при частых его пересборках могут несколько упростить жизнь.

Если вы постоянно (или преимущественно) работаете с одним конфигурационным файлом ядра, то чтобы каждый раз не вводить в командной строке опцию «KERNCONF=MYKERN», укажите эту опцию в файле /etc/make.conf. Правда, не забывайте после этого явно указывать файл GENERIC, если захотите пересобрать ядро по умолчанию.

Иногда бывает, что рабочее ядро остаётся, но его конфигурационный файл безвозвратно теряется. Конечно, составление конфигурации с нуля – лучший способ навести в ядре порядок. Однако не всегда на это есть время и силы. Для подстраховки можно добавить в конфигурационный файл ядра такую строку:

```
options INCLUDE_CONFIG_FILE
```

бот? А зачем нужна поддержка NTFS, Ext2/3, Reiserfs и прочих, если единственной системой была, есть и будет FFS (ну, может, ещё ZFS через годик-другой, когда притрётся), поскольку разводить «зоопарк» на боевом шлюзе не придёт в голову даже самому отъявленному экспериментатору?

Понятно, что всё лишнее будет непременно из конфигурации ядра исключено. Только вот, как уже упоминалось выше, всё, что не указано в конфигурации, по-прежнему будет собираться в виде модулей. То есть ждать придётся столь же долго... Впрочем, можно и не ждать!

Попробуем минимизировать не только ядро, но и время, затрачиваемое на его сборку. Для начала по традиции уберём лишнее.

Например:

- Определитесь с нужным семейством процессоров. Как минимум, i486 сейчас уже мало где остались, и совсем необязательно загромождать ядро кодом поддержки оногo.
- PROCFS, а с ней и PSEUDOFs в ряде случаев можно безболезненно отключить. Некоторые утилиты (преимущественно отладочного характера, такие как truss) могут требовать поддержки PROCFS, но в большинстве случаев можно обойтись и модулем.

Это позволяет сохранить текущий конфигурационный файл в самом ядре (в двоичном файле). Несколько лишних килобайт проблемой не станут, зато если вы вследствие печального стечения обстоятельств потеряете конфиг, на основе которого собиралось ядро, то всегда сможете его восстановить, используя команду strings, вытаскивающую из двоичного файла строковые фрагменты:

```
# cd /boot/kernel
# strings -n 3 kernel | \
sed -n 's/^___/p'
```

Перенаправив вывод в файл и немного подчистив при необходимости (к сожалению, последовательность из трёх символов подчёркивания, идентифицирующая строки сохранённой конфигурации, встречается и в других местах ядра; как правило, такой «мусор» появляется в самом начале полученного вывода), вы получите исходную конфигурацию, и даже со всеми комментариями, которые там были изначально.

- На совместимости с предыдущими версиями (опции COMPAT\_\*), на мой взгляд, лучше не экономить. Впрочем, если очень хочется, можно поэкспериментировать и в этом направлении.
- INET6 в ближайшие месяцы вы собираетесь использовать? Вряд ли.
- Списки доступа (UFS\_ACL)? Вещь полезная, но не везде – не думаю, что на интернет-шлюзе или DNS-сервере нельзя будет обойтись стандартными правами доступа.
- NFS, MSDOSFS, CD9660 на сервере часто используете? Если нет – долой из ядра, хватит и поддержки в модуле... Хотя, с другой стороны, наличие этих опций будет не слишком обременительно для системы, зато вероятность столкнуться с проблемами при работе с CD- и Flash-дисками несколько уменьшится.
- В принципе на боевом сервере можно исключить и средства отладки, особенно если для тестирования есть отдельная машина, где в случае необходимости можно будет воспроизвести проблемную ситуацию и «снять» нужные дампы.

С имеющимися у вас устройствами, думаю, сами разберётесь (не забывайте только про устройство miibus, требу-

емое для работы некоторых сетевых карт; его исключение – довольно распространённая ошибка). Я обычно в ядро включаю то, что работает постоянно. То, в чём необходимость возникает сравнительно редко, проще оставить модулем. Это же правило я применяю и к различным опциям (например, поддержку пакетных фильтров как-то привык «вкомпилировать» в ядро). Впрочем, это только моё мнение.

Если подходить к этому вопросу более детально, то следует учитывать, что использование модулей обеспечивает дополнительную гибкость (вы динамически можете подгружать нужные модули, например, в случае добавления нового оборудования). С другой стороны, каждый модуль – это дополнительные структуры в памяти плюс дополнительное время на «стыковку» при загрузке. Впрочем, объёмы требуемой памяти не слишком велики по современным меркам, да и затраты времени пренебрежимо малы (тем более на серверах, где загрузка – не самая частая операция). Так что вопрос лежит, скорее, в плоскости личных предпочтений. Иногда рассматривается также аспект безопасности (можно собрать монолитное ядро и полностью запретить от греха подальше загрузку модулей, скажем, в результате перевода системы на `securelevel 1` или выше), но здесь мы не будем вторгаться в эту тему.

С этим, думаю, всё понятно. А как влиять на то, какие модули должны быть собраны? В конфигурацию ядра можно добавить удобную для таких случаев опцию:

```
makeoptions MODULES_OVERRIDE='cd9660 _  
netgraph nfsserver nfsclient'
```

При наличии такой строки модули будут собраны только поддержка CD9660 (вдруг когда-нибудь понадобится CD-диск подмонтировать), NFS и интерфейсов netgraph. Остальное попросту не будет собираться, не отнимая ни времени, ни места на диске. (Названия модулей соответствуют именам каталогов в `/usr/src/sys/modules`, и, как правило, по названию несложно догадаться об их предназначении.)

Естественно, приведённый выше пример не следует рассматривать в качестве эталонного – вы и только вы можете определить, какие модули

вам нужны, а какие нет. Также нужно учитывать, что таким образом можно очень легко привести систему в неработоспособное состояние, поэтому проверьте сначала по `kldstat`, какие же модули используются системой в различных режимах работы, чтобы ничего не забыть. Ну и несколько раз подумайте – а правда ли вы сможете жить без звука на своём боевом сервере?

## Make.conf вам в помощь

Если характер работы сервера таков, что список модулей, которые могут понадобиться, практически не меняется (частный случай – полное отсутствие модулей, если вы привыкли работать исключительно с монолитным ядром), то параметр `MODULES_OVERRIDE` можно задать в файле `/etc/make.conf` – это значение будет оказывать влияние на все собираемые ядра. Таким образом, есть два пути жёстко задать список модулей – в `make.conf`, если все ваши ядра должны будут использовать один и тот же набор модулей, и в конфигурационном файле ядра (опция `makeoptions MODULES_OVERRIDE`), если для каждого ядра необходимо (или желательно) задавать свой набор модулей.

Есть более кардинальный путь – опция `NO_MODULES` в том же `make.conf` позволяет вообще отключить сборку модулей при сборке ядра. Опция `MODULES_WITH_WORLD` оставляет вам шанс – при её наличии модули будут собираться, но не с ядром, а с «миром» (во время выполнения команды `make buildworld`). Поскольку сборка всей системы выполняется сравнительно редко (при обновлении системы да изредка при устранении той или иной ошибки, оказывающей влияние на многие подсистемы ОС), а пересборка ядра не всегда требует перекомпиляции всех модулей, то определённый смысл в этом есть. Если же потребуется пересобрать какой-то из модулей, это в любое время можно сделать вручную:

```
# cd /usr/src/sys/modules/<имя модуля>  
# make  
# make install
```

При необходимости можно запустить команду `«kldxref /boot/kernel»` (иногда модули размещаются и в отдельном каталоге – `/boot/modules`), что-


бы обновить «подсказки» ядру, где и какие модули искать. Хотя обычно эта команда автоматически запускается при выполнении цели `install`. Собрать все модули вручную можно, выполнив команду `make all install` в каталоге `/usr/src/sys/modules`.

В дополнение к `MODULES_OVERRIDE` есть опция `WITHOUT_MODULES`, которая позволяет исключить сборку конкретных, указанных в ней модулей (из тех, что останутся для сборки после применения опции `MODULES_OVERRIDE`). Особого смысла разрешать определённые модули в `MODULES_OVERRIDE` и тут же исключать часть из них в `WITHOUT_MODULES` нет. Но если не использовать `MODULES_OVERRIDE`, то с помощью `WITHOUT_MODULES` можно исключить те модули, которые заведомо не нужны (например, драйверы звуковых карт), но при этом выполнить сборку всего остального «на всякий пожарный случай».

## Несколько предостережений напоследок

Если вы используете модули, но решили не пересобирать их каждый раз вместе с ядром, внимательно следите за тем, влияет ли исправление тех или иных критических ошибок на ваши модули – не исключена ситуация, что, скрупулёзно выполнив все предписания из рассылки `freebsd-security`, вы на самом деле останетесь с открытой уязвимостью в модуле, который не пересобирался вместе с ядром.

И не забывайте, экспериментируя с ядром, оставлять пути отступления, копируя работоспособное ядро в отдельный каталог. Это позволит вам в случае проблем загрузиться с прежним ядром, разобраться в проблеме и устранить допущенные ошибки. Также имеет смысл сохранять устанавливаемое при инсталляции системы ядро `GENERIC` (если его нет, то всегда можно собрать на основе одноимённого файла в каталоге конфигурационных файлов ядра). Когда-нибудь оно сможет вас выручить, например, если придётся в аварийном порядке загружаться на оборудовании, поддержка которого в вашем рабочем ядре не предусматривалась.

Удачи! 





**12**  
лет

**НАША КОМПАНИЯ ПРЕДОСТАВЛЯЕТ  
ЛИНИИ СВЯЗИ В САМЫХ НЕПРОХОДИМЫХ  
МЕСТАХ МОСКВЫ**

**10 МБИТ - \$500, ВКЛЮЧЕНО МНОГО ТРАФИКА.  
ANYTHING ELSE?**

**ЗВОНИТЕ, ДОГОВОРИМСЯ!**

г. Москва, Хлебный переулок 2/3, тел. 291-61-32, 202-61-43 (круглосуточно)  
e-mail: [support@redline.ru](mailto:support@redline.ru)



# Не допустите потери данных! Ленточная библиотека к вашим услугам

*Виталий Банковский*

**Какое самое кошмарное событие в работе системного администратора? Правильно, потеря всех данных. Тогда он вспоминает, что собирался сделать архивирование данных в 1995 году. Знакомо? Если еще нет – тогда эта статья для вас.**

**И**так, предстоит задача оценки и внедрения системы создания резервных копий серверов в ситуации, когда объем первичных средств (дополнительные накопители, CD/DVD) уже недостаточен для сохранения растущих объемов данных. Для начала предлагаю вам проанализировать три наиболее используемых типа систем хранения резервных копий данных, а также программные и аппаратные средства, обеспечивающие сам

процесс создания и сохранения резервных копий. На втором этапе расскажу о внедрении системы создания копий с применением одного из типа хранилища – ленточной библиотеки.

## **Выбор хранилища резервных копий**

При выборе типа хранилища резервных копий данных я рассматривал три варианта хранилища архивных данных:

- Дисковый массив.

- DVD-RAM-библиотека.
- Ленточная библиотека.

Сразу скажу, что хотя DVD-библиотеки и выглядят привлекательно с точки зрения надежности, стоимость таких систем в настоящее время остается очень высокой.

Для начала давайте оценим стоимость все трех решений для объема 14 Тб (см. **таблицы 1-3**). Как видите, цена решения на ленточной библиотеке



составляет почти в два раза дешевле, чем стоимость сохранения копий данных на жестких дисках и почти в 8 раз дешевле стоимости решения на основе DVD-библиотеки.

## Стабильность

В среднем одна лента способна выдерживать порядка 250 полных циклов перезаписи. Я использовал приблизительно 6 лент каждую неделю, т.е. 24 ленты в месяц. С 60 лентами, загруженными в ленточную библиотеку, каждая лента используется в среднем 2,5 раза в месяц. Таким образом, мы получаем, что в среднем одна лента способна прослужить около 100 месяцев ( $250/2,5=100$ ). Конечно, все зависит ещё и от условий окружающей среды. Например, если температура часто меняется или присутствует пыль, то это может значительно сократить время жизни ленты. На первый взгляд, стабильность системы на диски выглядит более высокой по сравнению с лентами, но как показывает опыт, время жизни SATA-дисков при очень высоких нагрузках составляет в среднем 1-2 года в зависимости от внешних факторов. Поэтому нужно учитывать нагрузку при выборе решения.

## Длительное хранение

Если вы хотите хранить ваши данные в течение длительного срока, например, банковские записи, то вы можете сохранить данные на лентах, затем выгрузить их из библиотеки и сохранить в другом безопасном месте на длительное время. В среднем ленты имеют срок хранения порядка 30 лет, правда, этот срок может резко сократиться при частом перезаписывании. И, как вы понимаете, такая схема практически недоступна в случае решения на дисках. Также сюда можно добавить потенциальный фактор, что жесткие диски могут просто не запуститься после столь длительного хранения из-за затвердевания смазки механических частей. Поэтому система хранения на лентах мне видится более гибкой, позволяющей решать обе задачи – хранение оперативных копий и возможность хранения данных в течение очень длительного времени. Например, работа может происходить по следующему сценарию: ежедневно производится запись изменений данных на ленту и раз в месяц

Таблица 1. Стоимость системы сохранения резервных копий данных на жесткие диски

Компонент	Пример	Стоимость
Корпус с 40 слотами для жестких дисков	RM8U8042	\$4,000 US
RAID-контролер, 24 порта	Areca ARC-1170 SATA II 24	2 x \$1,500 US = \$3000 US
Материнская плата с процессором и памятью	–	\$1500
Жесткие диски, 28 штук, 500 Гб каждый	Hitachi, Seagate	28 x \$130 = \$3640
<b>Окончательная стоимость:</b>		<b>\$12,410 US</b>

Таблица 2. Стоимость системы сохранения резервных копий данных на ленточную библиотеку

Компонент	Пример	Стоимость
Ленточная библиотека с LTO2 накопителем	DELL PowerVault 136T	\$5,000 US
Лента, 72 картриджа	Fujitsu LTO2	72 x \$30 = 2160
<b>Окончательная стоимость:</b>		<b>\$7,160 US</b>

Таблица 3. Стоимость системы сохранения резервных копий данных на DVD-библиотеку

Компонент	Пример	Стоимость
DVD-библиотека с 1525 слотами	Plasmon D-1525 DVD	\$36,545 US
DVD RAM 4.7 Гб плюс картридж производителя	–	\$640 US за упаковку из 40 носителей, 30 упаковок, итого: \$19200 US
<b>Окончательная стоимость:</b>		<b>\$55,745 US</b>

Источник: [http://www.opticaljukeboxes.com/dvd?plasmon\\_d-1525.htm](http://www.opticaljukeboxes.com/dvd?plasmon_d-1525.htm).

создается полная копия всех данных, затем кассеты изымаются и помещаются в удаленное безопасное место.

## Масштабирование

К уже имеющейся библиотеке можно добавить новые. При наличии двух SCSI-портов один архивирующий сервер может обслуживать до 15 библиотек с суммарным объемом 210 Тб.

## Охлаждение и потребление энергии

Dell PowerVault 136-T использует порядка 110 Ватт, тогда как решение на 28 дисках и сервере использует порядка 800-1000 Ватт. Так как рекомендованная рабочая температура жестких дисков составляет 40-50°C, то в случае решения на жестких дисках нужно позаботиться о качественной охлаждающей системе, и это тоже нужно учитывать при составлении окончательной сметы при выборе решения. Плюс, если процесс создания архивных копий затягивается на многие часы, то стоимость потребленной электроэнергии может составить внушительную сумму.

## Доступность

Из-за того, что системы хранения на лентах являются синхронными, только одна операция доступна в какой-то момент времени. Например, если вы хо-

тите восстановить ваши данные, то вы будете вынуждены остановить текущую процедуру архивирования. Системы хранения на дисках лишены этого недостатка, что является большим преимуществом перед лентами, особенно когда необходимо иметь асинхронный доступ к данным, например, если вы предоставляете ваше решение многим клиентам, которые хотят иметь параллельный доступ.

Вам необходимо рассмотреть все требования и выбрать наиболее подходящее решение. Единственное, что можно посоветовать, так это начать с более дешевой конфигурации на ленточной библиотеке, а затем добавить хранилище на дисках, таким образом вы можете хранить полные данные на лентах за последние несколько месяцев и одновременно воспользоваться преимуществами хранения на жестких дисках.

## Структура системы

Я покажу шаги, необходимые для создания хранилища на лентах. Наша система будет состоять из следующих компонентов:

- Архивирующий сервер (сервер резервного копирования).
- Ленточная библиотека.

Архивирующий сервер собирает данные с серверов, сжимает, сохраня-

ет на собственный носитель для временного хранения и последующей записи на ленту. Кроме этих базовых операций, сервер также создает расписания сохранения полных и частичных данных с серверов.

## Выбор аппаратного обеспечения

Попробуем выбрать аппаратное обеспечение, необходимое для создания нашей системы. Как вы помните, есть два компонента архивирующего сервера, которые интенсивно используются: процессор для сжатия данных и накопитель для временно-го хранения данных. Исходя из этого, у нас есть выбор построения системы на основе простенького P4 с небольшим жестким диском до сервера с аппаратной компрессией и высокопроизводительным, вместительным хранилищем SAN.

Также нужно учитывать, что процесс сбора данных с серверов использует немалое количество ресурсов подсистем ввода-вывода, и если ваши серверы достаточно нагружены, то вам необходимо учитывать и этот фактор для выбора конфигурации, которая могла бы собирать данные серверов в минимально возможное время для предотвращения перегрузки серверов в час пик.

Таким образом, можно рассмотреть три класса аппаратного обеспечения.

### Начальный уровень

Подходит для небольшого количества серверов (например, от 1 до 20 серверов с 100-200 Гб на каждом сервере) и в случае, если вы не ограничены временными рамками для процесса архивирования. Для такого решения можно воспользоваться системой с одним-двумя процессорами и непроизводительным SATA-накопителем.

### Средний уровень

Этот уровень можно порекомендовать для 200-300 серверов, но если и здесь вы не ограничены по времени. Подойдет система с 2-4 ядрами, SCSI/SAS/FC-накопителями на 400-800 Гб. Вы можете спросить: «Почему SCSI/SAS/FC предпочтительнее?». Накопитель должен быть способен передавать порядка 600-1000 Гб в день, и на данный момент только накопители серверного

класса с интерфейсами SCSI/SAS/FC способны выдержать такую нагрузку.

### Высший уровень

Важным отличием этого решения от двух предыдущих является способность системы архивировать данные с серверов в максимально короткое время, таким образом, производительность серверов в час пик не пострадает. Для этой конфигурации вы можете воспользоваться контроллером аппаратного сжатия ANA362-PCIX, который предоставляет скорость до 3 Гб в секунду. Для обеспечения такой скорости сохранения на архивном сервере вам также необходим соответствующий накопитель, способный работать на этой скорости. Приблизительно можно рассчитать его конфигурацию по формуле:

$$hNumber = bSpeed/hSpeed$$

где:

- hNumber – количество дисков, необходимых для накопителя;
- bSpeed – средняя скорость передачи архивного сервера;
- hSpeed – средняя скорость записи на каждый жесткий диск.

Для примера возьмем ситуацию – вы хотите сохранять данные на скорости 1 Гб в секунду, и каждый накопитель способен сохранять на скорости 30 Мб в секунду. Таким образом, вам необходимо, как минимум, 5 жестких дисков. Конечно, чем больше дисков установлено, тем большую скорость вы можете получить. Хотя при возрастании количества дисков кривая зависимости скорости от количества дисков будет падать, и в этом случае можно подумать о создании массива RAID10. Так как цена на SAN-накопители падает в последние годы (стоимость начального SAN-накопителя на 14 слотов составляет порядка \$2500 US), то такое решение может рассматриваться как наиболее эффективное по соотношению качества, скорости и стоимости.

## Инсталляция аппаратного обеспечения

Я использовал «среднюю конфигурацию» со следующими компонентами:

- Два процессора AMD 270 с двумя ядрами в каждом.

- Четыре 300 Гб SCSI-диска, собранные в массив RAID5.
- Ленточная библиотека Dell Powervault 136-T с 60 кассетами (доступно до 72 кассет).
- Два LTO-2-накопителя, установленных в библиотеку.

Таким образом, полный объем хранилища составил порядка 12 Тб, которого было достаточно для сохранения 8 Тб, включая частичные и полные архивы.

Инсталляционный процесс включает в себя два шага – подключение кабелей и загрузку кассет в библиотеку.

### Подключение кабелей

Вам необходимо последовательно соединить все SCSI-устройства. Если у вас 2 накопителя на лентах, то вам понадобится 3 SCSI-кабеля и один терминатор. Шаги подключения приведены ниже:

- Подключите первый разъем автозагрузчика (tape exchanger) в SCSI-порт архивирующего сервера.
- Второй разъем автозагрузчика должен быть подключен к первому разъему первого ленточного накопителя.
- Второй разъем первого накопителя должен быть подключен к первому разъему второго накопителя.
- И второй разъем второго накопителя должен быть закрыт SCSI-терминатором.

Структура подключения приведена на рис 1.

## Установка программного обеспечения

Я использовал программный пакет Amanda (<http://www.amanda.org>). Предварительно были рассмотрены разные программы, но комбинация возможностей Amanda сыграла решающую роль в выборе последней:

- **Бесплатность.** Если у вас большое количество серверов, то лицензионные отчисления могут поставить крест на всем решении или проделывать большую дыру в бюджете компании.
- **Безопасность.** Шифрование на уровнях передачи и хранения данных. Шифрование на уровне передачи является особенно важным,



если серверы расположены в месте, отличном от расположения системы архивирования.

■ **Развитый планировщик.** Пока другие системы лишь предоставляют доступ к командам архивирования данных и вам необходимо самому определять стратегию архивирования, Amanda имеет собственный планировщик задач архивирования, способный выполнять такие нетривиальные требования, как распределение запусков задач полного архивирования по всему циклу архивирования.

## Инсталляция Amanda на сервер

В работе я использую Linux, а конкретнее – CentOS 4.4. Поэтому все дальнейшие указания рассчитаны на эту операционную систему, хотя Amanda работает на большинстве UNIX-подобных операционных системах.

Скачайте amanda с сайта <http://sourceforge.net>, распакуйте и проинсталлируйте, как написано в инструкции, или следуйте нижеприведенному примеру. Я использовал версию 2.4.5p1:

```
tar -xzf amanda-2.4.5p1.tar.gz
cd amanda-2.4.5p1
./configure --with-user=root --with-group=root
make
make install
```

По умолчанию имя конфигурации называется «DailySet1», и она расположена в /usr/local/etc/amanda/DailySet1. Вам необходимо скопировать конфигурационные файлы из каталога example/\* в каталог /usr/local/etc/amanda/DailySet1/.

Также вам надо установить программу mtx для операций с ленточными накопителями.

## Подготовка ядра для сервера

Также вам необходимо включить опции ядра для поддержки автозагрузчика и ленточного накопителя. Вы можете воспользоваться модулями или статически включить поддержку в ядро. На наших серверах в целях безопасности мы используем ядра с полностью выключенной поддержкой модулей.

Необходимо включить следующие опции в ядре Linux (см. **рис. 2**):

- SCSI Tape support;
- SCSI Media changer support;
- Probe all LUNs on each SCSI device;
- SCSI generic support.

После установки нового ядра и перезагрузки сервера введите команду «dmesg», и если все настроено правильно, вы должны увидеть ваши устройства:

```
Vendor: DELL Model: PV-136T Rev: 3.37
Type: Medium Changer ANSI SCSI revision: 02
Vendor: IBM Model: ULTRIUM-TD2 Rev: 53Y3
Type: Sequential-Access ANSI SCSI revision: 03
Vendor: IBM Model: ULTRIUM-TD2 Rev: 53Y3
Type: Sequential-Access ANSI SCSI revision: 03
```

## Настройка Amanda

Теперь речь пойдет о настройках, которые необходимо применить, чтобы заставить DELL PowerVault 136T рабо-

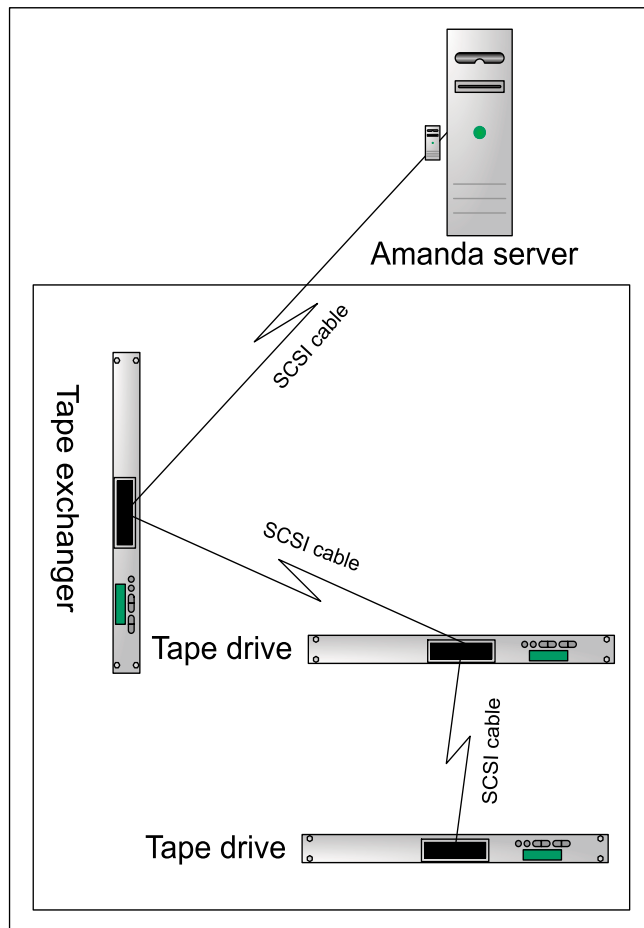


Рисунок 1. Схема подключения библиотеки к серверу

тать. Как упоминалось ранее, я использовал LTO2 (200gb/400gb) drives.

В нашем случае конфигурационные файлы были расположены в /usr/local/etc/amanda/DailySet1. Два файла, которые подлежат правке: changer.conf и amanda.conf.

## Настройка amanda.conf

Большинство опций подходят для типичных случаев, но есть такие, которые необходимо изменить.

Имя вашей организации:

```
org "Bigsoft Home"
```

Адрес администратора системы архивирования. На этот адрес будут отправляться отчеты об архивировании. Если у вас большое количество серверов, то нужно позаботиться, чтобы все почтовые системы могли успешно доставить большие письма.

```
mailto:report@domain.com
```

Количество параллельных процессов архивирования. Я получил число максимального количества процессов, равное 24 на 4 ядрах AMD 270 (два процессора, четыре ядра). Если скорость превышает 1 Гб в секунду, то вам необходимо гигабитное и выше подключение к сети:

```
inparallel 12
```

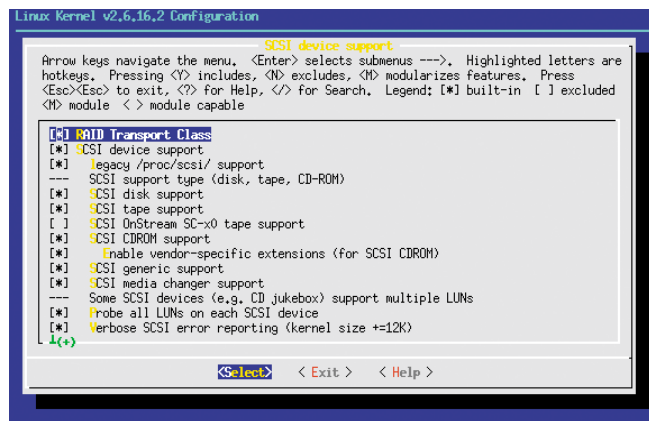


Рисунок 2. Конфигурация ядра Linux

Максимальная скорость для использования сервером. Это не жесткое ограничение и лишь помогает планировщику в определении максимального количества запущенных процессов для получения скорости, не превышающей этот предел:

```
etusage 600000 Kbps
```

Если на ваших серверах расположено громадное количество файлов (порядка несколько миллионов), то необходимо увеличить это значение по умолчанию, иначе процесс подсчета размера всех файлов закончится неудачно.

```
etimeout 208000
```

## Настройка автозагрузчика

В этом разделе мы расскажем, как настраивать Amanda для использования автозагрузчика лент, установленного в библиотеке. Параметры автозагрузчика находятся в двух файлах – amanda.conf и changer.conf.

Для начала займемся amanda.conf.

```
Runtapes 5
```

Количество лент, используемых для каждого запуска. Если это число меньше, чем необходимо для сохранения ежедневных данных, то вы получите сообщение об ошибке, и Amanda перейдет в degraded режим. Вам необходимо подобрать это число экспериментальным путем или по предварительной оценке из расчета суммарный объем данных плюс максимальный объем файлов, измененных между запусками процедур архивирования.

```
tpchanger "chg-zd-mtx"
```

Тип программы управления автозагрузчиком. Если у вас SCSI-автозагрузчик, то автор рекомендует использовать программу chg-zd-mtx как наиболее развитую и «понимающую» большинство SCSI-автозагрузчиков.

```
tapedev "/dev/nst0"
```

Путь к ленточному накопителю.

```
changerfile "/usr/local/etc/amanda/DailySet1/changer"
```

Путь к системному файлу статуса автозагрузчика.

```
changerdev "/dev/sg2"
```

Путь к устройству автозагрузчика. Вам необходимо найти число после «sg» с помощью запуска программы «dmesg» и найти порядок автозагрузчика в списке SCSI-устройств. В нашем случае SCSI RAID имел число 0, SCSI-контроллер имел число 1 и автозагрузчик имел число 2.

```
tapetype LTO2
```

Тип ленточных кассет. Amanda.conf содержит список практически всех типов кассет, из которого нужно выбрать используемый в вашей системе, например, LTO2, LTO3, или недавно появившийся LTO4. Понятно, что при покупке библиотеки у вас есть выбор, какой тип ленточного накопителя вы установите в систему.

```
amrecover_changer "chg-zd-mtx"
```

Типы программы для управления загрузчиком для процесса восстановления.

Далее займемся changer.conf. Есть несколько опций, которые необходимо поменять для PowerVault 136-T:

```
eject > 1
```

Накопители поддерживают команду eject для выбрасывания кассеты в автозагрузчик.

```
sleep 5
```

Подождать 5 секунд перед началом использования кассеты после загрузки.

```
cleanmax 10
```

Максимальное количество использования чистящего картриджа. Это число может меняться, поэтому необходимо свериться с руководством по эксплуатации конкретного типа чистящего картриджа.

```
changerdev /dev/sg0
```

Путь к автозагрузчику.

```
havebarcode 1  
havereader=1
```

Как описано в разделе «Нанесение меток на ленту», PowerVault 136-T имеет собственное устройство чтения штрих-кодов, и для его использования нужно включить эту опцию:

```
labelfile /var/log/amanda/labelfile.txt
```

Файл, где сохраняется список кассет, и их метки:



```
offline_before_unload=1 offlinestatus=1 OFFLINE_BEFORE_UNLOAD=1
```

Как правило, ленточные накопители требуют команды «offline» перед тем, как кассета может быть выгружена.

### Настройка временного хранилища

Как вы уже знаете, Amanda сохраняет данные на собственное временное хранилище, и затем, когда оно заполняется или процедура архивирования завершена, сохраняет данные из этого хранилища на ленту. Необходимо описать хранилище в конфигурационном файле amanda.conf:

```
holdingdisk hdl {
    comment "main holding disk"
    directory "/home/amanda" # Путь к данным на диске
    use 300 Gb                # Доступное пространство
    chunksize 1Gb             # Разбить данные на куски по 1 Гб
}
```

Вы можете настроить несколько систем хранилища. Например, если на сервере установлены несколько накопителей.

### Настройка стратегии архивирования

Рассмотрим, как настроить тип процедуры архивирования и как составлять список серверов, подлежащих копированию.

### Настройка стратегии

Сперва необходимо описать стратегии для Amanda. Для большинства ситуаций одной стратегии уже достаточно, хотя можно настроить множество стратегий для специфичных случаев.

```
define dumptype default
{
    global
    estimate calcsite
    program "GNUTAR"
    dumpcycle 14
    comment "root partitions dumped with tar"
    compress server fast
    index
    priority medium exclude list "amandaexclude"
    tape_splitsize 20 Gb
}
```

Ниже приведены описания каждой опции:

- **global** – означает, что эту стратегию можно использовать независимо в списках серверов. Например, можно настроить несколько стратегий, затем объединить их вместе и придать статус «global». Для простоты мы не использовали такую схему построения стратегий.
- **estimate calcsite** – используемый метод для определения общего размера файлов на серверах. Существует два наиболее полезных варианта этой опции – calcsite и server. В случае calcsite Amanda запустит небольшую программу на каждом сервере, которая просуммирует размер всех файлов. Это наиболее аккуратный способ для оценки объема, но может занять продолжительное время в случае большого количества файлов. Второй вариант server указывает Amanda использовать данные, полученные из предыдущих запусков. Если объем данных сильно разнится от запуска к запуску, то это может привести к составлению неправильного расписания заданий.

- **program «GNUTAR»** – программа для сбора данных на клиентах. Если не стоит задача делать дампы файловых систем, то это – оптимальная опция.
- **dumpcycle 14** – как часто необходимо создавать полный архив серверов. В нашем случае мы остановились на двух неделях.
- **compress server fast** – выбор стороны, на которой будет происходить сжатие данных. Есть два варианта – server – для сжатия на архивирующем сервере и client – для сжатия на стороне клиента. У меня была возможность установить 4 ядра на архивирующем сервере, поэтому я использовал архивирование на стороне сервера. Максимальная скорость сжатия составила порядка 600 Мб в секунду. Дополнительно можно установить один из уровней сжатия – best, custom, fast.
- **index** – указывает Amanda, что необходимо создавать базу данных содержимого на кассетах. По умолчанию эта опция выключена. Но это необходимо включить, иначе будет невозможно сделать поиск данных на кассетах.
- **exclude list «amandaexclude»** – на каждом диске, на каждом клиенте необходимо расположить этот файл, который может содержать пути и маску файлов и директорий, которые необходимо исключить из архивирования (например, лог-файлы). Даже если необходимо включить все файлы, этот файл должен существовать, но может быть пустым. Иначе процесс архивирования завершится неудачно. Для подробностей обратитесь к разделу «Исключение и разделение данных».
- **priority medium** – для некоторых дисков на клиентах можно указывать различные уровни приоритетов: high, medium, low. Если система архивирования не имеет достаточно места для сохранения данных, она выберет диски с более высоким приоритетом для замещения дисков с меньшим приоритетом, таким образом, важные данные с большим приоритетом получают большую гарантию сохранности.
- **tape\_splitsize 20 Gb** – для уменьшения фрагментации ленточного пространства вы можете разбить большие архивы на более мелкие на момент записи на ленту. Например, если объем ваших дисков в среднем составляет 100 Гб, то однозначно проблема фрагментации проявится, потому что каждый раз Amanda будет вынуждена искать свободное место на лентах на 100 Гб. Ограничение максимального размера архива позволит записывать архивы кусками по 20 Гб (как в данном примере). Сегментация больших архивов на более мелкие позволит существенно уменьшить проблему фрагментации носителей.

### Описание клиентов

На этом этапе мы опишем серверы-клиенты, а также каталоги, которые подлежат архивированию. Специальный файл disklist отвечает за это описание (по умолчанию он находится в каталоге /usr/local/etc/amanda/DailySet1). Этот файл содержит список каталогов, которые необходимо архивировать, например:

```
server1.domain.com / {
    default
}
```

```
server1.domain.com /boot {
  default
}
server1.domain.com /var {
  default
}
server1.domain.com /usr {
  default
}
server1.domain.com /home {
  default
}
```

Вы могли бы спросить: «Почему бы просто не определить корневой каталог «/» вместо списка каталогов?». Когда Amanda запускает программу сбора данных (tar) на серверах, то используется опция «stay on single filesystem», которая указывает tar оставаться на текущей файловой системе. Таким образом, монтирование по NFS или другие манипуляции с файловой системой не приведут к двойному или циклическому архивированию. Я использую отдельные разделы для /boot, /home/, /usr, and /var, поэтому необходимо было указать все разделы. Также, если какой-то раздел содержит большие объемы данных, то вместо указания этого каталога необходимо использовать список подкаталогов.

Для подробностей обращайтесь к разделу «Исключение и разделение данных».

## Создание меток на лентах и кассетах

Перед использованием библиотека должна знать о кассетах, которые установлены. Для этого мы должны обучить библиотеку, и этот процесс включает два шага:

- инициализация библиотеки;
- создание списка кассет для Amanda.

### Инициализация библиотеки

Первоначально кассеты не имеют никаких меток, которые позволили бы библиотеке идентифицировать каждую кассету. Для этого необходимо купить специальные бумажные метки и разместить их на каждую кассету. Их можно купить на сайте <http://www.issidata.com> (USA) или на <http://www.invictus.ru> (Россия) или просто напечатать с помощью GNU-Barcode. Каждая метка имеет уникальный цифровой и штрих-коды, причем последний используется сканером штрих-кода для поиска кассет. После создания меток на кассетах поместите кассеты в библиотеку. Процесс помещения кассет может различаться для каждого типа библиотеки, поэтому лучше обратиться к документации производителя.

### Создание списка кассет для Amanda

После того как мы разместили все кассеты в библиотеку и библиотека нашла их, время приступить к созданию меток Amanda на каждой ленте, что может быть выполнено с помощью следующей команды:

```
amlabel DailySet1 DailySet1-NR slot SlotID
```

где NR-номер кассеты (любое число, но желательно, чтобы оно совпадало с номером слота), и SlotID – номер слота в библиотеке. Например, если у вас 60 кассет, то можно воспользоваться следующим скриптом:

```
#!/usr/bin/perl
use strict;
foreach my $i(1..60)
{
  system("amlabel -f DailySet1 DailySet1-$i slot $i");
}
```

## Запуск и проверка

Таким образом, мы выполнили все первоначальные шаги и подошли к финальной стадии – запуск процесса архивирования.

Всего существует три режима работы процесса архивирования:

- архивирование всех данных всех серверов;
- архивирование конкретного сервера;
- архивирование конкретного диска конкретного сервера.

Для начала попробуем создать резервную копию одного диска нашего сервера:

```
amdump DailySet1 server1.domain.com /home
```

Эта команда указывает Amanda сделать копию данных, расположенных на сервере server1.domain.com в каталоге /home. Процесс занимает некоторое время и включает в себя следующие этапы:

- запуск планировщика задач;
- оценка объема данных на клиенте;
- сбор данных и отправка на временное хранилище архивирующего сервера;
- запись архивных данных с временного хранилища на ленту.

Если есть желание понаблюдать за процессом, то можно увидеть процессы calcsite, tar, sendbackup на клиенте и gzip на архивирующем сервере. Как только процедура архивирования завершится, необходимо проверить результат всего процесса.

### Проверка архива

После того, как мы завершили архивирование, можно проверить результаты процесса с помощью команды:

```
amadmin DailySet1 info servername [disk]
```

В нашем случае это должно выглядеть вот так:

```
amadmin DailySet1 info server1.domain.com /usr
```

```
Current info for server1.domain.com /usr:
Stats: dump rates (kps), Full: 2109.9, 1071.6, -1.0
Incremental: -1.0, -1.0, -1.0
compressed size, Full: 36.8%, 36.8%,-100.0%
Incremental: -100.0%,-100.0%,-100.0%
Dumps: lev datestamp tape file origK compK secs
0 20070517 DailySet1-1 66 1288890 474720 225
```

Здесь можно видеть уровень архива (полный или инкрементальный), имя кассеты, где был сохранен архив, дату, количество файлов, оригинальный и сжатый объемы архива и количество секунд, потраченных на процедуру. Если все выглядит правильно, то можно запускать систему в рабочем режиме, т.е. ежедневно.



## Исключение и разбивка данных

В разделе будут описаны два очень важных момента в работе системы – как исключить данные из процесса архивирования и как разбить большой объем данных на несколько архивов меньшего размера.

### Исключение данных

Как уже было показано, в нашей стратегии архивирования мы указали файл, который содержит список файлов, которые необходимо исключить из архивов:

```
define dumptype default
{
.....
exclude list "amandaexclude"
.....
}
```

Файл amandaexclude должен быть расположен в верхнем каталоге каждого каталога, определенного в файле disklist. Например, если определен /home в файле disklist, то файл amandaexclude должен быть расположен в /home/amandaexclude. В этом файле указаны каталоги и файлы, которые не должны быть архивированы:

```
log/httpd/*
log/httpd2/*
log/httpd2-ssl/*
log/httpsd/*
log/mailllog*
tmp/*
*.tmp
*.temp
```

Обращаем внимание, что элементы списка должны быть записаны от начала каталога из disklist. Для примера, если у вас есть /var из disklist, и если вы укажете /var/log/httpd в файле excludeamanda, то Amanda решит, что каталог /var/var/log/httpd должен быть исключен, что неверно.

### Разбивка данных

К сожалению, одним из недостатков Amanda является невозможность размещения одного каталога на нескольких кассетах, таким образом, архивирование каталогов, превышающих 200 Гб (после сжатия), невозможно. Конечно, можно указать список подкаталогов из сверхбольших каталогов, но проявляется одна проблема, которую я поясню на основе следующего примера:

```
/home/mysql/
/home/www/

/home/users/user1
/home/users/user2
```

Для того чтобы исключить ошибки и ручной труд, можно воспользоваться следующей командой для поиска подкаталогов типа /home/users/user\*\*\*:

```
find /home -t d -mindepth 2 -maxdepth 2
```

Таким образом, будут найдены все подкаталоги, которые нужно описывать отдельно в disklist. Но нам еще необходимо найти каталоги с меньшей глубиной:

**STORAGE  
EXPO**

**Storage Expo**

**Единственная в России  
выставка-конференция  
по системам хранения  
данных.**

На одной площадке – выставки

**infosecurity**  
RUSSIA

**DOCUMENTATION**

**26–28 сентября  
2007**

Москва, Экспоцентр на Красной Пресне



[www.storage-expo.ru](http://www.storage-expo.ru)

Генеральные информационные спонсоры:

Открытые  
системы

Cnews

Информационные спонсоры:

Storage

computerworld

Директор

softline

intelligent

ИКС

СИСТЕМНЫЙ  
администратор

Информационный  
журнал

PCweek

connect

БАНКОВСКИЕ  
ТЕХНОЛОГИИ

СЭТ

СЭТ

СЭТ

СЭТ

СЭТ

СЭТ

Организаторы:

РЕСЭК

Reed Exhibitions®

```
find /home -t d -mindepth 1 -maxdepth 1
```

Если результаты обеих команд включить в disklist, то он будет выглядеть следующим образом:

```
/home/mysql/
/home/www/
/home/users/
/home/users/user1
/home/users/user2
```

Таким образом, в список каталогов попадает сверхбольшой каталог /home/users, и в результате задача по разбиению данных остается нерешенной.

Для решения этой проблемы достаточно включить каталоги из /home/users в список для исключения директории /home как показано:

```
server1.domain.com /home
{
default2
exclude append /home/users/user1
exclude append /home/users/user2
}
server1.domain.com /home/users/user1
{
default
}
server1.domain.com /home/users/user2
{
default
}
```

**Замечание:** используется новая стратегия «default2», которая не имеет опции «exclude», иначе она перекроет опцию «exclude append».

## Восстановление с Amanda

Теперь самое главное – восстановление данных из архива. Сейчас мы разберем, как восстанавливать данные на стороне архивного сервера. Как восстанавливать данные на стороне клиента – тема следующей статьи. Итак, сперва необходимо найти кассету, на которой находятся интересующие нас данные.

Например, если нужно восстановить данные каталога /home с клиента server1.domain.com, то на стороне архивного сервера нужно выполнить команду:

```
amadmin DailySet1 info server1.domain.com /home
```

Если система успешно работала и данные присутствуют на ленте, то вы должны увидеть приблизительно такую картинку:

```
Current info for server1.domain.com /home:
Stats: dump rates (kps), Full: 2186.8, -1.0, -1.0
Incremental: 1413.2, -1.0, -1.0
compressed size, Full: 88.2%, -100.0%, -100.0%
Incremental: 66.0%, -100.0%, -100.0%

Dumps: lev datestamp tape file origK compK secs
0 20070403 DailySet1-10 7 34495940 30409476 13906
1 20070517 DailySet1-59 124 3532300 2330312 1649
```

Оказывается, что у нас есть две копии каталога /home но с различным уровнем сохранения. Уровень «0» означает полную копию каталога /home и уровень «1» означает

инкрементальный архив данных, которые были изменены с момента создания полной копии.

Для получения наиболее свежих данных необходимо извлечь и распаковать оба архива, что включает в себя два шага.

Загрузка нужной кассеты в привод:

```
amtape DailySet1 label DailySet1-1
```

Извлечение архива с ленты с помощью команды amrestore:

```
amrestore /dev/nst0 server1.domain.com /home
```

где:

- /dev/nst0 – накопитель на ленте;
- server1.domain.com – имя клиента;
- /home – каталог, который был определен в disklist.

Если архив успешно был извлечен с ленты, то в текущем каталоге вы обнаружите файл server1.domain.com.\_home.20070403xxxxx.0.1, что является tar-архивом сжатым с помощью gzip.

Следующим этапом необходимо достать копию инкрементального архива:

```
amtape DailySet1 label DailySet1-59
amrestore /dev/nst0 server1.domain.com /home
```

И как результат этого действия, вы должны получить файл server1.domain.com.\_home.20070517, который также является tar-архивом, сжатым с помощью gzip. Далее, раскрыв оба архива с помощью tar, вы получите наиболее свежую копию данных, доступную в архиве.

## Заключение

Я не стремился изложить полное руководство по созданию системы резервного копирования, а лишь рассмотрел основные понятия и базовые принципы, необходимые для создания собственной системы, которая более года успешно используется в нашей компании.

Многие расширенные компоненты остались за рамками статьи, такие как:

- Планирование расписания задач.
- Проверка целостности архивов.
- Использование нескольких ленточных накопителей.
- Обслуживание и мониторинг ленточных библиотек.
- Аппаратное сжатие.
- Дамп файловых систем и остановка серверов баз данных перед архивированием.

Но сегодняшнего материала уже достаточно для понимания, как устроена и работает система резервного копирования, и в будущем мы постараемся осветить другие аспекты, возникающие в процессе эксплуатации системы. 🌐

*Ни автор, ни редакция не несут ответственности за возможные последствия при использовании информации из данной статьи.*





#### Mandriva Linux 2007

Дистрибутив Mandriva (панее, до слияния с Connectiva называвшийся Mandrake), по праву считается идеальным для неподготовленного пользователя. Mandriva Linux невероятно прост в установке благодаря современному графическому установщику. Гордость дистрибутива – комплект графических утилит для настройки системы, объединенные в Mandriva Control Center. Установив Mandriva, вы сможете настроить абсолютно все, от звуковой карты до файрволла, не прибегая к помощи командной строки.

#### Cedega

Продукты Mandriva Linux 2007 Discovery и PowerPack включают TransGaming Cedega, позволяя запускать Windows-версии игр.

TransGaming Technologies создала уникальную технологию, позволяющую разработчикам собирать игры для одной системы и затем легко запускать их на других.

Технология TransGaming уникальна тем, что разработчикам не нужно думать о поддержке кроссплатформенности. TransGaming Cedega позволяет запускать популярнейшие игры, такие как Battlefield 2, Elder Scrolls IV: Oblivion, World of Warcraft, Civilization IV, Madden 2006 и множество других. Нет лучшего способа играть в Linux!

#### LinDVD

Продукты Mandriva Linux 2007 Discovery и PowerPack включают InterVideo LinDVD, позволяя просматривать DVD-диски абсолютно легально и без долгой настройки.

InterVideo -- лидирующий производитель программного обеспечения для просмотра DVD, а также мультимедиа-приложений.

#### la Ora

Последний раз Мандрива меняла тему рабочего стола ещё в версии 9.1, это была Galaxy. Для 2007 мы разработали с нуля новую тему назвав её la Ora ("здравствуйте" на языке франкоговорящих поленизийцев), поменяв там всё начиная от рамок окна заканчивая виджетами и иконками. Новая тема проще и легче, более яркая, хоть и используется всего несколько цветов.

#### 3D

Поддержка нового трехмерного рабочего стола (AIGLX или Xgl) и новая утилита для его настройки (drak3d): Mandriva -- единственный дистрибутив, предоставляющий легкий доступ к обеим технологиям, так что совместимость с оборудованием настолько широка, насколько это вообще возможно. Drak3d может сам определить лучший 3D-сервер. AIGLX и Xgl доступны в KDE и Gnome.

#### Новый RPMdrake

Mandriva разработала лучшую утилиту для установки, удаления и обновления программ. Новый RPMdrake дает вам информацию о том, какие пакеты у вас установлены, какие могут быть установлены, что рекомендует Mandriva, какие обновления доступны и т.д.

#### Invictus Firewall

Mandriva разработала Invictus Firewall, высоконадежный брандмауэр для кластерных систем. Множество брандмауэров на машинах может быть настроено за считанные минуты, без отрыва их пользователей от работы.

#### CRM, ERP

Tiny ERP является бесплатным программным продуктом для интеграции данных и повышения продуктивности. Включен в Powerpack+. Пакет обрабатывает бизнес-процессы, продажи, финансы, поддерживает цепочки и менеджмент проекта... TinyERP дает возможность SOHO-пользователям наблюдать за их бизнесом.

Joomla -- открытая система управления контентом (CMS). Используется для всего, начиная с простых веб-сайтов и заканчивая сложными корпоративными приложениями. Мы выбрали Joomla потому, что она проста в установке, настройке и при этом надежна.

#### BitDefender

BitDefender предоставляет решения для защиты сетей (антивирус, анти-спам, анти-spyware) для корпоративных и серверных нужд. BitDefender отслеживает трафик, блокируя вирусы, троянских коней и другие вредоносные приложения, защищая пользователей и их данные.

BitDefender -- это:

- Комплексная технология анти-спама
- Управление пользователями и группами
- Совместимость с SNMP
- Продвинутая система обновления



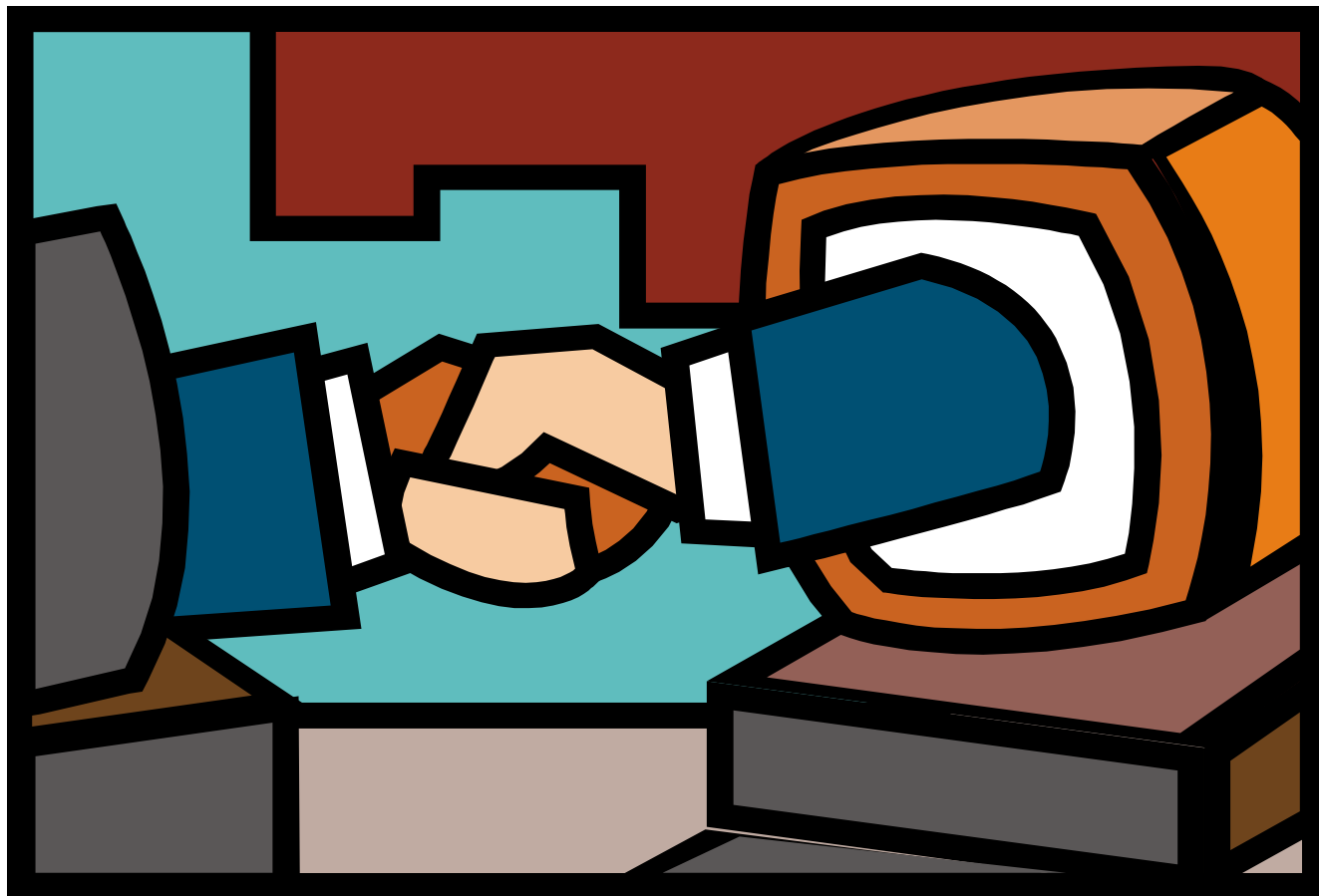
Закажите продукты Mandriva (Mandrakelinux) в Линуксцентре или у наших партнеров !

[www.linuxcenter.ru/mandriva](http://www.linuxcenter.ru/mandriva)

Линуксцентр представляет авторизованные курсы Mandriva Linux, сертифицированные LPI.org

[www.linuxcenter.ru/training](http://www.linuxcenter.ru/training)

# Доступ к Active Directory с помощью прилинкованного SQL-сервера



**Иван Коробко**

**Ни для кого не секрет, что скорость получения данных из Active Directory с помощью штатных средств в сценарии оставляет желать лучшего. Одно из решений проблемы – использовать прилинкованный SQL-сервер.**

Осуществляя доступ к Active Directory с помощью ADsDSOObject, обеспечивают полный доступ к свойствам ее объектов: их можно создавать, удалять, изменять свойства. Основной недостаток использования ADsDSOObject-провайдера – очень низкая скорость получения данных. Например, если читать из Active Directory свойства 500-600 объектов, отфильтровывая их из общей массы, то эта процедура занимает по времени 1-3 минуты. Увеличить скорость чтения данных можно, используя в качестве провайдера прилинкованный к Active Directory SQL-сервер.

Скорость решения аналогичной задачи сокращается до нескольких секунд. Однако не все так хорошо, как кажется с первого взгляда. Во-первых, с помощью прилинкованного сервера можно осуществлять только быстрый поиск и чтение данных. Так что записывать данные придется с помощью ADODB-соединения. Во-вторых – по умолчанию прилинкованный сервер имеет ограничение по количеству выводимых записей – 1000. Это ограничение – изменяемый параметр (см. KB243281, Controlling the Active Directory Search Buffer Size (<http://support.microsoft.com/kb/243281>)), но все-таки необходимо

о нем помнить при формировании запросов.

## **Теория создания прилинкованного сервера**

Прилинкованный сервер можно создать двумя способами – программным и вручную.

### **Создание прилинкованных серверов вручную**

Чтобы создать прилинкованный сервер вручную, необходимо войти в «SQL Server Enterprise Manager → SQL Server Group → Сервер → Security → Linked Server» и в контекстном меню выбрать



«New Linked Server...». В диалоговом окне присутствуют следующие параметры (см. **рис. 1**):

- **Linked name** – произвольное имя создаваемого сервера. Максимальная длина 128 символов.
- **Provider name** – имя провайдера выбирается из списка, например Microsoft Jet 4.0 OLE DB Provider. Максимальная длина этого обязательного параметра – 128 символов. Остальным параметрам значения присваиваются по необходимости.
- **Product name** – комментарий прилинкованного сервера размером до 128 символов.
- **Data Source** – имя источника данных или его IP-адрес. Максимальная длина 4000 символов.
- **Provider String** – строка соединения, в которой могут быть заданы имя, пароль и другие характеристики доступа, например – «Encrypt Password=False;Integrated Security=SSPI;». Максимальная длина 4000 символов.

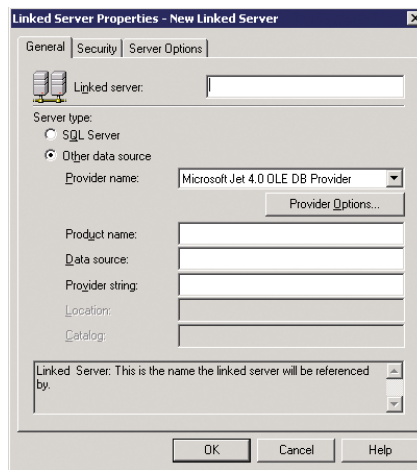


Рисунок 1. Создание прилинкованного сервера

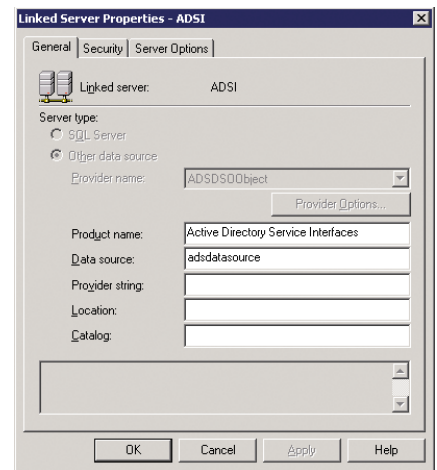


Рисунок 2. Прилинкованный к AD сервер

OLE DB Provider for Microsoft Directory Services" does not provide either the tables or views. Therefore you will get the error "Error 7301: Could not obtain a required interface from OLEDB provider ADsDSOObject"

Не обращайте внимания на него и переходите к созданию запроса.

Во второй вкладке – «Security» осуществляется конфигурация безопасности. Для прилинкованного сервера к Active Directory настройки можно оставить по умолчанию: «Be may using the login's current security context».

Третья вкладка – «Server Options». Удостоверьтесь, что отмечены опции Data Access и Use Remote Collation. Использование RPC в случае соединения с Active Directory не обязательно.

## Создание прилинкованного сервера к Active Directory на практике

Для создания прилинкованного к AD сервера используется провайдер OLE DB Provider for Microsoft Directory Services (ADsDSOObject). Именно его необходимо выбрать в списке «Provider Name» во вкладке «Settings». В поле «Data Source» указывают adsdatasource. Рекомендуется добавить описание созданного сервера в поле «Product Name», например Active Directory Service Interfaces. Остальные настройки остаются без изменений (см. **рис. 2**).

Если по какой-то причине OLE DB Provider for Microsoft Directory Services провайдер отсутствует в предлагаемом списке, необходимо изменить значение параметра AllowInProcess (тип DWORD) в ветви HKLM\Software\Microsoft\MSSQLServer\Providers\ADSDSOObject на 1 (см. **рис. 3**).

Существует альтернативный вариант прилинкованного сервера с помощью Microsoft Jet 4.0 OLE DB Provider. Все настройки остаются прежними, за исключением Provider String:

```
Provider=ADsDSOObject;Encrypt Password=False;Integrated
Security=SSPI;Mode=Read;Bind Flags=0;ADSI
Flag=-2147483648
```

В созданном прилинкованном сервере находятся два объекта – Tables и Views. При попытке посмотреть их наполнение провайдер данных выдаст сообщение об ошибке:

## Программное создание прилинкованного сервера

Для программного создания прилинкованного сервера программным способом используется функция sp\_addlinkedserver, у которой следующий синтаксис:

```
sp_addlinkedserver [ @server = ] 'server'
[ , [ @srvproduct = ] 'product_name' ]
[ , [ @provider = ] 'provider_name' ]
[ , [ @datasrc = ] 'data_source' ]
[ , [ @location = ] 'location' ]
[ , [ @provstr = ] 'provider_string' ]
[ , [ @catalog = ] 'catalog' ]
```

где:

- server – имя создаваемого прилинкованного сервера;
- product\_name – его описание;
- provider\_name – имя провайдера, к которому прилинковывается сервер;
- data\_source – источник данных – имя или IP-адрес ресурса;
- location – местонахождение базы как интерпретатора OLE-DB провайдера;
- provider\_string – строка соединения, содержащая параметры создаваемого соединения, при необходимости;
- catalog – имя каталога, который будет использоваться как временный во время соединения с провайдером.

На практике запрос, формирующий прилинкованный сервер (см. **рис. 2**) к Active Directory, следующий:

```
sp_addlinkedserver 'ADSI', 'Active Directory Service Interfaces',
'ADSDSOObject', 'adsdatasource'
```

## Использование прилинкованного сервера

Прежде чем рассказывать о чтении данных через прилинкованный сервер, приведу пример получения данных из AD

с помощью обычного ADODB-соединения. Рассмотрим задачу формирования списка компьютеров в текущем домене. Листинг на VBScript:

```
Set objConnection = CreateObject("ADODB.Connection")
Set objCommand = CreateObject("ADODB.Command")
objConnection.CommandTimeout = 120
objConnection.Provider = "ADsDSOObject"
objConnection.Open "Active Directory Provider"
Set objCommand.ActiveConnection = objConnection

Set sql=objConnection.execute("SELECT cn FROM ↵
'LDAP://DC=firm,DC=ru' WHERE objectClass='Computer' ")
sql.Movefirst

Do Until sql.EOF
    Wscript.Echo sql.Fields("cn").Value
    sql.MoveNext
Loop
```

В данном и во всех последующих листингах для наглядности имя домена намеренно присутствует в явном виде.

## Query Analyzer

Чтение данных в Query Analyzer осуществляется с помощью:

```
openquery( linked_server , 'query' )
```

где linked\_server – имя прилинкованного сервера, а query – SQL-запрос, заключенный в кавычки.

Запрос, формирующий список компьютеров, входящих в домен, включает в себя подзапрос, в котором непосредственно идет обращение к AD:

```
select * from openquery
(ADSI,
'
    select cn
    from 'LDAP://DC=firm,DC=ru'
    where objectclass='computer'
')
```

**Замечание:** в SQL-запросе «select cn from "LDAP://DC=firm,DC=ru" where objectclass="computer"» имя домена и параметр фильтра заключаются в двойные апострофы, а не в кавычки.

Характеристики, считываемые из Active Directory, могут относиться к одному из следующих типов данных: строка, массив, бинарное значение, число. Создавая более сложные SQL-запросы, учитывайте тип данных считываемой переменной. Используя функцию Convert, осуществляйте преобразование типов. Она имеет три параметра: type –

тип данных, к которому необходимо преобразовать переменную, num – максимальное ограничение количества символов, field – имя поля. При считывании данных из AD данные преобразуются к строке переменной длины: varchar(50). Синтаксис функции выглядит следующим образом:

```
openquery( linked_server , 'query' )
```

Рассмотрим характерный пример. Требуется построить таблицу, в которой будет две колонки – UserName и Description. В первую колонку должны попасть все имена пользователей в домене. Им соответствует значение поля cn в AD. Во вторую – должности соответствующих сотрудников, которые зафиксированы в поле Description его учетной записи.

В основном запросе вместо «\*» должны быть указаны два поля. Причем данные необходимо преобразовать, а столбцы переименовать. Преобразование типов данных осуществляется с помощью описанной ранее функции convert(), а переименование столбцов – с помощью инструкции OldFieldName as NewFieldName, где OldFieldName – считанное имя поля, а NewFieldName – отображаемое. Таким образом, основной запрос выглядит так:

```
Select Convert(varchar(50), cn) as UserName,
Convert(varchar(50), description)
From openquery (ADSI, '...')
```

Поскольку желаемое название второго столбца совпадает с именем переменной, то нет необходимости его переименовывать.

С помощью вложенного запроса считываем данные из AD:

```
Select cn, description from 'LDAP://DC=firm,DC=ru' ↵
where objectclass='person' and not objectclass='computer'
```

Суммируя сказанное, получим следующий запрос:

```
Select Convert(varchar(50), cn) as UserName,
Convert(varchar(50), description)
From openquery (ADSI,
'Select cn, description
from 'LDAP://DC=firm,DC=ru'
where objectclass='person' ↵
and not objectclass='computer'
')
```

## VBScript

Для подключения к SQL-серверу на VBScript также используется ADODB-соединение, однако связь с AD идет не напрямую через ADsDSOObject, а с помощью прилинкованного сервера.

С помощью функции CreateObject создают два объекта: Adodb.Connection – для соединения с SQL-сервером и Adodb.Recordset – с прилинкованным к нему сервером. В строке соединения не нужно указывать имя базы, поскольку ни к одной из них подключения не осуществляется:

```
set a=CreateObject("Adodb.Connection")
str="driver={sql server};server=SQLServer; ↵
trusted_connected=yes;"
a.open(str)
a.cursorlocation=3
```

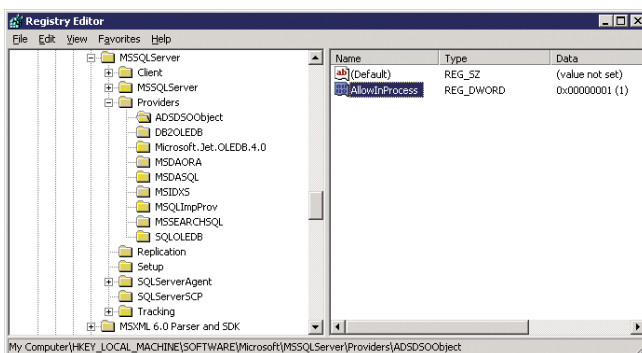


Рисунок 3. Провайдер OLE DB Provider for Microsoft Directory Services в реестре



```
set rs=CreateObject("Adodb.Recordset")
str_g="select * from OpenQuery (ADSI, 'select cn _
from 'LDAP://DC=firm,DC=ru' _
where objectclass='computer' ')"
rs.open str_g, a, 1, 2, 1
rs.movefirst
Do Until rs.EOF
Wscript.Echo rs.Fields(0).Value
rs.MoveNext
Loop
```

**Замечание:** если созданный скрипт запускается от имени локального, а не доменного пользователя, то SQL-сервер выдаст сообщение об ошибке:

```
An error occurred while preparing a query for execution against
OLE DB provider 'ADsDSOObject'.
OLE DB error trace [OLE/DB Provider 'ADsDSOObject'
CommandPrepare::Prepare returned 0x80040e14].
```

## Практика использования прилинкованного сервера

Ранее говорилось об ограничении прилинкованного сервера: он может использоваться только для чтения данных. Записать какие-либо параметры в AD с его помощью невозможно. Комбинация чтения данных из AD с помощью прилинкованного сервера и запись их в базу с помощью ADO DB позволяют создавать быстро работающие скрипты, которые можно интегрировать в ASP, ASPX-файлы. Предположим, что необходимо анализировать поле telephonenumber всех учетных записей пользователей в Active Directory, и если поле содержит информацию – записать в него «\*\*\*».

Соответствия объектов классам AD

Тип объекта	Значение objectclass	Тип объекта	Значение objectclass
Computer	Top	OU	Top
	Person		OrganizationalPerson
	OrganizationalPerson	Printer	Top
	User		Leaf
Contact	Computer		ConnectionPoint
	Top		PrintQueue
	Person	SharedFolder	Top
	OrganizationalPerson		Leaf
Group	Contact		ConnectionPoint
	Top		Volume
InetOrgPerson	Group	User	Top
	Top		Person
	Person		OrganizationalPerson
	OrganizationalPerson		User
	User		
	InetOrgPerson		

Алгоритм сценария следующий: с помощью прилинкованного сервера сформируем запрос, который будет выводить список пользователей, у которых поле telephonenumber пустое. Прежде чем создавать скрипт на VBScript, настоятельно рекомендуется сформировать запрос к прилинкованному серверу в Query Analyzer. Это позволит ускорить создание скрипта. Для удобства контроля в Query



**Международная  
специализированная  
выставка-конференция  
по информационной  
безопасности**

На одной площадке – выставки



[www.infosecuritymoscow.com](http://www.infosecuritymoscow.com)

**26–28 сентября 2007**

Москва, Экспоцентр на Красной Пресне  
Павильон 8, зал № 1, 2



Платиновый спонсор выставки Infosecurity: **Microsoft**

Генеральные информационные спонсоры: **Открытые системы** **СNews**

Генеральный Интернет партнер: **Positive Technologies**

Информационные спонсоры:



Организаторы:



Analyzer сделаем в таблице два поля – имя (UserName) и номер телефона (Tel), которым соответствуют поля cn и telephonenumber. В подзапросе непосредственно к AD укажем оба эти поля.

Теперь нужно правильно сформировать фильтр where. Во-первых, необходимо отфильтровать учетные записи пользователей от всех объектов (см. **таблицу**). Как видно из таблицы, objectclass должен принадлежать к классу Person или User и не принадлежать к классу Computer. Поэтому фильтр должен быть таким:

```
objectclass='person' and not objectclass='computer'
```

К нему необходимо добавить еще одно условие:

```
not telephonenumber='''
```

#### Замечание:

1. Обратите внимание, что инструкция «telephonenumber is NULL» не будет работать, так как в запросе к AD используется упрощенная версия интерпретатора SQL, многие функции не поддерживаются.
2. Необходимо помнить, что последовательность выражений в запросе играет роль: наивысший приоритет у первого выражения, наименьший – у последнего.

Учитывая описанное, составим SQL-запрос к AD через прилинкованный сервер:

```
select
convert(varchar(50), cn) as UserName,
convert(varchar(50), telephonenumber) as Tel
from openquery
(ADSI, '
select cn, telephonenumber
from 'LDAP://DC=firm,DC=ru'
where objectclass='person'
and not objectclass='computer'
and not telephonenumber='''*тел.*''
')
```

Сценарий будет работать гораздо медленнее, если, к примеру, фильтр телефонного номера вынести из подзапроса в основной, поэтому старайтесь использовать все фильтры в непосредственном запросе к Active Directory. Приведу пример неправильного использования фильтра. Красным отмечены внесенные в листинг изменения:

```
select
convert(varchar(50), cn) as UserName,
convert(varchar(50), telephonenumber) as Tel
from openquery
(ADSI, '
select cn, telephonenumber
from 'LDAP://DC=firm,DC=ru'
where objectclass='person'
and not objectclass='computer'
and not telephonenumber='''*тел.*'' */
')
where telephonenumber is null
```

Добившись правильной работы сценария, перейдем к формированию скрипта на VBScript.

Запись значений параметров в Active Directory осуществляется с помощью ADODB-соединения с использованием провайдера ADsDSOObject. Исходными данными являются distinguishedName – местоположение объекта и имя корректируемого поля, поэтому созданный SQL-

запрос необходимо трансформировать, заменив поле cn на distinguishedName.

Сценарий работает по следующему алгоритму: сначала создается запрос. Его результатом является список, каждая строка которого содержит два параметра. Они передаются в функцию записи параметров.

Рассмотрим отдельно сценарий записи данных в Active Directory. Изменение атрибутов любого объекта осуществляется с помощью метода Put() с предварительным получением к нему доступа:

```
Domain = GetObject("LDAP://rootDSE").Get( "
"defaultNamingContext")
Set oUser = GetObject("LDAP://cn=Ivanov,Ivan,"& Domain)
oUser.Put "Description", "Иванов Иван Петрович"
oUser.SetInfo
Set oUser = Nothing
```

Первый аргумент метода Put – изменяемое поле, второй – его значение. Описанному алгоритму соответствует следующий сценарий:

```
Domain = "LDAP://" + GetObject("LDAP://rootDSE").Get( "
"defaultNamingContext")

set a=CreateObject("Adodb.Connection")
str="driver={sql server};server=SQLServer; "
trusted_connected=yes;"
a.open(str)
a.cursorlocation=3


set rs=CreateObject("Adodb.Recordset")
str_q="select convert(varchar(50), distinguishedName ) as
as Path, convert(varchar(50), telephonenumber) as
as Tel from openquery (ADSI, '
select distinguishedName , telephonenumber
from 'LDAP://Domain+'' where objectclass='person'
and not objectclass='computer'
and not telephonenumber='''*тел.*'' )"
rs.open str_q, a, 1, 2, 1
rs.movefirst
Do Until rs.EOF
WriteDate (rs.Fields(Path).Value, rs.Fields(Tel).Value)
rs.MoveNext
Loop

Function WriteDate(a,b)
Set oUser = GetObject("LDAP://"&a)
oUser.Put " telephonenumber", b
oUser.SetInfo
Set oUser = Nothing
End Function
```

## Заключение

Прилинкованные серверы, кажущиеся с первого взгляда неудобными и громоздкими в использовании, позволяют значительно повысить скорость работы приложений, в которых они применяются. Отсутствие возможности записи в прилинкованные базы с помощью сервера может быть не только недостатком, но и преимуществом.

Если необходимо добиться, чтобы все пользователи имели доступ к базе данных только на чтение, – использование прилинкованного сервера является идеальным вариантом для решения задачи с точки зрения администрирования. Если же необходимо обеспечить возможность делать изменения в базе – используйте сервер для получения необходимой для записи информации и записывайте данные традиционным способом.

Такой подход обеспечивает увеличение скорости работы созданных приложений. 



# Время надежных решений

ИЗДАНИЕ 1 – НОМЕР 2



Windows Server 2003

## WINDOWS SERVER ОБГОНЯЕТ LINUX



Том Нэги для «Времени надежных решений»

**CONTIDROM**, легендарный полигон Continental AG в окрестностях Ганновера, Германия.

### ГОРЯЧИЕ НОВОСТИ:

«Windows Server обеспечивает надежную среду с возможностью централизованного администрирования и управления».

Пауль Швефер,  
директор по информационным  
технологиям Continental AG



*Новая информационная система гарантирует ведущему поставщику продукции для автомобильной промышленности 99,9% надежность*

Майкл Беттендорф

ГАННОВЕР, январь 2007 г. – включая управление групповыми политиками, позволило Швиферу сделать вывод с нашей прежней системой», – говорит Пауль Швифер, директор по информационным технологиям корпорации Continental AG, одного из крупнейших поставщиков продукции для автомобильной промышленности со штатом 85 000 сотрудников по всему миру. Несовершенные инструменты управления не позволяли команде Швифера поддерживать работоспособность системы на том высоком уровне, который требуется Continental AG, поэтому была необходима смена платформы.

Сначала рассматривалось решение на базе Linux. Однако после тщательной оценки команда Швифера пришла к заключению, что она не может обеспечить надежную и прогнозируемую среду, необходимую Continental AG. И в результате они выбрали Microsoft® Windows Server® 2003.

Наличие мощных средств оптимизации и настройки, включая управление групповыми политиками, позволило Швиферу сделать вывод об очевидных преимуществах Windows Server® 2003 в сравнении с Linux. «Windows Server обеспечивает надежную среду с возможностью централизованного администрирования и управления», – говорит Швифер, уверенный, что безукоризненная управляемость служит залогом высокой надежности. «Воссоздание подобного уровня сервиса в среде Linux было бы сложным и дорогостоящим делом», – утверждает он.

Принятое решение полностью себя оправдало. С момента внедрения Windows Server 2003 поддерживает 99,9% надежность распределенной среды компании Continental AG.

### ГОРЯЧИЕ НОВОСТИ: Настроение IT-профессионалов напрямую связано с надежностью

Подтверждая глобальную тенденцию, IT-профессионалы, такие, как директор по информационным технологиям корпорации Continental AG Пауль Швифер, выражают удовлетворение (см. выше) высокой надежностью Windows Server.

Продолжение на 3 стр.



# Разворачиваем кластер Microsoft Exchange

**Андрей Бирюков**

**Надежность – зачастую основное требование, которое предъявляется к любой системе. Не являются исключением и различные информационные системы, например сервис электронной почты. Один из наиболее распространенных способов обеспечения отказоустойчивости этой службы – почтовый кластер Microsoft Exchange.**

## **Вступление к продолжению**

Сервис электронной почты является неотъемлемой частью бизнес-процессов в любой компании, независимо от ее размеров. А такие мощные почтовые системы, как Microsoft Exchange или Lotus Domino, предоставляют, помимо отправки и приема почтовых сообщений, также средства планирова-

ния и организации бизнеса. Очевидно, что при таком положении вещей почтовая система становится, пожалуй, самым критичным сервисом, и даже минутный простой этой системы чреват большими неприятностями для системных администраторов. Возможным решением проблемы отказоустойчивости является использование кластеров. Сегодня я расскажу о развер-

тывании и обслуживании кластеров Microsoft Exchange. Материал является продолжением статьи [1], посвященной кластерам на базе Microsoft.

## **Когда кластер не поможет...**

Так как внедрение кластерных систем связано с определенными, иногда весьма серьезными финансовыми за-



тратами, прежде чем приступить к описанию технологии, мне бы хотелось обсудить такой вопрос: от каких проблем помогают кластеры, а от каких – нет? Кластерные технологии предоставляют отказоустойчивость, но не гарантируют ее. Другими словами, несмотря на использование данной технологии вам не стоит забывать о таких вещах, как регулярное резервное копирование, обеспечивающее сохранность данных и настроек, резервирование и дублирование служб и приложений (например, развертывание нескольких почтовых релейов, серверов DNS и т. д.).

Следующий важный момент, связанный с обслуживанием почтовых систем. До 80% простоев почтовых служб связано с человеческим фактором, т.е. с ошибками администраторов и технических специалистов (если в вашей сети рядовой пользователь может вывести из строя почтовую систему, то дела совсем плохи, и кластер тут точно не поможет). В такой ситуации почтовый кластер также не слишком полезен, ведь ошибки допускаются людьми, и техника не всегда способна определить, верно ли выполнены те или иные действия администратора. Кластер предназначен для защиты прежде всего от аппаратных сбоев.

Не забудьте про масштабируемость вашего решения. Организации с течением времени расширяются, увеличивается количество рабочих мест, учетных записей электронной почты и т. д. В связи с этим выбирайте аппаратное обеспечение для вашего кластера с запасом по мощности и ресурсам. Иначе вы рискуете столкнуться с ситуацией, когда ваш отказоустойчивый кластер будет справляться с запросами пользователей все медленнее и медленнее. Это общий принцип, который актуален не только для кластеров, но и для любых других систем. И, наконец, немаловажный вопрос стоимости внедрения. Необходимо определить стоимость простоя и исходя из этого подобрать конфигурацию кластерного решения. Не очень разумно разворачивать четырехузловой кластер в сети из 50 пользователей, однако не менее неразумно использовать для почтовой системы одиночный сервер в сети из нескольких тысяч пользователей.

Итак, думаю мои размышления по поводу внедрения кластерных тех-

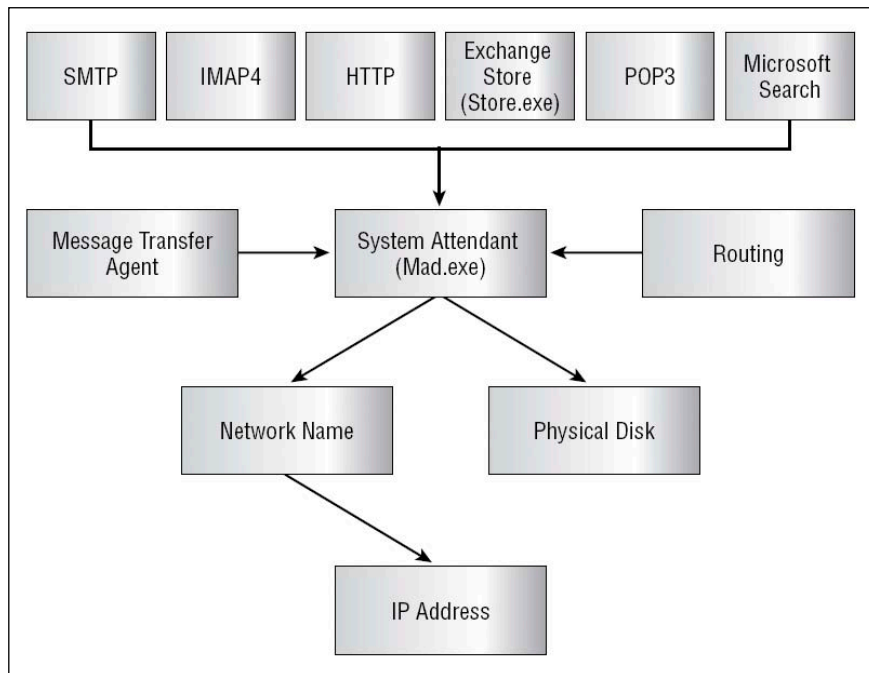


Рисунок 1. Схема зависимости ресурсов в кластере Exchange

нологий и проблем, связанных с этим, помогут вам лучше определиться с теми требованиями и задачами, которые вы предъявляете к данной технологии. Для того чтобы проверить, поддерживается ли ваше аппаратное обеспечение Windows Server 2003, вы можете воспользоваться ресурсом <http://www.microsoft.com/whdc/hcl/default.mspx>.

## Постановка задачи

Имеется два сервера: Node 1 и Node 2. Необходимо развернуть почтовую систему на базе отказоустойчивого кластера. В результате мы должны получить почтовый кластер. Данная почтовая система должна быть создана на основе двухузлового отказоустойчивого кластера, который назовем Mail.

## Архитектура

Прежде всего определимся с редакциями Microsoft Exchange, которые мы можем использовать. По аналогии с операционной системой необходимо использовать редакцию Enterprise Edition, так как Standard не поддерживает кластеризацию. Microsoft Exchange 2003 Enterprise Edition поддерживает до 8 узлов, но в качестве примера я буду рассматривать установку двухузлового кластера.

Для кластерных приложений типа Exchange возможны два режима рабо-

ты: Active/Active и Active/Passive. То есть в первом случае в каждый момент времени оба узла обрабатывают задачи Exchange, во втором случае только один узел обрабатывает задачи, а второй простаивает. Microsoft настоятельно рекомендует использовать режим Active/Passive, так как использование режима Active/Active приводит к появлению ограничений в использовании аппаратных ресурсов узлов, а также к проблемам с отказоустойчивостью.

Перед тем как начать процесс установки, нам необходимо развернуть кластер на основе службы Microsoft Cluster Service. Подробное описание, как это сделать, читайте в статье [1]. Напомню, что перед установкой нужно подготовить кворум-устройство, то есть общий диск, который будут использовать все узлы кластера. В данном случае емкость этого диска должна превышать 100 Гб, при этом для отказоустойчивости лучше всего использовать аппаратные RAID-1 или RAID-5. Также при создании кластера Exchange вам потребуется использовать оба сетевых адаптера на каждом из узлов. Это обусловлено необходимостью оптимизации пропускной способности сети. Предназначение сетевых интерфейсов аналогично описанным в предыдущей статье: Heartbeat и LAN. Первый предназначен для обмена сообщениями о состоянии узлов кластера, а второй служит для связи с внешней

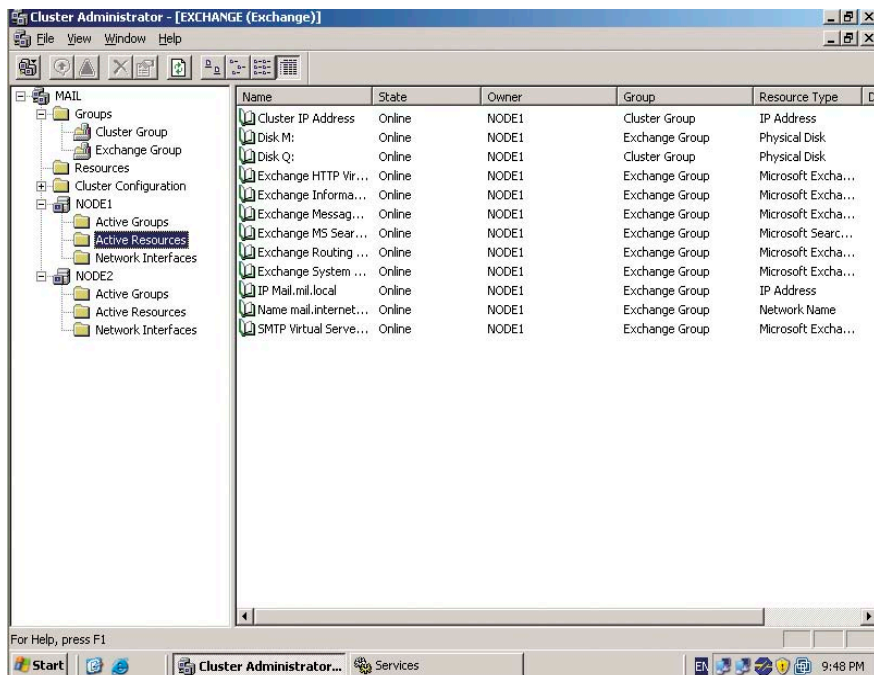


Рисунок 2. Установленный почтовый кластер Exchange

сеть. Обмен данными в кластере осуществляется через кворум-устройство, не через сеть.

Итак, в случае правильного выполнения рекомендаций статьи [1] у вас должен был получиться отказоустойчивый двухузловой кластер под названием Mail, как и предполагалось в разделе «Постановка задачи».

## Учитываем ограничения

Для того чтобы лучше спланировать использование кластером некоторых аппаратных ресурсов, в частности, жесткого диска, вам необходимо ознакомиться с рядом ограничений в Microsoft Exchange.

В Exchange 2003 есть жесткое ограничение на количество хранилищ, не более четырех групп на один сервер. Как правило, четырех хранилищ вполне достаточно для решения задачи средней сети.

Развивая тему ограничений, используемых в кластере Exchange, привожу список служб, используемых в Active/Passive-кластере:

- System Attendant;
- Information Store;
- Routing Engine;
- Message Transfer Agent (one per cluster group);
- POP3, IMAP4, SMTP, and HTTP protocols;
- MS Search;
- Exchange Management.

Все прочие службы, такие как шлюзы, коннекторы Exchange и другие, должны быть установлены на отдельных серверах.

## Приступая к установке

Прежде чем запустить файл установки, нам придется проделать некоторые предварительные работы, помимо установки кластера Microsoft Cluster Service. Для начала необходимо убрать все ненужные настройки и сетевые службы, так как они замедляют работу кластера, а также снижают уровень защищенности системы. Так, для внутреннего интерфейса Heartbeat не нужны настройки DNS и шлюз по умолчанию. Также удалите на внутреннем интерфейсе службы Client for Microsoft Networks, File & Printer Sharing for Microsoft Networks.

На закладке «Advanced Properties» в разделе «Internet Protocol (TCP/IP)» выберите «DNS» и отключите «Register This Connection's Address In DNS». Затем выберите закладку «WINS» и удалите все IP-адреса WINS-серверов. Также отключите «Netbios over TCP/IP».

Кроме сетевых служб, также желательно отключить следующие службы на каждом из узлов кластера:

- Distributed Link Tracking Client;
- Distributed Link Tracking Server;
- Distributed File System;
- Remote Access Connection Manager;

- Print Spooler Service;
- License Logging Services;
- Computer Browser.

Следующим этапом проверьте соответствие наименования дисков на каждом из узлов кластера. Например, в нашем случае имеются два узла, у каждого из них имеется диск Q, P, R. Ситуация, при которой на одном узле эти диски видны как Q, P, R, а на другом L, M, N, недопустима. На обоих узлах должны быть видны Q, P, R. Также проследите за тем, чтобы Exchange на всех узлах был установлен на локальном ресурсе и имел идентичную структуру каталогов и файлов.

Также удостоверьтесь, что на каждом из узлов установлены следующие службы: Web, NNTP, SMTP, ASP.NET.

И еще хотелось бы напомнить о том, что крайне нежелательно размещать какие-либо сторонние приложения на узлах кластера (за исключением приложений, взаимодействующих с почтовой системой, таких как почтовый антивирус).

После завершения выполнения предварительных настроек можно приступать к началу инсталляции.

Прежде всего необходимо запустить /Domainprep для подготовки домена Active Directory к установке Microsoft Exchange. Обратите внимание, что для запуска вам потребуются права из группы Domain Admins.

Далее, на первом узле кластера (том, который предполагается использовать в качестве «хозяина» ресурса) запускаем установочный файл setup.exe. В нашем случае это Node 1. В первом окне после лицензионного соглашения видим Component Selection Screen. Обычно используется типичная (Typical) установка компонентов. В этом же окне необходимо указать расположение каталога, в который будет установлен Exchange. Ещё раз обращаю внимание на то, что на всех узлах кластера этот путь должен быть одинаковым, но располагаться этот каталог должен на локальном ресурсе.

Далее нажимаете «Next» и производите установку. В результате по завершении процесса установки Exchange установлен, но сервисы не настроены. Аналогичную операцию необходимо проделать и на втором узле кластера Node 2.

## Объединяем ресурсы

Теперь приступаем к самому интересному – к настройке почтового кластера. Оба узла содержат файлы, необходимые для поддержки Exchange Virtual Server, виртуального сервера, который в качестве физической структуры использует наш кластер. Первым делом проверьте, видят ли оба узла общий кворум-ресурс. Затем в консоли Cluster Administrator необходимо создать группу. Для этого нажимаем правой кнопкой мыши на разделе «Groups», и выбираем «Create A New Group». Далее указываем наименование группы и ее описание. На следующем шаге указываем предпочтительного владельца ресурса. В нашем случае это будет Node 1.

После этого нам необходимо создать ресурс. Однако тут придется сделать небольшое отступление. Как уже упоминалось в предыдущей статье [1], ресурсы в Microsoft Cluster Service, как правило, обладают зависимостями. Для Exchange эти зависимости отображены на **рис. 1**.

Как видно из рисунка, ключевым элементом в схеме зависимостей яв-

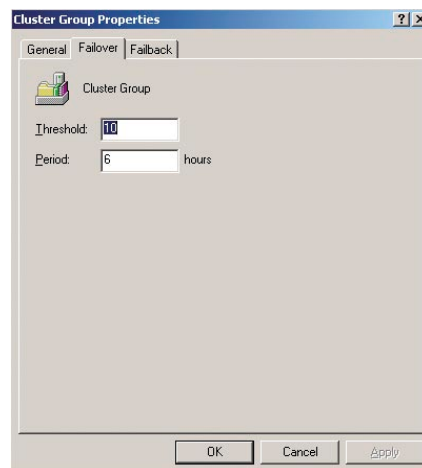


Рисунок 3. Политика перехода отключения при сбое

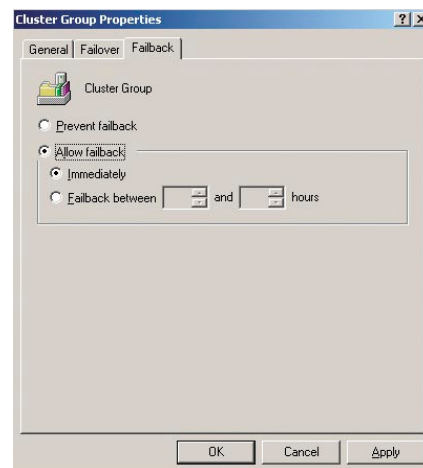


Рисунок 4. Политика возвращения ресурса

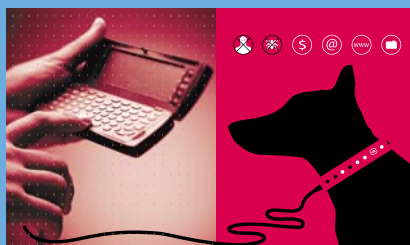
ляется служба System Attendant – ключевой компонент Microsoft Exchange. Так что такая зависимость вполне оправдана. От этой службы зависят службы протоколов SMTP, HTTP, IMAP, POP3, а также Exchange Store и Microsoft Search. Также служба связана с Message Transfer Agent и Routing. В свою очередь System Attendant зависит от Network Name и Physical Disk. A Network Name в свою очередь традиционно зависит от IP Address. За под-

робностями, описывающими построение зависимостей, рекомендую обратиться к [2].

Итак, все эти ресурсы необходимо будет создать для успешного функционирования кластера. Причем создавать нужно в соответствующей последовательности. Начнем с ресурса IP Address. Выбираем «New → Resource». В появившемся окне тип ресурса IP Address, а также имя, описание и группу, к которой принадлежит данный ресурс. В сле-

## ПРИГЛАШАЕМ ПОСЕТИТЬ

Международные специализированные выставки-конференции



### Infosecurity

4-я выставка-конференция по информационной безопасности

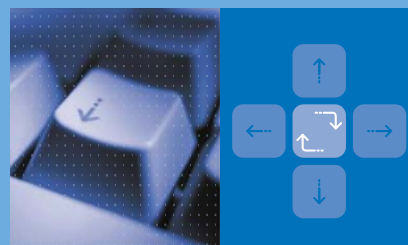
[www.infosecuritymoscow.com](http://www.infosecuritymoscow.com)



### Storage Expo

3-я выставка-конференция по системам хранения данных

[www.storage-expo.ru](http://www.storage-expo.ru)



### Documation

2-я выставка-конференция по управлению корпоративной электронной информацией

[www.documation.ru](http://www.documation.ru)

3 выставки пройдут одновременно:

26 – 28 сентября 2007  
Москва, Экспоцентр

Платиновый спонсор: **Microsoft**

Организаторы: **РЕСЭКС** и **Reed Exhibitions®**

Обменяйте открытку на приглашенный билет при входе на выставки или зарегистрируйтесь на одном из сайтов выставок-конференций



дующем окне указываем возможных владельцев, это узлы Node 1 и Node 2. Затем необходимо прописать IP-адрес ресурса, который будет использоваться для доступа к кластеру.

В соответствии со схемой следующим требуется указать сетевое имя. Обратите внимание на то, что это имя впоследствии будет использоваться для подключения профилей почтовых клиентов Outlook к почтовому кластеру. Прodelываем действия, аналогичные описанным в предыдущем разделе. Только в качестве создаваемого ресурса указываем Network Name. Соответственно, в окне «Dependencies» необходимо выбрать «IP address». В качестве сетевого имени кластера указываем Mail.

Следующий ресурс – это Disk Resources. Так же как и ранее, указываем в качестве ресурса Disk Resource и выбираем общие кворум-устройства. Необходимо указать все общие диски, используемые для хранилища, журнала событий и т. д. В качестве зависимости указываем «Network Name».

Создав Disk Resources, мы подготовили наш кластер к созданию ре-

сурсов, используемых непосредственно Exchange. Первым из этих ресурсов должен быть Exchange System Attendant. Для этого выбираете «Exchange Server Group», далее «Create → New», далее «Exchange System Attendant Resource». Укажите оба узла в качестве возможных владельцев ресурса. В окне зависимостей нужно указать только Network Name. У вас может возникнуть ошибочное мнение, что нужен также IP-адрес, но так как сетевое имя уже зависит от IP-адреса, то в списке зависимостей его выделять не нужно. После этого определяем administrative group, в которой данный виртуальный сервер Exchange будет создан. Будьте внимательны, сменить административную группу потом будет невозможно. Далее выбираем «Routing group», в которой будет создан данный виртуальный сервер. В отличие от предыдущего действия, это впоследствии можно будет изменить. Затем нужно указать пути к почтовым базам (databases) и журналам событий (transaction logs). И наконец, после завершения указания путей в следующем окне мы получаем рабочие ресурсы Exchange. Вы-

глядеть это должно следующим образом (см. **рис. 2**).

Обратите внимание на то, что все ресурсы должны иметь состояние Online. Если это не так, нужно вручную запустить остановленный ресурс.

Далее откройте «Exchange System Administrator» на одном из узлов свеже-созданного кластера.

Затем «Administrative Group», контейнер «Servers». Выбираем «Mailbox Store», после чего открываем закладку «Database». Здесь, возможно, указан локальный путь к почтовому хранилищу, необходимо указать путь на общем ресурсе.

После завершения всех этих нехитрых манипуляций вы получаете работоспособный, отказоустойчивый кластер.

### Если что-то пошло не так...

Что делать, если в процессе создания кластера что-то пошло не так и вы получили сообщение об ошибке или какие-то ресурсы не запускаются?

Проверьте, не использует ли какой-либо из узлов кластера TLS/SSL.

## РЕГИСТРАЦИЯ ОТКРЫТА НА САЙТАХ:

[www.infosecuritymoscow.com](http://www.infosecuritymoscow.com)

[www.storage-expo.ru](http://www.storage-expo.ru)

[www.documation.ru](http://www.documation.ru)

### Что ожидает Вас на выставках Infosecurity, Storage Expo, Documation 2007?

- Выставки проходят в 10 странах мира и являются ведущими на международном рынке.
- На одной площадке - ключевые игроки отрасли.
- Новые решения и услуги, технологические перспективы.
- Бесплатные конференции: круглые столы, презентации участников, выступления идеологов отрасли, авторов книг и публикаций, представителей госструктур и ассоциаций, а также практиков, готовых поделиться своим опытом.

#### Кому:

Руководителям компаний, департаментов и служб безопасности, ИТ и ИБ специалистам

#### От кого:

**infosecurity**  
RUSSIA

Организаторы:

**STORAGE**  
**EXPO**

**РЭСДК**  
ВЫСТАВОЧНОЕ  
ОБЪЕДИНЕНИЕ

**DOCUMATION**  
2007

Reed Exhibitions®

**Обменяйте открытку на приглашенный билет при входе на выставки или зарегистрируйтесь на одном из сайтов выставок-конференций**

В случае, если вам требуется использование защищенных каналов, обратитесь к документации по Exchange на Microsoft.com.

Удостоверьтесь, что каталог SMTP\Mailroot находится на кворум-ресурсе, не на локальном диске узла.

Проверьте соответствие букв дисков на узлах в кластере.

Еще одна проблема, с которой вы можете столкнуться, особенно после перезагрузки или отключения узлов кластера, – это то, что ресурсы Exchange «повисают» в состоянии Pending Online. В такой ситуации необходимо проверить доступность контроллеров домена Microsoft Active Directory. Как правило, узлы не могут переключиться в состояние Online, если контроллер домена недоступен.

Если проблема имеет более сложное решение, просмотрите сообщения об ошибках в журналах событий на узлах кластера.

## Тонкая настройка

Теперь необходимо произвести некоторые дополнительные настройки для обеспечения дополнительной отказоустойчивости и надежности. Прежде всего необходимо определиться с политиками отключения при сбое. Этот процесс очень важен, так что я рассмотрю его более подробно.

Когда один из узлов кластера выходит из строя (политика Failover), с данного узла перестают приходить сигналы Heartbeat. Другие узлы кластера обнаруживают отсутствие одного из узлов, и запускается процесс передачи владения (ownership) рабочим узлам кластера. Информация о передаче владения находится на кворум-устройстве. В случае возвращения в строй выбывшего узла (политика Failback) происходит обратная передача владения рабочему узлу.

Политики перехода Failover и Failback доступны в разделе свойства Exchange Server.

В политике перехода отключения при сбое нужно определить два параметра поведения кластера: пороговое значение количества сбоев (threshold) за интервал времени (period). Значения по умолчанию это 10 сбоев ресурса в группе за 6 часов. Такие значения этих параметров будут вполне приемлемы для нашего двухузлового клас-

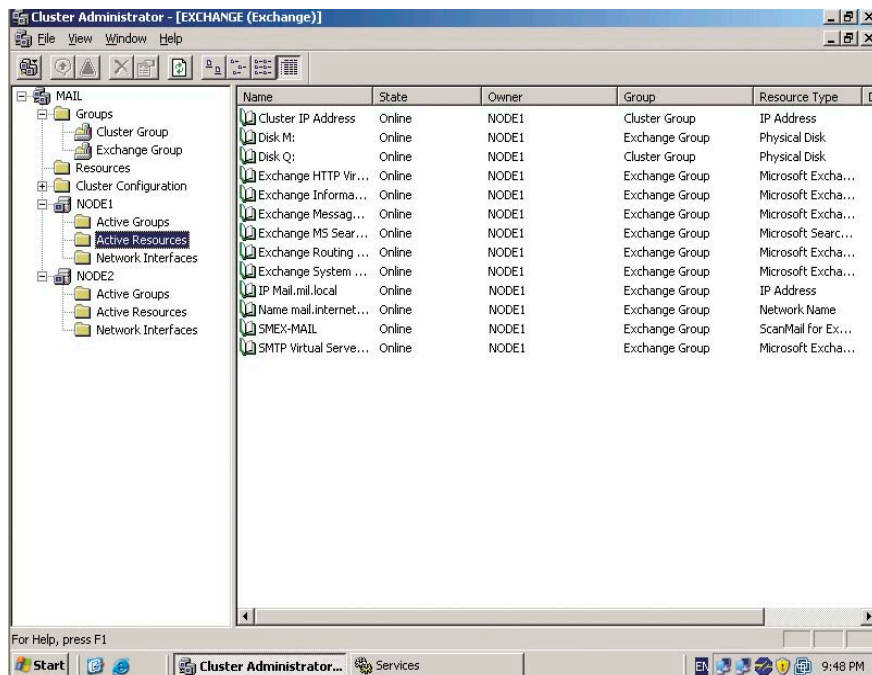


Рисунок 5. Ресурсы кластера

тера (см. рис. 3).

Политика возвращения ресурса аналогична политике выхода из строя. Но здесь вы можете запретить Failback. Это необходимо в тех ситуациях, когда смена владельца ресурса может привести к сбоям приложений кластера. В случае, если вы хотите разрешить возвращение ресурса, то вы можете разрешить делать это немедленно (Immediately) или же в определенный интервал времени, например, в нерабочие часы, когда нагрузка на кластер минимальная (см. рис. 4).

Как правило, вместе с почтовым сервером в крупных сетях используется также различное дополнительное программное обеспечение, например, антивирус, антиспам, система шифрования и т. д. Что касается средств защиты от нежелательных почтовых сообщений (антиспама), то мое мнение, что данная служба должна располагаться на почтовом шлюзе (relay) и не должна расходовать ресурсы нашего кластера.

Что же касается таких средств, как почтовый антивирус, то перед развертыванием кластера необходимо узнать, поддерживает ли ваш антивирус кластеризацию. Как правило, все современные антивирусные системы для почтовых серверов позволяют осуществлять установку на кластерные системы. При этом антивирус после установки превращается в ре-

сурс кластера, и вы можете управлять им так же, как и прочими ресурсами. В следующем примере используется Trend Micro ScanMail for Exchange в качестве антивирусной системы для почтового сервера (см. рис. 5).

Основным инструментом управления почтовым кластером является консоль Cluster Administration. Работа с почтовым кластером имеет свои особенности, в частности, нужно быть очень осторожным при работе с ресурсами, остановка основных, таких как System Attendant, приведет к остановке всех зависимых ресурсов.

К тому же не стоит забывать о тех вопросах, которые освещались в параграфе «Когда кластер не поможет...».

## Заключение с продолжением

Тема реализации кластеров на основе служб Windows ещё не заканчивается. Не стоит обходить стороной такую службу, как Network Load Balancing, и установку кластера с её помощью. В следующей статье читайте создание кластера на основе NLB, а также о его настройке и обслуживании.

1. Бирюков А. «Разворачиваем кластер на основе Windows Server 2003». //Системный администратор, №5, 2007 г. – с. 50-55.
2. J. McBee. «Microsoft Exchange Server 2003: 24 seven», Sybex.

# Строим сетевую инфраструктуру для системы 1С:Предприятие



*Сергей Алаев*

Ваших сотрудников не устраивает медленная работа системы 1С:Предприятие, и вы планируете перейти на клиент-серверное решение? Использование сервера терминалов и средств публикации приложений поможет справиться с этой проблемой, а также обеспечит возможность доступа к программе удаленных пользователей.



## Прелюдия

Ни для кого не секрет, что 1С:Бухгалтерия получила широкое распространение в различных предприятиях и организациях. Развитие и укрупнение организации неизменно связано с ростом объемов хранимой и перерабатываемой информации, а также увеличением количества одновременно работающих пользователей с программой. Возникает ситуация, при которой обеспечить приемлемую производительность работы, используя способ хранения данных в виде файлов dbf, и передачи в процессе работы всей БД на клиентский компьютер, не представляется возможным.

Выход из этой ситуации заключается в том, чтобы сменить архитектуру на клиент-серверную. Для этого потребуется перейти на SQL-версию 1С:Предприятие и Windows SQL-сервер или использовать другие решения, например, установить сервер терминалов на базе Windows Server 2003.

Это также удобно, если планируется организация работы удаленных рабочих мест.

Использование средства публикации приложений на удаленные рабочие столы 2X ApplicationServer позволит передавать приложение как есть, без элементов рабочего стола и дополнительных окон, что избавит пользователя от лишних хлопот и, кроме этого, защитит передаваемые данные. Особенно это актуально, если для доступа к приложению работники будут использовать Интернет. Основные возможности 2X ApplicationServer:

- простая возможность публиковать как обычные, так и системные приложения;
- передача приложения без окон и полная интеграция с локальным рабочим столом и панелью задач удаленного пользователя;
- встроенные возможности фильтрации доступа к приложениям (например, по пользователям или IP-адресам);
- запуск пользователем множества копий опубликованных программ в рамках одной сессии с возможностью их полного восстановления;
- возможность запускать опубликованные Windows-приложения в среде Linux и Mac;

- SSL-шифрование передачи данных и другие.

Терминальный клиент, входящий в состав Windows («Удаленный рабочий стол») не обладает никакими дополнительными возможностями, кроме как запускать программу, прописанную в среде пользователя. Поэтому после установки и испытания 2X ApplicationServer в действии вы поймете, чем отличается работа со специализированными средствами терминальной работы и стандартными решениями от Microsoft.

## Установка и настройка сервера терминалов

Желательно обновить Windows Server 2003 до SP1, чтобы иметь последнюю версию RDP-протокола передачи данных.

Для установки сервера терминалов запускаем мастер настройки сервера: «Пуск → Настройка → Панель управления → Администрирование → Управление данным сервером». Здесь нажимаем кнопку «Добавить или удалить роль». Мастер установки выведет список всех ролей нашего сервера. Среди них выберем «Сервер терминалов» и нажмем кнопку «Далее».

После установки сервера терминалов система автоматически перезагрузится.

Настроить новые подключения для служб терминалов, изменить параметры существующих подключений и удалить их позволяет компонент «Настройка служб терминалов» в разделе «Администрирование».

Здесь в свойствах существующего подключения необходимо на вкладке «Параметры клиента» отключить следующие возможности: сопоставление LPT- и COM-портов, а наибольшую глубину цвета выставить в значение «16 бит». Этого вполне достаточно для компьютеров, входящих в локальную сеть организации.

Если будут работать компьютеры, использующие низкоскоростные способы подключения, например, по модему, этот параметр можно будет переопределить в настройках клиента 2X-сервера. Все оставшиеся настройки на вкладках можно не трогать. Они позднее будут заданы в консоли 2X ApplicationServer (см. рис. 1).

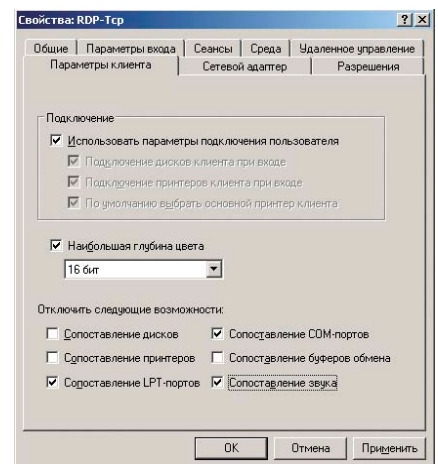


Рисунок 1. Настройка сервера терминалов

Вам потребуется в течение 120 дней установить в разделе «Установка и удаление программ» «Панели управления» необходимый компонент – Terminal Server Licensing и активировать его. Именно на этот срок для клиентов будут выдаваться временные лицензии на подключение.

При этом целесообразно использовать схему лицензирования «На устройство».

Запускаем консоль «Лицензирование сервера терминалов» в разделе «Администрирование» и в списке серверов выбираем наш сервер. В меню «Действие» нажимаем «Активировать сервер», а далее следуем инструкциям мастера активации сервера терминалов.

Также советуем отключить срабатывание механизма «Предотвращения выполнения данных» (Data Execution Prevention, DEP). Для этого открываем и редактируем в «Блокноте» файл C:\boot.ini. Ищем строку с параметром /noexecute и меняем его значение на AlwaysOff (/noexecute=AlwaysOff).

После этого необходимо перезагрузить систему. Это позволит предотвратить блокирование как самой программы 1С:Предприятие, так и драйверов некоторых принтеров, например, CANON Laser Shot LBP-1120, которые возможно будут использоваться удаленными пользователями по общему доступу.

Теперь можно приступить к установке 1С:Предприятия (в ходе инсталляции необходимо выбрать локальный режим установки, например, на диск D:\1C\Distib) и стандартного ПО, необходимого для работы (архиваторы, ко-

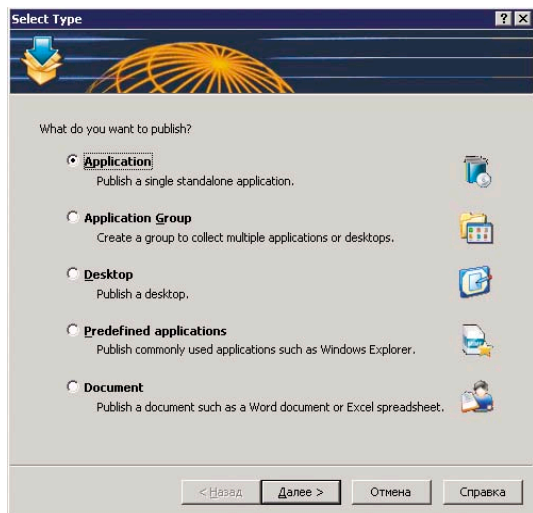


Рисунок 2. Список публикаций

деки, XML-парсера, Microsoft .NET-2.0 или старше, драйверы ключа HASP для 1С, версии не ниже 4.98, менеджера лицензий HASP от «Аладдина» (<http://www.alladin.ru/catalog/hasp/hasp4>), версии не ниже 8.20, MS Office, и прочее).

Менеджер лицензий устанавливать нужно с типом загрузки «Service» и отказаться от установки драйвера ключа, идущего в комплекте, так как он имеет более раннюю версию.

Конфигурации 1С устанавливаем в отдельные папки, например, D:\1C\Buh, D:\1C\Zarplata, D:\1C\Sklad.

Отдельно создадим папку D:\1C\Archive, куда будем делать копии баз данных.

Обратите внимание, что установка всех программ необходимо производить с помощью утилиты «Установка и удаление программ» (в «Панели управления»). В открывшемся окне нажмите кнопку «Установка новой программы» и следуйте дальнейшим указаниям мастера. Это делает программы доступными в терминальном режиме.

Все действия выполняются из-под учетной записи Администратора.

## Добавление пользователей сервера терминалов

В разделе «Администрирование» заходим в «Управление компьютером» и выбираем раздел «Локальные пользователи и группы». В меню «Действие» добавляем учетные записи для пользователей программы 1С, имеющих право входа в терминалы. Логика следующая: по умолчанию все учет-

ные записи входят в группу «Users», и пользователи не имеют достаточных прав выполнить ряд настроек в Windows Server 2003, требующих повышенных привилегий.

С целью экономии времени, пока находимся в нужном разделе администрирования, мы их сразу включаем в группу «Administrators» (Администраторы) и «Remote Desktop Users» (Пользователи сервера терминалов).

Добавление в группу «Администраторы» является временным. После того, как

авторизуемся с помощью клиента 2Х-сервера из-под учетной записи каждого пользователя сервера терминалов и запустим удаленный «Рабочий стол» для настройки параметров пользовательского окружения (какие настройки – я опишу чуть позже), мы исключим членство пользователей в группе «Администраторы». В результате работники не смогут делать несанкционированные действия и менять настройки в Windows Server 2003.

Называть учетные записи пользователей можно как удобно, главное потом задать пароль на вход в систему. Дополнительные настройки для учетных записей заключаются в том, чтобы на закладке «Удаленное управление» снять галочку с флажка «Запрашивать разрешение пользователя» и установить переключатель в секции «Уровень управления» на «Взаимодействие с этим сеансом». Это позволит

администратору 1С контролировать работу удаленных клиентов и в случае непредвиденных ситуаций корректно завершать или сбрасывать сеансы, а главному бухгалтеру – визуально наблюдать и непосредственно оказывать помощь своим подчиненным.

К пользователям 1С мы еще вернемся, теперь перейдем к главному.

## Установка и настройка 2Х ApplicationServer

Большого от встроенных оснасток настройки и управления сервером терминалов Windows 2003 ничего не требуется. Опытные администраторы, конечно, позаботятся о более «тонкой» настройке политики безопасности сервера, но оставшаяся часть работы заключается в конфигурировании 2Х ApplicationServer.

Закачиваем ApplicationServer с сайта <http://www.2x.com>, предварительно зарегистрировавшись на нем, и приступаем к установке. Замечу, что компания позволяет бесплатно работать с продуктом 5 пользователям одновременно.

Продукт состоит из серверной (2XAppServer-LoadBalancer.msi) и клиентской частей.

Серверную часть устанавливаем на компьютер, работающий под управлением Windows Server 2003. В процессе установки инсталлятор предложит выбрать тип установки – выбираем «Single Terminal Server» и жмем кнопку «Next».

После установки запуститься «2Х Console», где производится настройка и публикация приложений.

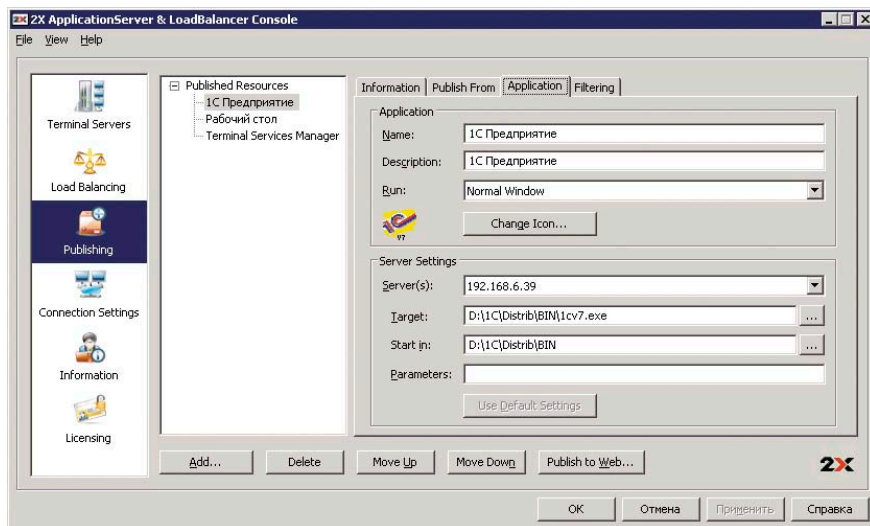


Рисунок 3. Публикация приложений

Весь этап конфигурирования заключается в прохождении всех строк в навигационном меню сверху – вниз.

Первая вкладка слева – «Terminal Servers». В окне свойств справа мы можем нажать на кнопку «Add» и ввести (лучше всего IP-адрес для скорейшего поиска) работающий сервер терминалов как по протоколу RDP, так и Citrix Server (ICA). По умолчанию здесь уже будет добавлен наш сервер, например, с IP-адреса 192.168.6.39.

Вкладка «Load Balancing» служит для настройки балансировщика загрузки нескольких терминальных серверов «2X LoadBalancer». Здесь нас интересуют только строки «Reconnect to disconnected sessions» и «Limit user to one session per desktop». Выставите галочки, чтобы их задействовать. Это позволит правильно восстанавливать отключенные сеансы и экономить ресурсы сервера.

На вкладке «Publishing» происходит самое главное. А именно, публикация программ для терминального использования и назначение фильтров на доступ к ним. В окне свойств нажимаем кнопку «Add» и выбираем, что мы будем публиковать (см. **рис. 2**).

Предоставленные средства позволяют организовать публикацию самостоятельных программ, установленных на Windows Server 2003, удаленные рабочие столы, предустановленные программные средства Windows Server 2003 (браузер Internet Explorer, системные утилиты, оснастки), отдельные файлы и объединять все это в группы. Выбираем первый пункт меню «Application» и нажимаем «Далее». В появившемся окне смотрим секцию «Server Settings», добавляем в строке «Target» файл запуска 1С:Предприятия (D:\1C\Distrib\BIN\1cv7.exe) и жмем «Далее». Автоматически заполнятся все оставшиеся настройки для публикации программы в терминальном доступе (см. **рис. 3**).

Переходим на закладку «Filtering» и активируем тип фильтра «User». Здесь надо добавить все ранее введенные учетные записи пользователей, которые будут работать в программе 1С, а также учетную запись «Администратор».

Важно понять, что фильтр «User» 2X-сервера не относится к встроенным средствам безопасности Windows

Sever 2003, и, не добавив в него необходимые учетные записи (в том числе Администратора), программа не опубликует приложение пользователю программы.

Главный бухгалтер организации должен иметь возможность запускать оснастку управления сервером терминалов «Terminal Services Manager» для перехвата управления сессиями, а администратор Windows Server 2003 и 1С, дополнительно, удаленный «Рабочий стол» для администрирования и обновления программ.

Поэтому публикуем «Рабочий стол» Windows Server 2003 с добавлением в фильтр учетной записи «Администратор» и группы «Администраторы», а также утилиту C:\Windows\system32\tsadmin.exe. Фильтр для tsadmin.exe должен содержать учетные записи, используемые администратором системы и главным бухгалтером. Таким образом, пока учетные записи пользователей 1С входят в группу «Администраторы», мы имеем возможность запустить удаленный «Рабочий стол» и выполнить настройки окружения. А затем, исключив их из группы «Администраторы», завершим сеанс, чтобы в дальнейшем пользователи не смогли «видеть» и запускать его. Напротив, главный бухгалтер и администратор 1С всегда смогут воспользоваться удаленным «Рабочим столом» и оснасткой «Terminal Services Manager».

Если с опубликованными приложениями будут работать пользователи на компьютерах, использующих dial-up способ подключения и получающих IP-адреса от DHCP-сервера, то рекомендую не использовать фильтр «IP Address».

На следующей вкладке «Connection Settings» необходимо установить «2X Client Gateway Port». По умолчанию его значение «80». Обычно на серверах и в маршрутизаторах порты 80, 443 открыты для передачи данных. Если на вашем сервере Windows Server 2003 не будет использоваться IIS-служба (HTTP-сервер), то можно оставить все как есть.

Если IIS задействована, то установим значение «2X Client Gateway Port» равным «81», рядом нажимаем кнопку «Advanced...» и значение «Forward requests to 2X Publishing Agent and HTTP Server» в строке «HTTP Server(s)» ме-

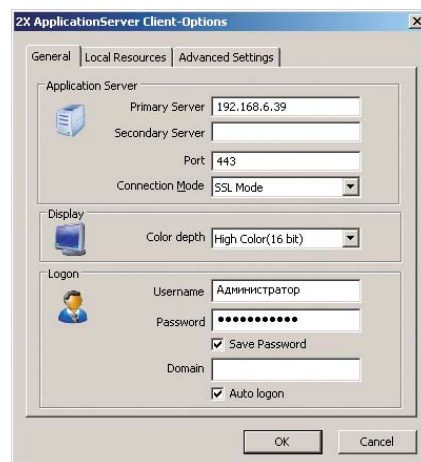


Рисунок 4. Настройка 2X ApplicationServer Client

няем на «<IP-адрес Windows 2003>:80» (в нашем примере 192.168.6.39:80). Это обеспечит доступ к веб-серверу.

Для защищенного доступа к опубликованным приложениям необходимо на закладке «Client Gateway» в секции «Security» поставить галочку «Enable SSL on Port 443». В самом низу нажимаем кнопку «Generate new certificate», вводим данные для единого сертификата доступа и сохраняем его на сервере. После этого для соединения с 2X-сервером можно использовать 443-порт с шифрованием передаваемых данных. Порт, прописанный в строке «2X Client Gateway Port», также будет доступен 2X-клиентам в режиме доступа «SSL Mode».

На вкладке «Connection Settings» имеются различные настройки для перенаправления портов сервера терминалов, агента и вспомогательных служб 2X. Желательно отключить «Broadcast 2X Client Gateway Address», чтобы сервер публикации не «засорял» сеть пакетами оповещения для быстрой настройки клиентов 2X.

Вкладки «Information» и «Licensing» пропускаем, нажимаем внизу «OK» и закрываем 2X ApplicationServer. Система готова для работы, осталось установить и настроить на клиентских компьютерах 2X ApplicationServer Client.

Устанавливаем его на компьютерах пользователей. Для настройки клиента запускаем в меню «Tools» пункт «Options». На закладке General указываем основные параметры для подключения (см. **рис. 4**).

На закладке «Local Resources» секции «Remote Computer Sound» выбираем «Do not play», чтобы не воспроиз-



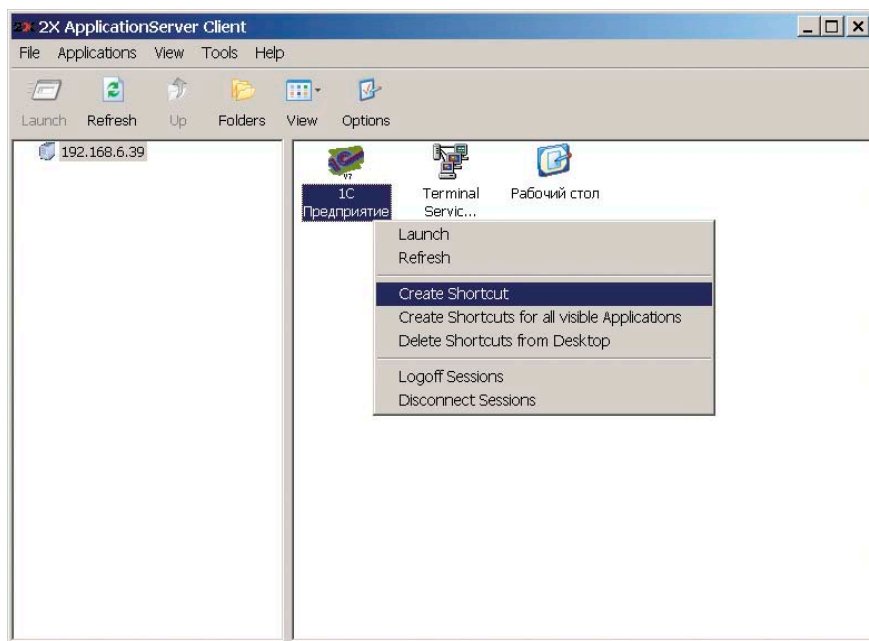


Рисунок 5. Создание ярлыка для 1С

водить звуки через локальный адаптер звука, а в секции «Local devices» оставляем галочку только на «Disk drives» для подключения локальных дисков клиента в терминальную сессию. Все эти настройки заменяют настройки оснастки «Настройка служб терминалов» в Windows Server 2003.

На последней закладке «Advanced Settings» советую снять галочку с «Do not warn if server certificate is not verified», чтобы избавить пользователя от процедуры ознакомления с сертификатом доступа при запуске опубликованных приложений.

После настройки и запуска 2X-клиента в рабочей области программа отобразит список всех опубликованных приложений, для которых в фильтре «User» консоли 2X-сервера добавлены нужные учетные записи.

Для Администратора будут доступны 1С:Предприятие, Рабочий стол и Terminal Services Manager, а для рядовых операторов 1С фильтр должен блокировать последнюю программу.

Для создания ярлыка на локальном рабочем столе пользователя кликнуть правой кнопкой мышки по иконке 1С и выбрать пункт «Create Shortcut» (см. рис. 5).

## Настройка печати и прав доступа пользователей к базам данных 1С

Запустим удаленный «Рабочий стол» из-под учетной записи всех пользова-

телей сервера терминалов и произведем следующие настройки на сервере: в свойствах экрана отключим заставку, потом в «Панели управления» откроем «Электропитание» и выберем период «Никогда» для опции «Отключение дисков» (при отсутствии активности на сервере). Тут же, на закладке «Дополнительно», снимем галочку «Запрашивать пароль при выходе из ждущего режима». «Разрешить использование спящего режима» тоже отключаем. Далее, в свойствах «Моего компьютера» на закладке «Дополнительно», нажмем кнопку «Параметры», и в секции «Быстродействие», на закладке «Визуальные эффекты», поставим флажок «Обеспечить наилучшее быстродействие». Все эти настройки обеспечат быструю и бесперебойную работу сервера терминалов. Кроме того, в процессе работы с опубликованной программой создается иллюзия, что программа присутствует на клиентском компьютере, однако все, что происходит на экране, лишь транслируется сервером 2X и грамотные настройки на сервере позволят удаленному пользователю «забыть», что он работает удаленно.

Теперь займемся принтерами. Разрешим общий доступ к локальным принтерам пользователей. И в опубликованном удаленном «Рабочем столе» устанавливаем ему его же локальный принтер, но уже как сетевой с помощью кнопки «Обзор» или указав пря-

мой IP-адрес и имя принтера, например, \\192.168.5.12\hp LaserJet 1160.

Для более надежной работы необходимо активировать учетную запись «Guest» на клиентских компьютерах и добавить её в свойствах принтера на закладке «Безопасность». Если у вас отсутствует закладка «Безопасность», то в свойствах «Проводника» уберите галку «Использовать простой общий доступ к файлам и принтерам».

Не закрывая удаленный «Рабочий стол», переносим «Мои документы» с Windows Server 2003 на локальный диск работника, присоединенный в терминальную сессию. Кликнем правой кнопкой мышки по значку «Мои документы», выберем свойства и нажмем кнопку «Переместить».

В обзоре присоединенные локальные диски будут выглядеть как сетевые диски, поэтому их не надо путать с локальными дисками сервера. Лучше переместить «Мои документы» с сервера в такую же папку «Мои документы» на локальной машине пользователя.

Теперь все отчеты из 1С будут по умолчанию сохраняться на локальной машине пользователя для дальнейшей с ними работы.

Небольшой совет: при выгрузке отчетности на дискету программа 1С предложит дисковод, размещенный на сервере (если таковой имеется), оператору надо сменить его на присоединенный локальный диск A:\ и создать на дискете папку, в которую будет осуществляться выгрузка, иначе 1С выведет сообщение об отсутствии дискеты.

Прежде чем выйти из удаленного «Рабочего стола», запустим оснастку «Управление компьютером» и в свойствах учетной записи на закладке «Членство в группах» удалим нашу принадлежность к группе «Администраторы». Нажмем кнопку «Пуск → Завершение работы → Завершение текущего сеанса» и выйдем из терминальной сессии.

Все вышеописанные действия необходимо проделать с оставшимися учетными записями пользователей сервера терминалов. После этого они не будут иметь административных прав на сервере. Соответственно, в консоли 2X-сервера, в фильтре

«User», опубликованного «Рабочего стола», удалим группу «Администраторы», запретив пользователям запускать его в клиенте 2X.

Для разграничения доступа пользователей к базам данных 1С:Предприятия в свойствах папки D:\1С выберем «Безопасность», удалим все учетные записи и группы, оставив только «Администратор», «SYSTEM», «СОЗДАТЕЛЬ-ВЛАДЕЛЕЦ», а потом добавим учетные записи пользователей 1С с полными правами. А в свойствах «Безопасности» каждого каталога с базами, находящихся на уровень ниже, мы будем удалять те учетные записи, пользователи которых не должны запускать определенные конфигурации 1С. Причем удаление прав и учетных записей надо производить, нажав на кнопку «Дополнительно» в закладке «Безопасность», отключив там галочку с пункта «Разрешить наследование разрешений от родительского объекта...». В появившемся диалоговом окне выбираем «Копировать» и удаляем лишние учетные записи. Для папки D:\1С\Archive строго оставляем только учетную запись администратора сервера, в функции которого входит резервное копирование данных.

Для управления сессиями сервера терминалов используется утилита «Terminal Server Manager». С её помощью можно отправлять сообщения подключенным пользователям, принудительно завершать и сбрасывать отключенные сессии, а также смотреть статистику сеансов.

Теперь 1С можно запускать непосредственно с рабочего стола пользователя. 2X установит терминальную сессию и само передаст программу как есть, без окон и удаленного рабочего стола.

Запускаем 1С и добавляем каждому пользователю путь к базе 1С, проверяем принтеры. В процессе работы оператор может запустить в рамках одной сессии неограниченное количество копий программы 1С и работать с несколькими конфигурациями одновременно, а также использовать другие программы, которые будут публиковаться, например, КонсультантПлюс и Гарант.

Если в вашей организации имеется прокси-сервер и используется firewall с SNAT, то, чтобы получить доступ к 2X-серверу через Интернет, необходимо настроить на нем переадресацию портов на Windows Server 2003.

Приведу пример, как это сделать в Linux. В настройках firewall добавляем два правила:

```
iptables -t nat -I PREROUTING -p tcp -d <внешний IP-адрес прокси-сервера> --dport <выделенный порт на прокси-сервере, например, 10443> -j DNAT --to-destination <IP-адрес Windows 2003 сервера>:3389

iptables -t filter -I FORWARD -s <IP Windows 2003 сервера> -d <внешний IP прокси-сервера> -p tcp --port <выделенный порт на прокси-сервере, например, 10443> -j ACCEPT
```

В настройках клиента 2X, соответственно, надо прописать внешний IP-адрес прокси-сервера и порт 10443. Клиент 2X-сервера под Linux представляет собой бинарный файл, запускаемый с нужными параметрами.

Например:

```
./appserverclient -s192.168.6.39 -a"1С Предприятие" -uAdministrator -ppassword
```

Обратите внимание, что наименование запускаемого приложения необходимо брать в кавычки.

Полный список всех параметров приведен в руководстве к 2X-серверу.

При испытании Windows-клиента 2X-сервера мною была выявлена следующая проблема: когда вы закрываете опубликованное приложение и в течение 20 секунд (столько времени 2X-сервер сохраняет в памяти закрытый сеанс для быстрого повторного запуска) снова его запускаете, то раскладка клавиатуры не будет переключаться. Поэтому приходится ждать некоторое время, чтобы повторно запустить опубликованное приложение. Причем при первом запуске приложения никаких проблем с раскладкой нет. В Linux-версии 2X-клиента данной проблемы замечено не было. Производитель советует в Windows Server 2003 использовать другое сочетание клавиш для переключения раскладки клавиатуры, нежели в локальном компьютере удаленного пользователя.

Какие-либо дополнительные ошибки, как, например, с Citrix ICA Client под Linux (при работе в нем на русской раскладке клавиатуры буква «Ы» всегда печатается заглавной, справедливости ради надо заметить, что маленькая «ы» получается при активированном CapsLock), связанные с работой 2X-сервера и опубликованных приложений, также не обнаружены.


В заключение хочется сказать, что с выходом продукции компании 2X Software Ltd на рынке программ для Windows Terminal Services прибавился очень серьезный игрок — средство публикации приложений на удаленные рабочие столы 2X ApplicationServer.

На сегодняшний день возможности Metaframe от компании Citrix являются лидирующими в области эмуляции локальных окон (seamless windows) и публикации приложений, а «стандартная связка» службы терминалов и ее клиента «Remote Desktop Connection», работающие по протоколу RDP, до сих пор не может обеспечить дополнительные потребности организаций, внедряющих терминальные решения.

Недостатки 2X ApplicationServer текущей версии 4.3: выявленная при его использовании ошибка, приводящая к нестабильному переключению раскладки клавиатуры с латиницы на русский, а также отсутствие встроенной возможности сопоставлять локальные принтеры удаленных пользователей в терминальную сессию. Но с выходом 5 версии продукта производитель обещает исправить все эти недостатки.

В ходе написания статьи на сайте компании 2X появилась новость о выходе 2X ApplicationServer v.5 Small Business Edition. Компания заявляет, что возможности нового продукта ничем не уступают решениям Citrix и нацелены на небольшие развивающиеся предприятия и предпринимателей.

Низкая ценовая политика, безопасный и полный доступ к приложениям, а также универсальный Printer Driver являются отличным решением для организации мобильных рабочих мест, удаленных офисов и обеспечивают полную избыточность удаленного управления и администрирования.

На этом всё. Удачи! 



# Система анализа квот на базе File Server Resource Manager



*Иван Коробко*

**В Windows Server 2003 RC2 появился наконец инструмент, позволяющий назначать квоты на использование дискового пространства серверов – File Server Resource Manager. Каковы достоинства и недостатки утилиты и как расширить ее возможности?**

Очень долгое время в операционных системах Windows отсутствовал инструмент, который позволял устанавливать квоты на дисковое пространство серверов и информировать по заданным правилам об использовании свободного места. В Windows Server 2003 RC2 появился штатный инструмент, позволяющий решить данную задачу – File Server Resource Manager. В системе

оповещения есть существенный недостаток. При заполнении дискового пространства, ограниченного квотой, может быть отправлено сообщение тому, кто его заполнил или перешел через установленную контрольную точку; а также службе поддержки по явно указанному e-mail-адресу. Однако оповестить об этом событии остальных сотрудников, имеющих права на эту папку, невозможно. Решить эту проблему мож-

но с помощью сценария, который будет запускаться при событии, генерировать и отсылать сообщение по почте о состоянии квоты всем пользователям, имеющим доступ к папке.

## **File Server Resource Manager**

В состав File Server Resource Manager, находящейся в «Панели управления», входят три инструмента:



- **Quota Management** – позволяет создавать шаблоны квот и назначать квоты на серверные папки;
- **File Screening Management** – ограничивает запись файлов указанных форматов (mp3, wav, avi, vob и т. д.) в папки;
- **Storage Reports Management** – создает отчеты, в том числе обеспечивает генерацию отчетов с помощью Scheduled Tasks.

## Quota Management

Состоит из двух компонентов: Quotas и Quota Templates. В разделе Quotas располагаются созданные на папки квоты, а в Quota Templates – шаблоны, на основе которых можно создавать квоты.

Логика подсказывает, что квоты удобнее и быстрее создавать с помощью шаблонов, поэтому сначала рассмотрим Quota Templates.

## Quota Templates

В Quota Templates присутствует несколько шаблонов по умолчанию. Несмотря на это, создадим собственный шаблон, кликнув правой кнопкой мыши по надписи Quota Templates и выбрав в появившемся меню «Create Quota Templates...».

В диалоговом окне (см. рис. 1) необходимо заполнить несколько полей. Программисты Microsoft предусмотрели возможность создания шаблонов на основе существующих: в верхней части диалогового окна в выпадающем списке «Copy properties quota templates (optional)» выберите подходящий шаблон и нажмите на кнопку «Сору». Осталось отредактировать импортированные параметры.

Рассмотрим подробнее поля вкладки «Settings»:

- **Template Name** – имя шаблона, которое будет отображаться в списке шаблонов; обязательное поле, ограниченное по длине 255 символами.
- **Label** – описание шаблона, расположенное справа от названия в общем списке; необязательный параметр.
- **Space Limit** – размер и тип квоты. Задавая размер квоты, необходимо тысячи отделять запятыми без пробелов, указывать размерность одним из значений вы-

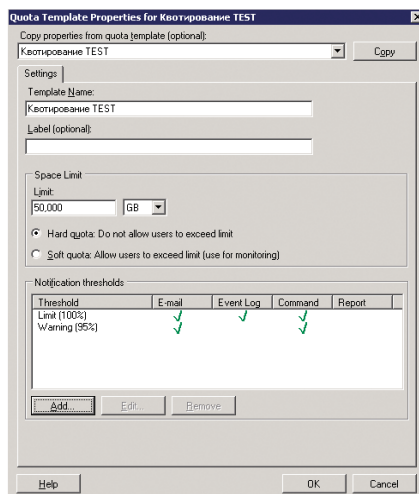


Рисунок 1. Диалоговое окно «Create Quota Templates...»

падающего списка: Kb, Mb, Gb, Tb. Квота может быть двух типов: Hard и Soft. Принципиальная разница заключается в том, что при превышении Hard-квоты система не даст записать информацию на диск, выводя сообщение об окончании места, и генерируется сообщение. При превышении Soft-квоты только генерируется соответствующее сообщение.

- **Notification thresholds** – задают пороговые значения, в соответствии с которыми будут генерироваться сообщения и их тип.

## Задание пороговых значений

Под пороговым значением понимается значение, указанное в процентах, по достижении которого происходит событие, на основе которого осуществляется указанное действие. Выполняемое действие зависит от настроек.

Задать новое пороговое значение можно, нажав на кнопку «Add» и указав в поле «Generate notifications when usage» reaches число в процентах, по достижении которого будет происходить событие. В появившемся диалоговом окне несколько вкладок, в каждой из которых задается свое событие:

- **e-mail Message** – используя эту вкладку, инициируют отправку двух сообщений: одно – администратору или службе поддержки (его текст невозможно изменить) и второе – пользователю, который инициировал событие (см. рис. 2). Есть возможность задать тему письма и создать шаблон письма.

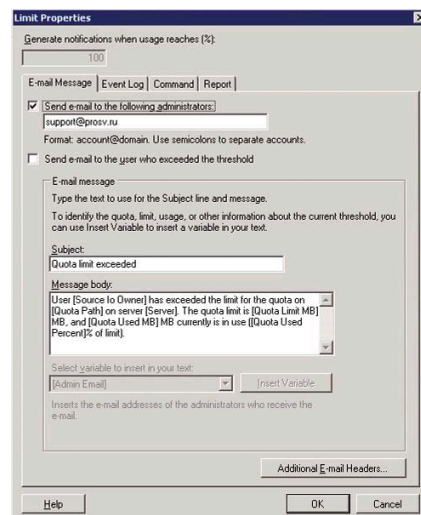


Рисунок 2. Вкладка «e-mail Message»

В него могут быть вставлены переменные, значения которых будут изменяться в зависимости от настройки квот и состояния анализируемой папки.

- **Event Log** – формируется запись в журнале событий на сервере на основе шаблона, содержащего различные переменные (см. рис. 3).
- **Command** – при наступлении события запускается сценарий (см. рис. 4). Для запуска скрипта на VBScript необходимо в поле «Run this command or script» указать путь к файлу-интерпретатору: %WinDir%\system32\wscript.exe. В качестве его аргумента в поле «Command Settings» вводят полный путь к файлу-сценарию: C:\Quota.vbs. Если он имеет параметры командной строки, то их указывают последовательно после имени сценария через пробел. FSRM поддерживает пере-

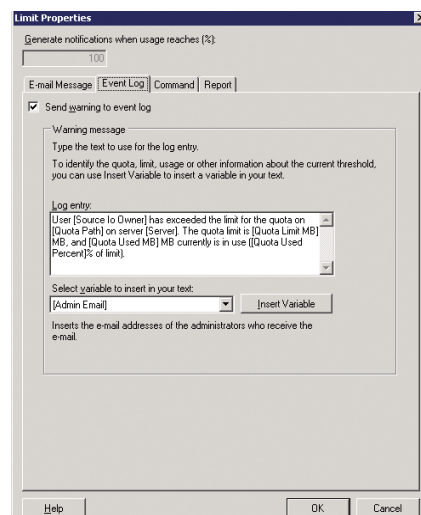


Рисунок 3. Вкладка «Event Log»

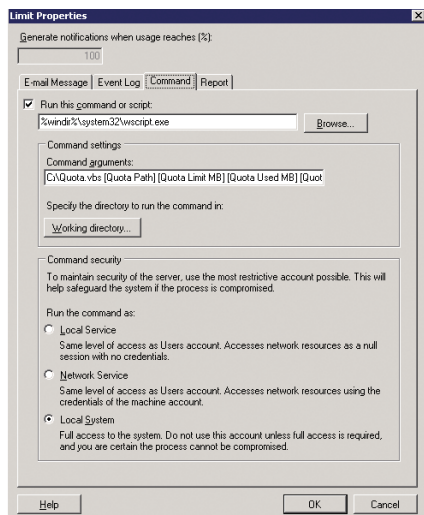


Рисунок 4. Вкладка «Command»

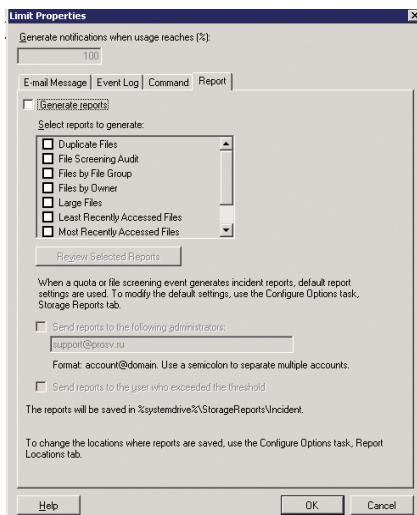


Рисунок 5. Вкладка «Report»

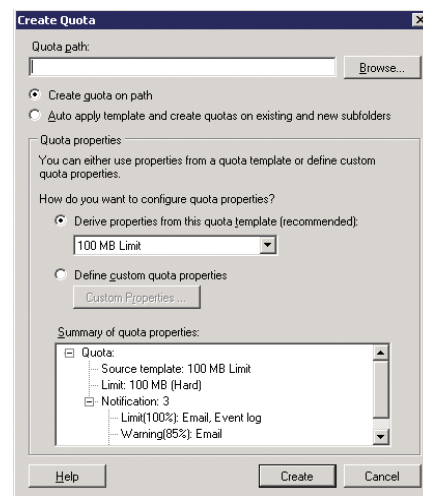


Рисунок 6. Диалоговое окно «Create Quota»

менные, которые также можно указать в качестве аргументов командной строки. Для успешной работы сценария необходимы, как правило, максимальные права доступа. Этого достигают выбором Local System в разделе «Command Security». С помощью сценария можно реализовать отправку сообщений всем пользователям, которые имеют право использовать данный сетевой ресурс. Как это сделать, читайте в разделе «Сценарий оповещения пользователей».

- **Report** – генерируется отчет по заданному критерию и отправляется по электронной почте администратору или в службу поддержки, либо сохраняется в виде файла в %SystemDrive%\StorageReports\Incident (см. рис. 5).

## Quotas

Для создания новой квоты на папку необходимо в FRSM войти в Quota Management и кликнуть правой кнопкой мыши по Quotas, а в контекстном меню выбрать «Create Quota». В появившемся диалоговом окне (см. рис. 6), нажав на кнопку «Browse», установить курсор на котируемой папке и нажать на кнопку «ОК». Для FRSM не важно, предоставлена ли папка в общий доступ или нет. Впоследствии папка должна стать сетевой, поскольку котируют локальную папку не имеет смысла.

В диалоговом окне необходимо задать один из вариантов создания квоты – «Create Quota on Path» (по умолчанию) или «Auto apply template and create quotas on existing and new folders» (см. рис. 6). В каждом из них есть возможность использовать имеющиеся шаблоны. Отличие методов заключается в возможности изменить в шаблоне существующие настройки для метода «Create Quota on Path».

Контролировать настройки назначаемой квоты можно с помощью окна «Summary of quota properties».

## Сценарий оповещения пользователей

Создавая квоту, обратите особое внимание на вкладку Command в диалоговом окне. Использование сценариев может значительно расширить возможности FRSM. Создадим скрипт, формирующий список сотрудников на основе настроек системы безопасности котируемой папки и отсылающий сообщение по электронной почте.

В качестве языка программирования рекомендуется выбрать VBScript или JScript. В данной ситуации это не принципиально. В качестве примера приведен сценарий на языке VBScript. Итог работы сценария – сообщение, разосланное всем сотрудникам, имеющим право доступа к котируемой папке. Оно примерно такого содержания:

**Тема сообщения:**  
Квота папки Отдел сбыта использована на 85% (8704.00 Мб).  
Размер Квоты 10240.00 Мб.

**Сообщение:**  
Уважаемый (ая) A.Ivanov  
Вы использовали установленную квоту на папку Отдел сбыта на 85%.  
Общий размер квоты 10240.00 Мб, из них занято 8704.00 Мб.  
Необходимо удалить ненужные данные из этой папки.  
С уважением, Служба поддержки.

Красным шрифтом выделены параметры, которые меняются в зависимости от ситуации: имя пользователя в сети, название котируемой папки, рубеж в процентном соотношении, израсходованное и предельное дисковое пространство. Все эти параметры транслируются из FRSM в сценарий с помощью аргументов командной строки:

```
C:\Quota.vbs [Quota Path] [Quota Limit MB] [Quota Used MB] [Quota Used Percent] [Quota Free MB] [Source Io Owner]
```

где:

- **[Quota Path]** – локальный путь анализируемой папки;
- **[Quota Limit MB]** – размер квоты в Мб;
- **[Quota Used MB]** – использованный размер квоты в Мб;
- **[Quota Used Percent]** – занятое дисковое пространства в процентах;
- **[Quota Free MB]** – размер доступного для записи дискового пространства в Мб;
- **[Source Io Owner]** – пользователь, превысивший установленный рубеж.

Чтение аргументов командной строки в сценарии осуществляется следующим образом:

```
Set objArgs = WScript.Arguments
a0=objArgs(0)
a1=objArgs(1)
```

```
a2=objArgs(2)
a3=objArgs(4)
a4=objArgs(4)
a5=objArgs(5)
```

Зная путь к каталогу (параметр a0), с помощью объекта adsSecurity получают доступ к параметрам безопасности NTFS этого каталога:

```
Set sec = CreateObject("AdsSecurity")
Set sd = sec.GetSecurityDescriptor("FILE://" + PathToFolder)
Set Dacl = sd.DiscretionaryAcl
For Each ace In Dacl
    Wscript.Echo ace.Trustee
    Wscript.Echo ace.AccessMask
    Wscript.Echo ace.AceType
Next
```

Считанные данные необходимо отфильтровать и обрабатывать. На каждую папку, расположенную на сервере, назначены права.

Перечень объектов, которые присутствуют в списке вкладки «Permissions», можно разделить на 2 части. Первая часть списка постоянна, вторая – вариативна.

В список постоянных объектов входят Domain Admins, System, Creator Owner.

Во второй – обычные пользователи, которым назначены права доступа в зависимости от выполняемых ими задач.

Фильтр объектов безопасности осуществляется с помощью функции InStr().

Имена объектов имеют формат Domain\ObjectName. В большинстве случаев объект – группа. Поскольку у группы может не быть почтового адреса, а пользователей, за редким исключением, он есть, то необходимо получить список пользователей, входящих в группу.

Для этого необходимо получить непосредственно имя группы:

```
GroupName=ace.Trustee
Right(cstr(GroupName), Len(GroupName)-InStr(GroupName, "\"))
```

Получив доступ к группе, с помощью провайдера WinNT можно определить список пользователей, входящих в нее, с помощью свойства объекта obj – members:

```
Set Obj=GetObject("WinNT://" & domain & "/" & group & ",group")
For Each member In obj.members
    Wscript.Echo cstr(member.name)
Next
Set Obj=nothing
```

**Замечание:** для операций с правами доступа к папке используют библиотеку ADsSecurity.dll, входящую в комплект ADSI Resource Kit. Перед использованием библиотеки необходимо зарегистрировать командой:

```
regsvr32 /s c:\Program Files\Microsoft\ADSI Resource Kit, \
Samples and Utilities\ResourceKit\ADsSecurity.dll
```

Для чтения назначенных прав доступа на объект используется объект AdsSecurity. Для назначения новых прав используется объект AccessControlEntry.

На заключительном этапе формируют текст сообщения и отправляют его по электронной почте с помощью CDO-объекта, используя CDO.Message и CDO.Configuration.

При создании письма должны быть указаны параметры:

■ **Адрес электронной почты пользователя, от имени которого отправляется сообщение.** Он не должен быть фиктивным. Рекомендуется использовать адрес службы поддержки Support@Firm.Ru. В листинге использована переменная MAIL\_FROM.

■ **DNS-имя почтового сервера**, например Mail.Firm.ru. В листинге – переменная MAIL\_SERVER.

■ **Адрес электронной почты получателя.** Поскольку письмо отправляется нескольким пользователям одновременно, то в сценарии формируется одно письмо, отправляемое одновременно нескольким адресатам, поэтому в поле MAIL\_TO заносят их почтовые адреса, разделенные символом (;).

■ **Тема письма в листинге сценария фигурирует в переменной MAIL\_SUBJECT.** Желательно, чтобы по теме письма сотрудник сразу мог понять, что это уведомление от службы о состоянии файловой системы, и не принимал его за спам:

```
MAIL_SUBJECT="Квота папки "+right(a0,len(a0)-
cstr(a0,"\")) +" использована на "+a3+"%
("+a(2)+" Мб) . Размер квоты "+a(1)+" Мб"
```

■ **Сообщение, отсылаемое пользователям, содержится в переменной MAIL\_BODY.** Для форматирования сообщения рекомендуется использовать для перехода на новую строку встроенную константу vbNewLine, для отбивки текста – константу табуляции vbNewTab:

```
mail_body = mail_body + "Уважаемый(ая) " + mail_to +
"!"+ vbNewLine
mail_body = mail_body + "Вы использовали установленную
квоту папки " + right(a0,len(a0)-cstr(a0,"\"))
+ " на " + a3 + "%." + vbNewLine
mail_body = mail_body + "Общий размер квоты на папку"
+ a1+ " MB, из них занято " + a2 + " MB."
+ vbNewLin + vbNewLine
mail_body = mail_body + "Необходимо удалить ненужные
данные с этой папки." + vbNewLin + vbNewLine
+ vbNewTab
mail_body = mail_body + "С уважением, Служба
поддержки." + vbNewLin + vbNewLine
```

Листинг отправки сообщения:

```
MAIL FROM="Support@Firm.Ru"
MAIL SERVER="Mail.Firm.ru"
MAIL TO=""
MAIL BODY=""
MAIL SUBJECT=""
...
MAIL SUBJECT=...
MAIL_BODY = MAIL_BODY + ...
...
Set iMsg = CreateObject("CDO.Message")
Set iConf = CreateObject("CDO.Configuration")
Set Flds = iConf.Fields
Flds.Item("http://schemas.microsoft.com/cdo/
configuration/sendusing") = 2
Flds.Item("http://schemas.microsoft.com/cdo/
configuration/smtpserver") = MAIL_SERVER
Flds.Item("http://schemas.microsoft.com/cdo/
configuration/smtpconnectiontimeout") = 10
Flds.Update
iMsg.Configuration = iConf
iMsg.To = MAIL_TO
iMsg.HTMLBody = MAIL_BODY
iMsg.From = MAIL_FROM
iMsg.Subject = MAIL_SUBJECT
iMsg.Send
```

Полный листинг сценария смотрите на сайте журнала



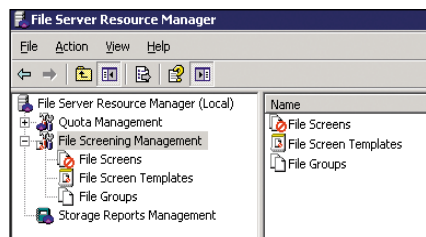


Рисунок 7. Раздел File Screening Management

ла [www.samag.ru](http://www.samag.ru) в разделе «Исходный код».

## File Screening Management

Помогает ограничивать запись файлов указанных форматов (mp3, wav, avi, vob и т. д.) в котируемую папку. Структура File Screening Management (см. **рис. 7**) повторяет структуру Quota Management: существуют предустановленные шаблоны – File Screen Templates, на основе которых создают новые шаблоны и сами правила – File Screens. Присутствует дополнительный раздел File Groups, в нем наборы расширений, обобщенные в группы.

## File Groups

В разделе File Groups находится список групп (см. **рис. 8**), в которых перечислены характерные расширения файлов. Этот список может быть изменен. Для этого достаточно два раза кликнуть на нужные группы. В появившемся меню присутствует два списка. В первом списке перечислены расширения файлов, которые нельзя будет записать в котируемую папку. Второй список – список исключений из перво-

го списка. Файлы с указанными расширениями можно записать в котируемую папку. Приоритет списка файлов исключений выше приоритета списка файлов включений.

Приведу пример. Системному администратору необходимо запретить запись файлов с расширением AVI, однако части из них – имеющим в начале имени символы MP4 необходимо разрешить доступ. Для решения этой задачи добавляют в список «Files to Include» все файлы с расширением AVI: \*.AVI и нажимают кнопку «Add», в список «Files to Exclude» – MP4\*.AVI, также нажимают кнопку «Add», затем «OK».

Всего в состав File Groups по умолчанию входит 11 групп: Audio and Video Files, Backup Files, Compressed Files, E-mail Files, Executable Files, Office Files, System Files, Temporary Files, Text Files, Web Page Files

Список групп можно пополнять новыми, выбрав в контекстном меню «File Groups», вызываемого правой кнопкой мыши, «Create File Group».

## File Screen Templates

В File Screen Templates по умолчанию несколько шаблонов: Block Audio and Video Files, Block E-mail Files, Block Executable Files, Block Image Files, Mirror Executable and System Files. Все, кроме последнего, – активные шаблоны, последний – пассивный. Файловый экран, созданный на основе активного шаблона, запрещает доступ файлам указанного типа и при их попытке запи-

сать генерирует сообщение по хранящемуся в нем шаблону и либо записывает его в журнал событий, либо отправляет его по электронной почте, либо выполняет указанную команду. Перечень действий зависит от настроек шаблона.

Создание шаблона File Screen Templates полностью повторяет создание шаблона Quota Templates за исключением вкладки Settings (см. **рис. 9**). В ней указываются группы файлов из раздела File Groups, которые будет обрабатывать экран, созданный на основе данного шаблона. Здесь же можно создать новую группу файлов или отредактировать существующую. В этой вкладке также указывается тип шаблона: Active Screening или Passive Screening. Все остальные настройки были описаны в разделе Quota Templates.

## File Screen

В отличие от Quotas в File Screen допускается создание объектов двух видов: File Screen и File Screen Exception.

## File Screen

Принципы настройки File Screen идентичны с принципами настройки Quotas. Новый файловый экран можно создать полностью вручную или с помощью готового шаблона.

## File Screen Exception

Благодаря наличию файловых групп – File Group, появилась возможность создавать ограничения непосредс-

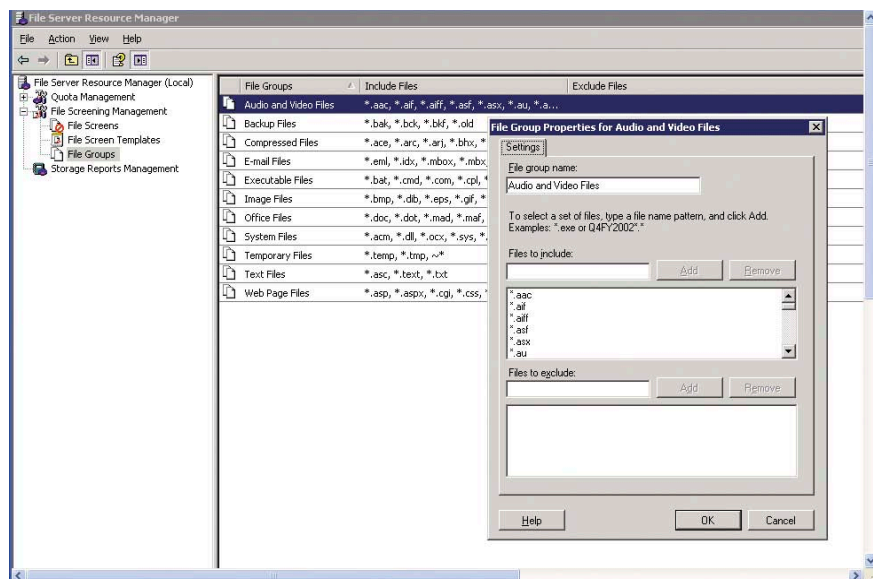


Рисунок 8. Раздел File Groups

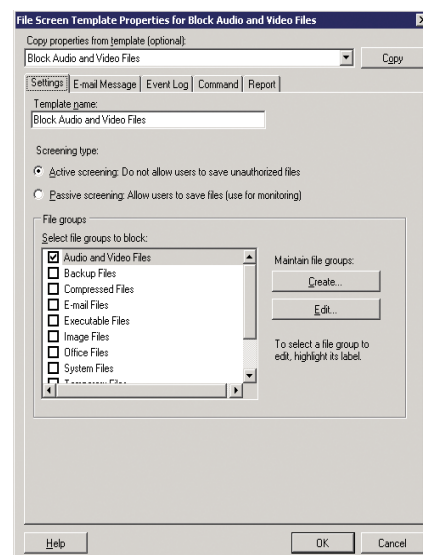


Рисунок 9. Раздел File Screen Templates

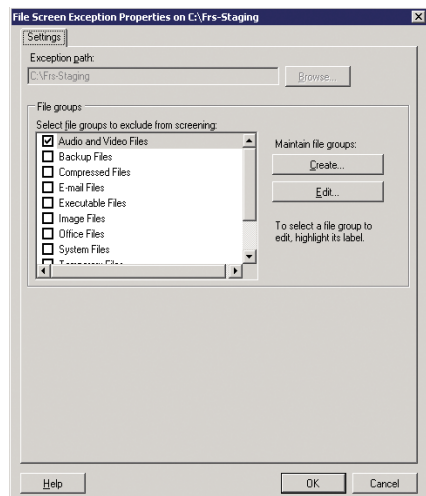


Рисунок 10. Вкладка «File Screen Exception»

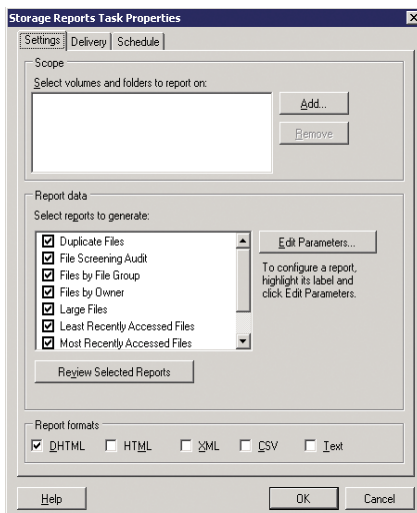


Рисунок 11. Вкладка «Settings»

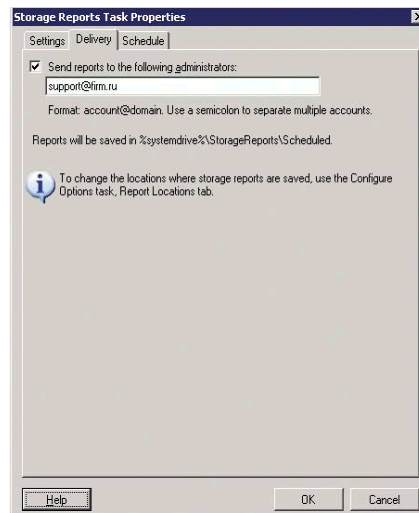


Рисунок 12. Вкладка «Delivery»

твенно на основе групп, а не шаблонов. Основное отличие File Screen Exception (см. рис. 10) заключается в том, что из него невозможно отправить пользователю сообщение в какой-либо форме.

## Storage Reports Management

С помощью этой службы создают различные отчеты, в том числе она обеспечивает генерацию отчетов с помощью Scheduled Tasks. В контекстном меню службы присутствуют три варианта:

- Schedule a New Report Task...
- Add or Remove Reports for a Report Task...
- Generate Reports Now...

### Schedule a New Report Task...

Если кликнуть на «Schedule a New Report Task...» левой кнопкой мыши, появится диалоговое окно с тремя вкладками «Settings», «Delivery» и «Schedule».

В первой из них – «Settings» (см. рис. 11) – необходимо набрать список анализируемых папок Scope и указать тип файла отчета. Предлагается выбрать один или несколько форматов из следующего списка: DHTML, HTML, XML, CSV, TXT для просмотра в Internet Explorer, Microsoft Excel, Microsoft Word или экспортировать его в базу данных, например в SQL. Также в этой же вкладке предлагается выбрать одно или несколько событий, на основе которых будет сгенерировано сообщение. Предполагается, что в следующей вкладке – «Delivery» (см. рис. 12) –

в случае необходимости будет указан адрес электронной почты, по которому будет отправлен отчет. Таким образом, администратор и сотрудники службы поддержки будут оперативно получать информацию о состоянии квот.

Особый интерес представляет вкладка Schedule (см. рис. 13). С ее помощью можно настроить регулярную генерацию файла отчета, например XML. Во вкладке «Schedule» нажмите на кнопку «Create Schedule...». В появившемся окне приведен список задач, выполняемых Task Scheduled. Для пополнения списка нажмите кнопку «New». Расписание запуска задачи можно изменить здесь, выбрав частоту выполнения задачи и время ее пуска. Если необходим запуск задачи каждые 20 минут, то надо нажать на «Advanced» и включить раздел «Repeat Task». В доступных полях необходимо сделать изменения: в поле «Every» установить значение 20 (min), в поле «Duration» – 24 (hours).

### Add or Remove Reports for a Report Task...

Для изменения параметров созданной задачи отчета необходимо воспользоваться вторым пунктом контекст-

тного меню «Add or Remove Reports for a Report Task...». Если дважды кликнуть на ранее созданную надпись, то видно, что все кнопки недоступны и можно только посмотреть существующие настройки.

Чтобы изменить расписание «Scheduled», необходимо в Панели управления запустить программу Scheduled Task и открыть там соответствующую задачу. FSRM создаст задачи, имена которых соответствуют следующему шаблону – Имя задачи + {GUID}, например FSRM\_Report\_Task{85aa8287-16b7-41f3-8af8-e44d235af653}.

### Generate Reports Now...

Часто бывают ситуации, в которых необходимо создать свежий отчет, и нет времени ждать, когда по расписанию создастся новый. Для решения такой задачи программисты Microsoft предусмотрели третий пункт контекстного меню «Generate Reports Now...». Появляющееся диалоговое окно в точности повторяет окно «Schedule a New Report Task...». Единственное различие – отсутствие вкладки «Schedule». Сформированные отчеты находятся в %systemdrive%\storage/reports/scheduled.

## Заключение

Несмотря на недостатки, которые можно ликвидировать с помощью скрипта, думаю, утилита будет востребована системными администраторами и использована, например, в системе обмена данными между подразделениями в крупных организациях.

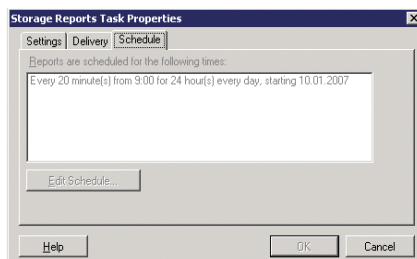


Рисунок 13. Вкладка «Schedule»



# Vyatta – Linux-дистрибутив для роутеров



*Сергей Яремчук*

**В конце февраля этого года компания Vyatta анонсировала вторую версию разрабатываемого ею дистрибутива, позволяющего превратить обычный ПК в маршрутизатор. Это решение позиционируется как конкурент продуктам нижнего уровня Cisco и Juniper. Что же такого особенного в Vyatta?**

Сначала никакого дистрибутива не было. Одной из первых разработок Vyatta был программный пакет Open Flexible Router (OFR), превращающий обычный ПК в маршрутизатор. Причем отмечалось, что производительность работы и уровень безопасности соответствовал коммерческим продуктам. С самого начала курс взят на открытость, так как, по мнению разработчиков, это значительно ускоряет устранение возможных недостатков и способствует быст-

рому развитию продукта и адаптации для всех возможных условий. Кстати, Vyatta – это санскритское слово, обозначающее «открытый». Компания видит свой продукт сетевым эквивалентом решений вроде Linux или Firefox, правда, который противопоставляется продуктам не от Microsoft, а от Cisco Systems.

## Особенности Vyatta

Проект Vyatta возник не на пустом месте. Основой OFR является eXtensible

Open Router Platform (XORP), платформа маршрутизации с открытым кодом, работающая в укреплённом варианте UNIX. Его разработкой занимается группа в International Computer Science Institute (ICSI) Беркли под руководством Atanu Ghosh, финансируют проект такие гиганты, как Intel и Microsoft, а также National Science Foundation и Vyatta. В настоящее время код XORP содержит 670,000 строк на языке C++, может быть скомпилирован на Linux, OpenBSD, FreeBSD, DragonFlyBSD, NetBSD,



Mac OS X и Windows Server 2003 и распространяется под BSD-подобной лицензией. Поддерживаются протоколы Border Gateway Protocol (BGP, с некоторыми расширениями под IPv6), Routing Information Protocol (RIP v2 для IPv4 и RIPng для IPv6), Protocol-Independent Multicast Sparse Mode (PIM-SM), Internet Group Management Protocol (OSPFv2 (RFC2328) и OSPFv3 (RFC2740), Multicast Listener Discovery (MLD), OSPF (Open Shortest Path First), IGMP и SNMP. Проект XORP предоставляет готовый LiveCD-дистрибутив, который можно использовать для тестирования. Хотя, наверное, спешить не стоит, так как Vyatta обладает большими возможностями. Так, Vyatta поддерживает протокол Virtual Router Redundancy Protocol (VRRP), что позволяет применять маршрутизатор как резервный, мгновенно берущий на себя обработку в случае сбоя основного. Кроме этого, в Vyatta включены разработки более чем 60 различных Open Source-проектов и свой код. Распространяется дистрибутив под BSD-подобной или GPL-лицензией. Но наряду с этим решением предлагается подписка на коммерческие редакции. Компания использует бизнес-модель, применяемую Red Hat, то есть производитель планирует предложить платные услуги и поддержку для пользователей маршрутизаторов Vyatta, в то же время само программное обеспечение доступно совершенно бесплатно.

Компанию основал в 2005 году Аллан Лайнванд (Allan Leinwand), который работал в Cisco еще в те времена, когда штат компании насчитывал около сотни сотрудников. Одним из управляющих Vyatta является Келли Харрелл (Kelly Harrell), бывший вице-президент по маркетингу в компании MontaVista, специализирующейся на решениях со встраиваемыми версиями Linux. Вероятно, поэтому одними из первых продуктов Vyatta были сетевые приставки-маршрутизаторы, работающие под управлением Linux и установленные на серверы Dell PowerEdge 850, оснащенные двумя портами Gigabit Ethernet. Последняя версия Vyatta Community Edition 2 представляет собой дистрибутив GNU/Linux на базе Debian, что прибавило ему дополнительной гибкости и возможностей, а также большую поддержку обо-

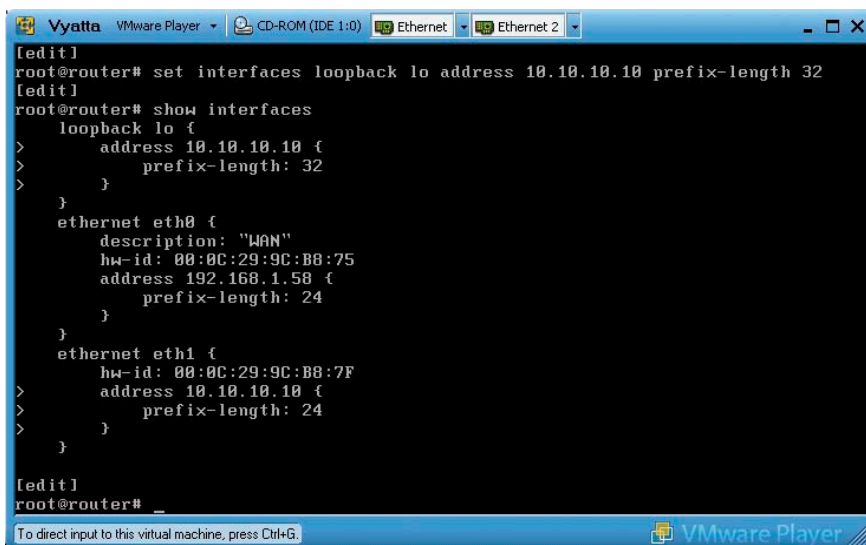


Рисунок 1. Просмотр настроек интерфейсов

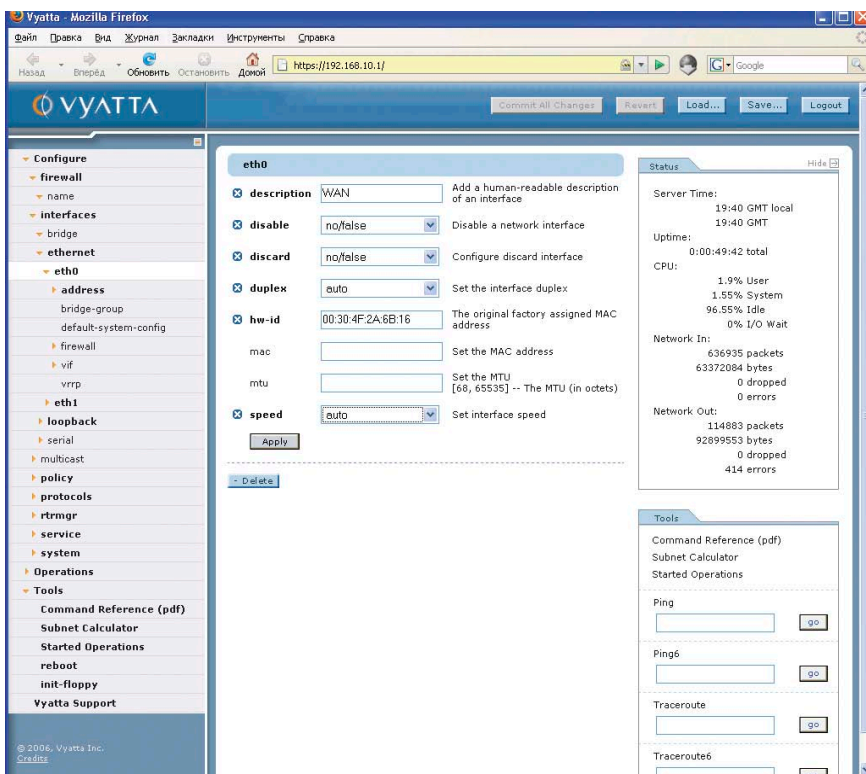


Рисунок 2. Веб-интерфейс Vyatta

рудования, в том числе и мультипортовых T1/E1 и T3-карт.

## Работа с Vyatta CE2

Для примера настройки соединим сеть с провайдером, то есть к порту eth0 будет подключен Интернет, а eth1 будет «смотреть» в локальную сеть. На сайте проекта можно скачать ISO-образ LiveCD-дистрибутива, который будет работать без установки на жесткий диск, конфигурационные файлы при этом можно сохранять на флорпи-диск или использовать TFTP-сер-

вер. Но при необходимости его можно установить на жесткий диск, а также Flash или USB-устройство. Также можно скачать готовый образ для виртуальной машины VMware.

После загрузки с образа регистрируемся как пользователь root или vyatta, пароль в обоих случаях vyatta. Во втором случае попадаем сразу в оболочку маршрутизатора. Если для входа использован root, дополнительно следует ввести команду xorpsn:

```
# xorpsn
```

```
Welcome to Vyatta on vyatta
root@vyatta>
```

Теперь можно приступать к настройкам. Чтобы просмотреть доступные команды, достаточно ввести знак вопроса «?». Сейчас нас интересует команда `configure`, набрав которую и попадаем в заветный режим настройки. Если нужно опять вернуться назад, достаточно набрать «exit». Причем если нужно сохранить все внесенные изменения, то вначале следует ввести «commit». Чтобы выйти без сохранения настроек, используйте «exit discard». Вначале следует ознакомиться с настройками по умолчанию, вводим «show», для перемещения вперед/назад используем клавиши <Пробел/b>.

В Vyatta (точнее XORP) используется Cisco-подобный командный интерфейс к настройкам. Для доступа к редактируемым настройкам необходимо использовать команду `edit`, установка нового значения производится с помощью `set`, а удаление – `delete`. Поддерживается традиционное автодополнение с использованием табуляции, поэтому полностью вводить команду не обязательно. Настраиваем первый сетевой интерфейс:

```
# edit interfaces ethernet eth0
[edit interfaces/ethernet/eth0]

# set description "WAN"
[edit interfaces/ethernet/eth0]

# set address 192.168.1.58 prefix-length 24
[edit interfaces/ethernet/eth0]
```

Смотрим:

```
# show
> description: "WAN"
hw-id: 00:0C:29:9C:B8:75
> address 192.168.1.58 {
>   prefix-length: 24
> }
```

Если все нормально, записываем:

```
# commit
[edit interfaces/ethernet/eth0]
OK
```

Если теперь снова использовать команду `show`, то в выводе уже не будут содержаться значки «>». Это означает, что это значение уже записано. Обратите внимание на подсказку `[edit interfaces/ethernet/eth0]`, которая помогает не заблудиться в дереве настроек, что бывает весьма полезным при глубокой вложенности. При входе в режим настройки сразу попадаем в корень, то есть подсказка будет выглядеть как `[edit]`. Перемещаться по дереву можно командой «up» либо для выхода в корень «exit», или «top». Например:

```
# up
[edit interfaces/ethernet]
```

Попробуем удалить описание:

```
# delete description

Deleting:
description: "WAN"
OK
[edit interfaces ethernet eth0]
```

Просмотрев настройки с помощью `show`, можно увидеть, что перед строкой `description` появился знак минус, говорящий о том, что планируется удаление этого параметра. Аналогично настраиваем и остальные интерфейсы:

```
# set interfaces ethernet eth1 address 10.10.10.10 ㄿ
    prefix-length 24
# set interfaces loopback lo address 10.10.10.10 ㄿ
    prefix-length 32
# commit
```

Просмотреть настройки интерфейсов можно, введя «`show interfaces`» (см. **рис. 1**). Далее необходимо указать имя узла и домена, к которому он принадлежит.

```
# set system host-name router
[edit]

# set system domain-name domain.com
[edit]

root@vyatta# commit
OK
```

Об успехе будет свидетельствовать и изменение имени системы в приглашении командной строки. И не забываем о шлюзе по умолчанию:

```
# set protocols static route 0.0.0.0/0 next-hop 192.168.1.1
```

Задаем DNS-сервер:

```
# set system name-server 192.168.1.1
```

В состав Vyatta входит сервер SSH, включив его, в дальнейшем все настройки можно производить удаленно:

```
# set service ssh
```

Нажав табуляцию, можно просмотреть список доступных сервисов:

```
# set service

Possible completions:
<[Enter]>      Execute this command
dhcp          dhcp settings
dhcp-server   DHCP configuration
http         Enable/disable HTTP protocol
nat          NAT configuration
ssh          Enable/disable SSH protocol
telnet       Enable/disable telnet protocol
{            Enter text on multiple lines
```

Как видите, есть еще веб-сервер, telnet и dhcp.

## Включение NAT и создание правил firewall

Включим NAT и разрешим исходящий трафик из сети, подключенной к `eth1`:

```
# create service nat rule 1
# edit service nat rule 1
# set type source
# set translation-type masquerade
# set outbound-interface eth0
# set protocols all
# set source network 10.10.10.0/24
# set destination network 0.0.0.0/0
# top
```

Если во внутренней сети находится веб-сервер, разрешаем к нему доступ извне:

```
# create service nat rule 2
# edit service nat rule 2
# set type destination
# set translation-type static
# set inbound-interface eth0
# set protocols tcp
# set source network 0.0.0.0/0
# set destination address 192.168.1.58
# set destination port-name http
# set inside-address address 10.10.10.30
# top
```

Чтобы просмотреть настройки, используем команду:

```
# show service nat
```

И не забываем подтверждать изменения командой commit.

Если при конфигурировании допущены ошибки, commit не сможет сохранить изменения, поэтому лучше сохранять изменения после каждой завершенной серии команд, чтобы потом долго не разбираться с проблемой.

## Настройка фильтрации пакетов

Для примера разрешим доступ к сети с адреса 170.20.0.45:

```
# set firewall name FW-1 rule 1 action accept
# set firewall name FW-1 rule 1 source address 170.20.0.45
```

И привязываем к интерфейсу:

```
# set interfaces ethernet eth0 firewall in name FW-1
# commit
```

OK

Смотрим правило:

```
# show firewall name FW-1
```

```
rule 1 {
  action: accept
  source {
    address: 170.20.0.45
  }
}
```

Если требуется уточнить протокол и порт, добавляем следующие конструкции:

```
# set firewall name FW-1 rule 1 protocol tcp
# set firewall name FW-1 rule 1 destination port-name http
```

## Веб-интерфейс

В дополнение к настройке с помощью командной строки Vyatta имеет и веб-интерфейс (см. **рис. 2**), чтобы его активировать, достаточно ввести:

```
# set service http
```

После этого в браузере набираем IP-адрес роутера, принимаем сертификат и регистрируемся как пользователь vyatta (root система не пустит).

Используя веб-интерфейс, можно просмотреть системную информацию, произвести большую часть настроек, доступных в консоли.

Все они находятся во вкладке «Configure». Правда, выигрывая в наглядности, проигрываем в удобстве, так как здесь нет никаких подсказок и автодополнения, поэтому все параметры придется помнить наизусть. Для сохранения изменений необходимо нажать кнопку «Commit All Changes», расположенную в верхней части меню.

Во вкладках «Operations» и «Tools» можно найти некоторые утилиты, с помощью которых можно проверить доступность узлов, установить дату, смонтировать дискету, просмотреть статистику сервисов и прочее.

## Сохранение настроек и установка на диск

При работе в LiveCD сохранить конфигурацию на дискету очень просто, если при загрузке вставить дискету в дисковод, она будет смонтирована автоматически, и с нее будет считана конфигурация. Для сохранения настроек вводим команду:

```
# save /mnt/floppy/config/config.boot
```

Если диск вставлен позже, можно смонтировать его обычным образом с помощью mount или использовать команду init-floppy.


Но использовать LiveCD-вариант в работе неудобно, в рабочей системе лучше его установить на жесткий диск. Для установки потребуется диск размером всего 512 Мб и 10 Мб для сохранения настроек. Далее регистрируемся как root и запускаем установочный скрипт:

```
# install-system
```

Далее будет произведена проверка подключенных устройств и предложен вариант создания разделов:

```
Partition (Auto/Parted/Skip) [Auto]:
```

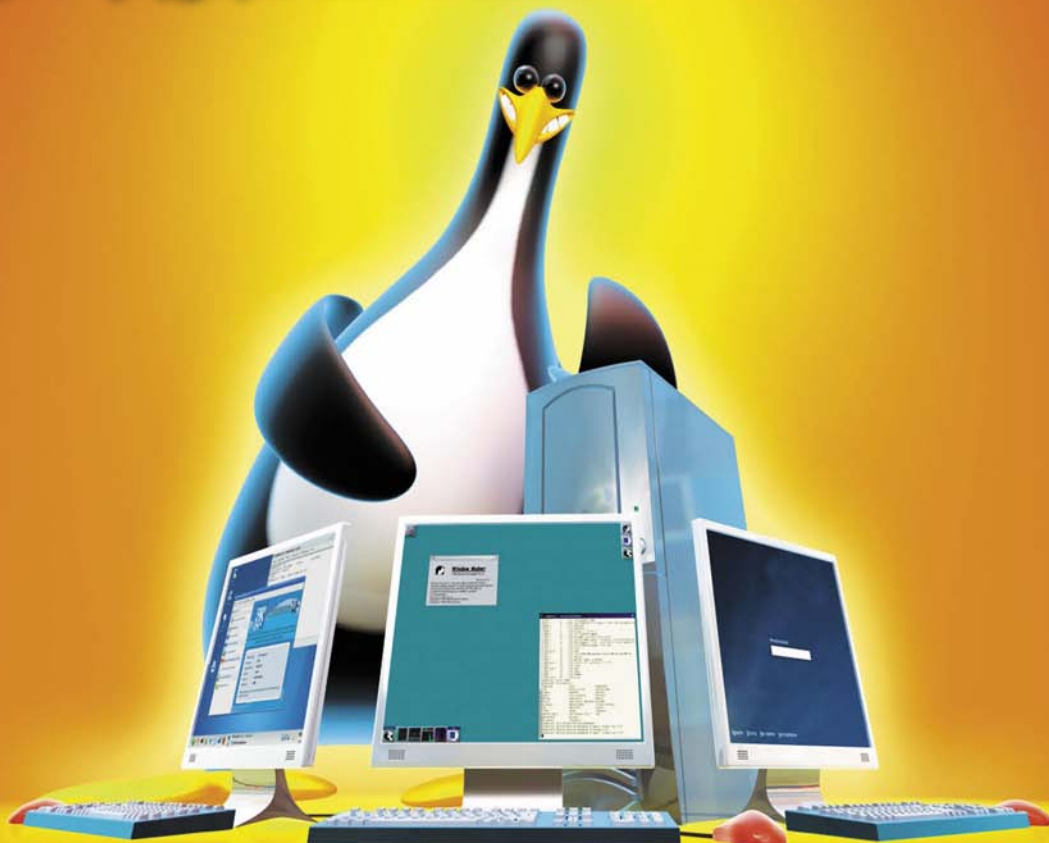
В самом простом случае достаточно выбрать вариант, предложенный по умолчанию. По окончании будет установлен загрузчик GRUB. Чтобы вручную сохранить настройки в этом варианте, достаточно ввести команду save без аргументов. Конфигурационный файл будет записан в /opt/vyatta/etc/config/config.boot.

В статье рассмотрен самый простой случай настройки маршрутизатора, достаточный для понимания принципа работы в Vyatta. Следует отметить хорошую документацию проекта, в которой можно найти как описание основных параметров, так и некоторые примеры конфигурирования Vyatta. 

1. Сайт проекта XORP – <http://www.xorp.org>.
2. Сайт проекта Vyatta – <http://vyatta.com>.



# ALT Linux 4.0 Server: что день грядущий нам готовит?



**Дмитрий Шурупов**

Одна из ведущих российских компаний, специализирующихся на решениях на базе Linux и Open Source, готовит к выпуску новую версию годами проверенного продукта.

## ALT Linux Server?

Семейство дистрибутивов ALT Linux, основывающихся на собственном ежедневно обновляемом репозитории пакетов Sisyphus, пополнил ALT Linux 4.0 Server. Продукт позиционируется как решение «для создания серверов любых типов» и будет сопровождаться технической поддержкой в течение не менее трех лет.

Обсуждение нового инсталлятора для ALT Linux 4.0 началось в почтовой рассылке для разработчиков еще в последний день прошлого года, а дискуссии о тестовых релизах 4.0 Server – в конце марта 2007. На момент написания статьи актуальной версией готовящегося дистрибутива являлся

выпуск от 1 июня (server-20070601.iso). В случае отсутствия проблем с этим выпуском планировалось обозначить его как релиз 4.0.1 и на его базе строить финальную коробочную редакцию ALT Linux 4.0 Server (к моменту выхода журнала из печати она как раз уже должна будет повсеместно появиться). Именно эта версия (для архитектуры x86\_64) и рассматривается сегодня.

## Важное напоминание

В обзоре представлена тестовая сборка ALT Linux 4.0 Server. Упомянутые проблемы могут быть устранены уже в финальной версии дистрибутива.

Тем не менее продукт был с успехом протестирован на оборудовании отече-

## Установка

Первое меню, возникающее на экране после загрузки с единственного установочного компакт-диска, обыденно, но и достаточно функционально. Предоставляется выбор загрузки с жесткого диска, запуска установки с произвольными параметрами для ядра Linux (в том числе есть и предопределенный вариант с отключенным ACPI), загруз-

ственных и зарубежных производителей. Кроме того, ALT Linux славится хорошими каналами связи между пользователями, службой технической поддержки и разработчиками, что позволяет надеяться на быстрое исправление обнаруживаемых ошибок.

ки в режиме «rescue» или обращения к утилите проверки оперативной памяти memtest86.

Кроме того, присутствует скромная система помощи по предлагаемым опциям, а также возможность смены источника установки (помимо CD их роль могут выполнять серверы FTP, HTTP и NFS) и выбора языка. Однако, несмотря на то что решения ALT Linux у многих ассоциируются с хорошей локализацией, уже здесь наблюдается недостаток. Языков на выбор 6: русский, английский, украинский, татарский, казахский, белорусский. Но присутствует поддержка лишь первых двух, в русской локализации текст на странице помощи неожиданно заканчивается.

Инсталлятор выглядит как приложение с графическим интерфейсом (на базе Qt) и работает поверх сервера Xorg (с самим дистрибутивом X-сервер по умолчанию не устанавливается). Первым делом он вновь просит установить нужный язык, предлагая уже чуть более скромный выбор: русский, английский, украинский, белорусский и... POSIX.

Затрудняюсь сообщить, когда последний успел стать «языком», зато, вне всяких сомнений, предположу, что выбрать здесь предлагают все-таки «локаль», заботливо оставив POSIX как вполне актуальный для кого-то вариант. На сей раз было замечено отсутствие лишь одного из обещанных «языков» – белорусского.

Далее установщик проходит по 11 привычным шагам:

1. Принятие условий лицензии.

## Готовящиеся новинки от ALT Linux

Стоит заметить, что в ALT Linux всерьез взялись за развитие серверного направления. Помимо рассматриваемого в обзоре продукта ожидаются и другие интересные решения:

- ALT Linux 4.0 Office Server ориентиро-

ван на использование в средних и крупных предприятиях, в государственных учреждениях;

- ALT Linux 4.0 Server-K – специальная защищенная версия, находящаяся в процессе прохождения сертификации Федеральной службы по техническому и экспортному контролю России.

2. Выбор способа смены раскладки клавиатуры. Возможных вариантов лишь 4, и нет, например, такого популярного сочетания, как <Alt+Shift>.
3. Подготовка жесткого диска: разделы, файловые системы, точки монтирования и т. д.
4. Установка базовой системы (копирование и инсталляция основных системных пакетов).
5. Установка загрузчика (LILO). Предусмотрена возможность сразу же задать для него пароль.
6. Пароль для суперпользователя root. Есть кнопка для случайной генерации пароля.
7. Добавление системного пользователя. Для пароля – аналогично.
8. Установка дополнительных пакетов. Предлагаются стандартные наборы для следующих серверов: SMTP, POP3/IMAP4, почтовые рассылки, NTP, Kerberos, Proxy, FTP, Caching name.
9. Настройка сети. Позволяет задать параметры для каждого найденного интерфейса, в том числе и беспроводного. Однако моя карточка wi-fi (ipw3945), к сожалению, в списке доступных не появилась.

10. Дата и время (задается страна и город для часового пояса).
11. Завершение инсталляции и сообщение о том, что веб-интерфейс для управления сервером будет доступен по адресу <https://localhost.localdomain:8080>.

В целом процесс установки очень прост, интуитивно понятен и не должен вызвать серьезных проблем у администратора. Инсталлятор, возможно, не так визуальнo красив, как у некоторых других GNU/Linux-дистрибутивов, но главное не в этом. Также отмечу еще один, на мой взгляд, существенный недочет: по ходу установки есть возможность возвращаться на шаг (или несколько) назад, но... В таком случае не сохраняются ранее введенные установки. То есть если (условно) вдруг на шаге 9 возникнет необходимость внести изменения в параметры шага 7, то после этого придется заново проходить шаг 8 и 9. Конечно, нельзя сказать, что это критично, но вот что не очень удобно – однозначно.

## Система

В основе ALT Linux 4.0 Server – Linux-ядро версии 2.6.18 и набор известных и проверенных серверных решений, подробнее о которых – позже. Управление пакетами ПО традиционно для дистрибутивов ALT Linux: адаптированная для RPM версия менеджера APT, родного для Debian GNU/Linux.

Как уже сообщалось, по умолчанию в системе нет графического X-сервера, однако по загадочным причинам установлены такие пакеты, как xterm и GTK+2. Причем у последнего присутствует и каталог с конфигурационными файлами (/etc/gtk-2.0), и даже свой скрипт в /etc/cron.daily с закомментированным вызовом gtk-update-icon-cache.

Одно из ключевых новшеств для дистрибутивов ALT Linux – появление

■ ALT Linux 4.0 Server   192.168.12.6		Справка	en	ru	uk
Система Виртуализация Сеть FTP сервер Прокси-сервер Почта Kerberos					
Сервер электронных рассылок DNS сервер ИБП NTP сервер Администратор системы Бакенды					
Установленные модули					
Название	Описание				
Информация о системе	Общая статистика по системе				
Обновления	Обновление системных пакетов				
Источники обновлений	Настройка источников с обновлениями				
Системные пользователи	Управление системными пользователями				
Виртуальные сервера OpenVZ	Управление виртуальными серверами OpenVZ				
Шаблоны OpenVZ	Создание шаблонов OpenVZ из профиля				
Профили OpenVZ	Создание собственных профилей OpenVZ				
Общие настройки сети	Имя хоста, DNS				
IP-интерфейсы	Управление IP-интерфейсами				
FTP сервер	Управление FTP сервером				
Прокси-сервер	Управление сервером Squid				
Postfix (Настройка SASL)	Включить/выключить аутентификацию (SASL)				
Kerberos сервер	Управление сервером Kerberos				
Сервер электронных рассылок	Управление сервером Mailman				

Рисунок 1. Главная страница веб-интерфейса

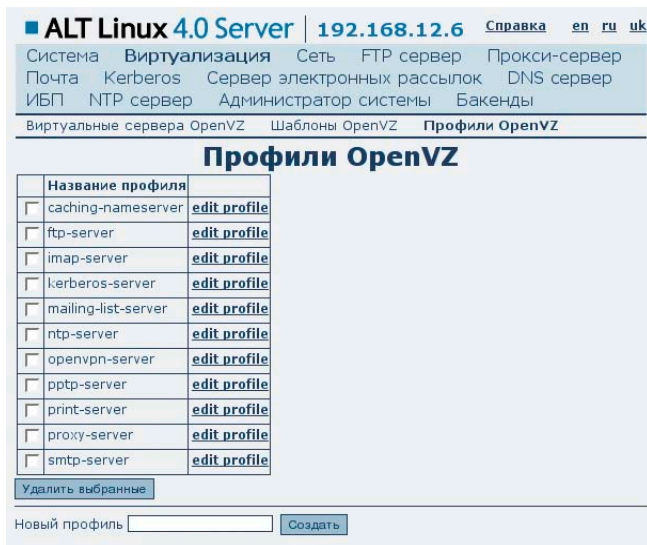


Рисунок 2. Список доступных профилей OpenVZ



Рисунок 3. Настройки ограничений по системным ресурсам для OpenVZ VE

ние системы виртуализации OpenVZ. Для того чтобы сразу приступить к работе с ней, достаточно выбрать соответствующий образ при загрузке (с «ovz» в названии файла – т.е., например, vmlinuz-2.6.18-ovz-smp-alt14). Конфигурация виртуальных серверов (как и многих других компонентов ALT Linux Server) доступна через систему настройки ALTerator, для которой есть веб-интерфейс – именно об этом и извещал инсталлятор на последнем шаге установки.

## Управление сервером через веб-интерфейс

Хотя веб-интерфейс на базе ALTerator, по умолчанию доступен на <https://127.0.0.1:8080>, и ориентирован на возможность удобного удаленного администрирования сервера, его простота позволяет эффективно работать с ним из-под консольного браузера links, входящего в дистрибутив ALT Linux Server. Для авторизации на этой странице необходимо указать логин и пароль системного суперпользователя (root).

Интерфейс снабжен помощью. Формально на трех языках (русский, украинский и английский), но на практике все же лишь на двух первых (причем помощь на русском – наиболее полная). Вместе с выбором другого языка помощи меняется и язык интерфейса.

В веб-интерфейсе доступен ряд вкладок для управления сервисами и настройки отдельных компонентов. Неполное перечисление реализованных в нем возможностей поможет сформировать представление об ALT Linux 4.0 Server в целом.

### ■ Система.

- ✓ Вывод общей информации: версия ядра, количество доступной и свободной оперативной памяти, swap, места на примонтированных разделах жесткого диска.
- ✓ Управление обновлениями с возможностью модификации списка источников.
- ✓ Управление пользователями: добавление, удаление, изменение данных (в том числе и пароля).
- ✓ «Альтернативы» – специальная система ссылок, обеспечивающая дополнительные имена для используемых по умолчанию программ. Ее файлы хранятся в /etc/alternatives. Например, по умолчанию /usr/sbin/httpd2 ссылается на /etc/alternatives/links/lusr/sbin/httpd2, а этот файл, в свою очередь – на /usr/sbin/httpd2.prefork.
- ✓ Системные объекты – выбор одного из доступных «режимов работы» для некоторых приложений. Например, использование утилиты write можно либо разрешить для всех («public»), либо – запретить («restricted»), а в случае с su – полезно разрешить только тем, кто входит в группу wheel («wheelonly»).

### ■ Виртуализация (OpenVZ).

- ✓ Изменение параметров (хост, IP, автоматический запуск, «VE capabilities», ограничения по системным ресурсам, дисковые квоты, доступ к устройствам) существующих виртуальных серверов (VE), добавление новых по одному из шаблонов.
- ✓ Создание шаблонов на основе профилей.
- ✓ Создание профилей. Среди стандартных есть заготовки для следующих серверов: caching nameserver, FTP, IMAP, SMTP, Mailing list, Kerberos, NTP, PTP, OpenVPN, print, proxy.

### ■ Настройка сети.

- ✓ Общие параметры: хост, DNS.
- ✓ Конфигурация интерфейсов: включение/выключение, DHCP, IP/маска сети/шлюз по умолчанию.

### ■ FTP (vsftpd 2.0.5).

- ✓ Общие параметры: доступ для анонимных и локальных пользователей, право записи.
- ✓ Anonymous: права на создание каталогов, загрузку файлов, переименование и удаление.
- ✓ Распределение прав на запись для выбранных локальных пользователей.

### ■ Proxy (Squid 2.6STABLE13).

- ✓ Хост и порт для приема подключений.
- ✓ Список подсетей, имеющих доступ к серверу.
- ✓ Черный список сайтов.



## Почта.

- ☑ SMTP (Postfix 2.3.11): включение (в т.ч. с фильтрацией)/выключение транспорта, SASL, выбор типа сервера аутентификации (Cyrus или Dovecot).
- ☑ POP3/IMAP (Dovecot 1.0): поддерживаемые протоколы (POP3, POP3+TLS/SSL, IMAP, IMAPS) и механизмы аутентификации (plain, login, CRAM-MD5, DIGEST-MD5, APOP, NTLM, GSSAPI, RPA, anonymous, OTP, SKEY). Возможно использование Dovecot как внешнего сервера аутентификации для Postfix.
- ☑ Защита от спама (Spamassassin 3.1.8): режим (удаление или установление метки), пороговое значение, включение белого списка, управление правилами и очками.
- ☑ Управление списками рассылок (Mailman 2.1.9).
- **Kerberos. Указание домена и пароля, управление списком принципалов.**
- **ИБП. Добавление устройств (название + порт) в upsd, поддержка upsdrrv.**
- **DNS (BIND 9.3.4).**
  - ☑ Список серверов для пересылаемых запросов.
  - ☑ Списки сетей, которым разрешено делать простые и рекурсивные запросы.
- **NTP (OpenNTPD 3.9p1).**
  - ☑ Может выступать в качестве клиента (т.е. только синхронизировать время у текущей машины) и сервера (предоставлять эти данные по запросам других машин).
  - ☑ Списки отдельных NTP-серверов и NTP-пулов.
- **Настройка сервера с веб-интерфейсом (порт, пароль, параметры SSL-сертификата).**

Стоит признать, что в теории красивое модульное решение для конфигуратора, построенного на базе ALTerator, на практике иногда оказывалось не очень удобным. В частности, при выполнении некоторых операций, связанных с OpenVZ и требующих значительного времени на выполнение, в интерфейсе сообщалось об успехе в совершении какого-либо действия,

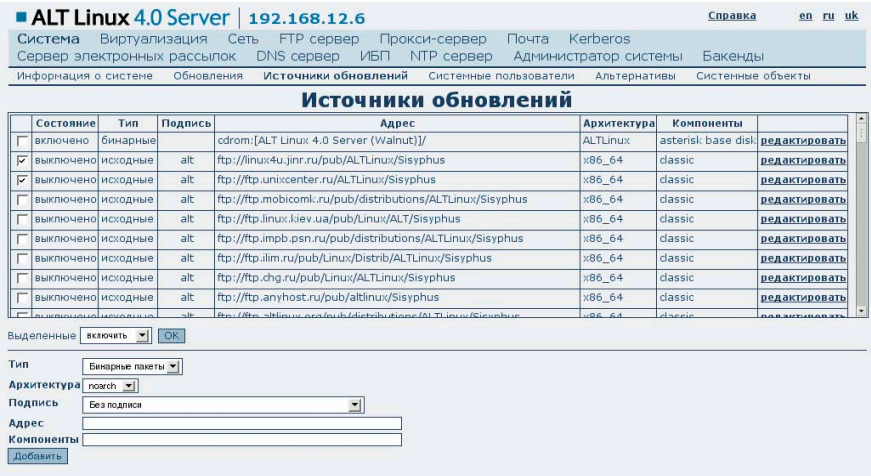


Рисунок 4. Список источников для обновления системы

а топ и фактическое положение вещей на сервере явно свидетельствовали о том, что процесс еще не завершен.

Еще одной приятной возможностью веб-интерфейса является поддержка RSS, способствующая элементарному мониторингу сервера. По словам разработчиков, в генерируемом RSS-файле должна содержаться информация о заполненности дисков и наличии обновлений (у меня же этот файл оказался фактически пустым).

## Другие возможности и пакеты ПО

Разумеется, возможности ALT Linux 4.0 Server не ограничиваются теми, что могут быть сконфигурированы через веб-интерфейс. И даже если не вдаваться в подробности по уже представленным в этом интерфейсе программным продуктам, можно выделить еще целый ряд предусмотренных в дистрибутиве пакетов.

Среди них:

- Asterisk PBX (1.4.4) – популярная программная YATC (пакеты для нее вынесены на CD в отдельный каталог – RPMS.asterisk).
- Nagios (2.7) – система сетевого мониторинга.
- jabberd2 (2.1.4) – демон для организации сетевого общения в реальном времени на базе протокола XMPP (именно он лежит в основе того, что все знают как Jabber),
- OpenLDAP (2.3.35), а также средства работы с другими серверами каталогов для централизованного управления в гетерогенных сетях.
- И, конечно, такие классические и не нуждающиеся в комментариях средства, как OpenSSH (4.6p1), PAM (0.99.6.3), GnuPG (1.4.7), Apache 1.3 (1.3.37 «Russian») и 2.2 (2.2.4), nginx (0.5.20), Samba (3.0.25), MySQL (5.0.41) и PostgreSQL (8.2.4), CVS (1.11.22), Git (1.5.1.6) и Subversion (1.4.3), Amanda (2.5.1)...

## Резюме

ALT Linux 4.0 Server оставил смешанные чувства. С одной стороны, дистрибутив – интересный, нужный и по многим моментам «правильный», но, с другой, – изобилует недочетами. Возможно, это было связано с тем, что рассматривалась тестовая сборка дистрибутива. С большой вероятностью можно предположить, что продукт найдет применение во многих компьютерных парках и серверных, однако для того чтобы попадать туда было проще, стоит довести до блеска свои системные компоненты. И тогда – в добрый путь!

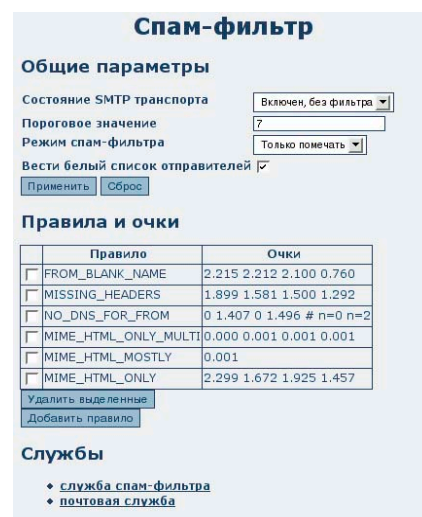


Рисунок 5. Настройки спам-фильтра

# Антивирус+Антиспам Dr.Web для почтовых серверов UNIX

*Сергей Супрунов*

**Когда начинаешь тонуть под наплывом спама и вирусов, хватаешься буквально за каждую соломинку... Но зачем полагаться на соломинку, когда к вашим услугам настоящий спасательный круг?**

**Р**ешений, направленных на противостояние спаму и вирусам, существует множество – от интегрированных в почтовые клиенты фильтров до дорогостоящих комплексных решений, ориентированных на применение в крупных корпорациях.

Бесплатно распространяемые открытые пакеты обычно демонстрируют высокую эффективность лишь при условии грамотного администрирования, то есть требуют глубокого понимания принципов работы почтовых систем, а также определенного внимания в процессе эксплуатации.

С другой стороны, коммерческие решения из разряда «поставь и забудь» зачастую отпугивают небольшие и средние компании своей ценой.

Рассматриваемый продукт компании «Доктор Веб» претендует на звание оптимального по соотношению «цена/качество» – при сравнительно небольшой стоимости разработчики предлагают нам комплексное, удобное в администрировании и весьма эффективное средство противодействия вирусам и спаму.

## Краткий обзор

Пакет «Антивирус+Антиспам Dr.Web для почтовых серверов UNIX», как следует из названия, предназначен для использования в составе серверов электронной почты, работающих на UNIX-подобных системах.

В настоящее время поддерживаются Linux, FreeBSD и Solaris. «Антивирус+Антиспам Dr.Web» способен взаимодействовать с Sendmail, Qmail, Postfix, Exim, CommuniGate Pro, Courier и ZMailer.

Также существует возможность построить продукт в режиме SMTP-прок-

си, что позволит работать практически с любым почтовым сервером, опираясь на стандартные протоколы SMTP и LMTP.

«Антивирус+Антиспам Dr.Web» построен по модульному принципу, благодаря чему можно почти безгранично наращивать его функциональность с помощью подключаемых расширений (плагинов).

Открытый комплект разработчика (SDK) предоставляет возможность разрабатывать необходимые функции самостоятельно.

В частности, именно в виде модулей реализованы функции проверки на вирусы (используется проверенный временем антивирусный пакет Dr.Web) и спам (фильтр, использующий технологию Vade Retro, см. врезку «Антиспамовый движок Vade Retro»). Также доступен модуль проверки заголовков сообщений на соответствие тем или иным правилам. Он позволяет администратору реализовать собственные проверки.

На **рисунке** показана структурная схема пакета.

Модуль Receiver, зависящий от используемого MTA (скажем, в случае Sendmail это будет drweb-milter), получает входящие сообщения и передает их на обработку подключенным плагинам (вы можете настраивать порядок обработки).

Модуль drweb-notifier занимается формированием различных отчетов о результатах проверки писем; Sender отвечает за дальнейшую передачу сообщений, успешно прошедших фильтрацию, а также за отправку служебных уведомлений администратору и отправителю/получателю, формируемых модулем drweb-notifier.

Модуль drweb-agent отвечает за работу всего пакета – именно от него все остальные компоненты получают параметры конфигурации. Он же занимается и сбором статистики.

Наконец, на модуль drweb-monitor возложена обязанность по запуску всех модулей и дальнейшее отслеживание их работоспособности (и при необходимости их перезапуск).

## Установка и настройка

Установка начинается с получения архива с основным пакетом. Для каждой пары «операционная система – MTA» имеется свой tar-файл. Например, для FreeBSD 6.x и Sendmail имя архива будет drweb-maild-sendmail-4.33.0-freebsd60.tar.gz. Очевидно, что номера версий со временем могут меняться.

Распаковка выполняется стандартно, после чего можно пойти двумя путями: автоматическая инсталляция с помощью сценария install.sh, или ручная установка, подробно описанная в поставляемой с пакетом документации.

Инсталляция пакета в автоматическом режиме прекрасно подойдет в большинстве случаев – скрипт грамотно следует особенностям системы, так что вам не придется, скажем, на FreeBSD искать двоичные файлы в /opt, а в дистрибутивах Linux самостоятельно подгонять rc.d-сценарий.

Применительно к FreeBSD могу отметить лишь пару незначительных моментов.

Во-первых, видимо, по соображениям совместимости с системами 4-х версий используется «старый», не поддерживаемый rcorder, формат сценария инициализации – sh-файл в каталоге /usr/local/etc/rc.d. Впрочем, на ра-

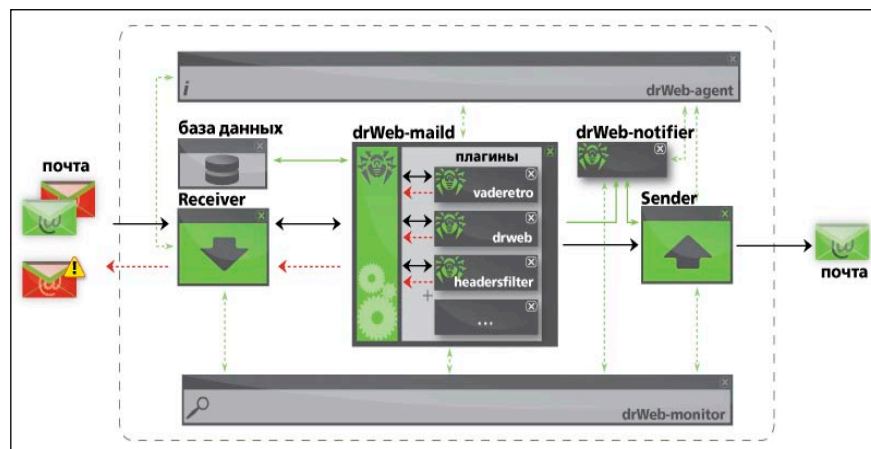
ботоспособности это не сказывается, да и создать при желании стартовый скрипт не так уж и сложно.

Во-вторых, то, что инсталлятор для интеграции с Sendmail вносит необходимые изменения непосредственно в `sendmail.cf`, может затруднить сопровождение системы. Ведь если вы настраиваете Sendmail через `mc`-файл (как оно и рекомендуется делать), то при любой правке конфигурации настройки, отвечающие за `mlfilter` для Dr.Web, вы потеряете. Так что все равно желательно добавить вручную нужные строки и в соответствующий `mc`-файл (что именно должно быть добавлено, хорошо расписано в документации).

Пожалуй, можно указать ещё один недостаток инсталлятора. При установке отечественного продукта хотелось бы и сообщения получать на родном языке. Впрочем, в составе пакета идёт подробная документация на русском языке, плюс с сайта можно скачать объёмное руководство в формате pdf.

После инсталляции основного пакета также нужно установить пакет обновлений (`updater`), отвечающий за поддержание в актуальном состоянии баз данных антивируса и антиспама, а также самих «бинарников».

Постинсталляционная настройка пакета заключается в редактировании трех конфигурационных файлов в каталоге `/etc/drweb` (или `/usr/local/etc/drweb` для FreeBSD): `agent.conf`, `monitor.conf` и `mail_sendmail.conf` (для другого MTA имя будет, естественно, другим). Они достаточно подробно прокомментированы и к тому же имеют вполне разумные значения по умолчанию (параметры, которые требуют



Структурная схема пакета

внимания с вашей стороны, запрашиваются настроенным скриптом во время инсталляции).

Далее, после установки нужных модулей расширения (модуль антивирусной проверки `drweb-mail-plugin-drweb-4.33-*` следует установить уже после того, как будет установлен и запущен сам антивирус, `drweb-4.33`) комплекс готов к работе (не забудьте перезагрузить почтовый сервер). Тонкую настройку плагинов можно выполнить, редактируя конфигурационные файлы, которые будут созданы в том же каталоге `etc/drweb`.

Антивирус показал себя превосходно — высокое качество работы, красивые и понятные пользователям уведомления об обнаруженном вирусе. Антиспамовый модуль, как ни странно, также с первых минут продемонстрировал неплохую эффективность. От немодифицированного французского пакета я, честно говоря, ожидал худших результатов на русскоязычных сообщениях. Правда, в данной версии `plugin-vaderetro` умеет лишь добавлять заголовки к письму да префикс к те-

ме сообщения, так что фильтрацию таких сообщений придется настраивать в почтовом клиенте или, скажем, с помощью `prosmail`. Кстати, справится с этой задачей и модуль фильтрации по заголовкам `headersfilter` при условии, что он будет обрабатывать сообщения после модуля `vaderetro`.

## Итоги

Итак, кому и зачем стоит покупать «Антивирус+Антиспам Dr.Web для почтовых серверов UNIX»? Прежде всего тем, кто заинтересован в надежной и эффективной защите почтового трафика без лишних усилий по администрированию и «сборке воедино» различных компонентов зачастую от разных разработчиков. Символические системные требования не станут преградой к использованию пакета в небольших предприятиях и даже в «домашних офисах», а гибкая тарифная политика позволит подобрать наиболее выгодный вариант именно для вашего случая.

Конечно, если ваша основная цель — экономия почтового трафика на сервере, то здесь «Антивирус+Антиспам Dr.Web» вам не помощник. Модуль `vaderetro` не использует методы «раннего обнаружения» типа DNSBL (отчасти из-за высокой вероятности ложных срабатываний), а для полного анализа за сообщение требуется принять полностью. Но если основным критерием для вас является эффективность работы сотрудников вашей фирмы или удобство клиентов, которым вы предоставляете услуги электронной почты, то здесь рассмотренное решение от компании «Доктор Веб» будет прекрасно служить вам.

## Антиспамовый движок Vade Retro

В основе антиспамового плагина продукта «Антивирус+Антиспам Dr.Web» лежит разработка французской компании GOTO Software под названием Vade Retro.

Она отличается высокой эффективностью и рядом уникальных возможностей, таких как эвристический анализатор спама, исключающий необходимость в предварительном обучении, взаимодействии с централизованными базами данных, «черными» списками и т. д., практически сразу после установки фильтр го-

тов к полноценной работе. Vade Retro распознаёт спам, подвергая анализу все части сообщения — заголовки, имена и содержимое вложений, текст письма, в том числе и HTML-код, — выявляя характерные признаки спама. Причём попытки спамеров обойти фильтры лишь увеличивают вероятность распознавания такого письма именно как спама.

Нужно отметить, что анализатор одинаково эффективен при обработке писем на любом языке, так что прекрасно справляется и с русскоязычным спамом без какой-либо адаптации.



# Развертываем корпоративную телефонную сеть на основе технологии VoIP

## Часть 1

Рашид Ачилов

Однажды начальник вызывает вас и, показывая на грудку коробок с надписями Samsung – Enterprise IP Solutions, говорит: «Это наша новая телефонная станция, которую мы поставим в филиале в другом городе. Она должна связываться с нашей основной станцией по VoIP. Во-первых, это позволит экономить на междугородке, а во-вторых, можно будет звонить по коротким номерам».

### Собери свою станцию

Итак, с чего начнется наша работа? Конечно же, с изучения того, что это разложено перед нами. Мы будем исходить из того, что новую станцию модели OS7200 нам необходимо подключить к уже действующей станции модели OS500. Следовательно, в минимальной комплектации (8 транков, 8 ЦАК, 16 АК, 4 VoIP-канала) коробок должно быть девять – большая коробка размером с 19" корпус компьютера для монтажа в 19" шкаф, в которой находится базовый блок, шесть коробок поменьше, одна еще меньше и одна совсем крошечная. Находятся в них:

- **Блок MCP** – блок центрального процессора АТС. Это мозг станции. На нем имеется разъем LAN для подключения в локальную сеть, а также другие разъемы и индикаторы, назначение которых подробно описано в документации [1].
- **Блок MGI** – блок VoIP. Имеет отдельный разъем LAN, которому назначается отдельный IP-адрес. В общем случае блоков MGI в станции может быть несколько (хотя для станции филиала это маловероятно, потому что на плате блока MGI имеется 4 посадочных места для модулей MGI2D, каждый из которых обеспечивает 4 одновременных разговора). Другие разъемы и индикаторы подробно описаны в документации [1].

- **Блок 8DLI** – блок, содержащий 8 комплектов ЦАК. В свободной части передней панели расположены индикаторы использования комплектов.
- **Блок 8TRK** – блок, содержащий 8 комплектов транковых (внешних) линий. Сюда подключаются входящие линии ТФОП и УАТС. На свободной части передней панели расположены индикаторы занятости каждого транка.
- **Блок 16SLI** – блок, содержащий 16 комплектов АК. Поскольку разъемы занимают всю площадь передней панели, никаких индикаторов на блоке нет.
- **Модуль кодеков MGI2D** – маленькая плата, устанавливаемая в соответствующие разъемы на плате блока MGI.
- **Носитель информации** – карта MMC, обычно объемом 64 Мб, с записанной на ней последней версией программного обеспечения станции. Поставляется в маленькой белой коробочке.

Распаковываем базовый блок и приступаем к сборке. Отвертка не понадобится. Удивляемся, почему в комплекте отсутствует силовой кабель питания? Не торопитесь звонить поставщику – кабель не входит в комплект поставки. Точно так же, как не входит документация, – не ищите ни пакет

с книжками, ни диск, лучше сразу идите на сайты производителей [4, 5] и загружайте документацию – [1-3]. В особенности полезным будет [3]. Несмотря на то что все описание, приведенное там, рассчитано на программирование с СТА, при программировании с РСММС из него можно почерпнуть множество полезной информации.

Распаковываем блок MCP. На блоке есть набор DIP-ключей и один переключатель, который нужно поставить в положение «Вкл.». DIP-ключи задают регион и размер номерного поля для номеров АК, транков и групп – по одному ключу на номерное поле.

По умолчанию все настроено на 4-значную нумерацию, можно переключить на 3-значную, только зачем? Регион задавать не имеет смысла, так как ключами можно задать только США, Англию или Корею, остальные только через программу-конфигуратор.

Если станция укомплектована дополнительными модулями, устанавливаемыми на блок MCP (см. [1] для более подробного описания), то устанавливаем их.

Слегка отводим вперед рычаг черного цвета в нижней части блока и утапливаем блок в разъемы базового блока, при этом рычаг фиксируется в закрытом положении. Для извлечения блока необходимо потянуть за рычаг.

Вынимаем карту MMC из маленькой белой коробочки и устанавливаем (этикеткой вверх, обрезом вправо, контактами вниз) в разъем на передней панели блока MCP.

Распаковываем блок MGI и модуль MGI2D, устанавливаем модуль MGI2D на плату блока MGI. Разъемы модуля MGI2D имеют ключи, установить неправильно его нельзя. Можно ориентироваться еще и по стрелке, нарисованной на плате MGI2D, – она должна указывать в центр платы блок MGI. Если станция укомплектована несколькими модулями MGI2D (максимум 4), устанавливаем все. Единственный переключатель на плате блока поставить в положение «Вкл.»

Распаковываем и устанавливаем остальные блоки. Никаких переключателей и разъемов для подключения дополнительных модулей на них нет.

Более подробное описание процесса сборки станции приведено в документации [2].

Все. Можно включать питание. Подключать Ethernet-интерфейс в локальную сеть пока не имеет смысла – на блоке MCP настроен адрес по умолчанию, а на блоке MGI он вообще равен 1.1.1.1. Поэтому сначала нам понадобится системный телефон, а в дальнейшем – программа-конфигуратор АТС.

## Телефон, да не простой

Для начала работы со станцией нам обязательно понадобится как минимум один системный телефон (СТА). Для определенности будем использовать наиболее дешевую модель – Samsung DCS-12B, двенадцатикнопочный телефон с двухстрочным ЖКИ-индикатором. Понадобится он нам для начального программирования станции, потому что адрес по умолчанию не сменить никак, кроме как с СТА. Понадобится он нам и для дальнейшего программирования и выяснения ошибок, потому что станция не имеет других интерфейсов подключения программы-конфигуратора, кроме COM-порта и доступа по Ethernet.

Что такое системный телефон? Это телефон, подключаемый к ЦАК, который, кроме того что он используется по назначению, предоставляет своему пользователю большой выбор сервисных функций, вплоть до програм-

## Терминология

В IP-телефонии применяется многочисленная специфическая терминология, большинство терминов которой пришло из «классической» телефонии. Для системных администраторов, которые, может быть, когда-то работали монтерами кросса или линейными монтерами, в ней не найдется ничего нового, но для тех, кто занимался исключительно компьютерами, она может оказаться незнакомой.

**ГТС (ТФОП, PSTN)** – городская телефонная сеть (телефония общего пользования). Подразумевается обыкновенная городская телефонная сеть.

**УАТС (PBX)** – учрежденческая АТС. Подразумевается локальная АТС крупного предприятия, которая может оказаться устаревшего типа (например, «Искра» – очень популярная среди УАТС).

**Комплект серийной линии (КСИ, серийный комплект, транк, TRK)** – физический компонент АТС, обеспечивающий взаимодействие с одной внешней телефонной линией (ГТС, УАТС). Как правило, КСИ группируются в блоки серийных линий, представляющие собой платы, устанавливаемые в слоты расширения АТС.

**Абонентский комплект (АК, SLI)** – физический комплект АТС, обеспечивающий взаимодействие с одним обыкновенным (аналоговым) внутренним телефонным

мированием кнопок через АТС, отображает номер и идентификатор звонящего абонента и т. д. Но в настоящий момент нас не интересуют пользовательские функции, нас больше интересует то, что с его помощью можно изменять настройки АТС. Для этого вначале освоимся с управлением АТС через него.

Непосредственно под дисплеем находятся три кнопки без названия, функции которых примерно аналогичны кнопкам на сотовых телефонах, когда возможное действие отображается на экране.

Во время обычного пользования СТА как телефоном, на экране в нижней строке отображаются действия, которые можно выполнить с их помощью. Но поскольку в режиме программирования задействованы обе строки, нам придется пользоваться кнопками вслепую.

Мы назовем их для определенности «левая под дисплеем» (ЛПД), «сред-

аппаратом. Как правило, АК группируются в блоки абонентских комплектов, представляющие собой платы, устанавливаемые в слоты расширения АТС. Блоки АК – основное содержание АТС.

**Цифровой абонентский комплект (ЦАК, DLI)** – то же самое, только предназначен для работы с цифровым (системным) телефоном, который, кроме основных функций, обладает рядом сервисных, в том числе возможностями по программированию АТС.

**Физический номер** – номер устройства (комплекта, порта), выделяемый жестко и без возможности изменения на основе расположения платы в слоте АТС. Изменяется при перемещении платы в другой слот.

**Логический номер** – номер устройства (комплекта, порта), назначаемый при конфигурировании АТС. Может меняться произвольное количество раз.

**LCR** – маршрут до абонента, определяемый по принципу меньшей стоимости (Less Cost Route).

**MMC** – отдельная микропрограмма, задающая некоторый определенный блок настроек АТС. Называется также блоком, командой или таблицей, хотя, по сути, все эти названия неверны.

**PCMMC** – так в документации обозначается компьютер, с которого выполняется программирование АТС.

няя под дисплеем» (СПД) и «правая под дисплеем» (ППД), при этом кнопка ППД находится рядом и немножко выше кнопки <Scroll>.

При программировании АТС кнопка ППД используется для перемещения курсора в следующую позицию, где можно вводить или изменять данные.

Кроме ППД, для программирования используются кнопки <Volume +> и <Volume ->, с помощью которых переходят на следующий (предыдущий) экран настроек, и кнопка <TRSF>, которая служит для запуска процедуры программирования или принятия изменений.

Инженеру телефонной сети обязательно необходимо иметь как минимум один СТА, потому что некоторые операции (например, MMC 818) можно выполнять только с СТА.

Следует также иметь в виду, что для большинства операций по программированию АТС необходимо пред-

## Модели АТС, выпускаемые компанией Samsung

В настоящее время Samsung выпускает большое количество офисных АТС, объединенных общей маркой OfficeServ (OS). Серия OfficeServ состоит из двух конструктивно различающихся подсерий. В одну из них входят OS12, OS100 и OS500, в другую – OS7200 и OS7400. Основное конструктивное различие между ними – OS12, OS100 и OS500 навешиваются на стену и для подключения телефонов используют соединительный кабель Amphenol, второй конец которого расщивается на стандартный кросс типа 66, а OS7200 и OS7400 имеют стандартные разъемы RJ-45. Основные параметры АТС приведены в **таблице 1**.

OS12 – наиболее простая модель серии – один монолитный блок, без возможности расширения. Несмотря на простоту, обладает всеми возможностями серии, в том числе возможностью объединения в сеть по VoIP.

OS100 – модель для малого и среднего офиса, позиционируемая как «экономичная». Обладает всеми возможностями

серии, в том числе и интеграцией по VoIP. Конструктивно выполнена в настенном моноблоке, расширяемом дополнительным мини-блоком. Она действительно экономичная..., пока не захочешь прикупить к ней блок MGI3 – укомплектованная станция на 6 транков, 3 цифровых и 16 аналоговых комплектов стоят порядка 30 тыс. руб., блок MGI3 – порядка 35 тыс. руб. (цены взяты с <http://www.officeats.ru>).

OS500 – «макси»-модель. Имеет две модификации – L (large) и M (medium). Конструктивно представляет собой настенный моноблок на 8 слотов. Модификация L может расширяться до 3 блоков, модификация M – до двух.

OS7200 – стоечный аналог OS100. Конструктивно выполнена в 19" корпусе, в который может быть установлено до 6 блоков. Наиболее популярная в настоящее время модель. Расширяется до двух корпусов.

OS7400 – «макси»-модель в стоечном исполнении. Унифицированная с OS7200 по блокам модель, которая расширяется до трех корпусов.

Таблица 1. Основные характеристики АТС Samsung серии OfficeServ

Модель	Максимальное количество портов	Количество VoIP-каналов	Расширяемость
OS12	20	4	нет
OS100	96	16	1 мини-блок
OS500	542	8 на модуль <sup>1</sup>	2 (M), 3 (L) блока по 8 слотов
OS7200	216	16 на модуль <sup>2</sup>	1 корпус на 6 слотов
OS7400	656	16 на модуль	2 корпуса на 6 слотов

<sup>1</sup> Модули нерасширяемые, устанавливаются в слот корпуса.

<sup>2</sup> Модули расширяемые, устанавливается карта MGI2D, каждая на 4 канала.

варительно разрешить эти действия, введя пароль технического специалиста, который по умолчанию равен 4321. Для ввода пароля предназначен MMC 800.

## Меняем адрес АТС по умолчанию

Первое, что нам необходимо сделать для того, чтобы начать настройку АТС, – это изменить IP-адрес блока MCP, установленный по умолчанию на тот, который нам необходим. Сделать это можно только с СТА.

Порядок действий следующий:

- <TRSF>, 800, появляется надпись «Enable Tech.Prog», а ниже «Passcode:», 4321.
- Вторая строка меняется на «Disable Tenant:1», <Volume ->, строка меняется на «Enable Tenant:1», <TRSF>.

■ <TRSF>, 830, появляется надпись «System IP address:», а ниже выведен установленный в данный момент IP-адрес.

■ ППД, ввести нужный адрес (при вводе дополнять неполные группы нулями, например для ввода 192.168.1.1 набрать 192168001001), <Volume +>.

■ Появится надпись «System Gateway:», а ниже будет выведен текущий установленный адрес шлюза по умолчанию.

■ ППД, ввести необходимый адрес шлюза по умолчанию, <Volume +>.

Таблица 2. План прозвонки

Номер	Описание	Входящие	Исходящие	Группа в MMC 614	Группа в MMC 601
4251	Директор		+	3	5001
4252	Администратор	+	+	1	5000, 5001
4253	Бухгалтер	+		2	5001
4254	Оператор			4	5002

■ Появится надпись «System Netmask:», а ниже будет выведена маска подсети по умолчанию 255.255.255.0.

■ Если эта маска вас не устраивает, нажать ППД и ввести новую маску, иначе пропустить этот пункт.

■ <Volume +>.

■ Появится надпись «System reset:», а ниже «Are you sure: NO».

■ ППД, <Volume +>, «NO» меняется на «YES».

■ <TRSF>, станция перезагружается с новым адресом.

## Наша «коробка с инструментами»

В ней не будет ни пинцета с изолированными ручками, ни длинной отвертки, словом, ничего такого, без чего немыслима была работа инженера кросса во времена координатных АТС. В ней будут два «инструмента» – Samsung OfficeServ Manager (OSM) и DeviceFileUploader (DFU). Первая программа предназначена для настройки станции, вторая – для обновления микропрограммного обеспечения. Обе программы распространяются бесплатно. Скачать их можно с <http://forum.officeats.ru>, правда, там все файлы зачем-то запаролены. Пароль на все архивы «forum.officeats.ru». Программа OfficeServ Manager состоит из основного блока, установочный архив которого объемом 50 Мб, и модуля модели OS7200 объемом 3 Мб. Программа DeviceFileUploader объемом 18 Мб. Установка проводится стандартным для Windows способом (надеюсь, упоминать о том, что обе эти программы существуют только под Windows, излишне?).

Сначала устанавливается основной блок. В нем может не оказаться поддержки OS7200 – не пугайтесь, поставьте, например, OS500. После установки основного блока запустите установку модуля поддержки OS7200. Не забудьте установить DeviceFileUploader – на самом деле он не является обязательной про-



граммой, но для обновления программного обеспечения станции она просто незаменима. Разумеется, обновление можно проделать без нее. Если хватает квалификации. Просто DFU берет на себя выполнение тех рутинных действий, в которых нельзя ошибиться, но которые являются обязательными.

Запускаем OSM. (см. **рис. 1**). Программа исключительно англоязычная, причем к ней нет и, видимо, никогда и не будет каких-либо русификаторов, русских ресурсов, русских справок и прочего, что обычно выпрашивают люди, которые не в ладах с английским.

Выбираем из списка установленных модулей OSM\_7200 и нажимаем значок с молотком для настройки параметров связи со станцией (см. **рис. 2**).

В нижних полях «Site» и «IP-address» вводим соответственно описание станции и ее IP-адрес, который мы только что установили с СТА, и нажимаем кнопку «Add». Для подключения к станции необходимо дважды щелкнуть мышкой по выбранной станции, при этом загружается рабочая оболочка. Для подключения к станции следует нажать на кнопку «Connect» (с изображением двух состыкованных сетевых узлов).

Рабочая оболочка проверяет доступность станции, и если она доступна, выдает запрос на пароль технического специалиста, который, как уже упоминалось, по умолчанию равен 4321 (см. **рис. 3**).

Если пароль введен верно, программа начинает загрузку настроек из станции. Эта процедура может занять некоторое время. Процесс загрузки настроек отображается на экране (см. **рис. 4**).

После загрузки начальных настроек отображается рабочее поле программы (см. **рис. 5**). Тех, кто никогда не видел до этого программы-конфигуратора, вид рабочего поля обычно повергает в некоторое недоумение – «И что же тут делать дальше?».

Действительно, OSM отличается редкостной недружелюбностью интерфейса – никаких мастеров, никаких подсказок, единственная страховка – от дублирования данных. По сути OSM – это всего лишь переложенный на компьютерный вариант СТА в той его части, что относится к программированию станции.

На панели инструментов находятся кнопки подключения/отключения станции, загрузки-выгрузки настроек в конфигурационный файл, просмотра версии прошивки и их обновления, справки и «О программе».

Основная работа проводится при загрузке в рабочее поле некоторой MMC, раскрывающийся список которых представлен слева.

Для загрузки определенной MMC следует щелкнуть по ней дважды. Имейте в виду, что загруженная MMC не выгружается автоматически при закрытии окна – она просто становится неактивной. Одновременно можно загрузить не более десяти MMC.

### Какие еще бывают блоки для OS7200

- ☑ **LCP** – модуль сопроцессора. Устанавливается вместо модуля основного процессора в дополнительный корпус при расширении станции.
- ☑ **TEPRI** – модуль подключения каналов T1/E1 или ISDN PRI.
- ☑ **4BRI** – модуль подключения каналов BRI.
- ☑ **8SLI** – модуль на 8 АК.
- ☑ **16DLI** – модуль на 16 ЦАК.
- ☑ **8HYB** – модуль на 8 гибридных (аналоговых или цифровых) комплектов.
- ☑ **8COMBO** – модуль на 8 АК и 8 ЦАК.
- ☑ **WIM** – модуль DSL-интерфейса, DMZ

и брандмауэра, а также модуль управления блоком LIM. Применяется для построения сети на базе станций в малых офисах – станция может использоваться в качестве брандмауэра и DSL-шлюза. Мы не будем рассматривать это решение.

- ☑ **LIM** – модуль на 16 портов обыкновенного Ethernet-коммутатора (при наличии модуля WIM работает как коммутатор второго уровня).
- ☑ **4DSL** – модуль на 4 DSL-канала для подключения удаленных устройств.
- ☑ **4WLI** – модуль интерфейсов с беспроводными станциями WBS24.
- ☑ **SVMi-20E** – модуль голосовой почты.

Полезную информацию несет также последняя строка окна программы – здесь выводятся состояние станции (ONLINE), тип подключения и подключенный узел (LAN REMOTE: Kemerovo\_shop [192.168.1.31]), версии программного модуля PCMMC и прошивки MCP (M:2.69-P:2.69), текущая установленная страна (ITALY), тип станции (OfficeServ 7200), дата и время в станции. То, что текущая в данный момент страна – Италия, не должно вызывать удивления – рисунок отображает состояние станции в мо-

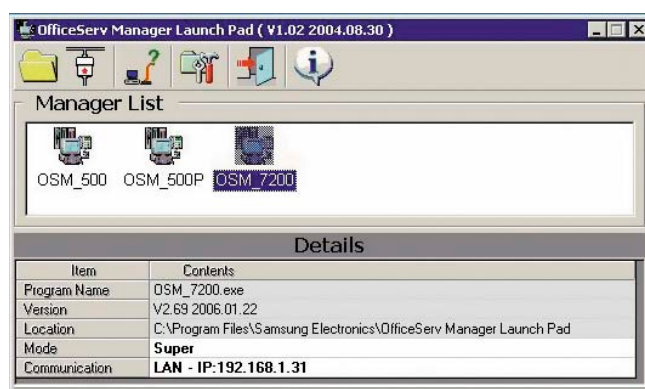


Рисунок 1. Начальный экран запуска OfficeServ Manager

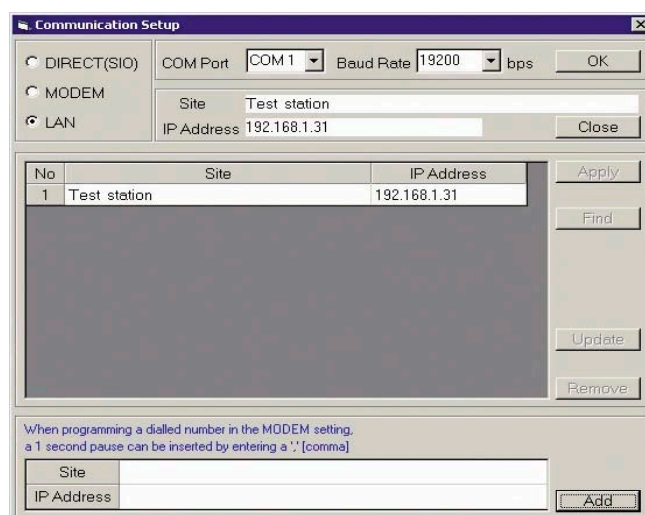


Рисунок 2. Экран настроек параметров связи со станцией

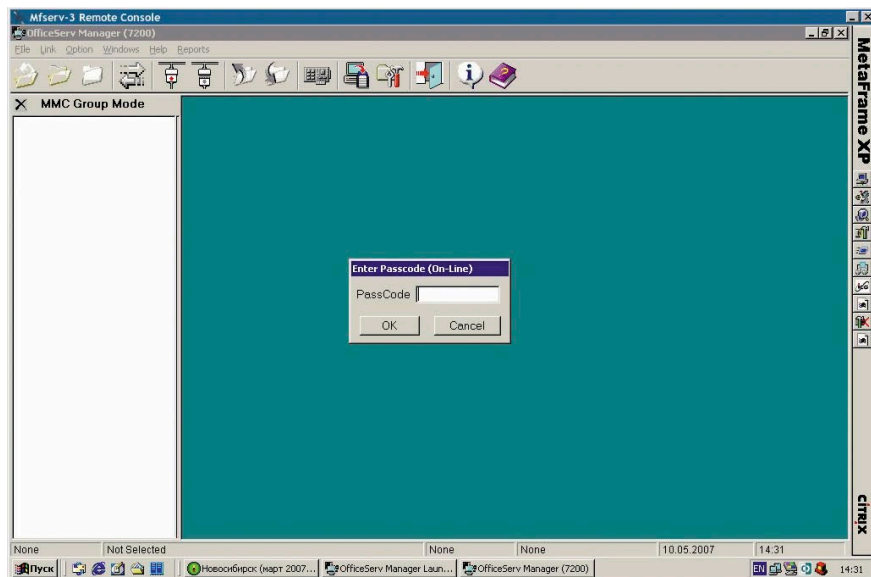


Рисунок 3. Запрос пароля для доступа к настройкам станции

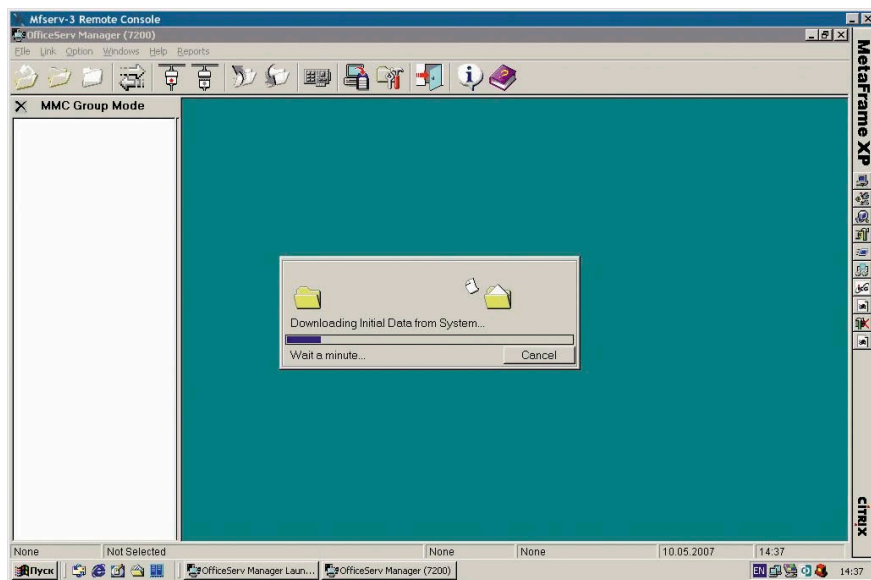


Рисунок 4. Загрузка начальных данных из станции в программу настройки

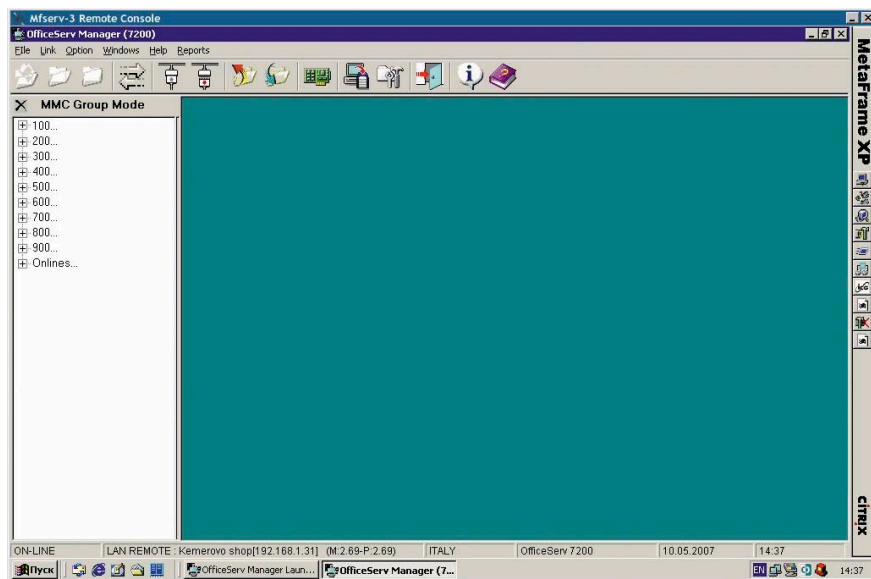


Рисунок 5. Рабочее поле программы Samsung OfficeServ Manager

мент первого включения, без выполнения каких-либо настроек, а в этот момент страна может быть установлена совершенно произвольно (лично мне попадались несколько раз Италия и Румыния).

Программу DeviceFileUploader мы опишем в разделе, посвященном перепрошивке программного обеспечения станции.

## Общая начальная настройка

Настройка станции филиала будет проводиться нами в два этапа:

- на первом этапе станция настраивается просто как обычная офисная станция, которая принимает звонки и направляет их на АК, которая позволяет одним звонить в город, а другим – нет, перехватывать звонки и т. д. – все возможности OfficeServ 7200 как офисной станции описаны в [1];
- на втором этапе вводятся специфические настройки для связи головной станции (мы договорились, что на ней работает OS500) и станции филиала.

Итак, первый этап настройки. Он включает в себя:

- первоначальную настройку (установку региона, даты и времени, типа транков, времени блокировки PCMMC, времени распознавания Flash);
- назначение АК-внутренних номеров и группировку их по возможностям доступа.

Беремся за дело. Для начала нужно установить регион. Настройки кода региона сохраняются в файле при выгрузке конфигурационных файлов, и программа-конфигуратор не даст загрузить в станцию файл с настройками, в которых код региона отличается от того, что установлен в станции. Код региона нужно устанавливать в первую очередь, потому что при изменении кода региона все остальные настройки (кроме IP-адреса блока MCP) сбрасываются в настройки по умолчанию.

Итак, открываем MMC 812, щелкаем по списку регионов и выбираем «Russia/CIS» (см. рис. 6).

Далее нужно увеличить время блокировки PCMMC, то есть время

бездействия, по истечении которого станция автоматически отключается от программы-конфигуратора, поскольку в каждый момент времени только один человек может подключиться к станции с помощью данной программы. По умолчанию оно равно 5 минут, что очень мало, когда постоянно параллельно настройке читаешь документацию. Открываем MMC 501, выбираем РСММС LOCK TIME и ставим максимально возможное значение – 60 мин (см. рис. 7). Дата и время устанавливаются в MMC 505 (см. рис. 8).

Далее мы установим время распознавания сигнала Flash. По умолчанию установлен диапазон 30-85 мс, мы изменим его на 10-90 мс, чтобы исключить ситуацию, когда краткое нажатие на рычаг телефона воспринимается не как повторное поднятие трубки, а как Flash (см. рис. 9). Время распознавания задается так же, как и время блокировки РСММС, в MMC 501.

Для выполнения следующего пункта нам большую помощь окажет таблица 2, которую обычно называют «планом прозвонки». В ней отмечается, какие АК должны принимать входящие вызовы, какие АК имеют право звонить в город, а какие – только набирать внутренние номера.

Здесь мы назначаем номера на четыре АК, а также определяем, что входящие звонки принимает АК с номером 4252, что исходящие звонки в город можно делать с номеров 4251 и 4252, что номер 4253 может звонить только на локальные номера. При этом следует учесть, что группы в MMC 601 – это «звонковые» группы, то есть здесь задается, на какие АК будет направляться вызов при его поступлении по той или иной линии, а группы в MMC 614 – это «группы доступа», где задается, какие АК имеют право пользоваться какими транковыми группами (а это могут быть транки, каналы МГИ и др.) и каким образом – отвечать на вызов, совершать вызов.

Выделив номера на АК, программируем их в MMC 724 (см. рис. 10).

Группировка АК может делаться по двум принципам:

- группировка по приему вызова с транка (какие АК будут звонить при приеме вызова по тому или иному транку). Это настраивается включением АК в определенную

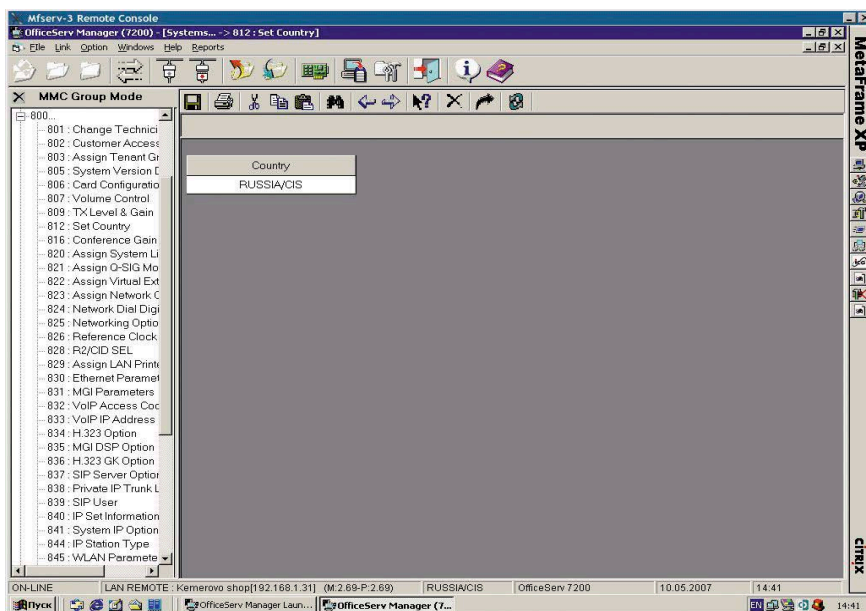


Рисунок 6. Установка кода региона

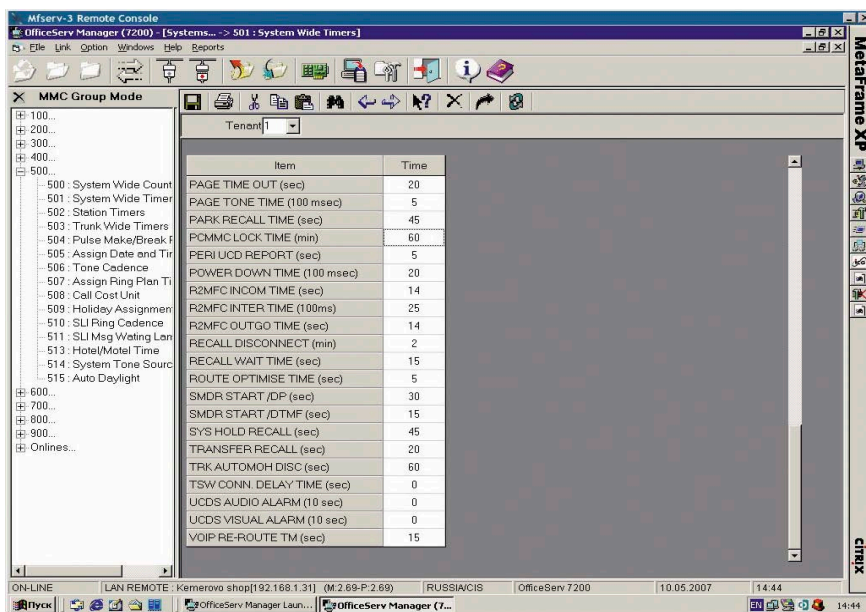


Рисунок 7. Установка времени блокировки РСММС

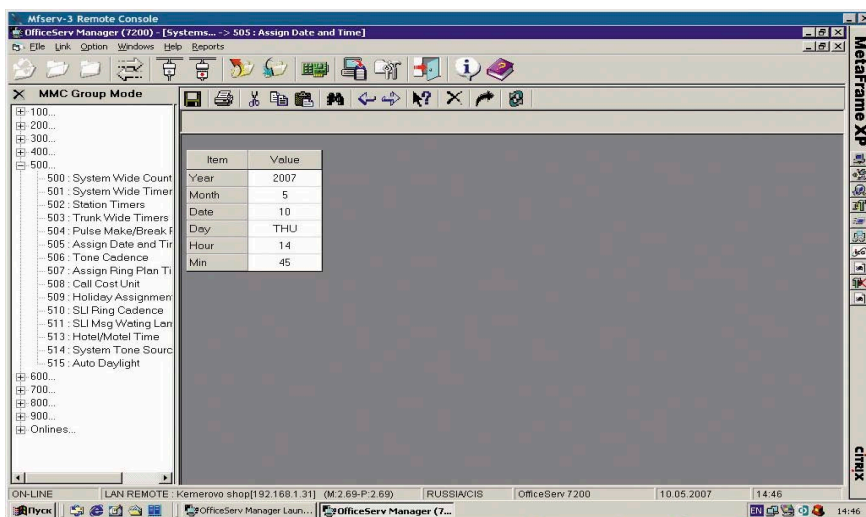


Рисунок 8. Установка даты и времени



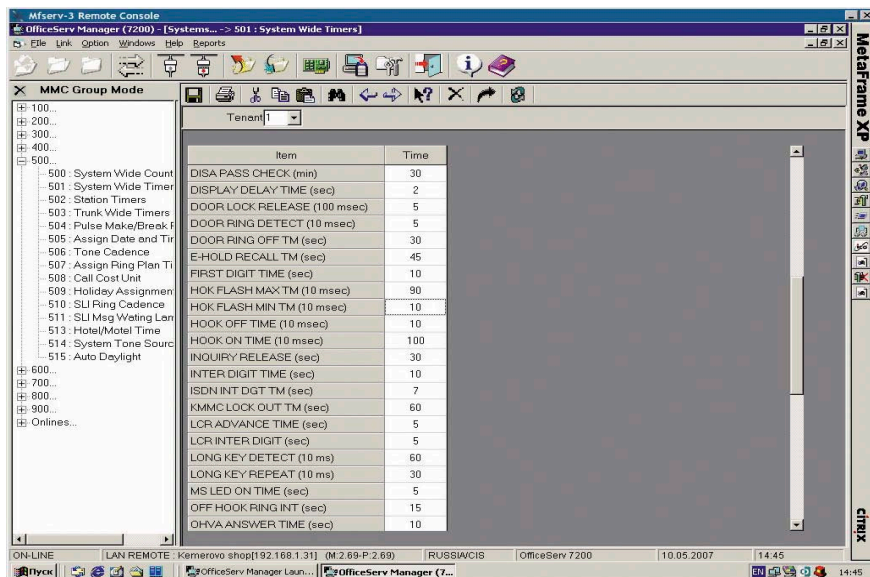


Рисунок 9. Установка времени распознавания сигнала Flash

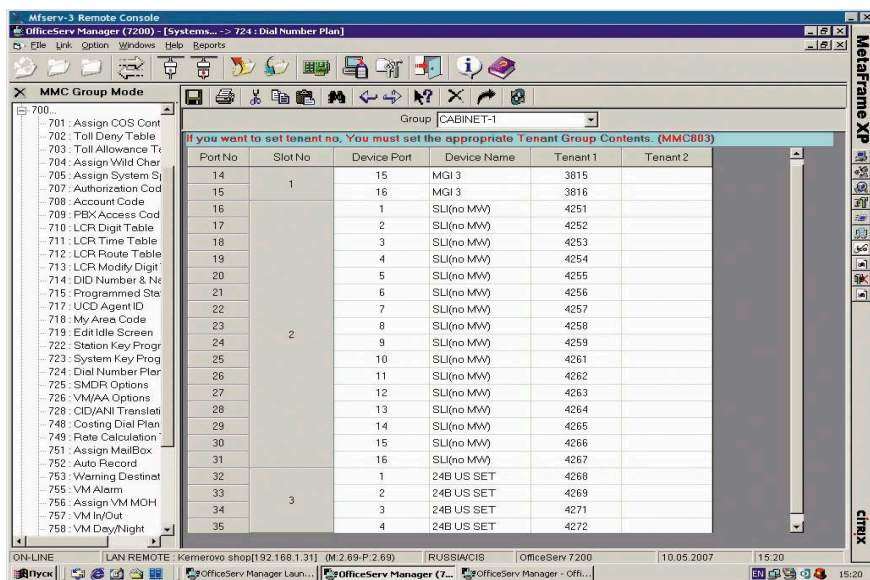


Рисунок 10. Задание номеров АК в номерном плане

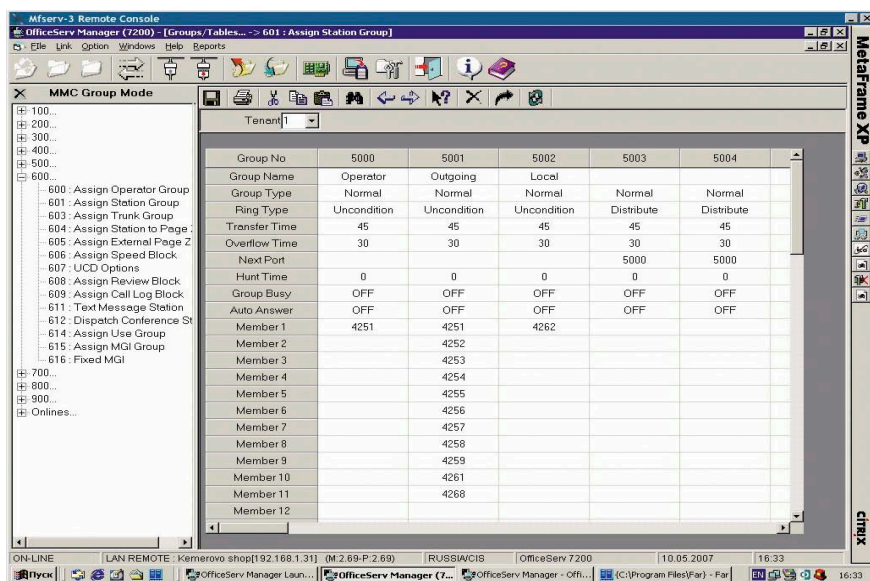


Рисунок 11. Включение АК в группы вызова

группу в MMC 601 (см. рис. 11) и направлением вызова с определенной транка на определенную группу в MMC 406 (см. рис. 12). По умолчанию все вызовы направляются на АК, включенные в группу 5000, которая называется «группой операторов», потому что, как правило, по этим номерам сидит секретарь, офис-менеджер или аналогичный персонал.

- **группировка по правам доступа к внешней линии.** Под внешней линией подразумевается не только транк, но и канал VoIP или других технических средств связи. Для этого формируются так называемые «группы доступа». Они совершенно независимы от групп приема вызова, для внутренних АК выделены группы 001-300, для внешних линий – 30-500. По умолчанию все транки включаются в группу 301, доступ к которой и регулируется в MMC 614. Предварительно в MMC 304 настраиваются нужные группы (в нашем случае 1, 2, 3 и 4, см. рис. 13, показана группа 2), в которых:

- ✓ в группе 1 не изменяется ничего (по умолчанию полный доступ);
- ✓ в группе 2 ставится Dial: No, Answer:Yes, это означает, что входящие в эту группу АК могут принимать вызовы, но не могут использовать линии данной группы для внешних вызовов;
- ✓ в группе 3 ставится Dial: Yes, Answer:No, это означает, что входящие в эту группу АК не будут принимать вызовы, приходящие по внешним линиям данной группы, но могут их (линии) использовать для совершения внешних вызовов;
- ✓ и в группе 4 ставится Dial:No, Answer:No, что означает: никаких прав на использование внешних линий данной группы.

После настройки групп доступа в MMC 614 каждому АК присписывается та или иная группа доступа (по умолчанию группа 1 – полный доступ, см. рис. 14).

После выполнения данных настроек станция готова к работе как простая офисная станция. Правда, здесь мы

не учитываем один момент. Поступающие звонки у нас будут направляться на выбранные нами АК независимо от того, какой сегодня день – рабочий или выходной, а также независимо от времени – утро, день, вечер... Вообще данная станция имеет шесть «планов звонка», которые задают время переключения станции с одного плана на другой. Эта возможность очень удобна для тех организаций, в которых в рабочие дни звонки принимает один человек, а в выходные, по вечерам, в праздники – другой. Настраивается это в MMC 507, и тогда в MMC 406 в колонках, соответствующих «планам звонков», указываются АК, принимающие вызовы в то время, когда используется тот или иной план. По умолчанию всегда действует план звонков 1 (Ring Plan 1).

## Заключение

Даже простая настройка АТС Samsung – занятие весьма нетривиальное. Программа-конфигуратор чрезвычайно неудобна и весьма недружелюбна, отсутствие не то что мастеров, а даже элементарных подсказок, что для того чтобы добиться того-то и того-то, необходимо править то-то и то-то, просто бьет в глаза наотмашь, приходится постоянно держать открытым руководство по программированию и то скромное количество литературы по программированию АТС, которое удалось найти [7, 8]. Конечно, после того как все эти операции будут проделаны несколько раз, привыкаешь, и ситуация уже не кажется столь неудобной. надеюсь, эта статья поможет вам освоиться с основами программирования АТС Samsung немножко быстрее.

1. GABD-000038, ред. 001 OfficeServ 7200. Общее описание – <http://www.samsungdocs.com>.
2. GANA-000012, ред. 001 Officeserv 7200. Руководство по установке – <http://www.samsungdocs.com>.
3. GABD-000131, ред. 001 OfficeServ 7200. Руководство по программированию – <http://www.samsungdocs.com>.
4. <http://www.samsung.ru>.
5. <http://www.miacom.ru>.
6. <http://forum.officeats.ru>.
7. [http://citycat4.land.ru/mini\\_ATS.djvu](http://citycat4.land.ru/mini_ATS.djvu).
8. [http://citycat4.land.ru/Progr\\_ATS\\_Samsung\\_Panas.djvu](http://citycat4.land.ru/Progr_ATS_Samsung_Panas.djvu).

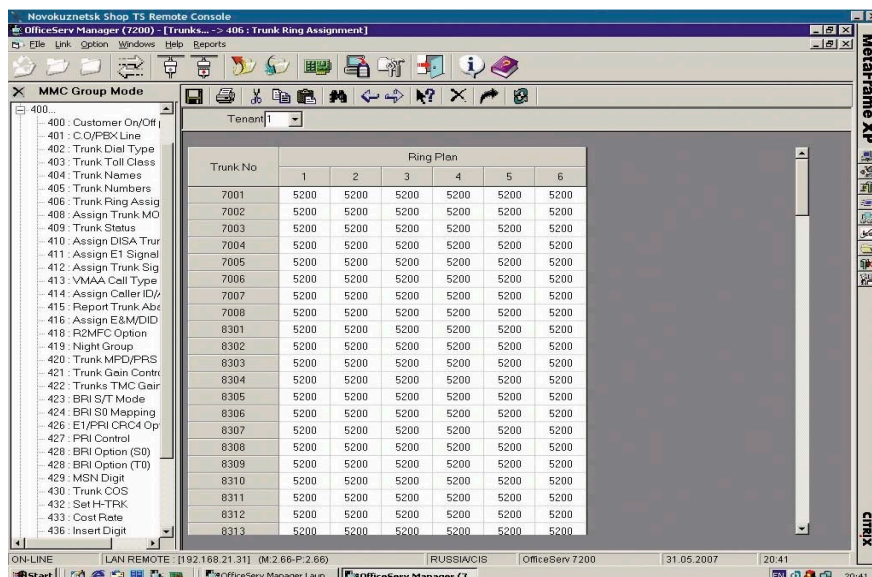


Рисунок 12. Назначение групп АК на прием вызовов с заданных транков

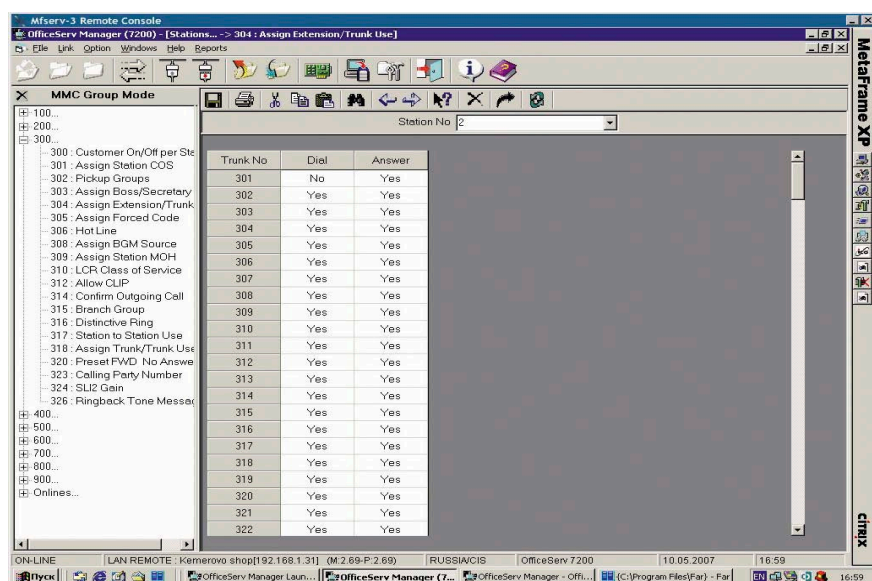


Рисунок 13. Настройка групп доступа к внешним линиям

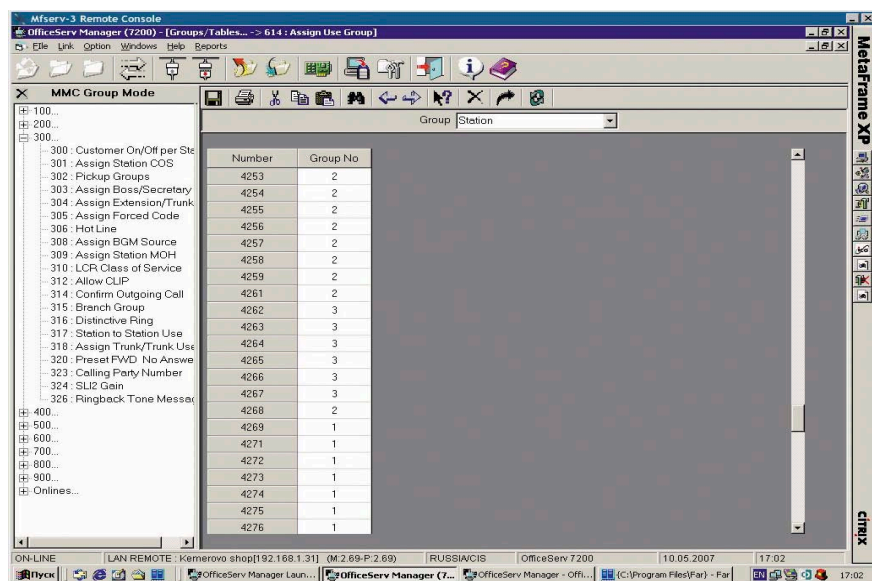


Рисунок 14. Задание групп доступа для АК



# СМИ уровня 2.0



**Благодаря аналитику Михаилу Елашкину я решила стать представителем этого вида средств массовой информации.**

*Я вернулся на свой пост в приемную директора, свалил бесполезные ключи в ящик и прочел несколько страниц из классического труда Я. П. Невструева «Уравнения математической магии». Эта книга читалась как приключенческий роман, потому что была битком набита поставленными и нерешенными проблемами.*

*Аркадий и Борис Стругацкие  
«Понедельник начинается в субботу»*

**М**ихаил Елашкин, руководитель компании Elashkin Research, создатель ITblogs.Ru – пространства для общения профессионалов IT-индустрии, похож на ларчик. Открываешь крышку – начинаешь бе-

седу: анекдоты, невыдуманные истории, идеи как из рога изобилия. Например, такая замечательная теория развития средств массовой информации: «Главная проблема бумажной прессы – то, что это СМИ уровня 1.0. Интерактивность ее какая? Статья появляется и затем обсуждается на сайте, постфактум. А интерактивность 2.0 в том, что человек в своем блоге пишет: «У меня появилась идея статьи». 5-6 специалистов его класса, его уровня, которым не надо ничего разжевывать, обсуждают с ним эту тему. С кем-то он соглашается, с кем-то спорит... После этого он пишет статью, в которой есть уже все подробные объясне-

ния, она обсуждается второй раз, с теми людьми, которым надо все растолковать. Многие вещи мы воспринимаем как одномоментные: вышла статья – и все. На самом деле это процесс. Люди вовлекаются, и это приносит гораздо больший эффект».

Мне показалось, что наша беседа с Михаилом Елашкиным тоже стала интерактивным прологом к созданию какого-то умного, большого материала о проблемах, близких IT-специалистам. А может быть, это будет даже книга, созданная на уровне 2.0. Во всяком случае вот они, темы для ваших читательских размышлений. Если у вас возникли возражения или вы найдете здесь



мысли, созвучные вашим, — не забудьте про обратную связь...

## Как сдавать ленинский зачет

*«Столичный город и приличная зарплата», — сказал бородатый негромко, но я услышал.*

*«Не надо, — сказал я. — Не надо мерить на деньги».*

*«Да нет, я пошутил», — сказал бородатый.*

*«Это он так шутит, — сказал горбоносый.*

*— Интереснее, чем у нас, вам нигде не будет».*

*«Почему вы так думаете?» — «Уверен».*

*Аркадий и Борис Стругацкие  
«Понедельник начинается в субботу»*

Меня давно интересовало: почему в менеджмент и IT-индустрию пришло так много людей из науки? На первый взгляд все понятно — образование позволило, лучшее в мире все-таки. Но ведь наличие диплома и желание выбраться из нищеты, в которую погрузилось бюджетное общество на закате советской власти и рассвете демократии, — это явно еще не все...

Михаил Елашкин задумался над моим вопросом: «Если бы наука финансировалась, остались бы вы в ней?». И решил, что вряд ли для него был возможен такой поворот судьбы: «Все-таки бизнес и информационные технологии — области, которые позволяют человеку получить то, чего он достоин. Наука — это патерналистское общество. Студент работает на дипломника, дипломник — на аспиранта, аспирант — на доктора, доктор — на академика... Ждать 40 лет, пока тебе дадут персональную машину от Академии наук, — это несерьезно».

С другой стороны, на новых должностях ученые смогли реализовать то, что дали им крепкая советская школа, университет, классическое образование: «Западного менеджера готовят начиная со школы. Учат всему: как писать заявление о приеме на работу, как разрешать конфликты и так далее. Когда он приходит на службу, у него наработан огромный запас шаблонов. Наши люди, которые пришли в бизнес из науки, с этими шаблонами не были знакомы, они знали, как сдавать ленинский зачет. Однако из науки ушла молодежь, те люди, которые стали бы ее цветом со временем. В новой для себя сфере они смогли разобрат-

ся без всяких шаблонов: за десять минут продумать ситуацию, поставить задачу, проанализировать возможности и так далее».

Сам Михаил Елашкин оставил в советском прошлом элитную физматшколу Новосибирского государственного университета и химфак МГУ. В 1990 году он закончил аспирантуру и окупился в проект — обучающие проекты и игры для Германии. Потом были Oracle, Novell, Intel и, наконец, своя компания.

Oracle, 1995 год. Судьба определилась сразу, потому что, уверен Михаил, «самое главное в нашей IT-индустрии — люди. Попасть в американскую корпорацию и при этом быть готовым учиться новому — все, карьера обеспечена! Я был в первой пятерке. Мы освоились. Что происходит дальше? Тебя встречает менеджер в коридоре: «Я взял еще пять человек, вот тебе моя кредитная карточка, купи им компьютеры и пристрой на какую-нибудь работу». Ты уже начальник группы. 2-3 такие группы — становишься начальником департамента. Наша первая пятерка пошла по разным путям. Один стал начальником службы технической поддержки, другой занялся образованием, третий — партнерской программой, меня понесло в продуктовый маркетинг. Каждый смог реализовать себя».

Сейчас Михаил хорошо знает людей своего поколения, со схожими судьбами. Круг тесен, слой тонок. Эти люди работают не за страх, а за совесть. Приходят в офис в 8 утра, уходят в 11 вечера, семью не видят, просиживают за компьютером все выходные.

А их молодые сотрудники живут совсем по другим правилам: приходят в 9, уходят в 6 и выставляют список требований: зарплату, машину, социальную страховку...

Это не значит, что предыдущие поколения остались верны советской дисциплине, совести, морали. «Люди, с которыми я общаюсь, в детстве читали «Понедельник начинается в субботу». Им не безразлично, что происходит с их компаниями. Для них выиграть в конкурентной борьбе — удовольствие большее, чем сходить на футбол».

Наверное, после всего вышеизложенного не нужно объяснять, поче-

му Михаил Елашкин не уехал в дальние края, хотя у него когда-то и виза в кармане была... «Я очень доволен, что никуда не уехал ни как ученый, ни как IT-специалист. Не знаю, почему... Мне нравится здесь. Был тут недавно в Парке Победы. Что мне понравилось: народ идет с российскими флагами. Приятно. По-моему, патриотизм — это важно для всей страны. Особенно такой, не навязанный, искренний. Мой сын пошел в День Победы поговорить с ветеранами, спросить, как это было. Нам ветеранов приглашали, они рассказывали, а мы читали книжки, играли в крестики-нолики. Здесь человек взял и сам пошел. Между нами говоря, я подумал: если бы народ так относился к Советскому Союзу, он бы вряд ли развалился». — «А сын у вас большой?» — «16 лет. На подготовительном отделении ВМК МГУ занимается. Сын пошел в тот же вуз, где я учился. Я вдруг обнаружил, что мои рассказы о том, как мы учились, веселились, для него не пустой звук. Для него честь — доказать, что он тоже может там учиться...»

## Бремя белого человека

*Но несмотря на все маленькие помехи и неприятности, несмотря на то что одушевленный теперь «Алдан» иногда печатал на выходе: «Думаю. Прошу не мешать», несмотря на недостаток запасных блоков и на чувство беспомощности, которое охватывало меня, когда требовалось произвести логический анализ «неконгруэнтной трансгрессии в пси-поле инкуб-преобразования», несмотря на все это, работать здесь было необычайно интересно, и я гордился своей очевидной нужностью.*

*Аркадий и Борис Стругацкие  
«Понедельник начинается в субботу»*

Интересно говорить с человеком, у которого есть аналитические способности. Я вообще перед такими людьми преклоняюсь. И кажется, что и все остальные должны их на руках носить, слушать внимательно да советы принимать к сведению. Михаил Елашкин сделал аналитику своей профессией. Его компания, как следует из официального релиза, «ставит своей целью развитие услуг IT-аналитики в России и СНГ и предоставление тех сервисов, которые ранее были недоступны



в этом регионе». Если неофициально, внешний анализ, который предлагает Елашкин, – это изучение технологий, сравнение технологий, исследование поведения людей и тенденций на рынке. Вещь нужная.

Ну как принимать правильное решение в бизнесе, если не знаешь его последствий? Например, дистрибьютерская фармацевтическая компания решила развивать новое направление. (Кстати, классная идея лично от Михаила Елашкина: распределенная система для аптек, позволяющая заказывать товары с сотового телефона).

Нужно выбрать технологию – от этого зависит 90% успеха. Вполне логично попросить сделать этот выбор квалифицированных специалистов. Ан нет...

В России аналитические услуги на аутсорсе – пока экзотика. То ли денег жалко, то ли, наоборот, не жалко средств на новую штатную вакансию – специалиста, который даст со-

вет по поводу конкретной ситуации, а потом будет заниматься чем придется.

Первое время, когда Михаил делал проекты и звонил в поисках информации в известные фирмы, ему задавали странный вопрос: «А что я буду иметь с аналитики?». Елашкин задавал встречный вопрос: «Вы хотите жить в цивилизованном рынке?» А про себя думал: «Ну, конечно, можно и без этого прожить, а есть прямо из кастрюли, руками».

Ему было сложно объяснить в коротком разговоре идеологию своей работы. Между тем, она проста: «Есть бремя белого человека. Приходят английские колонизаторы, захватили новый штат в Индии. Что они делают? Первым делом учреждают суд, открывают больницу, школу, заставляют почистить улицы, строят туалеты для туземцев, заставляют мыть руки и так далее. Это никаким образом не сказывается на качестве биз-

неса. Но англичане несут цивилизацию индийцам». Это в общем-то шуточная метафора.

Если серьезнее, нормальный рынок – это не только производители, потребители и между ними посредники, но и люди, которые пишут о рынке и анализируют его – пресса и аналитики. «Без них, – говорит Михаил, – рынок может существовать, но тогда он будет неэффективный. Люди не понимают, что на рынке происходит, принимают неэффективные решения».

В чем заключается работа аналитика? Любопытно заглянуть на «кухню» специалиста, которому могут заказать какую угодно тему, ведь сегодня спросом пользуется одна вещь, а завтра другая. Невозможно же, в самом деле, знать все обо всем?!

«Я научился выгружать знания об одном и загружать о другом. Я умею добывать информацию, умею задавать вопросы техническим экспертам. Моя работа заключается не в том, что я сел и о чем-то написал. Я подписан примерно на 20-30 новостных рассылок и каждый день читаю 3-4 десятка статей. Ты должен постоянно отслеживать, что происходит, думать об этом, общаться с людьми... За эти постоянные «тренировки», конечно, не платят. Это как у боксеров. Он получает деньги за один бой. Но этот бой у него раз в год, все остальное время он готовится».

Вот и хорошему аналитику могут заплатить за один проект 6-7 тысяч долларов. Деньги большие, но вполне заслуженные, ведь чтобы выдать качественный результат, специалист работает день и ночь, без отдыха, потому что тему нужно прочувствовать, сжиться с ней, уйти в нее с головой... Это ведь не контора, в которую пришел, поработал и ушел отдыхать, позабыв о проблемах в офисе.

Между тем, кто-то пытается сбивать цены на услуги аналитических компаний, не понимая, что это и глупо, и губительно – если цена становится ниже какого-то рассчитанного уровня, либо снижается качество работы, либо компания умирает.

«Любимая моя тема – производительность тяжелых систем. Самая красивая, интересная, научная. У нас в России человек 10-15 понимают эту тему глубоко. Может, больше».

## Дирижер оркестра

Институт был битком набит сотрудниками. Казалось, их было даже больше, чем в будний день. (...) Трудовое законодательство нарушалось злостно, и я почувствовал, что у меня исчезло всякое желание бороться с этими нарушениями, потому что сюда в двенадцать часов новогодней ночи, прорвавшись через пургу, пришли люди, которым было интереснее доводить до конца или начинать сызнова какое-нибудь полезное дело, чем глушить себя водкой, бессмысленно дрыгать ногами, играть в фанты и заниматься флиртом разных степеней легкости. Сюда пришли люди, которым было приятнее быть друг с другом, чем порознь, которые терпеть не могли всякого рода воскресений, потому что в воскресенье им было скучно.

Аркадий и Борис Стругацкие  
«Понедельник начинается в субботу»

Сидеть рядом с квалифицированным специалистом и не задать ему глобальный вопрос — грешно. Я спрашиваю: «Что будет с потоками информации, которая все время накапливается? Сфера IT с ней сможет справиться?» — «Человек — очень дорогая вещь. Его нельзя заменить в полной мере машиной. Поисковые машины обладают скоростью, не доступной человеку. Но иногда эта скорость ничем не может вам помочь, и «релевантность в соответствии с запросом» тоже. Например, мне нужен умный человек, хорошо разбирающийся во внутренних механизмах операционной системы Solaris и понимающий работу контейнеров. Сразу оговорюсь, что я знаю ответ — это Павел Анни из Sun. У него есть собственный блог, на котором два раза в год он пишет посты, после которых специалисты по UNIX хватаются за голову: «Десять лет этим занимаюсь, только сейчас понял».

Предположим, мы делаем запрос. Вываливаются два миллиона ссылок. Они выстроены по принципу: где этих слов больше встречается. Включаем индекс цитируемости. Да не цитируют Пашу, потому что его знают десять человек таких же сумасшедших, как он! А этих десятих знают сто человек, а на них уже ссылаются, потому что то, что говорит Паша, способны понять немногие. Паша говорит для таких же гур, которые потом могут разжевать остальным. Как мне найти такую информацию?» Михаил считает, и с этим трудно спорить, что в прессе читатель ищет личность. Он открывает журнал или га-




зету не всегда потому, что ему нравится редакционная политика или все издание «от корки до корки», но часто из-за того, что он хочет прочитать статью конкретного журналиста. Растет роль личности — падает ценность информации. «Увеличение количества информации будет приводить к тому, что ее большие куски будут никому не нужны», — уверен Елашкин.

Собственно, на этом построен проект ITblogs.ru. Ведь блог — это крайняя степень персонализации. Михаил собрал в него людей, которым интересно общаться друг с другом, которым есть чем поделиться с коллегами и которые, самое главное, не относятся ни к одной из трех категорий. Это еще одна любопытная теория: «Многие из тех, кто в 1995-1996 годах пришел в этот бизнес, стали либо большими начальниками, либо собираются на пенсию, либо превратились в циников. Человек приезжает на конференцию за десять минут до своей презентации. Все отлажено, движения отработаны, как у автоматчика. Он осматривает зал. Ему говорят: «Ваша очередь». Он открывает ноутбук, подключает, делает презентацию, затем сворачивается и уезжает. Это шоу-бизнес. Я сам много лет мотался по стране, красиво рассказывал. Толкаешь речь — и все твои. Раньше в гостиничных анкетах я писал в графе «род занятий» — «шоу-бизнес».

И вот, несмотря на то что многие люди, что называется, перегорели, Михаил

Елашкин сумел-таки склотить «костяк» сообщества и отправиться на поиски единомышленников. «Я подумал: может быть, людям времени не хватает? Я дам им возможность асинхронного общения. Сегодня один написал, у второго времени ответить нет, он в командировке, вернулся и отреагировал. Я разговариваю с людьми, нахожу другие блоги, приглашаю. Сам почти ничего не пишу, только легкие вещи. У меня нет времени разобратся в чем-то серьезном и написать на эту тему. Я сейчас — дирижер оркестра. Моя задача — создавать «струнные», «щипковые», «духовые» группы, вдохновлять людей, будоражить — давай сделаем, попробуем. Это в основном организационная работа.

Я не подбираю авторов по принципу — нравится мне или не нравится. Есть авторы, мнение которых лично мне интересно. Есть авторы, которые интересны другим. Если он умный и ему есть что сказать, всегда найдется аудитория, которая будет его слушать. Любый пост должен содержать не информацию: смотрите сюда, прочитайте вот это, а какую-то идею. Человек пишет: я прочитал книгу по управлению проектами, они говорят то-то и то-то, я 20 лет управляю проектами, по моему опыту, надо делать так и никак по-другому».

Строгий подход. Но разве не привлекательный? Вы не согласны? 

Текст: Оксана Родионова,  
фото: Владимир Лукин



# Система аутентификации веб-пользователей WebAuth

*Сергей Яремчук*

Интернет-технологии сегодня популярны как никогда. В той или иной форме их использование можно встретить в любой компании, как в виде общедоступных сервисов, так и для организации доступа к внутренним ресурсам компании. И тем острее встает вопрос об обеспечении безопасности таких каналов доступа, в первую очередь о надежности аутентификации пользователей.

На страницах журнала уже шла речь о достоинствах и недостатках стандартных типов аутентификации basic и digest [1, 2] и был дан пример одной из более защищенных реализаций DACS (Distributed Access Control System). Но это не единственное решение. В Стэнфордском университете уже несколько лет успешно используется система одноразовой регистрации (SSO – single sign-on) WebAuth. Пользователь, который хочет получить доступ к одному из ресурсов, регистрируется только один раз на центральном сервере (<http://weblogin.stanford.edu>, см. рис. 1) при переходе на другой веб-сайт этой группы серверов вводить пароль уже не потребуется. Если пользователь имеет право посетить ресурс, он к нему будет допущен автоматически.

## Принцип работы системы WebAuth

WebAuth реализован в качестве модуля веб-сервера Apache 2.x. Хотя есть порт и для IIS (см. далее по тексту). Система работает с любым веб-браузером, поддерживающим SSL/TLS и cookies, без необходимости установки дополнительных приложений и не требующих включения Java или JavaScript. Вся схема аутентификации построена поверх Kerberos, при этом билеты (ticket) упаковываются в сеансовый cookies (token), который и используется каждый раз в случае необходимости, для подтверждения полномочий. Хотя для подтверждения полномочий предусмотрены варианты передачи билетов через URL или POST.

Для работы WebAuth требуется наличие трех компонентов. Кроме веб-браузера (User-Agent – UA) необходимо настроить сервер, который должен поддерживать схему аутентификации WebAuth-enabled Application Server (WAS). Чтобы не допустить попадания cookies третьему лицу, соединение между UA и WAS обязательно защищается с помощью SSL/TLS, сам ticket шифруется с использованием сеансового ключа.

Для подтверждения полномочий пользователя задействуется еще один сервер – WebKDC. Его задачами являются: проверка подлинности пользователя и выдача cookies, уточнение информации о пользователе у WAS, об-

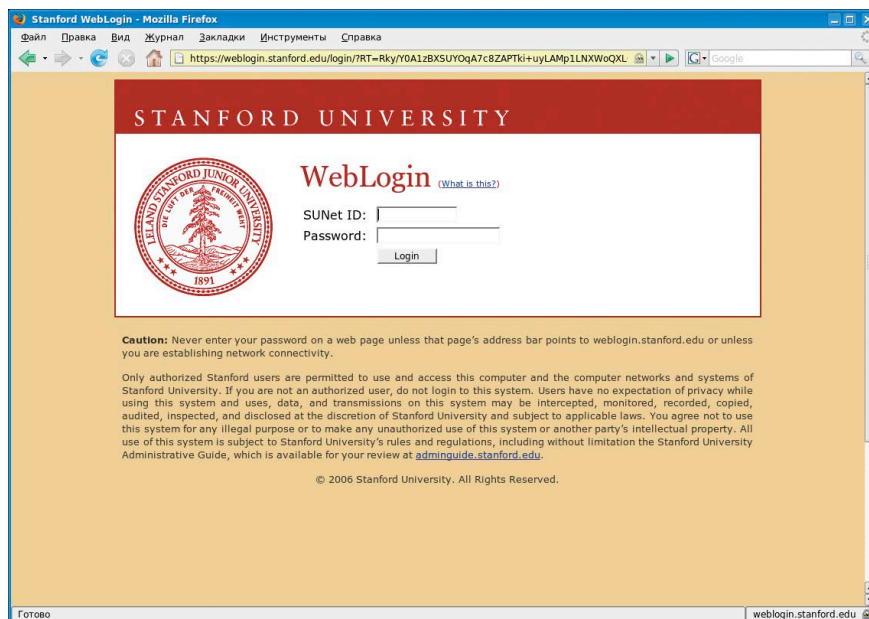


Рисунок 1. WebLogin Стэнфордского университета



Рисунок 2. Регистрация пользователей в WebAuth (нужно включить cookies)

новление cookies, срок жизни которых истек, установка ключей для WAS. Для всей сети серверов используется один такой сервер, который может находиться в одной сети или вообще по другую сторону океана. Пользователь, который хочет получить доступ к ресурсу, защищенному с помощью WebAuth сервером WAS, сначала перенаправляется на страницу Weblogin, которая находится на WebKDC, после получения cookies он уже попадает на нужную страницу. Регистрация пользователя требует 10 шагов, из них первые два – это обмен ключами между WAS и WebKDC при первоначальном подключении и получение результата `krb5_mk_req`.

Да и единственным полностью эффективным способом удалить используемый cookies, чтобы никто не мог им

воспользоваться в дальнейшем, является закрытие веб-браузера. Хотя сервис поддерживает специальную страницу logout, предназначенную для этих целей. Отметим, что ticket, передаваемый посредством URL, имеет очень короткий период жизни по сравнению с вариантом использования cookies – не более 5 минут. Если по истечении этого времени попытаться повторно использовать такой URL, будет запрошен cookies, содержащий билет, если cookies удовлетворяет всем условиям, доступ будет разрешен.

Для подтверждения наличия учетной записи пользователя, может быть использован любой механизм, поддерживаемый Apache, встроена интеграция с LDAP.

Распространяется WebAuth по X11-подобной (<http://www.gnu.org/licenses/>)

```
grinder@grinder:~$ sudo apt-cache search webauth
libapache2-webauth - Apache 2 modules for WebAuth authentication
libapache2-webkdc - Apache 2 modules for a WebAuth authentication KDC
libwebauth-perl - Perl library for WebAuth authentication
libwebauth1 - Shared libraries for WebAuth authentication
libwebauth1-dev - Development files for WebAuth authentication
libwebkdc-perl - Perl library for WebAuth authentication
webauth-tests - Tests for the WebAuth authentication modules
webauth-utils - Command-line utilities for WebAuth authentication
webauth-weblogin - Central login server for WebAuth authentication
grinder@grinder:~$
```

Рисунок 3. Пакеты Ubuntu

info/X11.html) лицензии, разрешающей бесплатно и без ограничений использовать, копировать, модифицировать, продавать и прочее, сохраняя уведомление об авторском праве.

## Установка WebAuth

Актуальной на момент написания статьи была версия 3.5.4. Версия WebAuth v3 базируется на Apache 2.x и MIT Kerberos v5 (можно использовать Heimdal Kerberos версией выше 0.7) официально представлена общественности в начале 2003 года. Поэтому период детских болезней, можно сказать, давно уже миновал, чего, правда, не скажешь о прозрачности настроек, с которыми придется повозиться, представленная документация также не всегда может помочь.

Сегодня WebAuth включен в репозитории многих дистрибутивов, поэтому самый простой способ установки – использование менеджера пакетов. Правда, называться пакеты могут по-разному. В Debian необходимо установить пакет `libapache2-webauth`. В Ubuntu команда поиска выдаст длинный список пакетов:

```
$ sudo apt-cache search webauth
```

```
libapache2-webauth - Apache 2 modules for WebAuth authentication
libapache2-webkdc - Apache 2 modules for a WebAuth authentication KDC
libwebauth-perl - Perl library for WebAuth authentication
libwebauth1 - Shared libraries for WebAuth authentication
libwebauth1-dev - Development files for WebAuth authentication
libwebkdc-perl - Perl library for WebAuth authentication
webauth-tests - Tests for the WebAuth authentication modules
webauth-utils - Command-line utilities for WebAuth authentication
webauth-weblogin - Central login server for WebAuth authentication
```

Все эти пакеты понадобятся при настройке и тестировании работы сервера. Именно в дистрибутивах Debian и Ubuntu по заявлению разработчиков WebAuth максимально поддерживается. На сайте проекта, кроме исходных текстов, доступны пакеты для Red Hat Enterprise Linux 4, Solaris и Windows. Правда, их версии не самые свежие, например zip-архив для Windows содержит версию 3.2.0, и этот порт подписан как `unsupported`. Судя по инструкции, использовать этот порт можно совместно с Apache 2.0.47. Порт для IIS 6.0 можно найти по адресу [5], его первоначальная реализация разрабатывалась также в Стэнфорде и содержала много ошибок, сейчас отдан на откуп сторонним разработчикам.

Другой проект SPIE [6] предлагает реализацию WebAuth на Java, все файлы, предлагаемые SPIE, можно также загрузить со страницы зачки проекта WebAuth.

При установке из исходных текстов, кроме Apache, с поддержкой SSL понадобятся MIT Kerberos v5, cURL и OpenSSL. Вот список необходимых пакетов в Ubuntu, выданных командой:

```
$ sudo apt-cache search webauth
```

```
apache2-threaded-dev libapr1-dev libaprutil1-dev
libcurl3-openssl-dev libdb4.4-dev libldap2-dev libpq-dev
libsqlite3-dev uuid-dev
```

В других дистрибутивах названия будут несколько другими. Теперь распаковываем полученный архив с исходными текстами, заходим внутрь и последовательно даем команды:

```
$ ./autogen
$ ./configure --enable-mod_webkdc
```

Остальные параметры включены по умолчанию, поэтому можно их не указывать. Если скрипт не найдет некоторые библиотеки, их потребуется указать с помощью `--with-krb5`, `--with-openssl`, `--with-curl` и `--with-ldap`.

Затем:

```
$ make
$ make check
```

```
...
Running all tests listed in ./TESTS. If any tests fail, run the failing
test program by hand to see more details. The test program will have the
same name as the test set but with "_test" appended.
```

```
libwebauth/attrs.....ok
libwebauth/base64.....ok
libwebauth/hex.....ok
libwebauth/key.....ok
libwebauth/random.....ok
libwebauth/token.....ok
```

```
All tests successful.
Files=6, Tests=7374, 0.99 seconds (0.74 usr + 0.14 sys = 0.88 CPU)
```

Если все тесты прошли успешно, устанавливаем:

```
$ sudo make install
```

В комплект WebAuth входит набор для тестирования работы сервиса, если планируется его использование, вводим:

```
$ sudo make install-tests
```

И если планируется на этом же компьютере использовать WebKDC:

```
$ sudo make install-webkdc
```

Теперь создаем каталог, в котором будут храниться настройки, принципы, токены и некоторые другие файлы:

```
$ sudo mkdir -p /etc/apache2/webauth
$ sudo mkdir -p /etc/apache2/webkdc
```

Смотрим, с правами какого учетного имени работает веб-сервер:



```
$ sudo grep User /etc/apache2/apache2.conf
```

```
User www-data
```

Этот пользовательский бюджет должен быть владельцем созданных каталогов:

```
$ sudo chown -R www-data:www-data /etc/apache2/webkdc ./
/etc/apache2/webauth
```

При установке с помощью пакетов, в Ubuntu эти два каталога можно найти в /etc. Поскольку мы имеем дело с Kerberos, поэтому в обязательном порядке синхронизируем время.

## Настройка WAS

Все настройки сервера, который для аутентификации будет использовать WebAuth, производятся в конфигурационном файле веб-сервера Apache – httpd.conf (в Ubuntu apache2.conf). Настройки можно условно разделить на две части: описание параметров модуля WebAuth и настройка доступа к ресурсам. Сначала первая часть:

```
# Загружаем модуль
LoadModule webauth module ./
/usr/lib/apache2/modules/mod_webauth.so
# Расположение AES-ключей и токенов для связи с WebKDC
# относительно корня веб-сервера
WebAuthKeyring webauth/keyring
WebAuthServiceTokenCache webauth/service_token_cache
# Расположение keytab-файла Kerberos
WebAuthKeytab webauth/keytab
# Адрес, куда будет перенаправлен пользователь для регистрации
WebAuthLoginURL https://grinder.com/login/
# Адрес для связи с сервером WebKDC
WebAuthWebKdcURL https://grinder.com/webkdc-service/
# Название сервиса, используемого для связи с WebKDC
WebAuthWebKdcPrincipal service/webkdc@GRINDER.COM
# Автоматическое перенаправление пользователя на SSL,
# при попытке соединиться по не защищенному каналу в доступе
# будет отказано и журнале появится запись:
# mod webauth: connection is not https, denying request
WebAuthSSLRedirect on
WebAuthDebug on
# Если используется сам подписанный сертификат
# для работы с WebKDC, добавляем
WebAuthWebKdcSSLCertFile webauth/webkdc.cert
# В отладочном режиме можно включить доступ
# к URL /webauth-status, который покажет статус работы
# mod_webauth
#<Location /webauth-status>
#   SetHandler webauth
#   Order allow,deny
#   Allow from all
#</Location>
```

Настройки просты и понятны. Остается только создать keytab. Kerberos – штука тонкая, и малейшая неточность приведет к тому, что WAS откажется работать, полностью блокируя доступ к серверу. В документации проекта по этому поводу только одна строка, рассказывающая, как получить такой файл со Стэнфорда. О настройках Kerberos в журнале уже говорилось [7], коротко напомним, как это сделать. Устанавливаем пакеты:

```
$ sudo apt-get install krb5-admin-server ./
krb5-kdc krb5-config krb5-user krb5-clients
```

Редактируем файлы /etc/krb5.conf и /etc/krb5kdc/kdc.conf под настройки своей системы. Запускаем два сервера:

```
$ sudo /etc/init.d/krb5-kdc restart
$ sudo /etc/init.d/krb5-admin-server restart
```

Теперь создаем принципы и ключи:

```
$ sudo kdb5_util create -s
```

Создаем принципал для административных целей:

```
$ sudo kadmin.local -q "addprinc admin/admin"
```

И далее в интерактивном режиме создаем все необходимые принципы для узла, KDC и пользователей:

```
$ sudo kadmin.local -p admin/admin
```

```
Authenticating as principal admin/admin with password.
kadmin.local: addprinc -randkey host/grinder.com
Principal "host/grinder.com@GRINDER.COM" created.
kadmin.local: addprinc grinder
Enter password for principal "grinder@GRINDER.COM":
Re-enter password for principal "grinder@GRINDER.COM":
Principal "grinder@GRINDER.COM" created.
kadmin.local: addprinc -randkey service/webkdc
Principal " service/webkdc@GRINDER.COM" created.
kadmin.local: ktadd service/webkdc
Entry for principal service/webkdc with kvno 3, encryption type
Triple DES cbc mode with HMAC/sha1 added to keytab WRFILE:
/etc/krb5.keytab.
Entry for principal service/webkdc with kvno 3, encryption type
DES cbc mode with CRC-32 added to keytab WRFILE:/etc/krb5.keytab.
kadmin.local: quit
```

Все созданные ключи принципа записываются в файл /etc/krb5.keytab. Этот файл и будем использовать при работе WebAuth. Лучше всего создать символическую ссылку:

```
$ sudo ln -s /etc/krb5.keytab /etc/apache2/webauth/keytab
$ sudo chown www-data:www-data /etc/apache2/webauth/keytab
```

Настройка доступа к ресурсам стандартна для Apache, здесь можно использовать любой удобный вариант. Чтобы включить проверку WebAuth, достаточно в файл .htaccess вписать:

```
AuthType WebAuth
Require valid-user
```

Или в httpd.conf описать ресурс таким образом:

```
<Location "/private/">
    AuthType WebAuth
    require valid-user
</Location>
```

Конечно, максимальная защита достигается при включении всех возможных проверок пользователя, в том числе и адреса:

```
<Location "/private/">
    AuthType WebAuth
    require valid-user
    order deny,allow
    deny from all
    allow from 192.168
    satisfy any
</Location>
```

Для удаления cookies без закрытия окна браузера можно использовать страницу logout:

```
<Location /private/logout>
    WebAuthDoLogout on
</Location>
```

Без WebKDC эта схема не будет иметь смысла, поэтому приступаем к его настройкам.

## Настройка WebKDC

Напомню, WebKDC не обязательно должен находиться на том же узле, что и WAS, учитывая, что безопасность всей системы WebAuth зависит от безопасности WebKDC, последний должен быть максимально защищен. Установки в конфигурационном файле веб-сервера практически аналогичны:

```
# Загружаем модуль
LoadModule webkdc_module \
    /usr/lib/apache2/modules/mod_webkdc.so
WebKdcServiceTokenLifetime 30d
WebKdcKeyring webkdc/keyring
WebKdcKeytab webkdc/keytab
WebKdcTokenAcl webkdc/token.acl
WebKdcDebug on
LogLevel debug

# Создадим алиасы
ScriptAlias /login "webkdc/login.fcgi"
ScriptAlias /logout "webkdc/logout.fcgi"
Alias /images "webkdc/images/"
Alias /help.html "webkdc/help.html"
```

Теперь по порядку. Как создавать файл keytab, показано выше, он должен соответствовать параметру WebAuthWebKdcPrincipal в конфигурациях WAS.

Файл keyring, в котором содержится AES-ключ, используемый при соединении с mod\_webauth ↔ mod\_webkdc, создается с помощью утилиты wa\_keyring:

```
$ cd /etc/apache2/webkdc
```

Создадим ключ, который будет действителен в течение двух дней:

```
$ sudo wa_keyring -f ./keyring add 2d
```

Посмотрим, что внутри:

```
$ sudo cat keyring
```

```
v=1;n=1;ct0=1179336753;va0=1179509553;kt0=1;
kd0=d31f548b8bab815b62afa96936105c2c;
grinder@grinder.com: /etc/apache2/webkdc
```

Все доступные ключи можно просмотреть с помощью параметра list:

```
$ sudo wa_keyring -f keyring list
```

```
Path: keyring

id Created Valid after Fingerprint
0 05/16/2007 20:32:33 05/18/2007 20:32:33 f08f5b1a75df2c1d2d38codfe570a75f
```

Шаблоны страниц, которые будут выведены пользователю при регистрации, ошибке и прочие, находятся в каталоге /usr/share/weblogin/generic/templates. В том случае, если установка производилась из исходных текстов, в файле /usr/share/perl5/WebKDC/Config.pm пути могут не совпадать с принятыми в дистрибутиве. Можно отредактировать их в нем, но лучшим вариантом является использование файла webkdc.conf, который должен находиться в подкаталоге /etc/apache2/webkdc.

Открываем его и указываем правильные настройки:

```
our $KEYRING_PATH = "/etc/apache2/webkdc/keyring";
our $TEMPLATE_PATH = "/usr/share/weblogin/generic/templates";
# Адрес, по которому будет находиться сервис WebKDC
our $URL = "https://localhost/webkdc-service/";
```

Для работы нам понадобится еще один файл token.acl, в котором описывается шаблон разрешенных токенов, которые может создавать WebKDC. Копируем пример на место:

```
$ sudo cp webauth-3.5.4/src/modules/webkdc/token.acl \
    /etc/apache2/webkdc/
```

Снимаем комментарий в первой строке и указываем шаблон:

```
krb5:service/*@grinder.com id
```

На этом настройки можно считать законченными. Перезапускаем веб-сервер:

```
$ sudo /etc/init.d/apache2 restart
```

В журнале веб-сервера должна появиться запись об успешной инициализации модулей:


```
[Wed May 16 21:47:35 2007] [notice] mod_webauth: initialized (3.5.4)
[Wed May 16 21:47:35 2007] [notice] Apache/2.2.3 (Ubuntu) PHP/5.2.1
WebAuth/3.5.4 WebKDC/3.5.4 SSL/0.9.7 configured -- resuming normal
operations
```

При попытке получить доступ к закрытому с помощью WebAuth ресурсу пользователь будет переключен на защищенное SSL-соединение и появится страница, запрашивающая пароль.

Пора подводить итог всего сказанного.

## Итоги

Без сомнения, WebAuth обладает достаточно впечатляющими возможностями, позволяя организовать безопасный доступ к защищенным ресурсам, используя один сервер для аутентификации. Правда, для того чтобы заставить эту систему полноценно работать, администратору придется потратить не один час на ее первоначальную настройку.

Но все затраты на установку и настройку затем с лихвой окупятся удобством в использовании. 

1. Мичурин А. Базовая HTTP-авторизация – защита от честных людей. //Журнал «Системный администратор», № 5, 2005 г. – С. 88-92.
2. Мичурин А. В чем сильные и слабые стороны HTTP digest-авторизации. //Журнал «Системный администратор», № 10, 2005 г. – С. 44-51.
3. Яремчук С. Система контроля доступа к веб-сервису DACS. //Журнал «Системный администратор», № 8, 2006 г. – С. 74-79.
4. Сайт проекта WebAuth – <http://webauth.stanford.edu>.
5. Сайт проекта WebAuth-IIS – <http://www.adunar.com/webauth>.
6. Сайт проекта SPIE – <http://spie.oucs.ox.ac.uk>.
7. Кондрин М. Развертываем Heimdal Kerberos. //Журнал «Системный администратор», № 7, 2005 г. – С. 20-25.



# XSPIDER 7

профессиональное средство мониторинга  
информационной безопасности

ЕДИНСТВЕННЫЙ СКАНЕР В МИРЕ  
СПОСОБНЫЙ ОПРЕДЕЛЯТЬ

130%

ОПУБЛИКОВАННЫХ  
УЯЗВИМОСТЕЙ



Для тех, кто хочет **ПОНИМАТЬ**, что происходит

Для тех, кто привык держать все **ПОД КОНТРОЛЕМ**

Для тех, кто предпочитает **предотвращать** проблемы, а не решать их

[www.xspider.ru](http://www.xspider.ru) • [www.ptsecurity.ru](http://www.ptsecurity.ru)  
(095) 744-0144 • факс (095) 744-0187

**Positive  
Technologies**  
МЫ ЗАЩИЩАЕМ СЕТИ



## Несколько уязвимостей в Apple Safari

**Программа:** Apple Safari 3 Beta.

**Опасность:** Критическая.

**Описание:** 1. Уязвимость существует из-за ошибки при обработке HTML-кода. Удаленный пользователь может с помощью специально сформированной веб-страницы выполнить произвольный код на целевой системе. Уязвимость существует в версиях Windows и OS X.

2. Уязвимость существует из-за ошибки в обработке протокола при обработке тегов IFRAME. Удаленный пользователь может выполнить произвольные команды на системе с привилегиями пользователя, запустившего браузер.

3. Уязвимость обнаружена в функции window.setTimeout() после изменения свойства window.location. Удаленный пользователь может с помощью специально сформированной веб-страницы выполнить произвольный JavaScript-код в браузере жертвы в контексте безопасности произвольного домена. Удачная эксплуатация уязвимости позволит злоумышленнику получить доступ к произвольным файлам куки и отобразить произвольные данные.

Также сообщается о различных уязвимостях, которые позволяют вызвать отказ в обслуживании системы.

**URL производителя:** [www.apple.com/safari](http://www.apple.com/safari).

**Решение:** В настоящее время способов устранения уязвимости не существует.

## Несколько уязвимостей в Apple QuickTime

**Программа:** Apple QuickTime 7.x.

**Опасность:** Высокая.

**Описание:** 1. Уязвимость существует из-за ошибки дизайна в ограничениях безопасности для QTObject-подклассов. Злоумышленник может выполнить недоверенный Java-код и получить доступ на чтение и запись в произвольные ячейки памяти.

2. Уязвимость существует из-за ошибки дизайна при обработке Java-апплетов. Удаленный пользователь может с помощью специально сформированного апплета просмотреть произвольные данные в памяти браузера.

**URL производителя:** [www.apple.com](http://www.apple.com).

**Решение:** Установите последнюю версию QuickTime 7.1.6 с сайта производителя.

## Переполнение буфера в Microsoft Office

**Программа:** Microsoft Office 2003, возможно другие версии.

**Опасность:** Критическая.

**Описание:** Уязвимость существует из-за ошибки в функции DeleteRecordSourceIfUnused() в MSODataSourceControl ActiveX-компоненте. Удаленный пользователь может с помощью специально сформированной веб-страницы вызвать переполнение буфера и выполнить произвольный код на целевой системе.

**URL производителя:** [www.microsoft.com](http://www.microsoft.com).

**Решение:** В настоящее время способов устранения уязвимости не существует.

## Переполнение буфера в OpenOffice

**Программа:** OpenOffice 1.1.x, OpenOffice.org 2.x, OpenOffice 1.0.x.

**Опасность:** Критическая.

**Описание:** 1. Уязвимость существует из-за ошибки при обработке тега «prdata» в RTF-файлах, в которых первый токен меньше второго. Удаленный пользователь может с помощью специально сформированного RTF-файла вызвать переполнение динамической памяти и выполнить произвольный код на целевой системе.

2. Уязвимость существует из-за использования копии уязвимой библиотеки FreeType. Удаленный пользователь может с помощью специально сформированного документа вызвать переполнение динамической памяти и выполнить произвольный код на целевой системе.

**URL производителя:** [www.openoffice.org](http://www.openoffice.org).

**Решение:** Установите последнюю версию 2.2.1 с сайта производителя.

## Переполнение буфера в Blue Coat K9 Web Protection

**Программа:** Blue Coat K9 Web Protection версии до 3.2.44.

**Опасность:** Высокая.

**Описание:** Уязвимость существует из-за ошибки проверки границ данных в management service (k9filter.exe) при обработке URL. Злоумышленник может с помощью специально сформированного HTTP-запроса на localhost на порт 2372 вызвать переполнение буфера и выполнить произвольный код на целевой системе.

**URL производителя:** [www.k9webprotection.com](http://www.k9webprotection.com).

**Решение:** Установите последнюю версию 3.2.44 или выше с сайта производителя.

## Уязвимость при обработке LHA-архивов в продуктах F-Secure

**Программа:** F-Secure Internet Security 2005-2007, F-Secure Anti-Virus 2005-2007, F-Secure Anti-Virus 5.x, F-Secure Anti-Virus Client Security 6.x, F-Secure Anti-Virus for Windows Servers 5.x, F-Secure Anti-Virus for Workstations 5.x, F-Secure Anti-Virus for Citrix Servers 5.x, F-Secure Anti-Virus for MIMESweeper 5.x, F-Secure Anti-Virus for Microsoft Exchange 6.x, F-Secure Internet Gatekeeper 6.x, F-Secure Anti-Virus for Linux 4.x, F-Secure Internet Gatekeeper for Linux 2.x.

**Опасность:** Высокая.

**Описание:** Уязвимость существует из-за ошибки проверки границ данных при обработке LHA-архивов. Удаленный пользователь может с помощью специально сформированного LHA-архива вызвать переполнение буфера и выполнить произвольный код на целевой системе.

**URL производителя:** [www.f-secure.com](http://www.f-secure.com).

**Решение:** Установите исправление с сайта производителя.

## Целочисленное переполнение в Amavis

**Программа:** AMaViS (A Mail Virus Scanner) версии до 4.21, amavisd-new 2.x.

**Опасность:** Высокая.

**Описание:** 1. Целочисленное переполнение обнаружено в утилите file. Удаленный пользователь может вызвать переполнение динамической памяти и выполнить произвольный код на целевой системе.

2. Уязвимость существует из-за некоторых регулярных выражений в file. Удаленный пользователь может указать специально сформированный файл и потратить все доступные ресурсы процессора на системе.

**URL производителя:** [www.amavis.org](http://www.amavis.org).

**Решение:** Установите последнюю версию 4.21 или выше с сайта производителя.

## Уязвимость при обработке данных в MiniWeb HTTP Server

**Программа:** MiniWeb HTTP Server 0.8.19, возможно более ранние версии.

**Опасность:** Высокая.

**Описание:** Уязвимость существует из-за ошибки при обработке входных данных в поле Content-Length в POST-запросе. Удаленный пользователь может с помощью специально сформированного POST-запроса вызвать переполнение динамической памяти и выполнить произвольный код на целевой системе.

**URL производителя:** [sourceforge.net/projects/miniweb](http://sourceforge.net/projects/miniweb).

**Решение:** В настоящее время способов устранения уязвимости не существует.

## Уязвимость при обработке параметров в Win32 API в Microsoft Windows

**Программа:** Microsoft Windows 2000, Microsoft Windows XP, Microsoft Windows 2003.

**Опасность:** Высокая.

**Описание:** Уязвимость существует из-за ошибки при обработке некоторых параметров в Win32 API. Удаленный пользователь может с помощью специально сформированной веб-страницы выполнить произвольный код на целевой системе.

**URL производителя:** [www.microsoft.com](http://www.microsoft.com).

**Решение:** Установите исправление с сайта производителя.

## Переполнение буфера в Trillian

**Программа:** Cerulean Studios Trillian версии до 3.1.6.0.

**Опасность:** Высокая.

**Описание:** Уязвимость существует из-за ошибки при обработке границ данных в UTF-8-строках. Удаленный пользователь может с помощью специально сформированного сообщения, просматриваемого пользователем, вызвать переполнение динамической памяти и выполнить произвольный код на целевой системе.

**URL производителя:** [blog.ceruleanstudios.com/?p=150](http://blog.ceruleanstudios.com/?p=150).

**Решение:** Установите последнюю версию 3.1.6.0 с сайта производителя.

## Уязвимость при обработке CAB-файлов в продуктах CA

**Программа:** CA Anti-Virus for the Enterprise (formerly eTrust Antivirus) r8, r8.1; CA Anti-Virus 2007 (v8); eTrust EZ Antivirus r7, r6.1; CA Internet Security Suite 2007 (v3); eTrust Internet Security Suite r1, r2; eTrust EZ Armor r1, r2, r3.x; CA Threat Manager for the Enterprise (formerly eTrust Integrated Threat Management) r8; CA Protection Suites r2, r3; CA Secure Content Manager (formerly eTrust Secure Content Manager) 8.0; CA Anti-Virus Gateway (formerly eTrust Antivirus eTrust Antivirus Gateway) 7.1; Unicenter Network and Systems Management (NSM) r3.0; Unicenter Network and Systems Management (NSM) r3.1; Unicenter Network and Systems Management (NSM) r11.1; Unicenter Network and Systems Management (NSM) r11.1.1; BrightStor ARCserve Backup r11.5; BrightStor ARCserve Backup r11.1; BrightStor ARCserve Backup r11 for Windows; BrightStor Enterprise Backup r10.5; BrightStor ARCserve Backup v9.01; CA Common Services; CA Anti-Virus SDK (formerly eTrust Anti-Virus SDK).

**Опасность:** Высокая.

**Описание:** 1. Уязвимость существует из-за ошибки проверки границ данных в vete.dll при обработке имени файла, содержащегося в CAB-архиве. Удаленный пользователь может с помощью специально сформированного CAB-файла вызвать переполнение стека и выполнить произвольный код на целевой системе.

2. Уязвимость существует из-за ошибки при обработке некорректно определенного поля coffFiles в CAB-архивах. Удаленный пользователь может с помощью специально сформированного CAB-архива вызвать переполнение стека и выполнить произвольный код на целевой системе.

**URL производителя:** [www.ca.com](http://www.ca.com).

**Решение:** Установите исправление с сайта производителя.

## Несколько уязвимостей в Mozilla Firefox

**Программа:** Mozilla Firefox версии до 2.0.0.4 и 1.5.0.12, Mozilla Thunderbird версии до 2.0.0.4 и 1.5.0.12, Mozilla SeaMonkey версии до 1.1.2 и 1.0.9.

**Опасность:** Высокая.

**Описание:** 1. Уязвимость существует из-за ошибок при обработке JavaScript. Удаленный пользователь может вызвать повреждение памяти и выполнить произвольный код на целевой системе.

2. Уязвимость существует из-за ошибки в методе addEventListener. Удаленный пользователь может внедрить произвольный сценарий в другой сайт и изменить важные данные.

3. Уязвимость существует из-за ошибки при обработке всплывающих окон XUL. Злоумышленник может подделать определенные части браузера (например, адресную строку).

**URL производителя:** [www.mozilla.org/products/firefox](http://www.mozilla.org/products/firefox).

**Решение:** Установите последнюю версию с сайта производителя.

Составил Александр Антипов

# Организуем доступ к базам данных при разработке кроссплатформенных приложений на C++/wxWidgets



**Владимир Тряпичко**

**Очень часто на форумах появляются вопросы, связанные с организацией доступа к базам данных для приложений на C++. Тема актуальная и очень интересная, хотя у новичков зачастую вызывает трудности. Но написание кроссплатформенных приложений на C++, использующих для своей работы базы данных, не является чем-то непосильным, кроссплатформенная разработка может оказаться увлекательным занятием.**

**Р**ечь пойдет о разработке приложений, использующих для своей работы базы данных SQLite. Учиться кросс-платформенной разработке на C++ мы будем на примере простейшего приложения, работающего с базами данных – адресной книги.

## Инструментарий

Для работы нам понадобятся:

- Библиотека wxWidgets-2.8.3 – <http://wxwidgets.org>.
- Библиотека SQLite3 – <http://sqlite.org>.
- Библиотека DatabaseLayer for wxWidgets – <http://wxcode.sourceforge.net/components/databaselayer>.
- Утилита wxActiveRecordGenerator (wxARG) – <http://wxcode.sourceforge.net/components/activerecord>.

## Windows

В качестве среды разработки будем использовать Microsoft Visual Studio 2005. Для создания кросс-платформенных приложений подойдет любая редакция Visual Studio, включая бесплатную Visual Studio 2005 Express Edition. В случае использования Visual Studio 2005 Express Edition необходимо дополнительно установить Microsoft Platform SDK.

## Настройка проекта в Visual Studio 2005

Для начала создадим новый проект (Win32 Project) в Visual Studio 2005 и назовем его SQLiteTest.

Затем распакуем архив с исходным кодом библиотеки DatabaseLayer в папку с нашим решением (Solution). Добавляем в Solution проект databaselayer\_

databaselayer\_sqlite.dsp из дистрибутива DatabaseLayer.

Теперь нам необходимо указать зависимости проектов. Наше приложение должно быть собрано после сборки библиотеки DatabaseLayer, поэтому в Solution Explorer жмем правой кнопкой на названии проекта SQLiteTest, выбираем пункт меню «Project Dependencies...», в списке проектов ставим маркер на названии проекта databaselayer\_sqlite и жмем «OK».

Далее выбираем пункт меню «Build → Configuration Manager» и указываем конфигурации каждого проекта для отладочной и финальной версии решения. При написании статьи использовалась статическая раздельная Unicode-сборка wxWidgets, поэтому для Debug-версии решения была выбрана конфигурация Static Unicode



Debug Multilib проекта `databaselayer_sqlite` и конфигурация Debug проекта `SQLiteTest`. Такие же действия необходимо выполнить и для Release-версии, заменив все вхождения слова Debug в названиях конфигураций на Release.

После этого распаковываем архив `sqlite-source-x_y_z.zip` в папку `databaselayer/sqlite/include` и архив `sqllitedll-x_y_z.zip` в папку `databaselayer/sqlite/lib`. В результате в папке `databaselayer/sqlite/lib` должны появиться файлы `sqlite3.dll` и `sqlite3.def`.

Всё это очень хорошо, но для использования динамической библиотеки в нашем проекте неплохо было бы иметь `.lib`-файл, которого у нас сейчас нет. Для того чтобы он у нас был, создаем два batch-скрипта:

Файл `setupvars.bat`

```
"C:/Program Files/Microsoft Visual Studio 8/VC/bin/vcvars32.bat"
```

Файл `export.bat`

```
lib.exe /def:sqlite3.def /machine:x86 /out:sqlite3.lib
```

Запускаем командную строку, переходим в папку `databaselayer/sqlite/lib` и по очереди запускаем два batch-файла:

```
setupvars
export
```

После выполнения этих нехитрых действий у нас должны появиться два файла: `sqlite3.exp` и `sqlite3.lib`.

Отлично, теперь создаем в нашем проекте `SQLiteTest` четыре новых файла: `SQLiteTestApp.h`, `SQLiteTestApp.cpp`, `SQLiteTestMainFrame.h` и `SQLiteTestMainFrame.cpp`.

Теперь открываем свойства проекта, переходим в раздел C/C++ и в настройках «Additional Include Directories» добавляем две новые записи, содержащие пути к заголовочным файлам `DatabaseLayer` и `SQLite`:

```
$(ProjectDir)../databaselayer/sqlite/include
$(ProjectDir)../databaselayer/include
```

Переходим в раздел `Linker` и в настройках «Additional Library Directories» добавляем записи, содержащие пути к статическим библиотекам `DatabaseLayer` и `SQLite`:

```
$(ProjectDir)../databaselayer/sqlite/lib
$(ProjectDir)../databaselayer/lib
```

В разделе «Linker → Input» в настройках «Additional Dependencies» добавляем записи:

```
advapi32.lib
comctl32.lib
uuid.lib
rpcrt4.lib
wxbase28ud.lib
wxmsw28ud_core.lib
wxmsw28ud_adv.lib
wxpngd.lib
wxcode_msw28ud_databaselayer_sqlite.lib
sqlite3.lib
```

Не забывайте, что суффикс `d` в названиях библиотек `wxWidgets` указывает на то, что используется отладочная версия библиотеки. Release-версии библиотек не имеют в названии этого суффикса.

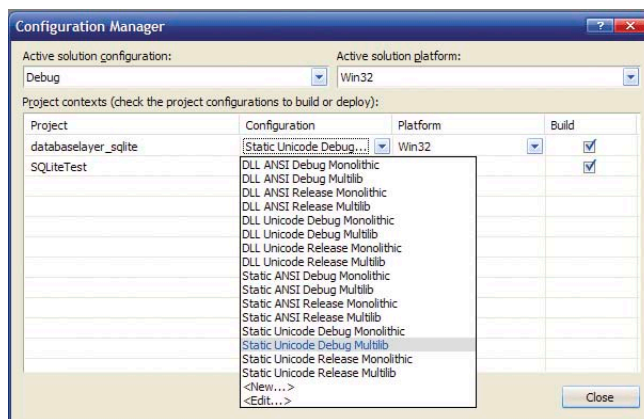


Рисунок 1. Окно конфигурирования сборки в Visual Studio 2005

Далее в разделе «Linker → General» для всех конфигураций указываем параметр `Output File` равным `«../bin/$(ProjectName).exe»` и в разделе `Debugging` – параметр `Working Directory` равным `«../bin»`. Это позволит генерировать исполняемый файл в отдельную папку.

Наконец, предварительная настройка завершена, и можно приступать к написанию кода.

## Пишем код

**SQLiteTestMainFrame.h** – заголовочный файл с описанием класса главного окна приложения:

```
#ifndef _SQLITE_TEST_MAINFRAME_H
#define _SQLITE_TEST_MAINFRAME_H

#include <wx/wx.h>

class SQLiteTestMainFrame : public wxFrame
{
public:
    SQLiteTestMainFrame();
    bool Create(wxWindow * parent,
               wxWindowID id, const wxString & title);

    DECLARE_EVENT_TABLE()
    void OnExit(wxCommandEvent & event);
};

#endif
```

**SQLiteTestMainFrame.cpp** – реализация класса главного окна приложения:

```
#include "SQLiteTestMainFrame.h"
#include "SQLiteTestApp.h"

BEGIN_EVENT_TABLE(SQLiteTestMainFrame, wxFrame)
    EVT_MENU(wxID_EXIT, SQLiteTestMainFrame::OnExit)
END_EVENT_TABLE()

SQLiteTestMainFrame::SQLiteTestMainFrame()
{
    Create(NULL, wxID_ANY, _("SQLite Addressbook"));
}

bool SQLiteTestMainFrame::Create(wxWindow * parent,
                                wxWindowID id, const wxString & title)
{
    bool res = wxFrame::Create(parent, id, title,
                               wxDefaultPosition, wxSize(700, 500));
    if(res)
    {
        CreateControls();
    }
    return res;
}
```

```
void SQLiteTestMainFrame::CreateControls()
{
    wxMenuBar * menuBar = new wxMenuBar;
    SetMenuBar(menuBar);

    wxMenu * fileMenu = new wxMenu;
    fileMenu->Append(wxID_EXIT, _("Exit\tAlt+F4"));

    menuBar->Append(fileMenu, _("File"));

    CreateStatusBar(2);
    Centre();
}

void SQLiteTestMainFrame::OnExit(wxCommandEvent & event)
{
    wxUnusedVar(event);
    Close();
}
```

**SQLiteTestApp.h** – заголовочный файл с описанием класса приложения:

```
#ifndef _SQLITE_TEST_APP_H
#define _SQLITE_TEST_APP_H

#include <wx/wx.h>
#include <DatabaseLayer.h>
#include <SqliteDatabaseLayer.h>

class SQLiteTestApp : public wxApp
{
    DatabaseLayer * m_Database;
public:
    virtual bool OnInit();
    virtual int OnExit();

    bool ConnectToDatabase();
    DatabaseLayer * GetDatabase();
};

DECLARE_APP(SQLiteTestApp)

#endif
```

**SQLiteTestApp.cpp** – реализация класса приложения:

```
#include <wx/image.h>
#include <DatabaseLayerException.h>
#include "SQLiteTestApp.h"
#include "SQLiteTestMainFrame.h"

IMPLEMENT_APP(SQLiteTestApp)

bool SQLiteTestApp::OnInit()
{
    if(!ConnectToDatabase())
    {
        wxFAIL_MSG(_("Error connecting to database!"));
        return false;
    }
    wxImage::AddHandler(new wxPNGHandler);
    wxImage::AddHandler(new wxJPEGHandler);

    SQLiteTestMainFrame * frame = new SQLiteTestMainFrame;
    SetTopWindow(frame);
    frame->Show();

    return true;
}

int SQLiteTestApp::OnExit()
{
    if(m_Database)
    {
        if(m_Database->IsOpen())
        {
            m_Database->Close();
        }
        wxDELETE(m_Database);
    }
    return wxApp::OnExit();
}
```

```
bool SQLiteTestApp::ConnectToDatabase()
{
    m_Database = new SqliteDatabaseLayer();
    wxString db_filename(wxT("addressbook.db"));
    PreparedStatement * pStatement(NULL);
    bool bCreate = !wxFileExists(db_filename);
    if(bCreate)
    {
        wxMessageBox(_("Database does not exist... recreating."));
    }
    try
    {
        m_Database->Open(db_filename);
        // Try to recreate tables
        try
        {
            m_Database->RunQuery(
                wxT("CREATE TABLE groups(id integer primary key, \
                    name varchar(128) not null,\
                    description varchar(512));"));
        }
        catch(DatabaseLayerException & e) {wxUnusedVar(e);}
    }
    try
    {
        m_Database->RunQuery(wxT("CREATE TABLE persons(\
            id integer primary key,\
            groupid integer not null,\
            first_name varchar(64) not null,\
            last_name varchar(64) not null,\
            gender boolean not null,\
            address varchar(128) not null,\
            city varchar(64) not null,\
            country varchar(32) not null,\
            phone varchar(32),\
            email varchar(128),\
            website varchar(260));"));
    }
    catch(DatabaseLayerException & e) {wxUnusedVar(e);}
    if(bCreate)
    {
        m_Database->RunQuery(
            wxT("INSERT INTO groups(name, description) \
                VALUES ('Friends', 'My friends')"));
        pStatement = m_Database->PrepareStatement(
            wxT("INSERT INTO persons(groupid, \
                first_name,last_name,gender,address,city,\
                country,phone) VALUES \
                (?, ?, ?, ?, ?, ?, ?)"));
        if (pStatement)
        {
            pStatement->SetParamInt(1, 1);
            pStatement->SetParamString(2, _("John"));
            pStatement->SetParamString(3, _("Doe"));
            pStatement->SetParamBool(4, 1);
            pStatement->SetParamString(5,
                _("SomeStreet st., 123/45"));
            pStatement->SetParamString(6, _("Some City"));
            pStatement->SetParamString(7, _("Some Country"));
            pStatement->SetParamString(8, _("+000-00-000-00-00"));
            pStatement->RunQuery();
            m_Database->CloseStatement(pStatement);
            pStatement = NULL;
        }
    }
    catch(DatabaseLayerException & e)
    {
        if(pStatement)
        {
            m_Database->CloseStatement(pStatement);
            pStatement = NULL;
        }
        wxFAIL_MSG(e.GetErrorMessage());
        return false;
    }
    return true;
}

DatabaseLayer * SQLiteTestApp::GetDatabase()
{
    return m_Database;
}
```

Итак, что же мы сделали: мы создали класс приложения SQLiteTestApp, содержащий указатель на объект класса DatabaseLayer, который и будет обеспечивать связь с на-

шей базой данных. При запуске приложения проверяется наличие файла addressbook.db, и в случае если файл не найден, он создается. Вместе с базой данных создаются две таблицы: groups и persons и заполняются тестовыми данными.

Главная форма приложения содержит строку меню и строку статуса и пока ничего не делает.

После успешной сборки приложения и его запуска в папке bin должен появиться файл базы данных addressbook.db.

Отлично, теперь можно приступить к работе с базой данных.

### Генерирование классов автоматизации доступа к базам данных с помощью wxActiveRecordGenerator

Устанавливаем утилиту wxARG, копируем из папки, куда была установлена wxARG, два файла wxActiveRecord.h и wxActiveRecord.cpp в папку SQLiteTest/wxActiveRecord. В настройках проекта SQLiteTest в разделе «C/C++ → General» в настройках «Additional Include Directories» добавляем новую запись:

```
./wxActiveRecord
```

Далее запускаем утилиту wxARG и выбираем пункт меню «File → Connect to database».

В появившемся диалоговом окне «Database Connection» указываем тип базы данных SQLite3 Database и путь к файлу addressbook.db, созданному нашим тестовым приложением. Жмем «Connect».

В диалоговом окне «Tables» выбираем таблицы groups и persons. Жмем «OK».

После этого в левой части главного окна wxARG появится список с выбранными таблицами.

Каждая таблица базы данных имеет ключевое поле id, поэтому на вкладке «Properties» в поле ID Field мы указываем поле id.

В нашей базе данных между таблицами groups и persons существует связь один ко многим, т.е. каждая группа может содержать множество контактов адресной книги.

Переходим на вкладку «Relations». Для таблицы groups:

- жмем кнопку «Has Many»;
- в диалоговом окне «Relation Properties» указываем название таблицы со стороны «многие», в нашем случае это таблица persons;
- указываем поле внешнего ключа в таблице persons, в нашем случае это groupid;
- значения остальных параметров можно оставить без изменений.

Для таблицы persons:

- жмем кнопку «Belongs To»;
- в диалоговом окне «Relation Properties» указываем название таблицы со стороны «один», в нашем случае это таблица groups;
- указываем поле внешнего ключа в таблице persons, в нашем случае это groupid;
- значения остальных параметров можно оставить без изменений.

В поле «Output Dir» указываем папку SQLiteTest и жмем «Generate».

После всех проделанных операций в папке с проектом SQLiteTest должны появиться файлы: Group.h, Group.cpp, Person.h и Person.cpp. Эти файлы нам необходимо добавить в проект.

Теперь можно приступить к внесению изменений в исходный код. Для начала в файле wxActiveRecord.h необходимо раскомментировать строку с макросом AR\_USE\_SQLITE, который указывает, что мы используем SQLite. В файле wxActiveRecord.cpp нужно исправить путь к заголовочному файлу wxActiveRecord.h.

В файле wxActiveRecord.h вносим изменения, необходимые для организации работы с базами данных SQLite:

```
...
// COMMENT OUT THE ONES YOU DON'T USE

// #define AR_USE_POSTGRES
// #define AR_USE_SQLITE
// #define AR_USE_MYSQL
// #define AR_USE_FIREBIRD
...
```

В файле wxActiveRecord.cpp необходимо исправить путь к заголовочному файлу:

```
...
#include "wxActiveRecord.h"
...
```

Если посмотреть на исходный код файлов, сгенерированных утилитой wxARG, то можно заметить, что каж-

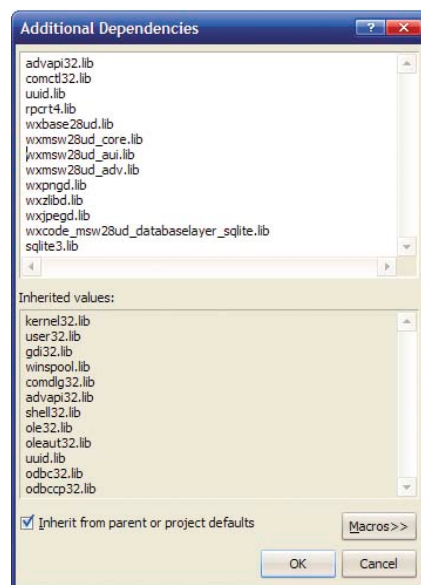


Рисунок 2. Список библиотек, необходимых для сборки проекта

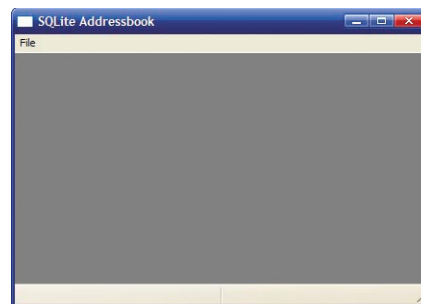


Рисунок 3. Главное окно приложения

дая пара .h/.cpp-файлов содержит описание и реализацию трех классов (где XXX – название таблицы):

- XXX – класс таблицы;
- XXXRow – класс типизированной записи таблицы;
- XXXRowSet – типизированный список записей.

И после всего сказанного, вооружившись полученными знаниями, продолжаем наш «happy coding».

В файле wxSQLiteTestApp.h добавляем методы доступа к таблицам базы данных в класс приложения:

```
...
#include <SqliteDatabaseLayer.h>
#include "Group.h"
#include "Person.h"

class SQLiteTestApp : public wxApp
{
    Group * m_GroupTable;
    Person * m_PersonTable;
    ...
public:
    ...
    Group * GetGroupTable();
    Person * GetPersonTable();
};
...
```



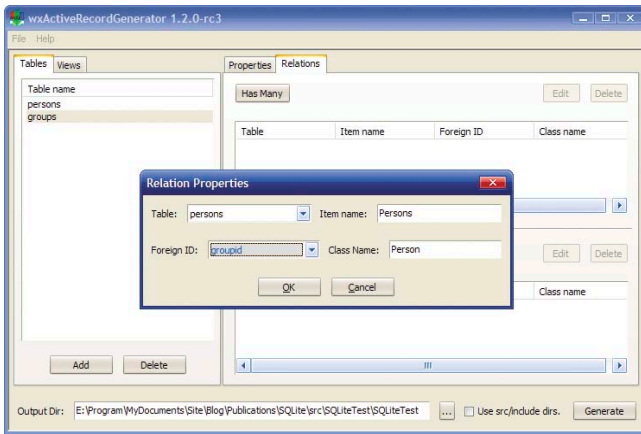


Рисунок 4. Настройка связей между таблицами базы данных в wxARG

**wxSQLiteTestApp.cpp** – загрузка данных при запуске приложения и освобождение памяти при завершении работы:

```
...
int SQLiteTestApp::OnExit()
{
    wxDELETE(m_PersonTable);
    wxDELETE(m_GroupTable);
    ...
}

bool SQLiteTestApp::ConnectToDatabase()
{
    ...
    try
    {
        m_GroupTable =
            new Group(wxGetApp().GetDatabase(), wxT("groups"));
        m_PersonTable =
            new Person(wxGetApp().GetDatabase(), wxT("persons"));
    }
    catch(DatabaseLayerException & e)
    {
        wxActiveRecord::ProcessException(e);
    }
    return true;
}
...
```

Итак, мы добавили новые члены класса SQLiteTestApp, обеспечивающие доступ к таблицам базы данных, и теперь можно приступать к созданию GUI.

## Графический интерфейс пользователя

Дистрибутив wxWidgets содержит несколько десятков свободно распространяемых иконок, которые мы можем использовать в нашем приложении. Создадим папку SQLiteTest/art и скопируем в нее файлы:

```
$ (WXWIN) /art/addbookm.xpm
$ (WXWIN) /art/delbookm.xpm
$ (WXWIN) /art/new.xpm
$ (WXWIN) /art/delete.xpm
```

В свойствах проекта в разделе «C/C++ → General» в настройках «Additional Include Directories» добавим запись:

```
./art
```

**wxSQLiteTestMainFrame.h** – добавляем элементы управления на форму:

```
...

class SQLiteTestMainFrame : public wxFrame
{
    wxListBox * m_GroupsListBox;
    wxListView * m_PersonsListView;
    wxHtmlWindow * m_PersonInfoPanel;
    wxToolBar * CreateToolBar();
    ...
};

#endif
```

**wxSQLiteTestMainFrame.cpp** – создание элементов управления:

```
...
#include <wx/splitter.h>
#include "new.xpm"
#include "delete.xpm"
#include "addbookm.xpm"
#include "delbookm.xpm"

...

void SQLiteTestMainFrame::CreateControls()
{
    ...
    wxBoxSizer * sizer = new wxBoxSizer(wxVERTICAL);
    SetSizer(sizer);
    wxSplitterWindow * splitter =
        new wxSplitterWindow(this, wxID_ANY,
            wxDefaultPosition, wxSize(500, 400), wxSP_3DSASH);
    splitter->SetMinimumPaneSize(100);
    sizer->Add(splitter, 1, wxEXPAND);
    m_GroupsListBox =
        new wxListBox(splitter, ID_GROUPS_LISTBOX,
            wxDefaultPosition, wxDefaultSize);
    wxSplitterWindow * personsplitter =
        new wxSplitterWindow(splitter, wxID_ANY,
            wxDefaultPosition, wxSize(500, 400), wxSP_3DSASH);
    personsplitter->SetMinimumPaneSize(100);
    m_PersonsListView =
        new wxListView(personsplitter, ID_PERSONS_LISTCTRL,
            wxDefaultPosition, wxDefaultSize, wxLC_REPORT);
    m_PersonsListView->InsertColumn(0, _("First Name"),
        wxLIST_FORMAT_LEFT, 120);
    m_PersonsListView->InsertColumn(1, _("Last Name"),
        wxLIST_FORMAT_LEFT, 120);
    ...
    personsplitter->SetSashGravity(1.0)
    splitter->SplitVertically(m_GroupsListBox,
        personsplitter, 160);
    personsplitter->SplitHorizontally(m_PersonsListView,
        m_PersonInfoPanel,
        personsplitter->GetSize().GetHeight()-180);

    SetToolBar(CreateToolBar());
    ...
}

wxToolBar * SQLiteTestMainFrame::CreateToolBar()
{
    wxToolBar * toolBar = new wxToolBar(this, wxID_ANY,
        wxDefaultPosition, wxDefaultSize, wxTB_FLAT|wxTB_TEXT);
    toolBar->AddTool(ID_ADD_GROUP, _("Add Group"),
        wxBitmap(addbookm.xpm));
    toolBar->AddTool(ID_DELETE_GROUP, _("Remove Group"),
        wxBitmap(delbookm.xpm));
    toolBar->AddSeparator();
    ...
    toolBar->Realize();
    return toolBar;
}
...
```

Для работы с классом wxHtmlWindow в свойствах проекта в разделе «Linker → Input» в настройках «Additional Dependencies» нам необходимо добавить библиотеку wxmsw28ud\_html.lib для конфигурации Debug и wxmsw28u\_html.lib для конфигурации Release.

Отлично, интерфейс приложения готов, теперь можно приступить к реализации функционала.

## Реализация функционала

**RecordIDClientData.h** – класс для хранения данных, ассоциированных с элементом списка:

```
...
#include <wx/clntdata.h>
class RecordIDClientData : public wxClientData
{
    int m_ID;
public:
    RecordIDClientData(int id) : m_ID(id) {}
    int GetID() {return m_ID;}
    ...
};
...
```

**wxSQLiteTestMainFrame.cpp** – работа с базой данных, загрузка и отображение контактов из адресной книги:

```
void SQLiteTestMainFrame::FillGroupsList()
{
    m_GroupsListBox->Freeze();
    m_GroupsListBox->Clear();
    GroupRowSet * allGroups =
        wxGetApp().GetGroupTable()->All();
    for(unsigned long i = 0; i < allGroups->Count(); ++i)
    {
        m_GroupsListBox->Append(allGroups->Item(i)->name,
            new RecordIDClientData(allGroups->Item(i)->id));
    }
    if(m_GroupsListBox->GetCount())
    {
        m_GroupsListBox->SetSelection(0);
        RecordIDClientData * data = (RecordIDClientData *)
            m_GroupsListBox->GetClientObject(
                m_GroupsListBox->GetSelection());
        if(data)
        {
            FillPersonsList(data->GetID());
        }
    }
    m_GroupsListBox->Thaw();
}

void SQLiteTestMainFrame::FillPersonsList(int groupid)
{
    m_PersonsListView->Freeze();
    m_PersonsListView->DeleteAllItems();
    GroupRow * thisGroup =
        wxGetApp().GetGroupTable()->Id(groupid);
    if(thisGroup)
    {
        PersonRowSet * allPersons = thisGroup->GetPersons();
        long item(0);
        for(unsigned long i = 0; i < allPersons->Count(); ++i)
        {
            item = m_PersonsListView->InsertItem(item,
                allPersons->Item(i)->first_name);
            m_PersonsListView->SetItem(item, 1,
                allPersons->Item(i)->last_name);
            m_PersonsListView->SetItem(item, 2,
                allPersons->Item(i)->email);
            m_PersonsListView->SetItem(item, 3,
                allPersons->Item(i)->phone);
            m_PersonsListView->SetItemData(item,
                (long)allPersons->Item(i)->id);
        }
        if(m_PersonsListView->GetItemCount())
        {
            m_PersonsListView->Select(0);
        }
    }
    m_PersonsListView->Thaw();
}

void SQLiteTestMainFrame::
    OnGroupListBoxSelected(wxCommandEvent & event)
{
    RecordIDClientData * data =
        (RecordIDClientData *)event.GetClientObject();
    if(data)
    {
        FillPersonsList(data->GetID());
    }
}
```

```
void SQLiteTestMainFrame::
    OnPersonListViewSelected(wxListEvent & event)
{
    long personid = event.GetData();
    PersonRow * person =
        wxGetApp().GetPersonTable()->Id((int)personid);
    if(person)
    {
        m_PersonInfoPanel->SetPage(wxString::Format(
            wxT("<html><body><h3>%s %s</h3></body></html>"),
            person->first_name, person->last_name));
        m_PersonInfoPanel->AppendToPage(wxString::Format(
            wxT("<b>Gender:</b> %s"),
            (person->gender?wxT("Male"):wxT("Female"))));
        m_PersonInfoPanel->AppendToPage(wxT("<hr>"));
        ...
    }
    else
    {
        m_PersonInfoPanel->SetPage(
            wxT("<html><body><h3>Can't find info about \
            selected person</h3></body></html>"));
    }
}

void SQLiteTestMainFrame::
    OnPersonInfoPanelLinkClicked(wxHtmlLinkEvent & event)
{
    #if defined( WXMSW )
        ShellExecute(NULL, NULL,
            event.GetLinkInfo().GetHref().GetData(),
            NULL, NULL, SW_SHOW);
    #else
        wxExecute(event.GetLinkInfo().GetHref());
    #endif
}
```

Список в левой части окна содержит названия групп. Каждый элемент списка содержит код группы. Привязка данных к элементам списка реализована с помощью объектов класса `RecordIDClientData`, каждый объект которого содержит код группы. Класс `RecordIDClientData` является производным от `wxClientData`, и его использование обеспечивает автоматическую очистку памяти при удалении элемента списка. Доступ к данным, ассоциированным с элементом списка групп, производится посредством метода `GetClientObject` класса `wxListBox`. При выборе записи в списке групп список контактов в правой части окна заполняется данными контактов выбранной группы.

При выборе элемента списка контактов, информационное поле в нижней части окна заполняется данными контакта, связанного с выбранным элементом списка. Каждый элемент списка контактов содержит в поле данных код контакта. Доступ к полю данных производится посредством метода `GetItemData` класса `wxListView`.



Рисунок 5. Главное окно приложения с загруженным списком контактов

При нажатии на ссылку с адресом электронной почты в информационном поле создается новое письмо в почтовом клиенте, назначенном по умолчанию.

С отображением данных мы закончили. Теперь нужно реализовать добавление новой записи в таблицу и удаление записей из таблицы.

Для начала создадим диалоговые окна ввода данных.

**EditGroupDialog.h** – описание класса диалогового окна редактирования группы:

```
#ifndef _EDIT_GROUP_DIALOG_H
#define _EDIT_GROUP_DIALOG_H

#include <wx/wx.h>

class EditGroupDialog : public wxDialog
{
    wxString m_GroupName;
    wxString m_GroupDescription;
    void CreateControls();
public:
    EditGroupDialog(wxWindow * parent);
    bool Create(wxWindow * parent,
                wxWindowID id,
                const wxString title);

    const wxString & GetGroupName();
    const wxString & GetGroupDescription();
};

#endif
```

**EditGroupDialog.cpp** – класс диалогового окна редактирования группы, создание GUI:

```
...
void EditGroupDialog::CreateControls()
{
    wxBoxSizer * sizer = new wxBoxSizer(wxVERTICAL);
    SetSizer(sizer);

    wxStaticText * nameLabel =
        new wxStaticText(this, wxID_ANY, _("Name:"));
    wxStaticText * descriptionLabel =
        new wxStaticText(this, wxID_ANY,
            _("Description:"));

    wxTextCtrl * nameEdit =
        new wxTextCtrl(this, ID_EGD_NAME_TEXTCTRL,
            wxEmptyString);
    wxTextCtrl * descriptionEdit =
        new wxTextCtrl(this, ID_EGD_DESCRIPTION_TEXTCTRL,
            wxEmptyString, wxDefaultPosition,
            wxSize(-1, 150), wxTE_MULTILINE);
    nameEdit->SetValidator(
        wxGenericValidator(&m_GroupName));
    descriptionEdit->SetValidator(
        wxGenericValidator(&m_GroupDescription));

    wxFlexGridSizer * fg_sizer =
        new wxFlexGridSizer(2, 2, 0, 0);
    fg_sizer->Add(nameLabel, 0,
        wxALIGN_LEFT|wxALIGN_CENTER_VERTICAL|wxALL, 5);
    fg_sizer->Add(nameEdit, 1,
        wxEXPAND|wxALIGN_CENTER_VERTICAL|wxALL, 5);
    fg_sizer->Add(descriptionLabel, 0,
        wxALIGN_LEFT|wxALIGN_CENTER_VERTICAL|wxALL, 5);
    fg_sizer->Add(descriptionEdit, 1,
        wxEXPAND|wxALIGN_CENTER_VERTICAL|wxALL, 5);
    fg_sizer->AddGrowbleCol(1);

    sizer->Add(fg_sizer, 1,
        wxEXPAND|wxTOP|wxLEFT|wxRIGHT, 5);
    sizer->Add(CreateButtonSizer(wxID_OK|wxID_CANCEL),
        0, wxALIGN_RIGHT|wxALL, 5);
}
...
```

**EditPersonDialog.h** – описание класса диалогового окна редактирования контакта:

```
#ifndef _EDIT_PERSON_DIALOG_H
#define _EDIT_PERSON_DIALOG_H

#include <wx/wx.h>

class EditPersonDialog : public wxDialog
{
    wxString m_FirstName;
    wxString m_LastName;
    wxString m_Address;
    wxString m_City;
    wxString m_Country;
    wxString m_Email;
    wxString m_Phone;
    void CreateControls();
public:
    EditPersonDialog(wxWindow * parent);
    bool Create(wxWindow * parent,
                wxWindowID id, const wxString title);

    const wxString & GetFirstName();
    const wxString & GetLastName();
    const wxString & GetAddress();
    const wxString & GetCity();
    const wxString & GetCountry();
    const wxString & GetEmail();
    const wxString & GetPhone();
};

#endif
```

**EditPersonDialog.cpp** – класс диалогового окна редактирования контакта, создание GUI:

```
...
void EditPersonDialog::CreateControls()
{
    wxBoxSizer * sizer = new wxBoxSizer(wxVERTICAL);
    SetSizer(sizer);

    wxStaticText * firstnameLabel =
        new wxStaticText(this, wxID_ANY, _("First Name:"));
    wxStaticText * lastnameLabel =
        new wxStaticText(this, wxID_ANY, _("Last Name:"));

    wxTextCtrl * firstnameEdit =
        new wxTextCtrl(this, ID_EPD_FIRSTNAME_TEXTCTRL,
            wxEmptyString);
    wxTextCtrl * lastnameEdit =
        new wxTextCtrl(this, ID_EPD_LASTNAME_TEXTCTRL,
            wxEmptyString);

    ...
    firstnameEdit->SetMinSize(wxSize(150,-1));

    firstnameEdit->SetValidator(
        wxGenericValidator(&m_FirstName));
    lastnameEdit->SetValidator(
        wxGenericValidator(&m_LastName));

    ...
    wxFlexGridSizer * fg_sizer =
        new wxFlexGridSizer(2, 2, 0, 0);
    fg_sizer->Add(firstnameLabel, 0,
        wxALIGN_LEFT|wxALIGN_CENTER_VERTICAL|wxALL, 5);
    fg_sizer->Add(firstnameEdit, 1,
        wxEXPAND|wxALIGN_CENTER_VERTICAL|wxALL, 5);
    ...
    fg_sizer->AddGrowbleCol(1);

    sizer->Add(fg_sizer, 1, wxEXPAND|wxTOP|wxLEFT|wxRIGHT, 5);
    sizer->Add(CreateButtonSizer(wxID_OK|wxID_CANCEL), 0,
        wxALIGN_RIGHT|wxALL, 5);

    sizer->Fit(this);
}
...
```

Теперь можно приступить к написанию обработчиков событий от кнопок на панели инструментов.

**SQLiteTestMainFrame.cpp** – добавляем возможность создания и редактирования контактов:

```
...
void SQLiteTestMainFrame::OnAddGroup(wxCommandEvent & event)
{
    ...
}
```



```

EditGroupDialog * dlg = new EditGroupDialog(this);
if (dlg->ShowModal() == wxID_OK)
{
    GroupRow * newGroup = wxGetApp().GetGroupTable()->New();
    newGroup->name = dlg->GetGroupName();
    newGroup->description = dlg->GetGroupDescription();
    newGroup->Save();
    FillGroupsList();
}
dlg->Destroy();
}

void SQLiteTestMainFrame::
    OnRemoveGroup(wxCommandEvent & event)
{
    int selection = m_GroupsListBox->GetSelection();
    RecordIDClientData * data = (RecordIDClientData *)
        m_GroupsListBox->GetClientObject(selection);
    if (data)
    {
        GroupRow * thisGroup =
            wxGetApp().GetGroupTable()->Id(data->GetID());
        if (thisGroup && (wxMessageBox(
            _("Do you really want to delete this group?"),
            _("Delete group"), wxYES_NO) == wxYES))
        {
            PersonRowSet * thisPersons = thisGroup->GetPersons();
            for (unsigned long i = 0; i < thisPersons->Count(); ++i)
            {
                thisPersons->Item(i)->Delete();
            }
            thisGroup->Delete();
            m_GroupsListBox->Delete(selection);
            if (m_GroupsListBox->GetCount()
            {
                m_GroupsListBox->SetSelection(selection <
                    m_GroupsListBox->GetCount() ? selection : 0);
                data = (RecordIDClientData *)
                    m_GroupsListBox->GetClientObject(
                        m_GroupsListBox->GetSelection());
                if (data)
                {
                    FillPersonsList(data->GetID());
                }
            }
        }
    }
}

void SQLiteTestMainFrame::
    OnAddPerson(wxCommandEvent & event)
{
    RecordIDClientData * data = (RecordIDClientData *)
        m_GroupsListBox->GetClientObject(
            m_GroupsListBox->GetSelection());
    if (data)
    {
        GroupRow * thisGroup =
            wxGetApp().GetGroupTable()->Id(data->GetID());
        if (thisGroup)
        {
            EditPersonDialog * dlg = new EditPersonDialog(this);
            if (dlg->ShowModal() == wxID_OK)
            {
                PersonRow * newPerson =
                    wxGetApp().GetPersonTable()->New();
                newPerson->groupid = thisGroup->id;
                newPerson->first_name = dlg->GetFirstName();
                newPerson->last_name = dlg->GetLastName();
                ...
                newPerson->Save();
                FillPersonsList(thisGroup->id);
            }
            dlg->Destroy();
        }
    }
}

void SQLiteTestMainFrame::
    OnRemovePerson(wxCommandEvent & event)
{
    long selection = m_PersonsListView->GetFirstSelected();
    PersonRow * thisPerson = wxGetApp().GetPersonTable()->Id(
        (int)m_PersonsListView->GetItemData(selection));
    if (thisPerson && (wxMessageBox(
        _("Do you really want to delete this record?"),
        _("Delete person"), wxYES_NO) == wxYES))
    {

```

```

        int groupid = thisPerson->groupid;
        thisPerson->Delete();
        m_PersonsListView->DeleteItem(selection);
        if (m_PersonsListView->GetItemCount()
        {
            m_PersonsListView->Select(wxMin(selection,
                m_PersonsListView->GetItemCount()-1));
        }
    }
}

void SQLiteTestMainFrame::
    OnRemoveGroupUpdateUI(wxUpdateUIEvent & event)
{
    event.Enable(m_GroupsListBox->GetSelection() >= 0);
}

void SQLiteTestMainFrame::
    OnAddPersonUpdateUI(wxUpdateUIEvent & event)
{
    event.Enable(m_GroupsListBox->GetSelection() >= 0);
}

void SQLiteTestMainFrame::
    OnRemovePersonUpdateUI(wxUpdateUIEvent & event)
{
    event.Enable(m_PersonsListView->GetFirstSelected() >= 0);
}
...

```

Как видно, кнопка удаления группы и кнопка добавления контакта активны только в случае, если есть активная запись в списке групп. Кнопка удаления контакта становится активной только в случае, если есть активная запись в списке контактов. При удалении группы удаляются и все связанные с ней контакты.

Ну вот. Мы закончили. Теперь собираем Release-версию программы и тестируем. Можно переходить к созданию проекта под Linux.

## Linux

Для сборки нашего проекта в Linux нам необходимо наличие в системе установленной библиотеки wxWidgets. Для большинства распространенных дистрибутивов wxWidgets доступна в виде готовых пакетов, но лучше всего будет не использовать готовые пакеты, а загрузить исходный код wxWidgets с официального сайта и собрать библиотеку вручную. Кроме исходного кода, дистрибутив wxWidgets содержит довольно большое количество примеров, которые могут оказаться очень полезными для начинающих. В качестве среды разработки в Linux мы будем использовать Eclipse с установленным C/C++ Development Tooling (CDT).

## Собираем SQLite

Для корректной работы нашего приложения необходим файл статической библиотеки libsqlite3.a, а также заголовочные файлы SQLite. В случае если в системе эти файлы отсутствуют, необходимо загрузить исходный код SQLite (sqlite-x.y.z.tar.gz), собрать его и установить:

```

./configure --enable-static
make
make instal

```

## Создание и настройка проекта в Eclipse

После сборки SQLite необходимо убедиться, что путь к файлам libsqlite3.so.\* находится в списке путей поиска библиотек. Я же просто создал ссылки на эти файлы в каталоге /lib. Теперь, если это еще не сделано, нужно удалить все .h

и .cpp-файлы, не относящиеся к проекту databaselayer\_sqlite из папок databaselayer/src и databaselayer/include, а также, папку databaselayer/tests.

После того как предварительная подготовка выполнена, запускаем Eclipse и в папке databaselayer создаем новый проект. Назовем его SqliteDatabaseLayer.

Далее идем в настройки проекта и в разделе «C/C++ Build → Miscellaneous» в поле Other flags дописываем:

```
`wx-config --cxxflags`
```

Заметьте, кавычки обратные, кнопка с тильдой («~») на клавиатуре.

После того как настройка библиотеки DatabaseLayer завершена, нужно создать проект для тестового приложения. Создаем новый проект Executable (Gnu) в папке SQLiteTest. В мастере создания проекта на вкладке настройки зависимостей необходимо указать проект библиотеки SqliteDatabaseLayer. В свойствах проекта в разделе «C/C++ Build → Directories» добавляем новые записи:

```
{ProjDirPath}/art  
{ProjDirPath}/wxActiveRecord  
{ProjDirPath}/../databaselayer/include
```

Заметьте, скобки фигурные, в отличие от настроек проекта в Visual Studio.

В разделе «C/C++ Build → Miscellaneous» в поле Other flags дописываем:

```
`wx-config --cxxflags`
```

В разделе «C/C++ Build → Libraries» добавляем новые записи:

```
SqliteDatabaseLayer  
sqlite3
```

Библиотеки должны быть добавлены именно в указанной последовательности, т.к. библиотека libSqliteDatabaseLayer.a зависит от libsqlite3.a.

И в списке Library search path добавляем запись:

```
{ProjDirPath}/../databaselayer/Debug
```

В разделе «C/C++ Build → GCC C++ Linker → Miscellaneous» в поле Linker flags дописываем:

```
`wx-config --libs`
```

Собираем проект с помощью «Project → Build Project».

## Запуск приложения и отладка

После успешной сборки неплохо было бы запустить наше приложение и проверить его на работоспособность. Выбираем пункт меню «Run → Run...» В диалоговом окне «Run» жмем правой кнопкой на элементе «C/C++ Local Application», выбираем пункт меню «New» (см. рис. 6). После этого у нас должна появиться новая конфигурация запуска с названием SQLiteTest Жмем кнопку «Search Project». В окне «Program Selection» выбираем наше приложение. Жмем

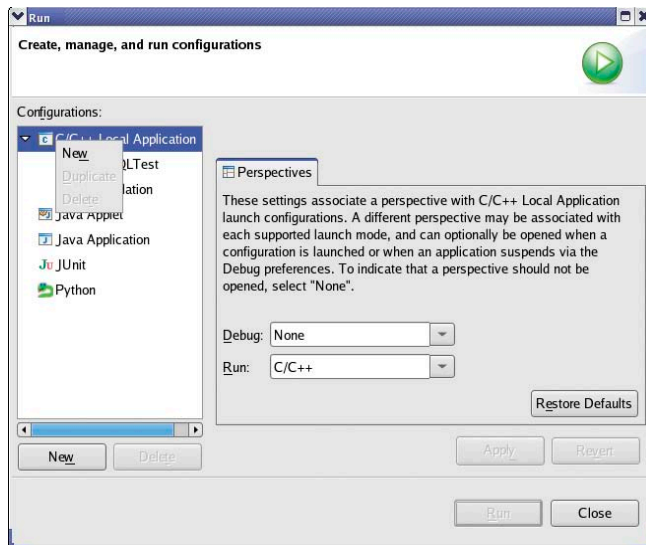


Рисунок 6. Создание конфигурации запуска приложения в Eclipse

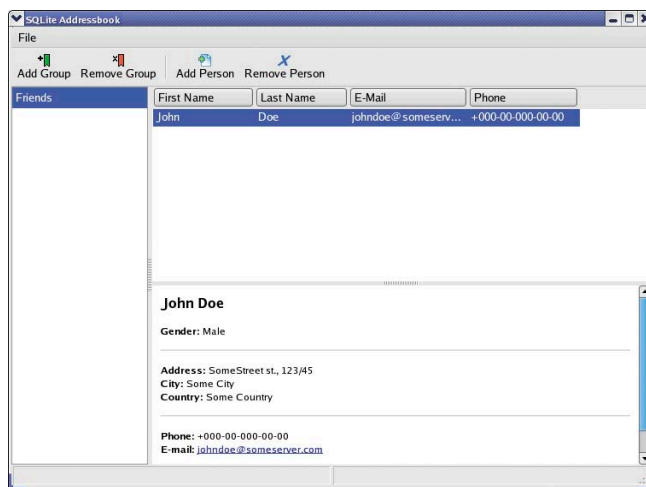




Рисунок 7. Внешний вид главного окна приложения в Linux

«OK». На вкладке «Debugger» в списке Debugger выбираем «GDB Debugger». Жмем «Run». Вот и результат. Получилось довольно опрятно (см. рис. 7).

## Заключение

Как видите, ничего сложного в разработке кроссплатформенных приложений нет, но, как и любой труд, кроссплатформенная разработка программного обеспечения требует опыта и сноровки. Надеюсь, материал послужит толчком для того, чтобы начать немного по-другому смотреть на свои проблемы и на способы их решения. Исходный код к статье можно загрузить отсюда: <http://wxwidgets.info/files/SQLiteTest.7z>.

1. <http://wxwidgets.info> – статьи, руководства, видео-уроки по программированию на C++/wxWidgets на русском. Единственный русскоязычный ресурс, посвященный кроссплатформенной разработке ПО с библиотекой wxWidgets.
2. <http://wxcode.sourceforge.net/components/activerecord/tutorial/wxARG-tutorial.php> – руководство по использованию библиотеки DatabaseLayer.
3. <http://wxcommunity.com> – дополнительные компоненты wxWidgets.
4. <http://wxforum.shadonet.com> – форум библиотеки wxWidgets.



**свежие  
решения  
бизнес-  
уравнений**

## Лицензирование

Softline работает на рынке программного обеспечения с 1993 года и обладает высшими статусами партнерства таких компаний, как Microsoft, Oracle, SAP, Symantec, Citrix, Adobe и многих других.

## Обучение

Учебный центр Softline, лидирующий на рынке IT-образования, предоставляет профессиональные услуги по обучению, тестированию и сертификации IT-специалистов.

## Консалтинг

Консалтинговое подразделение Softline Solutions обладает уникальным опытом по внедрению и разворачиванию инфраструктурных решений и систем управления бизнесом для компаний любого масштаба.

**softline**<sup>®</sup>  
ЛИЦЕНЗИРОВАНИЕ. ОБУЧЕНИЕ. КОНСАЛТИНГ

119991 Москва, ул. Губкина, 8. Тел./факс: +7 (495) 232-00-23  
E-mail: [info@softline.ru](mailto:info@softline.ru), <http://www.softline.ru>

Москва, Санкт-Петербург, Екатеринбург, Казань, Красноярск, Нижний Новгород, Новосибирск,  
Омск, Ростов-на-Дону, Самара, Уфа, Хабаровск Минск Киев Ташкент Астана, Алматы  
Бишкек Баку Душанбе



# Судебные войны: оберегай своё, не посягай на чужое

## Часть вторая – программная



Дмитрий Мороз

Так уж повелось, что, в отличие от мира аппаратного обеспечения, судебные разбирательства между компаниями, занимающимися разработкой программных продуктов, проходят намного ожесточеннее, да к тому же длятся значительно дольше. А уж суммы результирующих штрафов и вовсе сводят с ума. За примерами далеко ходить не надо.

### Противостояние Apple и Microsoft

Соперничество между этими «гигантами» рынка уходит своими корнями ещё в 1985 год. Именно тогда, накануне выпуска первой версии Windows (являвшейся в то время лишь графической оболочкой для MS-DOS), в гости к Microsoft заглянули юристы Apple, выразившие мнение своего руководства по отношению к внешнему виду будущего продукта. Компания была недовольна тем, что облик Windows копирует многие элементы внешнего вида из её операционной системы MacOS. В своё оправдание Microsoft отметила, что в качестве прототипа ею были использованы разработки в области графических интерфейсов, произведённые лабораторией Xerox PARC, но никак не Apple.

24 октября 1985 г. состоялась встреча представителей руководства обеих компаний. Президент Microsoft Билл Гейтс заявил напрямую, что если Apple предпримет против его компании какие-либо правовые нормы от-

носительно графического интерфейса Windows, MacOS может навсегда распрощаться с новыми версиями программ Word и Excel (во многом благодаря которым платформа Macintosh в середине 80-х достигла большой популярности) и других продуктов. Дабы не усугублять накалившуюся обстановку, Билл Гейтс предложил руководству Apple лицензировать его компании внешний облик MacOS.

Злосчастный договор, подготовленный юристами Apple для подписания Microsoft 22 ноября, содержал неправильную формулировку текста, которая впоследствии сыграла с «яблочной» компанией злую шутку. Согласно договору Apple предоставляла Гейтсу полную свободу независимого развития графических интерфейсов, или, говоря проще – право копировать любой элемент внешнего вида MacOS.

В ноябре 1985 года Windows 1.0 увидел свет. Спустя два года Microsoft представила миру новую версию своей разработки – 2.0. Её интерфейс, в особенности иконки на Рабочем сто-

ле, а также накладывающиеся друг на друга окна, были практически неотличимы от таковых в MacOS. Несмотря на всё несовершенство первых версий Windows, Microsoft за короткий срок смогла продать свыше двух миллионов её копий, что говорило о росте популярности продукта. Данные обстоятельства никак не радовали руководство Apple, в результате чего 17 марта 1988 года компания выдвинула иск против компании Гейтса, обвинив её в незаконном копировании графических элементов интерфейса MacOS.

В своё оправдание Microsoft заявила, что действовала сугубо в рамках договора 1985 года. В подтверждение своих слов компания предоставила общественности части этого документа.

Тем временем, выпустив в 1990 году Windows 3.0, Microsoft смогла в течение одного года продать три миллиона копий своей ОС, серьёзно подорвав позиции MacOS.

Разбирательство по факту незаконного копирования графических эле-

ментов интерфейса длилось вплоть до 1993 года, когда суд отклонил претензии Apple. Согласно постановлению, из 189 графических элементов, заявленных в иске Apple, 179 были лицензированы Microsoft в соглашении относительно Windows 1.0, а оставшиеся 10 попросту не подлежали регистрации, поскольку они не были созданы самой компанией либо же были единственно возможным графическим представлением конкретных данных. Впоследствии Apple апеллировала к Верховному суду США, однако в феврале 1995 года тот поставил на деле «жирный крест».

Проиграв столь важное дело, Apple решила отомстить Microsoft другим способом. В 1992 году небольшая компания Canyon заключила с «яблочной» компанией партнёрское соглашение, согласно которому она будет разрабатывать программное обеспечение, позволяющее при помощи технологии Apple под названием QuickTime проигрывать аудио- и видеoinформацию на компьютерах, работающих под управлением Windows. Стремясь вызвать интерес к своей технологии со стороны независимых разработчиков, Apple пошла на беспрецедентный шаг, позволив перенести её на «вражескую» платформу.

В результате стараний Canyon в ноябре 1992 года на свет появилось программное обеспечение под названием QuickTime for Windows.

Одновременно с ним был анонсирован конкурирующий продукт производства Microsoft – Video for Windows. В июле 1993 года разработчик микропроцессоров компания Intel совместно с Canyon начали работать над единым интерфейсом управления дисплеем (DCI), который стал частью Video for Windows.

«Час икс» наступил в конце 1994 года, когда Microsoft опубликовала спецификации DCI для производителей графических чипов. «Покопавшись» в программном коде, сотрудники Apple обнаружили полную идентичность некоторых частей кода, написанных Canyon, таковым, написанным этой компанией для QuickTime for Windows.

Буквально на следующий день, 6 декабря 1994 года, Apple подала иск против Canyon, обвинив её в нарушении авторских прав, а также распространении коммерческих тайн. Microsoft

узнала об этом судебном процессе лишь из официального письма юристов Apple. На встрече представителей руководства обеих компаний сотрудники Microsoft заявили, что спорный код составляет менее одного процента от общего его количества и его можно без особых проблем заменить. Компания согласилась самостоятельно изъять из Video for Windows весь код Canyon, дабы урегулировать иск мирным путём. Несмотря на отказ Apple пойти навстречу, сразу по окончании собрания сотрудники Microsoft принялись за работу, и уже через несколько дней свет увидела новая версия программы, не содержащая спорного кода.

Судебные распри по поводу графического интерфейса операционных систем, а также QuickTime были урегулированы 6 августа 1997 года, когда между двумя компаниями было подписано единое соглашение. Согласно ему Apple обязалась сделать браузер Internet Explorer главным инструментом веб-серфинга для платформы Macintosh, тогда как Microsoft обещала выпускать новые версии пакета Microsoft Office на протяжении следующих пяти лет. Кроме того, компания инвестировала в Apple 150 миллионов долларов.

## «Яблоко» раздора

В довершение всех судебных тяжб по поводу аппаратно-программных разработок в закромах у Apple до недавних пор находилось, пожалуй, наиболее длительное разбирательство за всю историю не только компании, но и рынка IT.

В 1978 году компания Apple Corps (основанная известной музыкальной группой The Beatles) подала иск против Apple Computer (далее просто Apple), обвинив её в нарушении прав на торговую марку. Судебное разбирательство было улажено в 1981 году подписанием соглашения, согласно которому Apple выплачивала Apple Corps 80 тысяч долларов, а также впредь должна была держаться подальше от музыкальной индустрии.

Порядком подзабытый иск был повторно «поставлен на кон» в 1991 году. В модельном ряде компьютеров Apple появились системы, способные хранить и воспроизводить музыку в формате MIDI, и Apple Corps решила, что подоб-

ным образом компания нарушает старый договор. На этот раз иск был улажен намного быстрее – выплатой Apple компенсации в 26 млн. долларов, а также судебных издержек на 8,5 млн. долларов. Кроме того, компании запрещалось производить и продавать физические носители музыки с нанесённым на них логотипом надкушенного яблока.

Отныне между обеими компаниями длилось перемирие, в очередной раз закончившееся в сентябре 2003 года с запуском Apple музыкального онлайн-сервиса iTunes. Согласно новому иску Apple Corp компания нарушала соглашение 1991 года и, как следствие, должна была отказаться от использования фирменного логотипа компании для продаж музыки через Интернет.

На сей раз удача улыбнулась Apple: спустя три года в мае 2006 года суд принял решение отклонить иск Apple Corp, поскольку «надкушенное яблоко» являлось логотипом магазина, но никак не продаваемой им музыки.

«Точка» в судебных тяжбах между обеими Apple была поставлена сравнительно недавно – 5 февраля 2007 года. Согласно подписанному компаниями договору Apple Computer отныне будет владеть всеми правами на торговые марки, в которых фигурирует слово Apple. Кроме того, Apple Corps лицензировала Apple музыкальное достояние Beatles для его продажи через iTunes. К сожалению, финансовые аспекты соглашения остались неизвестны.

## Телефон без имени

В завершение истории судебных тяжб Apple нельзя не рассказать об иске, поданном против Apple производителем телекоммуникационного оборудования компанией Cisco Systems за право обладания торговой маркой iPhone.

Права на эту марку iPhone принадлежат Cisco ещё с 2000 года, когда компания приобрела их вместе с предыдущим владельцем – Infogear Technology. Стоит отметить, что одно из подразделений Cisco, Lynksys, с 2006 года производит интернет-телефоны под названием iPhone.

Со слов представителей Cisco, Apple вела переговоры с компанией на предмет лицензирования торговой марки на протяжении нескольких лет. К сожалению, 9 января 2007 года, за несколько

часов до объявления Стивом Джобсом iPhone на выставке MacWorld 2007, стороны так и не достигли согласия. Сразу после выступления юристы Cisco потребовали от Apple завершить переговоры до конца дня, иначе они будут вынуждены обратиться в суд. Компания не отреагировала на предупреждение, в результате чего 11 января Cisco подала судебный иск, в котором говорилось о незаконном использовании Apple торговой марки iPhone.

В качестве защиты представители обвиняемой стороны отмечают, что Apple имеет полное право использовать данную торговую марку, поскольку ее телефон по конструкции и принципам работы отличается от продукции Linksys. Уверенная в своей правоте и силах, Apple 16 января попыталась зарегистрировать торговую марку iPhone в Канаде, однако неудачно. Пока же у обеих компаний есть время уладить разногласия до июня – месяца выпуска телефона Apple на рынок.

## Две стороны одной медали

Я открыл сегодняшнюю статью рассказом об Apple неспроста: судебные разбирательства, в которые была вовлечена компания, можно назвать одними из наиболее интересных. Однако если судить с позиции наиболее «жесточких», здесь вне конкуренции – Microsoft.

Монополизм этого «гиганта из Рэдмонда» даёт о себе знать: каждый новый шаг Microsoft на пути к абсолютному контролю на рынке сопровождается очередным громким судебным иском, выдвигаемым против неё. Среди производителей аппаратного обеспечения в аналогичной ситуации находится Intel, о судебной «жизни» которой я рассказывал в прошлом номере журнала. Видимо, такова судьба всех компаний, доминирующих в своём сегменте рынка.

Описывать многочисленные судебные разбирательства, выпавшие на долю Microsoft, нет смысла, так что я расскажу лишь о наиболее громком и скандальном – антимонопольном процессе.

В конце прошлого века Microsoft стала негласным монополистом на рынке операционных систем: более 80% компьютеров по всему земному шару работали под управлением различных

версий Windows. Подобная тенденция намечалась и в области офисных пакетов, где у компании с её Microsoft Office позиции также были велики.

В 1994 году на свет появился первый веб-браузер под названием Mosaic, разработанный в Национальном центре США по использованию суперкомпьютеров (NCSA). Позже выходцы из этого центра основали собственную компанию Netscape Communications, в недрах которой они занялись разработкой браузера на основе Mosaic. В результате был создан новый «обозреватель Паутины» под названием Navigator, быстро завоевавший большую популярность.

Microsoft запоздало начала освоение сети Интернет со своим Internet Explorer, поэтому для его скорейшей популяризации предприняла соответствующие меры.

Значительные средства, потраченные на развитие проекта (который, в отличие от конкурента, было решено сделать бесплатным), а также большое количество первоклассных программистов, работавших на компанию, сделали своё дело, и в 1997 году оба конкурирующих браузера соревновались уже на равных. Наибольшим недостатком на тот момент были разные подходы программ по обработке HTML-страниц, в результате чего сайт, заточенный разработчиком под Netscape Navigator, мог некорректно отображаться в Internet Explorer и наоборот.

Извечное стремление Microsoft к контролю всего рынка дало знать о себе и на этот раз. Дабы «малой кровью» сделать свой браузер доминирующим на рынке, компания пошла на беспрецедентный шаг. В новую версию операционной системы Windows 98 Internet Explorer был встроен изначально, причём его интеграция в систему была столь плотной, что пользователю приходилось работать с ним, даже несмотря на возможную личную неприязнь.

Антимонопольным организациям США, а также Netscape подобный ход пришёлся не по вкусу, в результате чего в мае 1998 года Министерство юстиции США, а также генеральные прокуроры 19 штатов страны подали против Microsoft серию исков, в которых компания обвинялась в нечестном обращении с потребителями и конкурентами. В случае с Netscape она использовала

своё монопольное положение на рынке операционных систем для обеспечения Internet Explorer лучших условий, ну а что касается пользователей – навязывала собственный продукт помимо их воли.

В последовавшем судебном разбирательстве принимали участие практически все сотрудники Microsoft, занимающие руководящие посты в компании. Сам Билл Гейтс был допрошен на суде в общей сложности на протяжении 17 часов. Кстати, спустя некоторое время плёнки с видеозаписью его допроса были с успехом проданы на интернет-аукционе eBay.

Министерство юстиции США потребовало от Microsoft извлечь из операционной системы браузер Internet Explorer и предлагать его отдельно, тем самым давая пользователям возможность выбирать между ним и продукцией конкурентов. Однако представители компании заявили, что удалить программу из ОС невозможно из-за её глубокой интеграции в систему.

В 1999 году к антимонопольному процессу, инициированному правительством США, присоединился ещё один крупный коллективный судебный иск, поданный против Microsoft в штате Калифорния. В нём компания обвинялась в завышении цен на свои операционные системы Windows 95 и Windows 98, запрашивая минимум на 40 долларов больше их реальной цены.

После длительного судебного разбирательства 5 ноября 1999 года суд вынес предварительное решение. Окружной судья Томас Пенфилд Джексон (Thomas Penfield Jackson) объявил, что Microsoft «признана монополистом, использующим свое доминирующее положение на рынке для подавления конкурентов». В конце 2000 года по постановлению Джексона компании предстояло разделение на две отдельные фирмы: первая будет заниматься исключительно операционными системами, тогда как вторая – остальным программным обеспечением, производимым Microsoft.

К счастью для компании, в начале 2001 года юристам удалось добиться того, чтобы дело было передано в апелляционный суд. После выдвинутых против Джексона обвинений в необъективности и личной неприязни к Microsoft новый суд отме-



нил его решение и отстранил от процесса. Новый судья, Колин Коллар-Котли (Colleen Kollar-Kotelly), сразу же заявила о желании пойти с компанией на переговоры и урегулировать дело мирным путём вне зала суда.

В 2001 году судебные разбирательства по поводу монопольного положения Microsoft на рынке перенесли на другую сторону земного шара – в Южную Корею. Тогда крупнейший южнокорейский оператор Daum Communications подал иск против Microsoft, обвинив её в нанесении ущерба бизнесу малых компаний путём интеграции в Windows XP программ Instant Messenger и Media Player.

Окончательный вердикт по поводу антимонопольного процесса в США был оглашён 6 ноября 2001 года. Согласно подписанному «внесудебному соглашению» между Министерством юстиции и Microsoft, компания обязалась предоставить производителям персональных компьютеров большую свободу в выборе предустановленного программного обеспечения. Также она должна была выпустить обновления к своим операционным системам с целью возможности скрытия пользователем на Рабочем столе ярлыков программ Internet Explorer и Media Player и установки альтернативных продуктов других производителей. Наконец, компании возбранялось требовать от производителей ПК обязательной установки Windows на все выпускаемые компьютеры.

Прокуроры девяти штатов отказались подписывать соглашение и потребовали от суда введения более жестких санкций по отношению к Microsoft. Среди их требований был выпуск операционных систем без встроенных Internet Explorer и Media Player, а также открытие исходного кода Windows, либо отдельных его элементов. Однако 1 ноября 2002 года суд отклонил их предложение.

В июле 2003 года закончилось следствие по коллективному иску штата Калифорния. Microsoft приняла решение выплатить 1,1 миллиарда долларов на его урегулирование. Отныне любой пользователь или организация, купившие продукты компании за шесть лет, начиная с февраля 1995 года, могут получить ваучеры стоимостью от 5 до 29 долларов для оплаты покупки программных и аппаратных продуктов практи-

чески от любого производителя. Две трети от неиспользованных средств будут перечислены в фонд калифорнийских государственных школ. Ещё 250 млн. долларов были потрачены компанией на оплату труда множества юристов, работавших над делом.

После окончания антимонопольного процесса в США настал черёд Европы. В начале 2004 года Европейская комиссия обвинила Microsoft в злоупотреблении своим доминирующим положением на рынке операционных систем. Свой первый иск против компании Еврокомиссия подготовила ещё в 2002 году, тогда он затрагивал желание Microsoft монополизировать рынок мобильных устройств. Теперь же основой для судебного иска стала интеграция в Windows XP медиаплеера Media Player, препятствующего нормальной работе аналогичных программ сторонних разработчиков.

24 марта 2004 года Еврокомиссия вынесла своё решение, согласно которому Microsoft была обязана выплатить штраф в размере 497 млн. евро. Кроме того, её обязали в течение трёх месяцев предоставить европейскому рынку специальную версию Windows XP с изъятым проигрывателем Media Player. Наконец, компания должна была предоставить поставщикам серверного программного обеспечения исходные коды части сетевых протоколов своей операционной системы Windows Server.

Не согласная с решением комиссии по третьему пункту, компания подала апелляцию, выплатив, тем не менее, предписанный ей штраф. Также через некоторое время в продажу поступила версия Windows XP с индексом N, в которой отсутствовал Media Player.

16 ноября 2005 года Microsoft обратилась за помощью в Министерство юстиции США, дабы та вмешалась в европейский антимонопольный процесс. Однако чиновники Минюста проигнорировали просьбу. Тогда компания призвала другие американские компании осудить действия Еврокомиссии, тем самым поддержав её в антимонопольных процессах. Спустя месяц Европейская комиссия посредством предупреждения напомнила Microsoft, что та не выполнила до конца решение суда

по антимонопольному процессу. В случае игнорирования компанию ждал очередной крупный штраф.

26 февраля 2006 года к так и не улаженному разбирательству Европейской комиссии присоединился коллективный иск, поданный против Microsoft рядом крупных компаний, среди которых оказались Oracle, IBM, Sun Microsystems, Nokia, RealNetworks и другие. В тексте документа истцы опять-таки сетовали на злоупотребление Microsoft своим монопольным положением на рынке, недобросовестную конкуренцию, а также невыполнение решения суда, вынесенного Еврокомиссией в 2004 году.

**Монополизм «гиганта из Рэдмонда» даёт о себе знать: каждый новый шаг Microsoft на пути к абсолютному контролю на рынке сопровождается очередным громким судебным иском, выдвигаемым против неё.**

Представители компании потребовали от членов комиссии проведения открытого судебного слушания. Таким образом, Microsoft хотела убедить общественность в неоправданности выдвинутых против неё обвинений. Комиссия просьбу компании отклонила.

16 марта Еврокомиссия, рассмотрев поданные Microsoft документы, вновь подтвердила вину компании, согласно которой она не выполняет решение суда по антимонопольному процессу 2004 года. В результате на неё был наложен штраф в размере 2,36 млн. долларов в день за период начиная с 15 декабря 2005 года.

9 декабря 2006 года подошло к своему завершению дело по аналогичному процессу в Южной Корее. Антимонопольное ведомство страны признало Microsoft виновной и обязало компанию выплатить Daum Communications 32 млн. долларов за ведение нечестной конкурентной борьбы и нарушение антимонопольного законодательства. Кроме того, судебное постановление предписало компании выпуск на территории Южной Кореи специальной версии Windows XP, из которой будут исключены программы Messenger и Media Player.

Наконец, последним «очередным» заявлением стало решение Еврокомис-

сии 27 марта 2007 года увеличить сумму ежедневного штрафа Microsoft с 2 до 5 млн. долларов. Компания до сих пор никак не отреагировала на этот шаг, впрочем, как и предыдущий. Думается, об антимонопольных процессах Microsoft мы ещё услышим, и не раз.

## Open Source под прицелом

В мире бытует мнение, что наиболее уязвимыми для судебных разбирательств являются компании, связавшие свою деятельность с программным обеспечением с открытым исходным кодом, например, той же Linux. Сильная сторона Open Source одновременно является и её слабиной: открытый исходный код большинства программ значительно облегчает компаниям поиск «зацепок», которые затем можно поставить «на кону» очередного судебного иска.

Наиболее яркий пример – ряд скандально известных судебных исков, направленных компанией SCO Group против всего Linux-сообщества.

Для начала немного истории. Операционная система UNIX была разработана в лабораториях Bell Laboratories компании AT&T ещё в конце 60-х годов прошлого века. Коммерческой выгоды в этой операционной системе AT&T не искала, скорее наоборот: она лицензировала исходный код UNIX System V ряду других компаний, а также предоставила его университетам для исследовательских целей. Одним из лицензиатов UNIX в 1985 году стала корпорация IBM, разработавшая свою версию системы под названием AIX. Спустя восемь лет AT&T продала все права на System V компании Novell, которая, в свою очередь, в 1995 году перепродала их Santa Cruz Operation.

Компания Caldera, неудачно начавшая свой бизнес в качестве разработчика и дистрибьютора одного из дистрибутивов на базе Linux, в 2001 году выкупила у Santa Cruz Operation её подразделение, занимавшееся UNIX. На следующий год она изменила своё название на SCO Group и вместо дальнейшего продвижения операционной системы, приступила к «защите» приобретённой интеллектуальной собственности.

В 1991 году финский студент Линус Торвалдс (Linus Torvalds) разработал ядро, получившее название Linux,

за основу которого была взята концепция UNIX. Благодаря открытости исходного кода ядра, полученного в результате использования лицензии GPL, сторонние разработчики быстро написали необходимое программное обеспечение для превращения Linux в полноценную операционную систему (GNU/Linux). Первые несколько лет своей жизни эта ОС, развиваемая независимыми программистами, практически не выходила за университетские стены. Однако на рубеже столетий она начала стремительно завоевывать популярность, «наступая на пятки» различным версиям UNIX. Многие компании по достоинству оценили преимущества операционной системы с открытым исходным кодом и решили помогать Linux в её дальнейшем развитии. Среди них оказалась и IBM, решившая вложить в систему один миллиард долларов, а также интегрировать некоторые из технологий, заложенных в AIX. Данный шаг и стал той «искрой», вызвавшей «пожар» между SCO и Linux.

6 марта 2003 года IBM была извещена о том, что против неё выдвинут судебный иск. SCO среди прочего обвиняла корпорацию в «незаконном распространении коммерческих тайн, нечестной конкуренции, невыполнении условий контракта, а также посягательстве на своё имущество». Согласно её данным, IBM незаконно использовала части исходного кода UNIX, интегрировав его в Linux. Спорными, по мнению SCO, оказались следующие компоненты ядра: симметричная мультипроцессорная обработка (SMP), механизм неоднородного доступа к памяти (NUMA), техника блокировки «чтения-копирования-обновления» (RCU), а также журналируемая файловая система IBM – JFS. Компания требовала от «Голубого гиганта» возмещения ущерба в один миллиард долларов (позже эта сумма была увеличена до трёх, а затем и до пяти млрд. долларов), изъятия из Linux всего «проблемного» кода, а также прекращения любой поддержки данной ОС.

Сразу после того, как новость облетела земной шар, стоимость акций SCO поднялась до 20 долларов за штуку. Правда, спустя короткий промежуток времени она быстро опустилась до своего прежнего уровня. Любопытный факт: сразу после повышения цены руководители SCO избавились от при-

надлежащих им акций. В результате возникло предположение, что целью всей затеи было мгновенное повышение котировок акций компании и быстрая их продажа с целью наживы. Ещё одна версия, циркулировавшая в то время, – желание руководства SCO продать свою компанию IBM.

На протяжении марта SCO вела переговоры с несколькими компаниями на предмет лицензирования исходного кода UNIX System V. Её старания увенчались определённым успехом: в мае 2003 года двое из списка потенциальных лицензиатов, Microsoft и Sun Microsystems, объявили о подписании с SCO соглашения и выплате ей 15,5 млн. долларов. Поскольку операционные системы Windows NT и Solaris содержали в себе часть кода System V, обе компании подобным образом пытались обезопасить себя от возможного возникновения в будущем правовых проблем, подобных ситуации с IBM.

В это же время SCO разослала письма в 1500 ведущих компаний мира, в которых она предупредила об иске против IBM и необходимости приобретения лицензии на System V при использовании Linux. В данную категорию попали и компании, занимающиеся разработкой дистрибутивов на основе этой ОС. Однако наибольший шок у общественности вызвал тот факт, что, по словам представителей SCO, любой независимый пользователь Linux потенциально мог стать жертвой разбирательства.

Сообщество OpenSource негодовало: как может компания, не предоставившая собственные официальные права на исходные коды System V, обвинять мир в совершении подобного «греха»? По словам представителей SCO, количество «позаимствованных» из SCO строк равнялось всего нескольким сотням, однако при 2,44 миллионах строк кода в ядре Linux v.2.4.2, а также 30 миллионах в типичном дистрибутиве на его основе данная цифра была просто смешной. К тому же вся операционная система была написана сотнями и тысячами программистов «с чистого листа», имеет хорошо задокументированное происхождение, а также всю публично доступную историю изменений.

28 мая 2003 года свою лепту внесла Novell, опубликовав пресс-релиз, в котором говорилось о ситуации с правами SCO на UNIX: «Насколько нам из-

вестно, в соглашении 1995 года не было ни слова о передаче SCO всех авторских прав на эту интеллектуальную собственность».

Позднее SCO заявила, что ею была обнаружена некая поправка к контракту, в которой говорилось о передаче части прав на UNIX. Что самое интересное, Novell копии этого документа у себя не обнаружила.

22 декабря очередное заявление Novell прояснило ситуацию: согласно новому пресс-релизу, к SCO действительно могла перейти часть прав, однако лишь после выполнения компанией определённых обязательств. К моменту публикации документа время на их осуществление уже закончилось. Между тем, 14 октября Novell не афишируя зарегистрировала часть авторских прав на UNIX, о чём стало известно лишь спустя два месяца. В довершение всего 22 декабря компания опубликовала пресс-релиз, в котором признала себя единственным держателем авторских прав на System V. Обиженная, SCO 20 января 2004 года обратилась в суд, потребовав от Novell передачи всех зарегистрированных накануне прав.

Вернёмся на несколько месяцев назад, в день 6 августа 2003 года, когда IBM подала встречный иск против SCO. В нём она обвинила компанию по нескольким пунктам, большая часть из которых в той или иной форме копировали таковые в аналогичном документе, поданном против «Голубого гиганта» несколько месяцев назад. Однако среди них нашлись и два новых подраздела, касавшиеся нарушения SCO четырёх патентов IBM, а также лицензии GPL. Небольшого пояснения требует как раз второй пункт.

До покупки прав на System V главной деятельностью SCO была разработка и продажа собственного дистрибутива Linux под названием OpenLinux. По словам одного из юристов организации Free Software Foundation Эбена Моглена (Eben Moglen): «С момента, когда SCO начала, посредством своего дистрибутива, распространять код под лицензией GPL, она тем самым дала каждому пользователю в мире право на его бесплатное копирование, модификацию и распространение. Это непосредственным образом касается и ядра Linux. Компания самостоятельно лицензировала его всему миру».

Так что ещё до начала судебного разбирательства с IBM SCO самостоятельно «вырыла себе глубокую яму». Впоследствии компания объявила о прекращении распространения OpenLinux, а также выступила с заявлением, гласившим: «За любой исходный код, который, возможно, был выпущен SCO под лицензией GPL, отвечают сотрудники компании, сделавшие это без необходимой юридической авторизации. В результате данный код не может считаться легитимным с позиции GPL-лицензирования».

Ещё одной компанией, ставшей на защиту Linux, стала компания Red Hat. 4 августа она подала иск против SCO, обвинив её в ущемлении прав пользователей программного обеспечения с открытым исходным кодом и Linux в частности.

Дальнейшее развитие столь шумевшего судебного процесса было продолжено 30 сентября 2003 года, когда, согласно решению федерального судьи Дейла Кимболла (Dale Kimball), SCO был дан месячный срок на предоставление примеров исходного кода из System V, которые, по её мнению, были нелегально скопированы в Linux и являются предметом судебного иска.

Срок действия решения Кимболла закончился 1 июля 2005 года, однако даже спустя полтора года SCO так и не предоставила необходимых данных. Нет, фрагменты кода компания представила ещё осенью 2003 года, однако полный список так и не был предъявлен.


В результате в «Постановлении об уменьшении количества претензий, предъявленных SCO к IBM», которое было опубликовано 28 июня 2006 года, федеральный судья Брук Велс (Brooke Wells), представляющая новые факты по данному судебному процессу, лишила SCO прав на предъявление претензий по 187 из 298 пунктов судебного иска, мотивируя своё решение их недостаточной обоснованностью. Оставшиеся 111 пунктов ещё не были рассмотрены в суде из-за отсутствия необходимых данных.

После вынесения судьёй Велс промежуточного решения акции SCO упали до отметки один доллар за штуку.

Что же касается Novell, ещё 29 июля 2005 года она подала ответный иск против SCO, обвинив её в клевете, нарушении условий контракта, а также отказе от проведения тщательного изучения документов. Сумма затребованной компанией компенсации была больше стоимости самой SCO, поэтому в случае проигрыша она должна была обанкротиться.

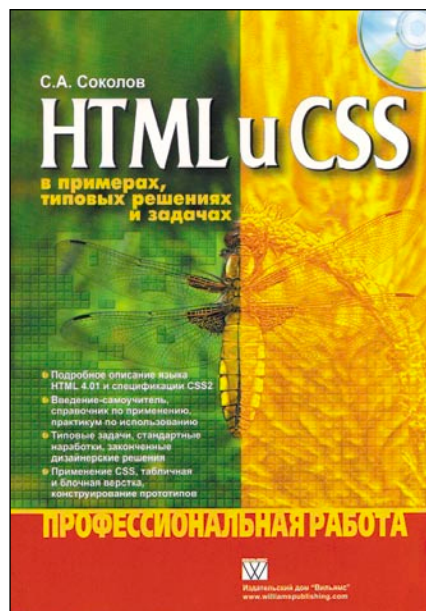
**Сильная сторона Open Source одновременно является и её слабостью: открытый исходный код большинства программ значительно облегчает компаниям поиск «зацепок», которые затем можно поставить «на кону» очередного судебного иска.**

К декабрю 2006 года стало ясно, что основные «боевые действия» развернутся как раз на поле битвы между SCO и Novell. Исход этого разбирательства и предопределил дальнейшее развитие событий в отношении иска SCO против IBM. Однако по состоянию на начало 2007 года судебные слушания по этому поводу были всё ещё не прекращены. Сегодня SCO – фактически банкрот. Согласно отчёту за последний финансовый квартал, опубликованному 17 января 2007 года, в активе у компании осталось менее 13 млн. долларов. С такими показателями SCO уже в середине этого года попросту не сможет продолжать финансировать свои судебные разбирательства. Как говорилось в сказке: «И осталась она у разбитого корыта...»

Борьба за выживание – извечная проблема. Присуща она и современным компаниям, работающим в сфере IT. Дабы узаконить свою продукцию на рынке, уберечь её от посягательств конкурентов, а также отстоять своё имя и престиж, фирмам приходится вступать в не менее свирепые и беспощадные войны. Остается лишь надеяться, что их «поле битвы» никогда не выйдет за стены зала суда. 

1. <http://www.appleinsider.com>.
2. <http://www.theregister.co.uk>.
3. <http://www.zdnet.com>.
4. <http://www.cnet.com>.
5. <http://blog.wired.com>.
6. <http://www.usatoday.com>.
7. <http://www.wikipedia.org>.





Книга разделена на 4 части: введение и «курс молодого бойца», основы HTML, основы CSS, типовые решения.

При этом знакомиться с предлагаемым базовым «курсом», начинающим сразу после краткого представления общих понятий, неопытным HTML-кодерам рекомендуется только

## HTML и CSS в примерах, типовых решениях и задачах. Профессиональная работа

Сергей Соколов

после того как они прочитают основы HTML и CSS.

В «курсе молодого бойца» первым делом рассматривается создание элементарной «визитки» с простым форматированием текста, а затем постепенно рассказывается о применении привычных возможностей оформления Web-страниц: взаимодействие HTML с каскадными таблицами стилей, ссылки и изображения, списки, таблицы, блоки и слои, формы, фреймы, внедрение скриптов на JavaScript (есть пример парсинга данных из XML).

В части, посвященной основам HTML (версии 4.01), перечислены наиболее популярные теги с многочисленными примерами их использования на практике. Аналогично и для основ CSS – только теперь обзору подлежат различные свойства текста, цве-

та, списков, блоков, таблиц, а также фильтры и трансформации для браузера Internet Explorer.

В типовых решениях можно найти рецепты по реализации более сложных вещей. Здесь уже автор, активно оперируя знаниями, которые читатель получил в начале книги, обучает актуальным приемам – например, верстке на div'ax. Все приводимые листинги сопровождаются комментарием с именем файла, который вы найдете на прилагаемом к книге компакт-диске.

- Издательство: «Вильямс»
- Год издания: 2007
- Количество страниц: 416
- ISBN: 978-5-8459-1192-6
- Цена: ≈ 232 руб.

Книга предоставлена издательством «Вильямс».



Емкое определение содержимому дается уже в предисловии: «В этой книге мы представим путеводитель для перехода программной индустрии от кустарного производства к промышленному...».

Само явление, «фабрики программного обеспечения» достаточно ново и, возможно, знакомо еще немногим.

## Фабрики разработки программ: потоковая сборка типовых приложений, моделирование структуры и инструменты

Джек Гринфилд, Кит Шорт, Стив Кук, Стюарт Кент, Джон Крупи

Но примечательно, что оно родилось как попытка добиться всеми желаемых эффектов при разработке ПО – высоких показателей таких параметров, как скорость, автоматизация, оптимизированность и качество.

При этом немаловажно, что над книгой работали специалисты Microsoft, а уж насколько доверять им в подобных вопросах – дело каждого.

По понятным причинам существенную часть издания составляет введение. И даже в нем само представление «фабрик» выдвигается лишь вслед за продолжительным анализом причин их возникновения и проблем у других существующих технологий и методик.

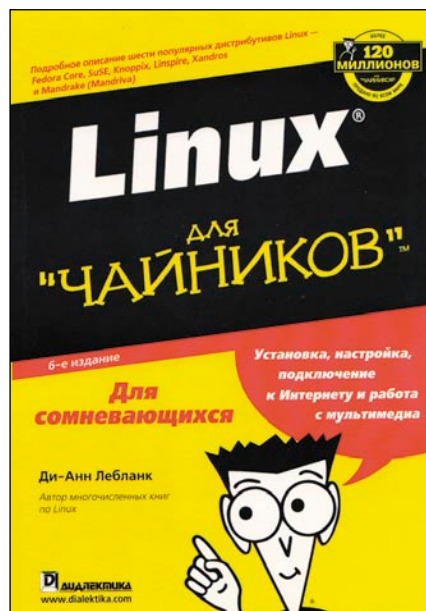
В разделе «Критические инновации» рассматриваются различные под-

ходы к моделям и программирование с их использованием, а затем – отдельные программы и линейки продуктов, компонентные архитектуры, трансформации и их применение.

В последних же главах подробно описан пример «фабрики ПО» и приведены ответы на часто задаваемые вопросы (например, проведено сравнение «фабрик» с RAD, MDA), а в приложениях – информация по абстракциям и UML.

- Издательство: «Вильямс»
- Год издания: 2007
- Количество страниц: 512
- ISBN: 978-5-8459-1181-0
- Цена: ≈ 396 руб.

Книга предоставлена издательством «Вильямс».



Главная отличительная черта издания соответствует его названию – легкий стиль изложения материала и утомляющая профессионалов дотошность в описании простейших вещей.

Однако во время чтения подробных инструкций невольно вспоминается, что так или иначе общение с новичками сводится именно к такому уровню.

## Linux для «чайников», 6-е издание

Ди-Анн Лебланк

Читателя знакомят с основными понятиями из области Linux и Free Software и тем, откуда все это берет начало. Далее рассматривается 6 дистрибутивов: Fedora Core, Linspire, Mandriva, SUSE, Xandros, Knoppix. Для всех, кроме последнего, описан процесс установки (особенно подробно – для Fedora Core). После этого рассказывается о процессе загрузки установленной операционной системы, представляются основы работы в графическом интерфейсе (GNOME и KDE) и приводится краткий обзор средств настройки рассматриваемых дистрибутивов.

Вторая часть книги посвящена подключению к Интернету и работе в нем (Mozilla, Evolution, Gaim).

В третьей части – основы работы в системе: устройство файловой системы и управление файлами (Nautilus, Konqueror), установка и обновление пакетов программного обеспечения (опять же для всех рассматриваемых

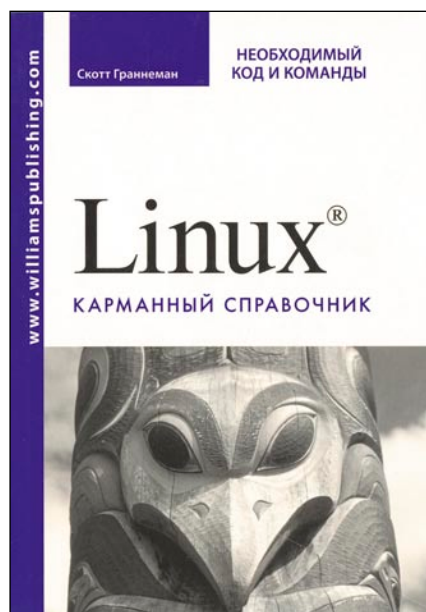
дистрибутивов, кроме Knoppix), базовая безопасность (здесь же – SSH), работа в bash, некоторые настройки рабочего стола.

В четвертой части рассмотрены популярные пакеты ПО: текстовые редакторы, OpenOffice.org, мультимедийные приложения, эмуляторы. В конце книги – решение популярных проблем и способы применения Knoppix.

Основной минус книги – она несколько устарела. Так, например, в ней рассматривается установка Fedora Core 3, а энтузиасты уже активно знакомятся с Fedora 7. Оригинал был написан в 2005 году – за это время мир Linux успел сильно измениться...

- Издательство: «Вильямс»
- Год издания: 2007
- Количество страниц: 464
- ISBN: 978-5-8459-1032-5
- Цена: ≈ 157 руб.

Книга предоставлена издательством «Вильямс».



Несмотря на предположение автора, что этот карманный справочник окажется полезным и для начинающих, и для опытных пользователей, актуальность для последних несколько преувеличена. Тем не менее книге удалось избежать участи стать очередной попыткой перепечатать страни-

## Linux. Карманный справочник

Скотт Граннеман

цы мануала в сжатом виде. Она предстает в виде добротного и компактного источника информации для тех, кто начинает или продолжает знакомиться с Linux и кому при этом интересна командная строка.

Автор, осветив общие моменты работы в консоли и объяснив, как получить справку по тем или иным командам, переходит к описанию более сложных приемов: объединение команд, перенаправления, межпроцессный канал, а затем – некоторым возможностям bash, упрощающим жизнь (история, алиасы...). Вдобавок к этому описываются решения различных задач, сгруппированных по классу. Среди них, например, можно выделить просмотр файлов (cat, less, head, tail) и печать (lpstat, lpr, lpq...), права доступа к файлам/каталогам (не забыты suid/sgid, sticky bit), архивация (zip, tar, gzip, bzip2), поиск (как по содержи-

мому – grep, так и по именам файлов/каталогов – locate и отдельно утилита find), системный мониторинг (ps, top, df...), сеть (ifconfig, ping, route...) и популярные сетевые клиенты/приложения (ssh, sftp, rsync, wget...).

В самостоятельные главы вынесены управление пакетами программного обеспечения (RPM и yum, dpkg и APT) и Samba для взаимодействия с Windows (nmblookup, smbclient, smbmount). Справочник содержит подробные (иногда даже кажется, что излишне подробные) примеры, иллюстрирующие действия тех или иных команд.

- Издательство: «Вильямс»
- Год издания: 2007
- Количество страниц: 416
- ISBN: 978-5-8459-1118-6
- Цена: ≈ 110 руб.

Книга предоставлена издательством «Вильямс».

Обзор книжных новинок подготовил Дмитрий Шурупов

# Редакционная подписка для физических лиц

- Вы можете оформить подписку на любой российский адрес.
- При заполнении квитанции **обязательно РАЗБОРЧИВО** укажите фамилию, имя, отчество полностью, почтовый индекс и адрес получателя (область, город, улица, номер дома, номер квартиры), контактный телефон.
- Вы можете оформить подписку с любого месяца на любой срок.
- В графе «Сумма» проставьте сумму за выбранное количество номеров. Стоимость одного номера журнала **150 руб.** За 10 месяцев (с марта по декабрь) – **1500 руб.** НДС и почтовые расходы включены в стоимость.
- Журнал высылается почтой простой бандеролью только после поступления денег на расчетный счет и **копии заполненного и оплаченного бланка, отправленной в редакцию по факсу: (495) 628-82-53 или на электронный адрес: info@samag.ru.**

<b>ИЗВЕЩЕНИЕ</b>	<div style="text-align: right; font-size: small;">Форма № ПД-4</div> <p><b>ЗАО Издательский дом "Учительская газета"</b>  <b>ИНН 7710058015/ КПП 771001001</b>  <b>Р. сч. 40702810600000013101 К. сч. 30101810300000000985</b>  <b>"НОМОС-БАНК" г.Москва БИК 044525985</b>  <b>Коды: по ОКПО 02577005, по ОКОНХ 87100, по ОКОПФ 07774</b></p> <hr style="border-top: 1px dashed black;"/> <p style="text-align: center;"><b>Вид платежа: Редакционная подписка на журнал "Системный администратор" за 2007 г.</b></p> <table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <tr> <td>01</td><td>02</td><td>03</td><td>04</td><td>05</td><td>06</td><td>07</td><td>08</td><td>09</td><td>10</td><td>11</td><td>12</td> </tr> <tr> <td> </td><td> </td><td> </td><td> </td><td> </td><td> </td><td> </td><td> </td><td> </td><td> </td><td> </td><td> </td> </tr> </table> <p>Дата _____ Сумма платежа: _____ руб. _____ коп.</p> <p><b>Информация о плательщике:</b></p> <p>_____</p> <p style="text-align: center; font-size: x-small;">(Ф. И. О. почтовый индекс, адрес и телефон)</p> <p>_____</p> <p>_____</p> <p style="text-align: right;">Подпись _____</p>	01	02	03	04	05	06	07	08	09	10	11	12												
01	02	03	04	05	06	07	08	09	10	11	12														
Кассир																									
<b>КВИТАНЦИЯ</b>	<div style="text-align: right; font-size: small;">Форма № ПД-4</div> <p><b>ЗАО "Издательский дом "Учительская газета"</b>  <b>ИНН 7710058015/ КПП 771001001</b>  <b>Р. сч. 40702810600000013101 К. сч. 30101810300000000985</b>  <b>"НОМОС-БАНК" г.Москва БИК 044525985</b>  <b>Коды: по ОКПО 02577005, по ОКОНХ 87100, по ОКОПФ 07774</b></p> <hr style="border-top: 1px dashed black;"/> <p style="text-align: center;"><b>Вид платежа: Редакционная подписка на журнал "Системный администратор" за 2007 г.</b></p> <table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <tr> <td>01</td><td>02</td><td>03</td><td>04</td><td>05</td><td>06</td><td>07</td><td>08</td><td>09</td><td>10</td><td>11</td><td>12</td> </tr> <tr> <td> </td><td> </td><td> </td><td> </td><td> </td><td> </td><td> </td><td> </td><td> </td><td> </td><td> </td><td> </td> </tr> </table> <p>Дата _____ Сумма платежа: _____ руб. _____ коп.</p> <p><b>Информация о плательщике:</b></p> <p>_____</p> <p style="text-align: center; font-size: x-small;">(Ф. И. О. почтовый индекс, адрес и телефон)</p> <p>_____</p> <p>_____</p> <p style="text-align: right;">Подпись _____</p>	01	02	03	04	05	06	07	08	09	10	11	12												
01	02	03	04	05	06	07	08	09	10	11	12														
Кассир																									



## Российская Федерация

- Подписной индекс: годовой – **20780**, полугодовой – **81655**  
Каталог агентства «Роспечать»
- Подписной индекс: **87836**  
Объединенный каталог «Пресса России»  
Адресный каталог «Подписка за рабочим столом»  
Адресный каталог «Библиотечный каталог»
- Альтернативные подписные агентства:  
Агентство «Интер-Почта» (495) 500-00-60, курьерская доставка по Москве  
Агентство «Вся Пресса» (495) 787-34-47  
Агентство «Курьер-Пресссервис»  
Агентство «ООО Урал-Пресс» (343) 375-62-74  
ЛинуксЦентр [www.linuxcenter.ru](http://www.linuxcenter.ru)
- Подписка On-line  
<http://www.arzi.ru>  
<http://www.gazety.ru>  
<http://www.presscafe.ru>

## СНГ

В странах СНГ подписка принимается в почтовых отделениях по национальным каталогам или по списку номенклатуры «АРЗИ»:

- **Азербайджан** – по объединенному каталогу российских изданий через предприятие по распространению

печати «Гасид» (370102, г. Баку, ул. Джавадхана, 21)

- **Казахстан** – по каталогу «Российская Пресса» через ОАО «Казпочта» и ЗАО «Евразия пресс»
- **Беларусь** – по каталогу изданий стран СНГ через РГО «Белпочта» (220050, г. Минск, пр-т Ф. Скорины, 10)
- **Узбекистан** – по каталогу «Davriy nashrlar» российские издания через агентство по распространению печати «Davriy nashrlar» (7000029, г. Ташкент, пл. Мустакиллик, 5/3, офис 33)
- **Армения** – по списку номенклатуры «АРЗИ» через ГЗАО «Армпечать» (375005, г. Ереван, пл. Сасунци Да-вида, д. 2) и ЗАО «Контакт-Мамул» (375002, г. Ереван, ул. Сарьяна, 22)
- **Грузия** – по списку номенклатуры «АРЗИ» через АО «Сакпресса» (380019, г. Тбилиси, ул. Хошараульская, 29) и АО «Мацне» (380060, г. Тбилиси, пр-т Гамсахурдия, 42)
- **Молдавия** – по каталогу через ГП «Пошта Молдовей» (МД-2012, г. Кишинев, бул. Штефан чел Маре, 134) по списку через ГУП «Почта Приднестровья» (МД-3300, г. Тирасполь, ул. Ленина, 17) по прайс-листу через ООО Агентство «Editil Periodice» (МД-2012, г. Кишинев, бул. Штефан чел Маре, 134)
- Подписка для **Украины**:  
Киевский главпочтамт  
Подписное агентство «KSS», тел./факс (044)464-0220

Ф.СП-1

Министерство связи РФ

АБОНЕМЕНТ на журнал

Системный

администратор

(индекс издания)

Количество  
комплектов:

на 200 год по месяцам

1	2	3	4	5	6	7	8	9	10	11	12

Куда (почтовый индекс)

(адрес)

Кому

(фамилия, инициалы)

ДОСТАВОЧНАЯ КАРТОЧКА

ПВ

место

ли-  
тер

на журнал

(индекс издания)

Системный  
администраторСтои-  
мостьпо каталогу  
за доставкуруб. коп.  
руб. коп.Количество  
комплектов:

на 200 год по месяцам

1	2	3	4	5	6	7	8	9	10	11	12

Куда

(почтовый индекс)

Кому

(адрес)

(фамилия, инициалы)

**Подписные  
индексы:**

**20780\***  
**81655\*\***

**по каталогу  
агентства  
«Роспечать»**

**87836**

**по каталогу  
агентства  
«Пресса  
России»**

\* **годовой**  
\*\* **полугодовой**

**УЧРЕДИТЕЛИ**

Владимир Положевец  
Александр Михалев  
**РУКОВОДИТЕЛЬ ПРОЕКТА**  
Петр Положевец

**РЕДАКЦИЯ**

**Исполнительный директор**  
Владимир Положевец  
**Ответственный секретарь**  
Наталья Хвостова  
sekretar@samag.ru  
**Технический редактор**  
Владимир Лукин  
**Главный редактор**  
**электронного приложения**  
**«Open Source»**  
Дмитрий Шурупов  
**Внештатные редакторы**  
Алексей Барабанов  
Андрей Бирюков  
Андрей Шетухин  
Рашид Ачилов

**РЕКЛАМНАЯ СЛУЖБА**

тел./факс: (495) 628-8253  
Евгения Тарабрина  
reclama@samag.ru

**Верстка и оформление**

maker\_up@samag.ru

**Дизайн обложки**

Дмитрий Репин  
Николай Петрович

**По вопросам распространения**  
**обращайтесь по телефону:**  
(495) 628-8253 (доб. 120)

107045, г. Москва,  
Ананьевский переулок, дом 4/2, стр. 1  
тел./факс: (495) 628-8253  
Сайт журнала: [www.samag.ru](http://www.samag.ru)

**ИЗДАТЕЛЬ**

ЗАО «Издательский дом  
«Учительская газета»

**Отпечатано типографией**

ГП «Московская Типография №13»  
Тираж 15000 экз.

Журнал зарегистрирован  
в Министерстве РФ по делам печати,  
телерадиовещания и средств массо-  
вых коммуникаций (свидетельство  
ПИ № 77-12542 от 24 апреля 2002 г.).

За содержание статьи ответственность  
несет автор. За содержание реклам-  
ных материалов ответственность не-  
сет рекламодатель. Все права на опу-  
бликованные материалы защищены.

# ЧИТАЙТЕ В СЛЕДУЮЩЕМ НОМЕРЕ:



## Групповые политики в доменах AD

Администратору локальной сети по роду своей деятельности на сознательность пользователей надеяться не приходится. В связи с этим появляется необходимость обезопасить рабочую среду всего предприятия и уберечь пользователей от их же бездумных действий. Назидания отдела IT для них, как правило, пустое сотрясение воздуха, а установка запретов на основе разрешений NTFS в средних и крупных предприятиях – задача слишком объемная. В этом случае для выполнения административных задач в доменах Active Directory компания Microsoft предлагает использование групповых политик. Подробности – в следующем выпуске журнала.

## Библиотека Prototype – ваш путь в Web-2

Требования к веб-разработке постоянно растут. Если для какого-нибудь программиста примером идеального пользовательского интерфейса является сайт lib.ru, то обычный пользователь такой аскетизм, скорее всего, не оценит, и самое страшное – не оплатит. Однако работа, направленная на повышение удобства и практичности пользовательского интерфейса зачастую отнимает много времени, которое хотелось бы потратить на разработку бизнес-логики приложения.

Разработчики настольных систем имеют в своем арсенале такие средства как MFC, Gtk, Qt и другие библиотеки. Обеспечить комфортную жизнь веб-разработчику поможет библиотека Prototype, о ней пойдет речь в июльском номере журнала.

## Технология NLB: отказоустойчивость без лишних затрат

Решения по обеспечению отказоустойчивости на сегодняшний день широко распространены и разнообразны: от дорогостоящих аппаратных комплексов до недорогих программных кластеров. Одним из недорогих средств является Network Load Balancing, служба, входящая в состав Windows Server 2003. Об особенностях ее настройки читайте в следующем номере.

## BusyBox: швейцарский нож для встраиваемых Linux-систем

Системные администраторы и пользователи UNIX/Linux-систем, несомненно, привыкли к работе со своей любимой командной оболочкой и к стандартным программным средствам. Но их повсеместное использование не всегда возможно. И тогда на помощь приходит BusyBox – упрощенный shell с набором компактных системных средств. Обзор BusyBox читайте в июльском выпуске.

## Уважаемые читатели!

**Продолжается подписка на 2-ое полугодие 2007 года.**

Приобрести новые и старые номера журнала  
вы можете через интернет-магазин [LinuxCenter.ru](http://LinuxCenter.ru).



Доставка почтой в любую точку России.