

Так видит журнал читатель, который забыл оформить подписку:

НОВОГОДНИЕ  
КАНИКУЛЫ ЗАТЯНУЛИСЬ

БЫСТРО РАСКУТИЛИ  
ТИРАЖ

УЕХАЛ В ОТПУСК

ПОСЛЕ ОТПУСКА  
АВРАТ НА РАБОТЕ

НЕОЖИДАННО  
ЗАКОНЧИТСЯ ДЕНЬГИ

Так видит журнал читатель, оформивший подписку:

ПОДПИШИТЕСЬ И ЧИТАЙТЕ!

Роспечать – 20780, 81655  
Пресса России – 88099, 87836  
Интер-почта – тел. (495) 500-00-60

№6(79) июнь 2009  
подписной индекс 20780  
www.samag.ru

Организуем систему резервного копирования для малого и среднего офиса

Windows 7: продолжаем знакомство

Доступная виртуализация: Citrix XenServer 5.0

Корпоративные VPN на базе Cisco

Система видеоконференций OpenMeetings

Построение каталога сервисов

Защита данных с помощью AD Rights Management Services

Обзор проекта Gnash

«Доктор Веб» дал старт первому российскому антивирусу для Mac OS X





ДВАДЦАТАЯ ЕЖЕГОДНАЯ ВЫСТАВКА  
ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

**SoftTool**

ВСЕРОССИЙСКАЯ НАУЧНО-ПРАКТИЧЕСКАЯ КОНФЕРЕНЦИЯ  
«ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В РОССИИ»  
КОНКУРС ЛУЧШИХ ПРОГРАММНЫХ ПРОДУКТОВ «ПРОДУКТ ГОДА»  
СОФТУЛИЙСКИЕ ИГРЫ

27-30 ОКТЯБРЯ 2009 ГОДА

ВТОРАЯ ЕЖЕГОДНАЯ ВЫСТАВКА  
ПЕРЕДОВЫХ РОССИЙСКИХ РАЗРАБОТОК, ПРОДУКТОВ И УСЛУГ

«ТЕХНОЛОГИИ ЭЛЕКТРОННОГО ГОСУДАРСТВА»

НАЦИОНАЛЬНЫЙ ФОРУМ

«ИНФОРМАЦИОННОЕ ОБЩЕСТВО, ЭЛЕКТРОННОЕ ГОСУДАРСТВО,  
ЭЛЕКТРОННОЕ ПРАВИТЕЛЬСТВО»

КРУГЛЫЙ СТОЛ С РУКОВОДИТЕЛЯМИ ИНФОРМАТИЗАЦИИ РЕГИОНОВ РОССИИ  
КОНФЕРЕНЦИЯ ПО СТАНДАРТИЗАЦИИ ИТ И ИНТЕРОПЕРАБЕЛЬНОСТИ

«SITOP 2009»



МОСКВА • ВВЦ • ПАВИЛЬОН 69

ВОСЬМАЯ ЕЖЕГОДНАЯ ВЫСТАВКА  
СИСТЕМ АВТОМАТИЗАЦИИ ПРОЕКТИРОВАНИЯ



КОНКУРС ИНЖЕНЕРНЫХ ПРОЕКТОВ «ТВОРЕЦ»  
САПР-ШОУ, «ВЕНДОРЫ БЕЗ ГАЛСТУКОВ»  
БЕСПЛАТНАЯ СЕРТИФИКАЦИЯ СПЕЦИАЛИСТОВ  
МАСТЕР-КЛАССЫ, ТОК-ШОУ, ПРЕЗЕНТАЦИИ

На выставке **SoftTool** Вы сможете познакомиться со всеми  
предложениями мирового рынка ПО



Организатор: компания «ИТ-ЭКСПО»  
Тел.: +7 (495) 624-7072, e-mail: softtool@softtool.ru



открытые  
системы



С К  
пресс



G NEWS

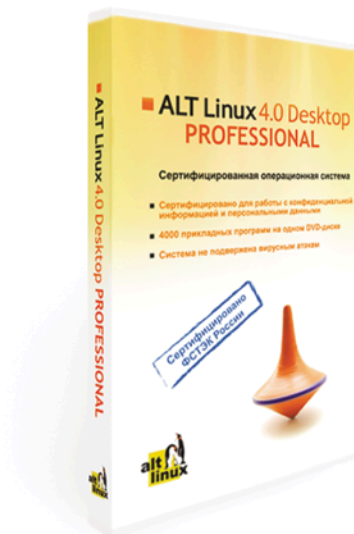
Пригласительные  
билеты на  
www.softtool.ru

# Сертифицированные продукты ALT Linux

## Для кого предназначены сертифицированные продукты?

- Для **организаций**, которым необходимо иметь **сертифицированное ПО**. Это многие государственные учреждения, оборонные предприятия и т.д.;
- Для **организаций**, работающих с **конфиденциальной информацией и персональными данными**. Под эту категорию попадают практически все фирмы, имеющие базу данных паспортов, номеров сотовых телефонов и т.п. (туристические фирмы, страховые компании, банки и т.д.), фирмы, проводящие анкетирование.

## ALT Linux 4.0 Desktop Professional сертифицированный продукт для рабочих станций



ALT Linux 4.0 Desktop Professional сертифицирован Федеральной службой по техническому и экспортному контролю (ФСТЭК России).  
Сертификат соответствия №1649 от 23 июля 2008:

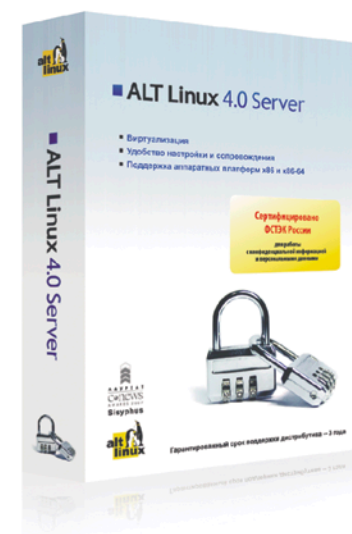
- Классификация по уровню контроля отсутствия недеklarированных возможностей (НДВ) — **4 уровень**.
- Показатели защищенности от несанкционированного доступа к информации (СВТ) — по **5 классу защищенности**.

ALT Linux 4.0 Desktop Professional — это:

- Удобная в работе операционная система, дающая пользователю возможность решать обычные задачи, не опасаясь вирусов и не затрачивая время на поиск нужных прикладных программ в сети Интернет и на полках магазинов;
- Дружественная программа установки, работа с которой будет особенно приятна начинающим пользователям;
- ALTerator — интуитивно понятный инструмент настройки и управления системой.

Рекомендуемая розничная цена: **3800 руб.**

## ALT Linux 4.0 Server Edition сертифицированный продукт для серверов



Всё, что можно сделать по настройке сервера без вмешательства пользователя, уже реализовано в дистрибутиве **ALT Linux 4.0 Server Edition**.

ALT Linux 4.0 Server Edition сертифицирован Федеральной службой по техническому и экспортному контролю (ФСТЭК России).

Сертификат соответствия №1501 от 8 ноября 2007:

- Классификация по уровню контроля отсутствия недеklarированных возможностей — **4 уровень**.
- Показатели защищенности от несанкционированного доступа к информации — по **5 классу защищенности**.

ALT Linux 4.0 Server Edition — серверный дистрибутив с широким спектром возможностей, включающий комплект готовых решений для актуальных задач организации: построения корпоративной сети и среды обмена информацией. Простые веб-интерфейсы управления, включённые в дистрибутив, позволяют существенно ускорить развёртывание корпоративного сервера.

Рекомендуемая розничная цена: **22000 руб.**

www.altlinux.ru

По вопросам приобретения: zakaz@altlinux.ru





## РЕПОРТАЖ

- 4 В Москве прошел пятый Форум по открытому коду**  
Ключевые события мероприятия.  
*Дмитрий Шурупов*

- 8 «Айдеко» представила интернет-шлюз IdecO ICS 3.0**  
19 мая состоялась пресс-конференция компании «Айдеко», приуроченная к выходу третьей версии ключевого решения компании – интернет-шлюза IdecO ICS.  
*Дмитрий Шурупов*

- 10 Новые беспроводные решения от Cisco**  
Компания Cisco представила новые решения в области беспроводных мобильных сетей связи семейства стандартов 802.11.  
*Андрей Бирюков*

## ТЕНДЕНЦИИ

## АДМИНИСТРИРОВАНИЕ

- 14 Организуем систему резервного копирования для малого и среднего офиса**  
Как создать простую систему резервного копирования, не требующую больших затрат, но при этом обеспечивающую необходимую надежность и управляемость.  
*Алексей Бережной*

- 24 Новые методы защиты и управления информацией**  
Используем программные продукты компании Paragon Software для решения проблем, связанных с защитой информации.  
*Сергей Соломатин*

- 26 Резервирование и восстановление объектов Active Directory в Windows Server 2008/2008R2**  
Подробно рассмотрим вопросы восстановления службы каталогов.  
*Сергей Яремчук*

- 32 Windows 7: продолжаем знакомство**  
Разочарованы в Windows Vista? Считаете, что ОС Windows 7 – это новая обертка старой операционной системы? Не торопитесь с выводами, Windows 7 есть чем удивить технического специалиста.  
*Илья Рудь*

- 37 Решение давно наболевшей проблемы**  
Вы когда-нибудь считали, сколько времени вы тратите на то, чтобы определить, какой кабель к чему относится? А сколько раз вам приходилось бегать с прозвонкой из серверной в кабинеты и обратно, пытаясь разобраться с давно забытой розеткой?  
*Денис Староверов*

- 38 Мониторинг Cisco IDS/IPS на примере модуля IDSM2 с помощью MRTG. Часть 2**  
Перед администратором систем обнаружения вторжений возникают вопросы рациональности использования ресурсов, соответствия заявленных производителем параметров реальным данным, возможности распределения сенсоров различной мощности по разным участкам сети. Для решения подобных задач может пригодиться MRTG.  
*Андрей Дугин*

- 40 Делегируем права на перемещение учетных записей пользователей в Active Directory. Часть 4**  
Завершаем разработку основного класса надстройки для Windows Server 2003, позволяющую разделить полномочия перевода пользователя из одного отдела в другой между локальными администраторами подразделений. Также рассмотрим использование регулярных выражений для упрощения обработки строк.  
*Вадим Андросов*

- 48 Доступная виртуализация: Citrix XenServer 5.0**  
Особенности эксплуатации программного продукта.  
*Андрей Панченко*

- 54 Построение каталога сервисов**  
Повышаем эффективность работы IT-службы.  
*Александр Башкиров*

- 58 Система видеоконференций OpenMeetings**  
Существенную часть времени сотрудники тратят на общение и обмен данными, поэтому актуальным становится применение систем конференц-связи, среди которых особую роль играют системы видеоконференций. Рассмотрим возможности и установку системы видеоконференций OpenMeetings.  
*Сергей Яремчук*

- 66 Обзор проекта Gnash**  
Часто у проприетарных программ, имеющих большую популярность, появляется свободная реализация. Одним из таких продуктов и стал Gnash – альтернатива закрытому флеш-плееру компании Adobe.  
*Игорь Штомпель*

## БЕЗОПАСНОСТЬ

- 70 Защита данных с помощью Active Directory Rights Management Services**  
Функционал, архитектура и возможности RMS.  
*Андрей Бирюков*

- 77 «Доктор Веб» дал старт первому российскому антивирусу для Mac OS X**  
Особенности нового продукта.  
*Валерий Ледовской*

## СЕТИ

- 78 Корпоративные VPN на базе Cisco**  
Преимущества и недостатки технологий построения VPN-туннеля: IPSec VPN Site-to-Site, Easy-VPN и DMVPN на базе маршрутизаторов Cisco.  
*Иван Панин*

## АДМИНИСТРИРОВАНИЕ «1С»

- 87 Очередное собрание ошибок**  
Прочитай и не делай так.  
*Андрей Луконькин*

## ЧЕЛОВЕК НОМЕРА

- 88 Романтик**  
Интервью с Дмитрием Курашевым, совладельцем и CEO компании Entensys.  
*Оксана Родионова*

65, 85, 86 BUGTRAQ

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

администратор

Стои-мость

по каталогу

руб. коп.

Количество комплектов:

за доставку

руб. коп.

на 200 год по месяцам

1	2	3	4	5	6	7	8	9	10	11	12

Куда

(почтовый индекс)

Кому

(адрес)

(фамилия, инициалы)

ИЗВЕЩЕНИЕ

ООО "С 13"

ИНН 7708654814/ КПП 770801001

Р.сч. 40702810300080001868 К.сч. 30101810100000000787

ОАО «УРАЛСИБ» г. Москва БИК 044525787

Коды: по ОКПО 84027582, по ОКОНФ 65

Форма № ПД-4

Вид платежа: Редакционная подписка на журнал "Системный администратор" за 2009 г.

01	02	03	04	05	06	07	08	09	10	11	12
						X	X	X	X	X	X

Дата

Сумма платежа: 1200 руб. 00 коп.

Информация о плательщике:

(Ф. И. О. почтовый индекс, адрес и телефон)

Подпись

Кассир

КВИТАНЦИЯ

ООО "С 13"

ИНН 7708654814/ КПП 770801001

Р.сч. 40702810300080001868 К.сч. 30101810100000000787

ОАО «УРАЛСИБ» г. Москва БИК 044525787

Коды: по ОКПО 84027582, по ОКОНФ 65

Форма № ПД-4

Вид платежа: Редакционная подписка на журнал "Системный администратор" за 2009 г.

01	02	03	04	05	06	07	08	09	10	11	12
						X	X	X	X	X	X

Дата

Сумма платежа: 1200 руб. 00 коп.

Информация о плательщике:

(Ф. И. О. почтовый индекс, адрес и телефон)

Подпись

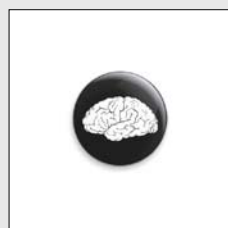
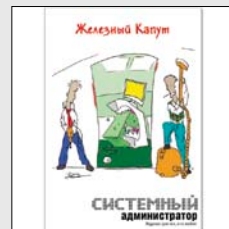
Кассир



printdirect

СИСТЕМНЫЙ администратор

Все товары:

[Футболки](#)[Постеры](#)[Кружки](#)[Значки](#)[Коврики для мышки](#)



Прогноз погоды на второе полугодие 2009.

В журнале «Системный администратор» ожидаются новые захватывающие и полезные статьи, истории известных компаний и отдельных продуктов.

Небо над админами будет безоблачное, обзоры выставок, конференций и других мероприятий в журнале позволят вам реже отрываться от компьютеров.

Июль будет ветреным и закончится солнечным Днем системного администратора.

Информация о сертификации, учебных центрах и комментарии экспертов по вопросам IT-сферы придут с севера.

Обильные осадки в виде админских призов выпадут в октябре. Во избежание похолодания не забудьте оформить подписку.



Все знают, что в редакции нашего журнала живет Админский приз. Мы называем его просто Приз. Случилось так, что к 2009 году Админский приз вырос и приобрел необыкновенные свойства. Он так и тянется к самым любознательным, опытным и общительным. А еще Приз стал очень капризным: он утверждает, что достанется только тем, кто даст правильные ответы на его загадки. Приз также обожает слушать истории. Любит интересные рассказы и с удовольствием сидит на форумах.

Приглашаем вас принять участие в розыгрыше призов «**Админский приз 2009**». Вам понадобится собрать коды из журналов и получить дополнительные коды за активность на форуме, за победы на чемпионате по игре «АУТСОРСЕР», за правильные ответы на задачи. Дополнительные коды увеличивают ваши шансы на победу!

Розыгрыш будет проходить в три этапа:

- I – участвуют коды из №7, 8, 9 за 2009 год и дополнительные коды, полученные с июля по август.
- II – участвуют коды из №10, 11, 12 за 2009 год и дополнительные коды, полученные с октября по декабрь.
- III – участвуют коды из всех шести номеров журнала за 2-е полугодие 2009 года и дополнительные коды, полученные участниками за весь период проведения конкурса.

Не так давно по адресу [http://www.samag.printdirect.ru/?partner\\_id=6206](http://www.samag.printdirect.ru/?partner_id=6206) открылась «Лавка админа», где можно приобрести разнообразные сувениры от журнала «Системный администратор».

Так полюбившийся вам на пакетах мозг запросто окажется ковриком у вас на столе.

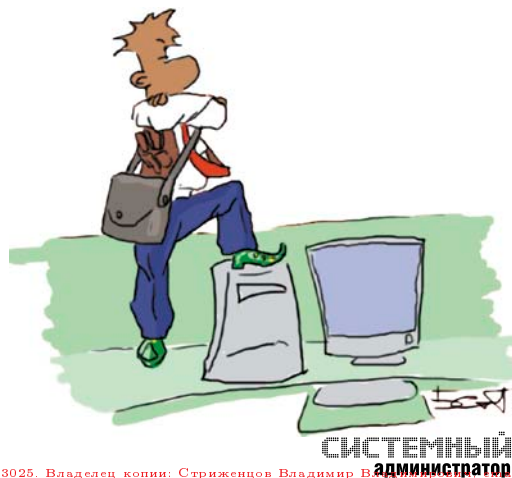
«Геноцид Юзеров» будет внушать всем ужас.

Коллекция плакатов обогатится админскими историями.

Админская игра «АУТСОРСЕР» скрасит ваш досуг.

Кружки порадуют вас внешним оформлением и содержимым.

Любителям минимализма возможно придется по вкусу значок!





# В Москве прошел пятый Форум по открытому коду

14 мая в Центральном выставочном комплексе «Экспоцентр» прошел уже пятый по счету Форум по открытому коду. На этот раз он состоялся в рамках международного конгресса и выставки информационных технологий для бизнеса «ИТ-Весна 2009» (<http://www.it-spring.ru>), организованного компанией «Форт-Росс».

## Открытие

Крис ДиБона (Chris DiBona), менеджер по Open Source-проектам в Google, открыл форум докладом об использовании ПО с открытым кодом в мире и конкретно в Google. Начало сообщения было посвящено общей статистике, помогающей оценить мировую популярность операционных систем, веб-серверов, веб-браузеров. От нее автор перешел к количеству исходного кода, доступного в интернете, и к лицензиям на софт. ДиБона, следуя традициям евангелистов термина «Open Source» (вместо проповедуемого Ричардом Столлманом и многими другими «Free Software»), заявил, что люди боятся таких лицензий, как GNU GPL и LGPL, поскольку их «сложно понять». В качестве более приемлемых вариантов для своих первых Open Source-продуктов он порекомендовал BSD License и Apache License. В Google же, по понятным причинам, используют самые разные лицензии.

Перейдя к теме Google, Крис ДиБона рассказал подробнее об использовании Open Source в этой компании. По его словам, в Google каждый сервер работает под управлением Linux, а также эта свободная ОС установлена более чем на 10 тысячах десктопов (в качестве дистрибутива используется Goobuntu – своя модификация Ubuntu Linux). На своих компьютерах

сотрудники компании вольны работать под любыми системами, поэтому на личных ноутбуках тоже нередко можно встретить Linux (у 25-50% всех инженеров). Очевидно, что диапазон Open Source-продуктов, применяемых в Google, этим не ограничивается. Особый интерес для компании представляют всевозможные инструменты разработки приложений и различные библиотеки. Если при работе с ними обнаруживаются какие-то проблемы, программисты не оставляют их без внимания: по словам докладчика, каждый месяц интернет-гигант создает около 200-300 патчей для Open Source-проектов. Эти проекты охватывают все программные компоненты, которые интересны Google и активно используются ею.

Затем ДиБона рассказал о некоторых открытых разработках компании: наборе готовых компонентов для веб-приложений Google Web Toolkit (<http://code.google.com/webtoolkit>), веб-браузере Chromium, на основе которого создаются сборки Chrome, мобильной платформе Android. Завершение было посвящено прогнозам на будущее. По мнению докладчика, к 2015 году в Интернете можно будет найти 6 миллиардов строк кода, а число активных Open Source-проектов вырастет со 100 тысяч до 300 тысяч (при оценке активности за 7 дней). Разумеется,

не обошлось без агитации присоединиться к мировому сообществу разработчиков ПО с открытым кодом и традиционного американского призыва «Join Us!».

## Панельная дискуссия

Следующим пунктом программы стала двухчасовая панельная дискуссия, которая должна была раскрыть тему «светлого будущего открытого кода в России». Уже на ранних ее этапах Дмитрий Комиссаров, тогда еще советник генерального директора компании «АйТи», а ныне уже генеральный директор новой компании «ПингВин Софт-вер», заявил, что в России вообще нет индустрии программного обеспечения. Эта мысль породила продолжительные споры, в ходе которых Павел Фролов, генеральный директор «ГНУ/Линукс-центр», ответил, что в Москве, может, и нет, а в других городах – немало интересных проектов ПО, про которые просто мало знают. В дальнейшем участники неоднократно вспоминали таких гигантов, как АBBYY и «Лаборатория Касперского», однако пришли к мнению, что их малочисленность не позволяет говорить о том, что индустрия все-таки есть и тем более развита.

Дмитрий Дмитриев из Linux Ink высказал позицию, согласно которой соотношение 5% энтузиастов из мира свободного ПО к 95% бизнесменов





Дискуссии в кулуарах



Крис ДиБона (Google) отвечает на вопросы



Доклад Владислава Шершульского (Microsoft)



Собралось немало слушателей



Участники панельной дискуссии



Панельная дискуссия. Модератор – Влад Габриэль (Microsoft)



Аудитория слушает доклад Криса ДиБоны



Участники круглого стола, посвященного национальной платформе



проприетарного не изменится. Затрагивались темы технического образования в России, заметной нехватки специалистов не только в области Open Source, но и информационных технологий в целом. В качестве итогов панельной дискуссии можно привести заявление Бориса Славина, возглавляющего Союз ИТ-директоров (СОДИТ), о том, что нужно создавать совместимые решения, и тогда потребители сами выберут лучшее. На мой же субъективный взгляд, пресловутое светлое будущее открытого кода в России осталась под не меньшим вопросом, чем было до начала прошедшей дискуссии.

## Microsoft и Open Source

Вторым ключевым докладом дня было выступление Владислава Шершульского из Microsoft. Присутствие представителей этой корпорации уже давно никого не должно смущать. Ее сотрудники не стесняются сообщать, что не первый год спонсируют проведение подобных мероприятий – на благо всей ИТ-индустрии. Доклад оказался достаточно интересным. Владислав начал с анализа подходов производителей программного обеспечения к разработке и продаже софта, приведя примеры как вертикальной модели (все решения поставляются одной компанией), так и горизонтальной, к которой сейчас многие пришли, а в Microsoft стремились изначально. Поэтому ключевая задача для корпорации и на сегодняшний день – сделать так, чтобы все хорошо работало на Windows. Ввиду растущей популярности Open Source-решений стало вполне естественно, что в Microsoft заинтересованы и в этом типе ПО – конечно, при условии его запуска в комбинации со своей системой и другими продуктами.

Шершульский подчеркнул, что надежды сторонников свободного ПО на значительный рост его популярности во время экономического кризиса необоснованны, поскольку в таких ситуациях очень важную роль играют риски, которые заметно вырастают в случае перехода на другую платформу. По его мнению, кризис лишь консервирует устоявшееся положение, а вот после него возможны совершенно различные последствия. Кроме того,

докладчик отметил, что Open Source-компании в последнее время заметно склоняются в сторону проприетарной модели, уходя от идеологии в пользу двойного лицензирования и подписок в стиле классических коммерческих продавцов. С целью подлить масла в огонь он процитировал на удивление многим относительно недавнее (март 2009 года) высказывание Эрика Реймонда, одного из лидеров мирового Open Source-движения, заявившего, что лицензии вроде GNU GPL вовсе не нужны (<http://www.nixp.ru/news/9614>). Этим представитель Microsoft хотел продемонстрировать противоречия, царящие даже среди самих поклонников FLOSS, – впрочем, трудно сказать, что историческое противостояние терминов «Open Source» и «Free Software» сколь-нибудь ново...

И еще одна интересная мысль, которую высказал Владислав, выразилась в заявлении, что в лицензиях, подобных GNU GPL, очень заинтересованы крупные производители «железа», «чтобы не появилось нового Microsoft».

## Национальная программная платформа

Завершалось мероприятие «круглым столом» по созданию национальной программной платформы, для участия в котором был приглашен депутат Государственной Думы ФС РФ Илья Пономарев. Он и начал дискуссию, рассказав немного о самом проекте. Как известно, подобные попытки предпринимались раньше, поэтому резонным кажется вопрос, зачем, собственно, это нужно теперь. У докладчика было три аргумента:


- конфликт в Грузии показал, что в стране заметная зависимость от зарубежных технологий (GPS, Google Maps), которые существенно мешают работе спецслужб;
- нынешний президент – сторонник свободного ПО и вообще интересуется подобными вопросами;
- кризис.

Последний фактор не только был назван решающим, но и позволяющим провести параллель с «похожими идеями» в США, где намерены провести огромные вливания в высокотехнологичный сектор с целью получить заметное преимущество после кризиса.

Сам же проект национальной программной платформы посвящен разработке собственной операционной системы для применения в бюджетных и государственных организациях. Проект довольно грандиозен и во все не должен привести к созданию очередного Linux-дистрибутива. Более того, даже такие компоненты, как ядро ОС, предлагается написать с нуля. В защиту такого громкого, но вызывающего некоторые сомнения заявления была высказана мысль, что нынешнее положение побуждает так или иначе создавать принципиально новую ОС, поэтому «мы в равных условиях с Google и Microsoft». Так почему бы не поручить какой-нибудь компании вроде «Яндекса» реализовать такой масштабный проект, вопрошал Илья.

Впрочем, другие участники «круглого стола», равно как и аудитория в зале, довольно скептически отнеслись к идее разрабатывать платформу с нуля, ссылаясь хотя бы на то, сколько на это потребуется времени и ресурсов. Хорошо подытожил данную позицию Дмитрий Комиссаров, заявивший, что разумнее сейчас создать такую платформу на базе компонентов из мира свободного программного обеспечения, но одновременно запустить ряд исследовательских проектов, которые со временем смогут принести заметную пользу.

## Итоги

К организации мероприятия по традиции замечаний фактически нет. Единственное – переводчица Криса ДиБоны заметно выпадала из контекста информационных технологий, что приводило как к забавным, так и к печальным моментам на протяжении всего выступления зарубежного гостя. В остальном – пятый Форум по открытому коду пусть и оказался довольно кратковременным, должен был стать полезным или хотя бы интересным основной аудитории, которой собралось немало. Проведенная панельная дискуссия никаких заметных результатов не принесла, но позволила всем высказаться и поговорить, в общем-то, на свободные темы. 

*Дмитрий Шурупов,  
фотографии предоставлены  
организатором мероприятия –  
компанией «Форт-Росс»*



**31 июля — 2 августа**

г. Калуга, р. Вырка, палаточный городок  
в районе деревни Колюпаново (Поляна Слетов).

Реклама



## Четвертый Всероссийский Слет Сисадминов



## Сисадмины! АйТишники! Компьютерщики! Сертифицированные системные инженеры!

Все, кто на «ты» обращается с компьютерной, серверной и, в общем-то, с любой техникой!  
Все, к кому тянутся вереницы юзверей: от секретарей до бухгалтеров!  
Все, кто конфеты и цветы не пьет!

Вы, именно вы, приглашаетесь на самое значимое IT-событие этого лета — Четвертый Всероссийский Слет Сисадминов. Целый год вы трудились, не отрывая пальцев от клавиатур, не отводя усталых глаз от мониторов, проводя бессонные ночи в тесной и холодной серверной.

**Настало время отдохнуть по-настоящему, по-сисадмински, на празднике жизни, посвященном всемирному Дню Системного Администратора!**

**[www.SletAdminov.ru](http://www.SletAdminov.ru)**

**[info@sletadminov.ru](mailto:info@sletadminov.ru)**

Организаторы  
Слета

**softline**<sup>®</sup>

**@mail.ru**

Информационный  
спонсор

**СИСТЕМНЫЙ  
администратор**

Партнеры  
Слета

**symantec**<sup>™</sup>



**eset**



**allsoft.ru**



# «Айдеко» представила интернет-шлюз Ideco ICS 3.0



**19 мая в московском пресс-центре «Прайм-ТАСС» состоялась пресс-конференция компании «Айдеко», приуроченная к выходу третьей версии ключевого решения компании – интернет-шлюза Ideco ICS.**

**М**ероприятие, к моему удивлению, получило более общее название: «Российские разработчики Linux-based продуктов: доля серверных решений на Linux значительно увеличится». Как выяснилось, такая тема пресс-конференции была обусловлена тем, что представители компании оттачивались от недавнего исследования IDC, согласно которому серверные Linux-решения становятся популяр-

нее. Представлявшийся продукт Ideco ICS 3.0 позиционируется как раз как одно из таких решений, способных обеспечить всю сетевую инфраструктуру компании. На сегодня это уже не просто интернет-шлюз, каковым он был первое время своего существования, а целый комплекс, обеспечивающий помимо управления доступом к Интернету такие функции, как антивирус и контентная фильтрация трафика, почтовый

сервер с защитой от спама, Web- и FTP-серверы. Всем этим можно управлять через удобный веб-интерфейс, использующий AJAX и другие современные блага цивилизации. Однако перечислять все особенности нового релиза продукта, пожалуй, не так интересно, ведь всю информацию можно легко найти на соответствующей интернет-странице ([http://www.ideco-software.ru/products/ideco\\_ics.html](http://www.ideco-software.ru/products/ideco_ics.html)).



## Технический аспект

Больше внимания я хотел бы уделить той информации из первых уст, которая не так широко афишируется и сосредоточена на технических подробностях устройства продукта и взаимодействии компании с Open Source-сообществом. Итак, Idecso ICS поставляется в виде самодостаточной программной «прошивки», которая легко устанавливается на компьютер, превращаясь в многофункциональный сервер. Внутреннее устройство таково, что это собственный дистрибутив GNU/Linux на базе Red Hat Enterprise Linux 4 с Linux-ядром 2.4 и другими популярными Open Source-компонентами: iptables в качестве файервола и NAT, прокси-сервер Squid, веб-сервер Apache и так далее. Заявляется, что дистрибутив «нестандартен» и особым образом защищен. Все это в сумме позволяет представителям компании сравнивать его надежность с аппаратными решениями.

За счет чего обеспечивается повышенная безопасность? Основная особенность заключается в том, что файловая система разделена на 3 части:

- только для чтения (здесь размещаются библиотеки, исполняемые файлы и другие неизменяемые компоненты);
- только для записи (логи, базы данных);
- смешанные (например, конфигурационные файлы, которые могут модифицироваться во время работы сервера).

Каждая часть файловой системы – это обычный chroot, без дополнительных надстроек. Узнав об этом, я поспешил поинтересоваться, почему не используются более продвинутые технологии вроде виртуальных серверов (OpenVZ, Linux-VServer), которые предоставляют гораздо большие возможности вроде ограничений по ресурсам. Ответом было заявление, что этого не требуется и такая архитектура обеспечивает достаточный уровень защищенности. На последовавший вопрос о том, что при такой организации произойдет, если какой-то отдельный сервис (который мог бы находиться на отдельном виртуальном сервере) начнет потреблять неадекватное количество ресурсов, мне лишь ответили, что из-

вестны случаи DoS-атак на конкретные компоненты Idecso ICS, которые ни к чему не привели, поскольку остальные сервисы продолжали нормально функционировать. Дальнейшие дискуссии на подобные темы, к сожалению, публике сочла неинтересными «технологическими дебрями».

## Сотрудничество с Open Source

Последняя тема, которая меня волновала в отношении использования Linux и Open Source в продукте компании, – взаимодействие с сообществом. Главный разработчик в ходе дискуссий заявлял, что «Айдеко» пишет патчи к задействованным в Idecso ICS компонентам с открытым кодом. Это спровоцировало несколько резонных вопросов: «Отдаете ли вы свои патчи основным разработчикам проектов обратно на включение в upstream?», «Распространяете ли модифицированный исходный код в соответствии с требованиями GNU GPL и подобных лицензий?».

Нужно отдать должное компании, что она хотя бы старается отправлять свои патчи разработчикам оригинальных версий программ, но, к сожалению, как правило (всегда?), их заплатки ориентированы на устаревшие версии приложений, поскольку в дистрибутиве приоритет отдается более старым и стабильным версиям ПО. И понятно, что авторам Open Source-проектов не очень-то интересны патчи к старым версиям продуктов, потому что необходимо оценивать возможность и це-

лесообразность их применения в актуальных релизах. В результате конкретные примеры успешного включения патчей «Айдеко» в основные ветви Open Source-продуктов так и не были названы. Касательно лицензионных вопросов последовал ответ, что компания высылает модифицированный исходный код по запросу.

## Итоги

По итогам пресс-конференции у меня сложилось двойственное впечатление о компании и ее ключевом решении Idecso ICS. С одной стороны, получился довольно успешный с коммерческой точки зрения продукт, построенный на базе готовых Open Source-компонентов и доведенный до уровня действительно удобного и эффективного применения в рамках предприятия. Это несомненная заслуга специалистов компании. С другой – мне не очень симпатично такое взаимодействие с миром программного обеспечения с открытым кодом, поскольку оно выглядит весьма односторонне.

Впрочем, нужно понимать, что сразу с места в карьер не прыгнешь, а компания еще молода. При этом ее усилиями подготовлена неплохая платформа для дальнейшего развития. Посмотрим, что будет дальше – сейчас еще рано исключать возможность смещения модели компании в сторону классических корпоративных Open Source-гигантов.

*Дмитрий Шурупов,  
фото предоставлены  
компанией «Айдеко»*





# Новые беспроводные решения от Cisco



**3 июня 2009 года в гостинице «Ренессанс-Москва» компания Cisco провела пресс-конференцию, на которой представила свои новые решения в области беспроводных мобильных сетей связи семейства стандартов 802.11.**

На пресс-конференции было подробно рассказано о стратегии Cisco в области беспроводной безопасности и представлена новая масштабируемая платформа контроллера для сетей Unified Wireless, используемая для построения высокоскоростных Wi-Fi-соединений. При этом особое внимание было уделено совершенствованию методов удаленных коммуникаций и поддержке концепции Cisco «виртуальный офис». Но обо всем по порядку.

В начале пресс-конференции технический директор Андрей Кузьмич кратко описал основные направления развития компании Cisco. Это использование приложений для совместной работы, обеспечение производительности для ресурсоемких приложений, поддержка новой волны клиентских

устройств и работа в условиях сложной мировой экономической ситуации. Прежде всего были представлены направления развития в бизнесе, такие как разнообразие Wi-Fi-устройств, повсеместное распространение беспроводных технологий и ожидание высокой производительности беспроводных решений, схожей с уровнем проводных.

В соответствии с этими направлениями была представлена программа «Взаимодействие в движении». Программа посвящена прежде всего технологии Wi-Fi, которой, по мнению Cisco, уделяется недостаточно внимания, так как разработчики уделяют больше внимания Wi-Max, 3G и другим. С учетом складывающейся в мире экономической ситуации беспроводные решения Wi-Fi являются одним из су-

щественных средств снижения расходов на IT-инфраструктуру. При этом Cisco предлагает не просто точки доступа, а, в отличие от конкурентов, полноценные инфраструктурные решения. При этом учитываются требования по безопасности и производительности беспроводной сети.

## Протокол 802.11n

Заданные в выступлении тезисы затем были развиты следующим докладчиком – менеджером по беспроводным технологиям Андреем Харитоновым.

Докладчик рассказал о протоколе 802.11n. Протокол обладает исключительной производительностью (более чем в 9 раз по сравнению с существующими сетями) как для данных, так и для голоса и видео, высокой надежностью, благодаря которой производится



меньше повторной передачи пакетов. Еще одним важным моментом является то, что Cisco рассматривает программу «Взаимодействие в движении» как средство доступа сотрудника к рабочим приложениям из любой точки, как со своего рабочего места, так и из дома или гостиницы. Протокол 802.11n обладает рядом физических свойств, таких как фокусировка сигнала в направлении пользователя для увеличения качества и пропускной способности клиентов 802.11a/g. Такая фокусировка позволяет избежать снижения пропускной способности в сетях с большим количеством абонентских устройств.

К сожалению, в России протокол 802.11n пока не сертифицирован.

### Унифицированная беспроводная сеть

Следующим представленным решением является технология беспроводной унифицированной сети. В рамках данной технологии были представлены новые модели точек доступа и контроллеров для различных предприятий. Контроллер является средством управления точками доступа, который также позволяет масштабировать беспроводную сеть при увеличении размеров сети. Так, например, контроллер серии 5500 может управлять 250 точками доступа. Технология уже была развернута в промышленной эксплуатации у нескольких крупных заказчиков.

### Новые функции Cisco MSE

Теперь на одном устройстве MSE можно разворачивать несколько сервисов, таких как учет контекста и wIPS. Также пользователи одного или нескольких сервисов мобильности могут разворачивать дополнительный сервис в ограниченном масштабе на определенное время. На конференции был приведен довольно интересный пример использования wIPS. Некоторые компании приобретают wIPS для защиты от несанкционированного использования Wi-Fi. То есть если в организации запрещено использование Wi-Fi корпоративными политиками безопасности, то wIPS позволяет обнаруживать ноутбуки с включенными беспроводными адаптерами и другие устройства доступа и показывать на карте их месторасположение.

### Технология Cisco ClientLink

Данная технология предназначена для повышения производительности смешанных режимов при работе клиентов 802.11a/g/n. ClientLink позволяет регулировать фазы и мощность сигналов двух передающих антенн для улучшения фокуса для устройств 11a/g.

Данная технология фокусирует сигнал в направлении пользователя для увеличения качества и пропускной способности клиентов 802.11a/g.

Еще одна новая функция – это BandSelect, управляемый выбор полосы 5 ГГц для точки доступа. Используемый диапазон 2,4 ГГц зачастую бывает перегружен при большом количестве беспроводных устройств в сети. Диапазон 5 ГГц сейчас поддержива-

ется большим количеством клиентских устройств (ноутбуки, смартфоны и т.д.), поэтому с помощью BandSelect клиенты могут подключаться на данном диапазоне. В случае использования принудительного подключения в определенном диапазоне (2,4 или 5 ГГц) подключение будет осуществляться только в данном диапазоне.

### Аппаратно-программные решения

Еще одним решением является использование точек доступа Cisco Aironet 1524, позволяющих организовывать полностью беспроводные сети, в которых точки доступа могут общаться с клиентами в диапазоне 2,4 ГГц, а между собой в диапазоне 5 ГГц. Это позволяет существенно уве-



Выступает Андрей Кузьмич, технический директор Cisco в России



Андрей Харитонов, менеджер по беспроводным решениям, демонстрирует беспроводную точку доступа Cisco Aironet 1250





Участники пресс-конференции на фуршете

личить пропускную способность беспроводной сети.

Cisco Wireless Control System (WCS) является средством управления беспроводной сетью. Оно включает в себя инструменты для планирования, внедрения, мониторинга, поиска неисправностей и отчетов в беспроводной сети. Основные функции WCS – это интуитивно понятный интерфейс, встроенные средства дизайна и планирования, иерархическая структура карт, мониторинг и обеспечение безопасности и настраиваемая отчетность. Одним из основных преимуществ WCS является консолидация функций управления инфраструктурой в рамках одной платформы.

## Лицензирование

Далее докладчик рассказал о лицензировании новых беспроводных решений

Cisco. Появление новых функций требует дополнительного лицензирования, так как не всем заказчикам нужны те или иные функции и гибкая политика лицензирования позволяет сэкономить при внедрении беспроводной инфраструктуры.

Лицензирование разбивается на 3 категории:

- лицензирование контроллера;
- лицензирование системы управления (WCS);
- лицензирование мобильных сервисов (MSE).

Лицензии имеют уникальное пакетирование для каждой из категорий.

Например, для контроллера 5500 возможны следующие виды лицензирования (см. рис. 1).

То есть чтобы увеличить масштаб решения, внедренного у заказчика,

необходимо закупить лицензии Base Upgrade, WPLUS Upgrade or Base Upgrade + WPLUS Upgrade.

Тестовая лицензия содержится в контроллере и составляет 60 дней. Лицензии предоставляются на один конкретный контроллер.

Как видно из рис. 2, система управления может лицензироваться как Standard и Enterprise. Лицензии Standard предназначены для небольших предприятий, от 50 до 500 точек доступа. При этом есть базовый набор функций Base и добавочный набор Plus, который кроме перечисленных базовых функций обладает также повышенной надежностью и средствами определения местоположения беспроводной точки доступа. В лицензии Enterprise доступен только набор Plus, который помимо всех функций Standard Plus также может устанавливаться на несколько серверов.

В завершение конференции было задано несколько вопросов, связанных с практической реализацией лицензирования. В частности, активно обсуждалось, каким образом Cisco ограничивает функционал систем управления при использовании неполного лицензирования.

Также на конференции были анонсированы еще несколько мероприятий, которые пройдут в ближайшее время. В частности, форум Cisco Expo Learning Club, который пройдет 17 июня в Москве и о котором я также планирую рассказать.

Андрей Бирюков,  
фотографии предоставлены  
организаторами  
пресс-конференции



Рисунок 1. Схема лицензирования контроллера 5500



Рисунок 2. Схема лицензирования системы управления WCS



## DeviceLock решил значительную часть проблем информационной безопасности ООО «Газпромнефть-Хантос»

«Предпочтение было отдано ПО DeviceLock по ряду причин: во-первых, в ходе тестирования DeviceLock не было выявлено каких-либо значительных проблем, либо ошибок в программе, которые приводили бы к неудовлетворительной работе в рамках заявленного функционала; во-вторых, удобство в использовании и отличное соотношение цена/качество; и, в-третьих, положительные отзывы коллег», – прокомментировал выбор DeviceLock начальник отдела защиты информации ООО «Газпромнефть-Хантос» Милашевский.

## SourceForge заменяет свои веб-наработки, покупает Ohloh

Компания SourceForge, известная своими веб-ресурсами для онлайн-сообществ и электронной коммерции, объявила об отказе от своих веб-разработок, предлагаемых всем авторам проектов, в пользу популярных Open Source-средств.

Владельцам проектов на SourceForge.net было разослано письмо, в котором им предлагалось выбрать одну из доступных опций миграции. На смену форумам SourceForge Discussion Forums пришел phpBB, на смену менеджеру задач TaskManager – TaskFreak!, dotProject и Trac, вместо DocManager предлагались MediaWiki и Trac, а сервис Diary and Notes можно было заменить на WordPress. Опрос пользователей проводился в течение 30 дней. Переход на сторонние Open Source-средства стал возможным благодаря предложению Hosted Apps, которое появилось на SourceForge в сентябре прошлого года.

Вскоре после этого SourceForge объявила о достижении договоренности по покупке Ohloh. Ohloh – созданный бывшими менеджерами корпорации Microsoft сайт, предоставляющий веб-сервисы и онлайн-платформу, предназначенную для разработки программного обеспечения с открытым кодом усилиями сообщества. Благодаря автоматизированному сбору данных из различных репозиторий (CVS, Subversion, Git) на Ohloh публикуется статистика о различных Open Source-проектах, их лицензиях и т.п.

SourceForge с покупкой Ohloh намерена интегрировать возможности этой платформы в свои ресурсы, улучшив таким образом онлайн-среду для Open Source-разработок. Команда разработчиков Ohloh присоединится к штату сотрудников SourceForge и продолжит развитие своих технологий. Финансовые подробности сделки SourceForge и Ohloh не разглашаются.

## ОС Moblin стала одним из главных трендов Computex

На прошедшей в Тайбэе (Тайвань) технологической выставке Computex трудно было проигнорировать заметное оживление вокруг мобильной Linux-системы Moblin. Изначально она создавалась Intel, но теперь ее разработкой руководит Linux Foundation.

Похоже, недавний релиз Moblin 2.0 Beta, популярность нетбуков и Linux на этих устройствах, а также грамотная политика Intel сделали свое дело. На Computex можно было увидеть много компьютеров с Moblin. Среди них – нет-

буки от таких компаний, как Hewlett-Packard, Asus, MSI и Hasee Computer, мобильные интернет-устройства от BenQ и Compal Electronics. Во время пресс-конференции Acer стало известно, что в компании уже озабочены установкой Moblin «на ряд своих продуктов». Причем это не только нетбуки Aspire One, но и ноутбуки, и даже настольные персональные компьютеры. Кроме того, уже были продемонстрированы нетбуки Acer Aspire One с Moblin на борту.

Тем временем компания Canonical, занимающаяся поддержкой Ubuntu Linux, объявила о намерении выпустить редакцию своего дистрибутива для нетбуков, Ubuntu Netbook Remix (UNR), на базе Moblin 2. До сих пор в основе интерфейса UNR был так называемый «UNR Launcher», заменяющий традиционное главное меню рабочего стола. Теперь стало известно, что в готовящейся редакции для интерфейса рабочего стола будут использоваться наработки Moblin.

Еще одной важной новостью про Moblin, объединившей ее с другим трендом – Google Android, стало объявление старшего вице-президента ультрамобильного подразделения компании Intel о том, что пользователи Moblin получат возможность скачивать приложения с онлайн-рынка приложений Android Market. Во время своего выступления на Computex он продемонстрировал нетбук с установленной ОС Moblin 2.0 Beta, в которой функционировали приложения для Android. Стоит также отметить, что недавно и разработчики Canonical анонсировали свои успехи по запуску Android-приложений в среде Ubuntu Linux. Пока официальных подробностей нет, но вполне вероятно, что это результат совместных усилий Open Source-проектов.

В качестве основы в Moblin используются наработки Open Source-проекта GNOME Mobile. Бета-релиз Moblin 2.0 состоялся в конце мая, и в нем появились такие новшества, как визуально обогащенный пользовательский интерфейс (с использованием технологий Clutter, DRI2 и KMS), «домашняя панель» с календарями, задачами, недавно использовавшимися файлами, агрегация и вывод контента из социальных сетей (пока только Twitter и Last.fm), новый веб-браузер на базе Mozilla, мультимедийный плеер с возможностью масштабирования показываемого изображения, обновленный менеджер подключений (ConnMan). Финальная версия Moblin 2.0 выйдет в конце этого года.

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



# Организуем систему резервного копирования для малого и среднего офиса



*Алексей Бережной*

**Как создать простую систему резервного копирования, не требующую больших затрат, но при этом обеспечивающую необходимую надежность и управляемость.**

**Н**аверное, нет необходимости говорить о важности резервного копирования. И не только для крупных организаций. Бизнес-информация любой, даже самой небольшой, компании нуждается в хорошей и своевременно сделанной резервной копии. Но далеко не каждая компания может позволить себе мощное и дорогостоящее решение на базе дорогих ленточных библиотек и известных программных продуктов, таких как Symantec Backup Exec. В то же время копировать (а иногда и восстанавливать данные) необходимо. Из создавшейся ситуации сам собой напрашивается несложный вы-

ход — создать некую систему резервного копирования на базе бесплатных программных продуктов на базе Linux. Как обычно бывает в небольших компаниях, сдать законченную систему нужно было еще вчера, поэтому основной акцент сделаем на простоте реализации, а также на возможности делегирования операций резервного копирования другому лицу, не обладающему навыками опытного администратора UNIX-систем.

## **Что угрожает нашим данным**

Бессмысленно пытаться создавать систему резервирования и восстановле-

ния данных без четкого понимания причин, которые могут привести к потере данных. Факторы эти могут быть как внешнего, так и внутреннего характера.

## **Внутренние факторы**

К этим факторам можно отнести уничтожение данных в связи с заражением компьютерным вирусом, удаление данных в связи с ошибочными или умышленными действиями пользователей, некорректной работой программ, сбоем оборудования, бросков напряжения и других факторов, носящих локальный характер и вызванных причинами, возникшими внутри офиса.



### Внешние факторы

Довольно подробный перечень данных факторов можно получить, заглянув на последние страницы большинства договоров, где указываются форс-мажорные обстоятельства, начиная от разломов земной коры и заканчивая действиями третьих лиц.

Соответственно если в офисе случился пожар или представители правоохранительных органов изъяли или опечатали оборудование, доступ к данным, содержащим важную для ведения бизнеса информацию, будет прекращен. (Здесь особенно важно понимать, что резервная копия, призванная сберечь наши бизнес-процессы, должна храниться вне территории офиса.)

### Способы организации резервного копирования

Существует несколько способов организации резервного копирования.

#### Установка внутреннего Backup-сервера

Защититься от большинства внутренних факторов можно, установив специальный файловый сервер для создания и хранения резервных копий. Таким образом, большая часть данных копируется по сети в период наименьшей загрузки, чаще всего ночью на жесткие диски сервера, специально выделенного для хранения резервных копий.

**Преимущества:** данная система легко организуется и требует относительно небольших затрат. Достаточно компьютера с большим объемом дискового пространства. Данный комплект вполне можно использовать в качестве платформы при организации файлового сервера для хранения резервных копий информации с других серверов и рабочих станций.

**Недостатки:** эта технология не подходит для защиты от внешних факторов, так как информация хранится на территории предприятия. Также она может оказаться бесполезной в случае заражения компьютерным вирусом или вредоносного воздействия других лиц, так как Backup-сервер, находящийся во включенном состоянии и доступный по сети, также может подвергнуться как вирусной, так и любой другой атаке.

### Копирование данных на сменный носитель

Эта технология предполагает наличие некоего устройства, способного писать на сменные носители данных. В совокупности с физической транспортировкой носителя, содержащего свежую копию данных, за пределы предприятия (в дальнейшем этот прием будем называть off-site) решение способно обеспечить сохранность данных в большинстве случаев.

**Преимущества:** защищает как от внутренних, так и от большинства внешних факторов.

**Недостатки:** требует дополнительное оборудование и программное обеспечение для резервного копирования. Замедляется процесс восстановления данных в связи с необходимостью обратной транспортировки носителя на территорию предприятия. Также требует наличия дополнительных навыков у лица, ответственного за сохранение и восстановление данных.

#### Копирование данных off-site посредством сетевых соединений

Этот метод заключается в копировании файлов по сети за пределы территории предприятия. При этом может использоваться как прямое подключение, так и защищенные интернет-соединения (VPN).

**Преимущества:** не требует физической транспортировки носителя.

**Недостатки:** требует скоростного сетевого подключения. Возможны трудности при восстановлении дан-

ных. При использовании интернет-соединения плата за трафик может составить значительную сумму.

### Подведем итоги

Наиболее рациональным представляется метод, сочетающий в себе наличие внутреннего Backup-сервера и копирование данных на сменный носитель. В этом случае появляется возможность значительно расширить возможности нашей backup-системы, используя технологию, когда данные в ночное время предварительно копируются на Backup-сервер, а уже оттуда выгружаются на ленту. Это позволит разгрузить компьютерную сеть и более эффективно использовать время, отведенное для резервного копирования. Так как при этом backup-сервер интегрирован с системой копирования на сменный носитель, при его организации необходимо ориентироваться на специфику аппаратных и программных средств, используемых при копировании данных на сменный носитель.

### Создание плана резервного копирования

Рассмотрим типы резервного копирования.

#### Полное копирование (Full backup)

Производится копирование данных в полном объеме.

**Достоинства:** самый надежный способ резервного копирования. В случае выхода из строя свежей резервной копии часть данных все равно можно восстановить с предыдущей копии. Са-

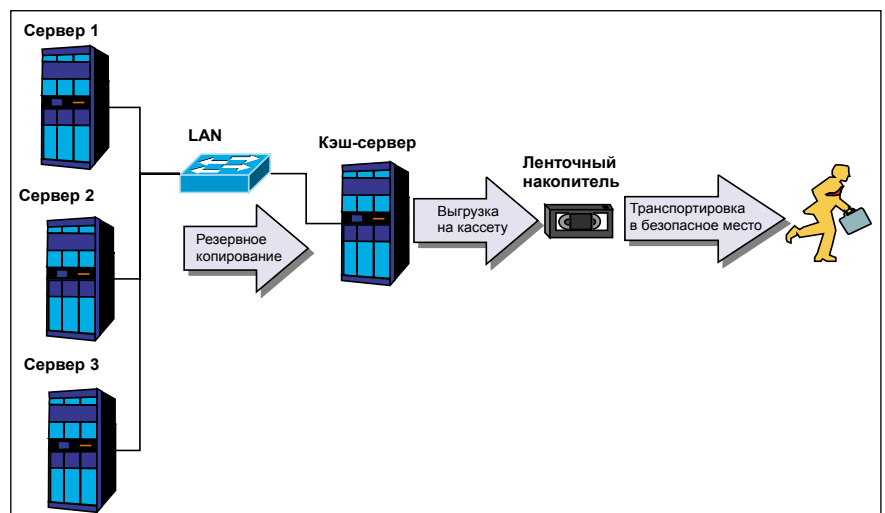


Рисунок 1. Схема, описывающая процесс резервного копирования



мый эффективный метод для быстрого восстановления информационной инфраструктуры предприятия.

**Недостатки:** требует носителей данных большей емкости и более продолжительного времени выполнения.

## Дифференциальное копирование (Differential backup)

Копируются только изменения с момента выполнения последнего Full backup. Данные копируются «нарастающим итогом», так что последняя копия будет содержать все изменения с момента последнего Full backup.

**Достоинства:** выполняется несколько быстрее, нежели Full backup. Повреждение одной из копий не приводит к потере всех данных за период (при наличии действительной копии Full backup).

**Недостатки:** так или иначе, все равно требуется регулярное выполнение Full backup. В случае повреждения носителя с полной копией (Full backup) данный экземпляр резервной копии становится бесполезен. Последняя копия, содержащая в себе все изменения за продолжительный период, может оказаться сравнима по размерам с Full backup.

## Инкрементное копирование (Incremental backup)

Выполняется копирование только информации, измененной после выполнения предыдущего Incremental backup.

**Достоинства:** самый быстрый метод резервного копирования. Занимает меньше всего объема.

**Недостатки:** самый ненадежный метод резервного копирования. В слу-

чае повреждения одной из копий все последующие копии становятся бесполезными. В случае повреждения носителя с Full backup становится бесполезен. Необходимо осуществлять off-site всех копий Incremental backup за период. Восстановление данных занимает продолжительное время.

## Подведем итоги

Тип копирования обычно диктуется финансовым положением и важностью данных. Если позволяет бюджет и данные представляют собой коммерческую ценность, предпочтительнее всего использовать Full backup.

Если бюджет минимален или данные не представляют большой ценности, то можно использовать Incremental backup.

Differential backup представляет собой некий компромисс, зачастую не всегда оправданный, так как может оказаться, что последняя копия требует объема дискового носителя и времени создания почти столько же, сколько и Full backup.

## Создание системы резервного копирования

Учитывая величину оборота компании, можно вычислить примерную стоимость одного бизнес-дня и соответственно важность коммерческих данных. В наших условиях целесообразно остановиться на следующем варианте.

В качестве метода резервного копирования используем сочетание Backup-сервера и накопителя на съемных носителях (например, ленточного накопителя).

План резервного копирования представляет собой ежедневный Full backup предварительно на Backup-сервер с последующей выгрузкой на ленту и транспортировкой в безопасное место (off-site) ленточного носителя данных (картриджа). В подобных системах Backup-сервер также называют кэш-сервером, стремясь подчеркнуть его промежуточное значение перед окончательным копированием на ленту (см. рис. 1).

## Планирование процесса восстановления

Создание резервной копии – это, безусловно, очень важная часть в системе защиты и восстановления данных. Но не менее важно знать, как будут восстанавливаться данные из резервной копии.

Поэтому при выборе системы резервного копирования следует опираться на стандартизированное решение, поддерживаемое большинством производителей оборудования и программного обеспечения.

Например, таким решением являются ленточные накопители (стримеры), поддерживающие стандарт LTO (Linear Tape Open), разработанный такими известными участниками компьютерного рынка, как IBM, HP и Seagate.

Примем за основу следующую схему восстановления:

- Мелкие, но срочные задачи по восстановлению данных, такие как реанимация испорченного по ошибке файла, выполняются с кэш-сервера.



Рисунок 2. Создание учетной записи при инсталляции системы

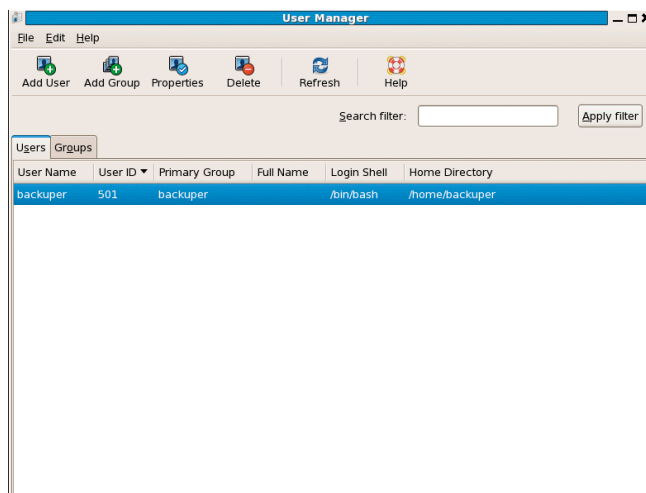


Рисунок 3. Создание учетной записи при помощи инструмента User Manager

■ В случае возникновения более серьезные проблем, например, когда нужно восстановить данные после серьезной аварии (после уничтожения большого количества файлов компьютерным вирусом и т.д.), а также в случае необходимости получения доступа к информации за прошлый период будем восстанавливать со съемного носителя, хранящегося в безопасном месте.

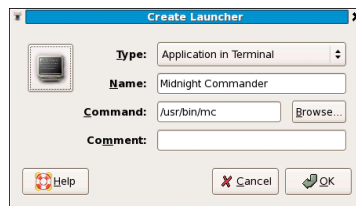


Рисунок 4. Создание ярлыка для запуска Midnight Commander

## Централизованный или децентрализованный метод?

Существует два метода организации получения данных, подлежащих резервному копированию: централизованный и децентрализованный.

В первом варианте за весь процесс резервного копирования отвечает единый программный комплекс, работающий по технологии «клиент-сервер». То есть имеется центральный сервер с установленным специализированным серверным ПО и программы-клиенты резервного копирования на компьютерах. Информация, подлежащая резервному копированию, собирается посредством этих самых клиентов. По такой схеме работает большинство известных коммерческих backup-систем, таких как Symantec Backup Exec. Также существуют бесплатные системы резервного копирования, в основном на базе Open Source, например Bacula, которые также работают по «клиент-серверной» технологии.

Второй метод – децентрализованный, означает отсутствие единого центра управления. В этом случае на каждом сервере установлена отдельная программа обеспечения резервного копирования, с помощью которой данные переносятся на другой носитель или сетевой ресурс. По такой схеме работает, например, программа ntbackup, поставляемая с современными операционными системами семейства Windows.

В нашем случае выбран децентрализованный метод резервного копирования. Данные с Windows-серверов, которых в нашей сети явное большинство, будут копироваться посредством программы ntbackup на сетевой ресурс кэш-сервера, с серверов на базе UNIX-систем – посредством программы tar. Причина довольно банальная: необходимо в кратчайшие сроки создать работающую backup-систему и делегировать полномочия по выполнению рутинных операций резервного копирования другому лицу. То есть система должна быть максимально простой и понятной, при этом не требующей изучения сложного программного комплекса, такого как Backup Exec или Bacula. Кроме того, не требуется установка программ-клиентов, так как и ntbackup и tar уже присутствуют в соответствующих операционных системах.

## Выбор программного обеспечения для организации сервера резервного копирования

В качестве операционной системы был выбран Linux CentOS за его совместимость с широко известной операционной системой Linux Red Hat Enterprise (RHEL), поддержку rpm пакетов и простоту установки и обслуживания. Когда подго-

тавливалось данное решение по резервному копированию, была доступна версия Linux CentOS 5.2, сейчас уже вышла версия 5.3 (<http://www.centos.org>).

Так как наш кэш-сервер просто обязан быть файловым сервером, мы должны будем установить программный пакет Samba для обеспечения функций файлового сервера в среде Windows, работающего по SMB-протоколу. Подробности можно узнать на сайте программы: <http://us6.samba.org/samba>.

Для облегчения задач по управлению и удаленному администрированию, а также для дальнейшего делегирования полномочий другим сотрудникам (например, администратору Windows-систем) будем использовать протокол RDP. Для этого установим программу xrdp для поддержки терминального доступа посредством RDP-клиента. Для работы xrdp нужен поднятый VNC-сервер, поэтому мы должны установить и его.

**Примечание:** программа xrdp в некоторых реализациях не всегда корректно работает с тем или иным RDP-клиентом. Например, в случае с xrdp-0.4.0-1.el5.rf для CentOS не поддерживается работа с последней версией RDP-клиента, поставляемого с Service Pack 3 для Windows XP. В подобных случаях рекомендуется пользоваться программой rdesktop, <http://www.rdesktop.org> (в частности, ее Windows-версией rdesktop.exe, скачать которую можно по адресу: [http://www.atomice.com/blog/?page\\_id=9](http://www.atomice.com/blog/?page_id=9)).

Для облегчения работы с файлами имеет смысл установить Midnight Commander – файловый менеджер, аналог небезызвестного Norton Commander.

Ну и наконец, необходимо установить программное обеспечение для поддержки работы с ленточным накопителем: HP Data Protector Express Single Server Edition, страница проекта: <http://h18000.www1.hp.com/products/storage/software/datapexp/sse/index.html>.

## Выбор оборудования для кэш-сервера

В качестве кэш-сервера был выбран старенький сервер SuperMicro в корпусе big tower.

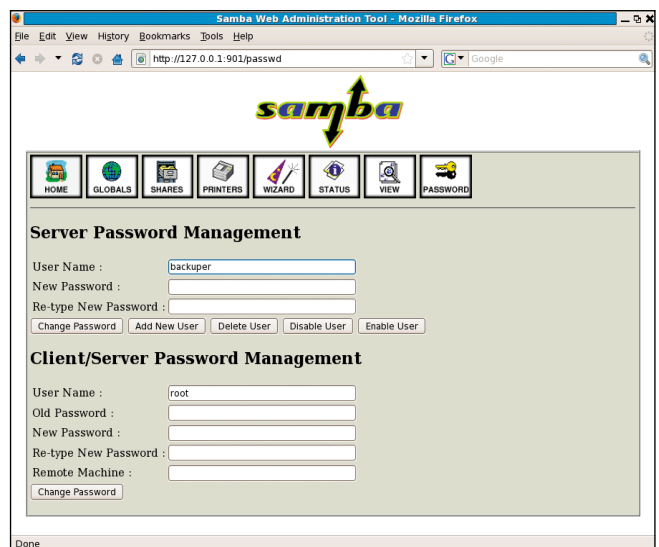


Рисунок 5. Добавление пользователя Samba посредством SWAT



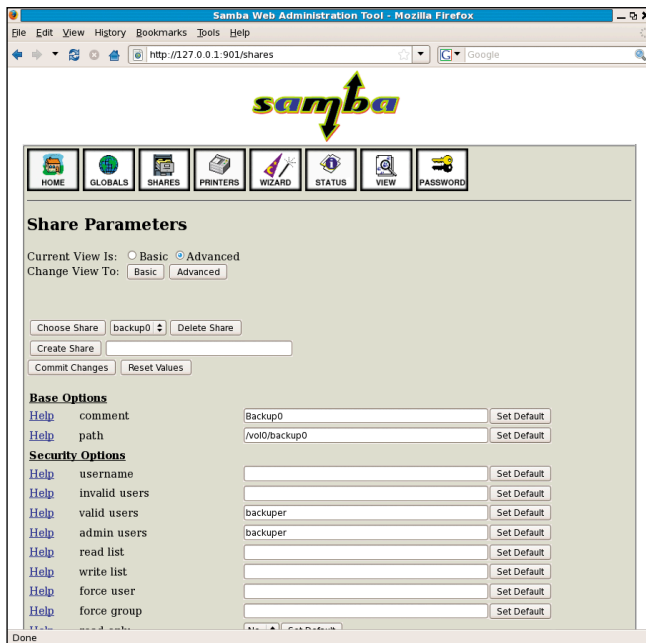


Рисунок 6. Создание сетевого ресурса Samba посредством SWAT

Аппаратное обеспечение сервера:

- Материнская плата: Super X6DHE-XG2.
- Объем ОЗУ: 1 Гб.
- Дисковые контроллеры:
  - ✓ встроенный в материнскую плату контроллер Adaptec Embedded Host Raid;
  - ✓ дополнительный RAID-контроллер LSI Logic MegaRAID Ser523 в формате PCI-X-133 с четырьмя портами для подключения SATA-дисков.
  - ✓ два жестких диска Seagate ST31000340AS емкостью 1 Тб, предназначенные для промежуточного хранения данных;
  - ✓ два жестких диска Seagate ST3500320NS емкостью 500 Гб для объединения в RAID1 и установки на них операционной системы;

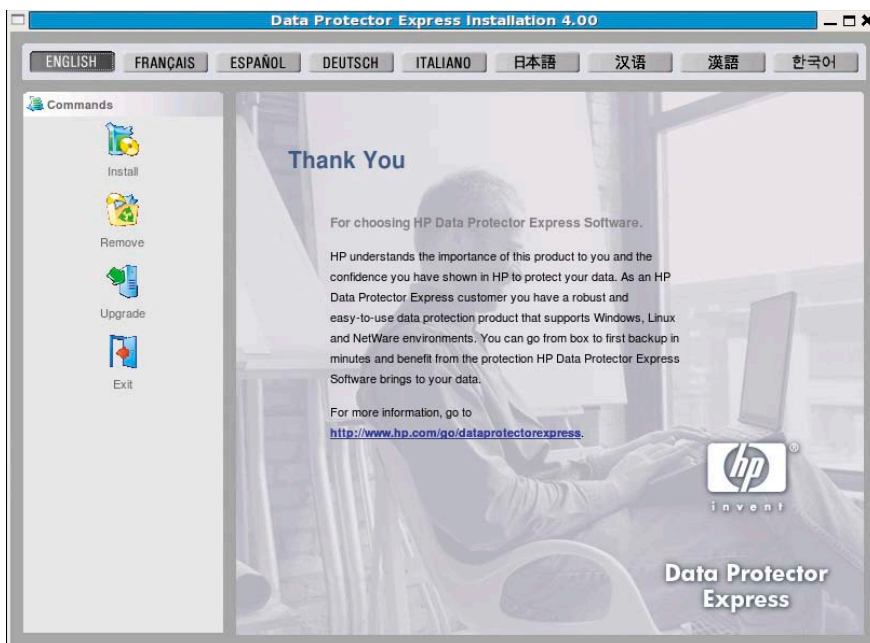


Рисунок 7. Окно установки программы HP Data Protector Express Single Server Edition

- ✓ RAID-контроллер SCSI для подключения ленточного накопителя LSI Logic LSI20320-HP в формате PCI-X-133 с внешним SCSI-интерфейсом;
- ✓ Ленточный накопитель HP Storage Works Ultrium 1840LTO4 вместе с кабелем для подключения к внешнему SCSI-интерфейсу.

Кратко прокомментирую выбор аппаратного обеспечения. Как можно догадаться из вышеописанной конфигурации сервера, его собирали из того, что было под рукой. А вот ленточный накопитель LTO4 вместе с SCSI с контроллером для его подключения и запасом сменных картриджей (кассет) был приобретен отдельно.

## Подготовка кэш-сервера

После того как мы полностью определились с оборудованием и программным обеспечением, пришло время воплотить наш проект в жизнь.

Первым шагом установим операционную систему на наш кэш-сервер. Так как в Linux-системах часто не поддерживаются те или иные модели host-RAID-контроллеров, имеет смысл не рисковать и для размещений непосредственно операционной системы собрать RAID1 на базе имеющегося контроллера известной модели LSI Logic MegaRAID Ser523 и двух SATA-дисков по 500 Гб. Оставшиеся два жестких диска по 1 Тб мы подключим к контроллеру на материнской плате без объединения в RAID-массив. Таким образом, сама операционная система и прикладное ПО будут установлены на RAID1, а два отдельных диска по 1 Тб предназначены для хранения временных резервных копий.

Сами жесткие диски по 1 Тб, предназначенные для хранения промежуточных копий, имеет смысл подключить и разметить во время установки системы. Создаем на каждом из дисков по одному тому и используем точки монтирования /vol0 и /vol1 соответственно.

Установка операционной системы производится в обычном режиме. При установке программного обеспечения в качестве шаблона инсталляции выбираем Server GUI. Из оконных менеджеров выбираем Gnome за его простоту и экономичность.

Из дополнительных программных пакетов необходимо установить Samba для организации файлового сервера в среде Windows, а также VNC-сервер для обеспечения работы xrdp. Также рекомендуется установить пакеты из категории «Development: Development Libraries, Development tools, Legacy Software development», чтобы иметь возможность в дальнейшем установить программное обеспечение.

И еще установим супердемон xinetd, чтобы иметь возможность запускать программу SWAT для управления сервером Samba.

Сразу при инсталляции создадим учетную запись (например, backuper),

из-под которой и будет производиться работа по резервному копированию (см. **рис. 2**).

Если по каким-либо причинам не удалось создать ее сразу, в дальнейшем можно будет воспользоваться инструментом User Manager, который запускается из основного меню: System → Administration → Users and Groups (см. **рис. 3**).

Далее входим в систему как root для выполнения первоначальной настройки.

**Примечание:** при невозможности воспользоваться программой User Manager можно воспользоваться командой `useradd` с соответствующими ключами.

Стоит немного сказать об основной концепции настройки программного обеспечения в нашем случае – максимально использовать возможности графического интерфейса. Большинство UNIX-гуру сразу бы запустили любимую оболочку (shell) командной строки, принялись вводить команды и редактировать конфигурационные файлы. Но в нашем случае предстоит непростой процесс передачи полномочий другому лицу, скорее всего мало знакомому с работой с интерфейсом командной строки в UNIX-системах. Поэтому все, что можно сделать через графический интерфейс, должно быть сделано именно так. Исходя из этих соображений, мы создадим на рабочем столе иконку для запуска Midnight Commander (см. **рис. 4**).

Как уже упоминалось выше, при настройке Samba мы также не будем отклоняться от намеченной стратегии и воспользуемся веб-интерфейсом под названием SWAT.

Так как SWAT запускается посредством супердемона `xinetd`, необходимо подредактировать файл `/etc/xinet.d/swat`

Вот как примерно должен выглядеть файл после редактирования:

```
# default: off
# description: SWAT is the Samba Web Admin Tool.
#               Use swat to configure your Samba server.
#               To use SWAT, connect to port 901
#               with your favorite web browser.
service swat
{
    port                = 901
    socket_type         = stream
    wait                = no
    user                = root
    server              = /usr/sbin/swat
    log_on_failure      += USERID
    disable             = no
}
```

Теперь можно запустить сам веб-интерфейс. Набираем в строке браузера (например, Mozilla Firefox) адрес `http://127.0.0.1:901` и, введя имя пользователя `root` с соответствующим паролем, попадаем в окно SWAT. Далее, воспользовавшись вкладкой Password, необходимо задать имя пользователя для доступа к назначаемым сетевым ресурсам. Для того чтобы избежать дополнительных проблем, настоятельно рекомендую использовать те же имя и пароль пользователя, которые уже заведены в системе. Поэтому вводим имя пользователя `backupер`, тот же пароль, что и при создании пользователя UNIX, и нажимаем кнопку Add New User, далее необходимо разрешить данную учетную запись, поэтому нажимаем кнопку Enable User (см. **рис. 5**).

**Примечание:** при невозможности воспользоваться программой SWAT можно использовать команду  `smbpasswd`

с ключами `-a` для добавления и `-e` для разрешения учетной записи пользователя Samba.

Для того, чтобы иметь возможность более гибко распорядиться дисковыми ресурсами (например, в дальнейшем убрать некоторые файлы из общего доступа, перенести их в другой каталог), создадим на подключенных дисках `vol0` и `vol1` каталоги `/vol0/backup0` и `/vol1/backup1`. Для того, чтобы пользователь `backupер` имел доступ в эти ресурсы, сменим владельца каталога на `backupер` и зададим соответствующие права. Для этих целей довольно удобно использовать Midnight Commander.

**Примечание:** при невозможности воспользоваться программой Midnight Commander нужно использовать команды: `mkdir` – для создания каталога, команды `chmod` и `chown` – для изменения разрешений и смены владельца (группы) соответственно.

В случае если по каким-то причинам не удалось сразу создать необходимые разделы и подключить диски, чтобы сделать это после инсталляции, придется немного поработать в командной строке.

Запускаем программу Terminal или любую другую оболочку командной строки. При необходимости переходим в режим суперпользователя `root`:

```
[root@backupsmall vol0]# su
```

```
Password:
```

Получаем список файлов SATA-устройств:

```
[root@backupsmall vol0]# ls /dev/sd*
```

```
/dev/sda /dev/sda1 /dev/sda2 /dev/sda3 /dev/sdb /dev/sdc
```

Файлы устройств: `/dev/sda`, `/dev/sda1`, `/dev/sda2` и `/dev/sda3` нас не интересуют, так как относятся к уже подключенному дисковому массиву RAID1 с операционной файловой системой. А вот `/dev/sdb` и `/dev/sdc` как раз и являются файлами устройств тех самых дисков, которые предстоит подключить.

Если возникли трудности с определением какой файл устройства какому диску принадлежит, можно воспользоваться командой `fdisk` с параметром `-l`:

```
[root@backupsmall vol0]# fdisk -l
```

```
Disk /dev/sda: 500.0 GB, 500093157376 bytes
255 heads, 63 sectors/track, 60799 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes

   Device Boot      Start         End      Blocks   Id  System
/dev/sda1  *           1         5222     41945683+   83  Linux
/dev/sda2                5223         6266       8385930    82  Linux swap / Solaris
/dev/sda3                6267        60799     438036322+   83  Linux

Disk /dev/sdb: 1000.2 GB, 1000204886016 bytes
255 heads, 63 sectors/track, 121601 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes

   Device Boot      Start         End      Blocks   Id  System

Disk /dev/sdc: 1000.2 GB, 1000204886016 bytes
255 heads, 63 sectors/track, 121601 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes

   Device Boot      Start         End      Blocks   Id  System
```

Для создания необходимого раздела на диске вызываем программу `fdisk`:



```
[root@backupsml vol0]# fdisk /dev/sdb
```

Первоначально программа выдает сообщение, подобное этому:

```
Device contains neither a valid DOS partition table, nor Sun,
SGI or OSF disklabel.
Building a new DOS disklabel. Changes will remain in memory only,
until you decide to write them. After that, of course,
the previous content won't be recoverable.
```

```
The number of cylinders for this disk is set to 121601.
There is nothing wrong with that, but this is larger than 1024,
and could in certain setups cause problems with:
1) software that runs at boot time (e.g., old versions of LILO)
2) booting and partitioning software from other OSs
   (e.g., DOS FDISK, OS/2 FDISK)
Warning: invalid flag 0x0000 of partition table 4 will be
corrected by w(rite)
```

Создаем новый раздел:

```
Command (m for help): n
```

```
Command action
e   extended
p   primary partition (1-4)
p
```

Выбираем тип раздела: первичный (primary) или расширенный (extended):

```
Partition number (1-4): 1
```

Так как на создаваемый раздел отводится весь объем жесткого диска, первый и последний цилиндр выбираем по умолчанию.

```
First cylinder (1-121601, default 1):
Using default value 1
Last cylinder or +size or +sizeM or +sizeK (1-121601, default 121601):
Using default value 121601
```

Проверяем список созданных разделов:

```
Command (m for help): p
```

В ответ программа выдаст информацию о созданных разделах:

```
Disk /dev/sdb: 1000.2 GB, 1000204886016 bytes
255 heads, 63 sectors/track, 121601 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
```

Device	Boot	Start	End	Blocks	Id	System
/dev/sdb1		1	121601	976760001	83	Linux

Записываем изменения и выходим из программы:

```
Command (m for help): w
```

```
The partition table has been altered!

Calling ioctl() to re-read partition table.
Syncing disks.
```

Создаем файловую систему на новом дисковом разделе:

```
[root@backupsml vol0]# mkfs.ext3 /dev/sdb1
```

Так как используемая нами файловая система ext3 яв-

ляется журналируемой, нет нужды проверять ее перезагрузкой. Отключаем эту функцию:

```
[root@backupsml vol0]# tune2fs -c 0 -i 0 /dev/sdb1
```

Создаем каталог для монтирования вновь созданного раздела с файловой системой:

```
[root@backupsml vol0]# mkdir /vol0
```

И монтируем файловую систему:

```
[root@backupsml vol0]# mount -t ext3 /dev/sdb1 /vol0
```

По аналогии размечаем и монтируем второй диск (/dev/sdc).

Для того чтобы созданные нами разделы автоматически монтировались при запуске, необходимо отредактировать файл /etc/fstab. Пример файла /etc/fstab:

```
[root@backupsml vol0]# vi /etc/fstab

LABEL=/          /               ext3 defaults 1 1
/dev/sdb1        /vol0           ext3 defaults 0 0
/dev/sdc1        /vol1           ext3 defaults 0 0
tmpfs            /dev/shm        tmpfs defaults 0 0
devpts           /dev/pts        devpts gid=5,mode=620 0 0
sysfs            /sys            sysfs defaults 0 0
proc             /proc           proc defaults 0 0
LABEL=SWAP-sda2  swap            swap defaults 0 0
```

Далее снова воспользовавшись SWAT, создаем общий ресурс для резервных копий. Переходим на вкладку Share. Далее задаем имя ресурса: в нашем случае backup0. Указываем путь к каталогу: в нашем случае /vol0/backup0 и пользователей, имеющих право доступа к каталогу valid users и admin users (см. рис. 6).

В конечном итоге конфигурационный файл Samba – smb.conf должен выглядеть примерно следующим образом:

```
[global]
workgroup = VAI.LAN
server string = Backup Server LT04
passdb backend = tdbsam
username map = /etc/samba/smbusers
ldap ssl = no
cups options = raw

[printers]
comment = All Printers
path = /var/spool/samba
printable = Yes
browseable = No

[backup0]
comment = Backup0
path = /vol0/backup0
valid users = backupuser
admin users = backupuser
read only = No
browseable = No

[backup1]
comment = Backup0
path = /vol1/backup1
valid users = backupuser
admin users = backupuser
read only = No
browseable = No
```

Где vol0 и vol1 – собственно и есть вышеописанные диски по 1 Тб для хранения резервных копий.

Ну и наконец переходим к настройке программного обеспечения для выполнения резервного копирования на ленту – HP Data Protector Express Single Server Edition. Для начала зайдём на страничку программы <http://www.hp.com/go/dataprotectorexpress/sse> для регистрации и получения ключа (valid key). Маленький секрет – желательно использовать MS Internet Explorer, так как в других браузерах скрипт может работать некорректно (например, мне в первый раз с Mozilla Firefox 3.0 и OpenSUSE Linux 11.1 ключ получить не удалось). Ответив на необходимые вопросы и получив на e-mail с valid key, приступаем к установке программы.

Для этого входим в систему как пользователь backupер, вставляем CD с программой, получаем доступ к CD (при необходимости монтируем носитель) и запускаем программу Terminal (командную строку).

Набираем команду su и вводим пароль пользователя root для перехода в режим суперпользователя. И, перейдя в каталог с примонтированным CD, запускаем программу install. Запустится окно установки программы (см. **рис. 7**).

В принципе здесь особо описывать нечего. Установка программы проходит штатным путем, с использованием понятного графического интерфейса.

В конце программа-инсталлятор предложит запустить HP Data Protector Express Single Server Edition.

К сожалению, так как программа была запущена из-под учетной записи root, то и ярлык для запуска программы также был создан в домашнем каталоге пользователя root. Для устранения этого нюанса нужно всего лишь скопировать ярлык с рабочего стола (Desktop) из домашнего каталога root на рабочий стол пользователя backupер и назначить соответствующие права.

## Создание запланированной задачи по резервному копированию

Как было описано выше, резервное копирование на ленту будет выполняться раз в день по схеме Full Backup. Поэтому мы не будем решать вопросы, связанные со сложной схемой планирования, ротацией носителей, и т.д. Все, что нам нужно, это создать зада-

чу по полному копированию выбранных каталогов кэш-сервера на ленту раз в день, при этом ленточный носитель будет каждый раз перезаписан.

Для начала запускаем программу HP Data Protector Express Single Server Edition. (Если программа уже запущена, данный шаг можно пропустить.)

При старте программы потребуются ввести пароль доступа. По умолчанию реквизиты для доступа: сервер localhost, имя пользователя admin, без пароля (см. **рис. 8**).

Далее запустится основное окно программы. Надо отдать должное разработчикам – программа имеет простой и понятный интерфейс, большинство операций выполняется при помощи «помощников» (Wizards) (см. **рис. 9**). Для получения информации по работе с программой на установочном диске имеется подробная документация.

По умолчанию при запуске программы сразу открывается раздел Wizards. (Для перехода в данный раздел можно воспользоваться иконкой Wizards в правой части окна.) Кликаем на значке Backup и переходим в окно выбора способа копирования. Кликаем на самой нижней иконке в левой части окна Backup Specific и переходим в окно Wizard – Welcome. В поле Enter the name for the command being created вводим имя нашего задания и щелкаем кнопку Next.

Теперь мы попадаем в окно Select files and folders, где выбираются фай-

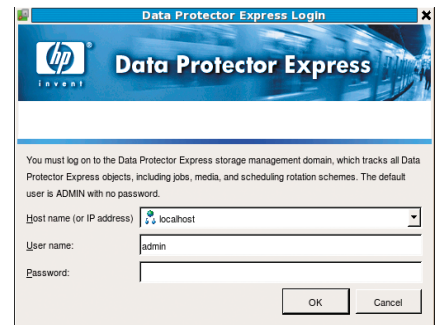


Рисунок 8. Окно ввода реквизитов

лы и каталоги, подлежащие копированию на ленту.

Далее после нажатия кнопки Next появляется окно Device Options. Здесь необходимо выбрать используемое устройство (Device to be used), а также установить некоторые параметры: «Автоформатирование» (Auto format – Auto format mode), «Имя нового носителя» (New media name) и др. (см. **рис. 10**).

Снова нажимаем кнопку Next. В открывшемся окне Job Options задаем следующие параметры (см. **рис. 11**):

- Backup Mode – Full (будем создавать полный бэкап).
- Auto verify mode – Quick verify (режим автопроверки. По умолчанию стоит Full verify, но режим полной проверки архива занимает весьма продолжительное время, сравнимое со временем выполнения копирования, поэтому в данном случае ограничимся проверкой на читаемость носителя, учитывая тот факт, что мы каждый день созда-

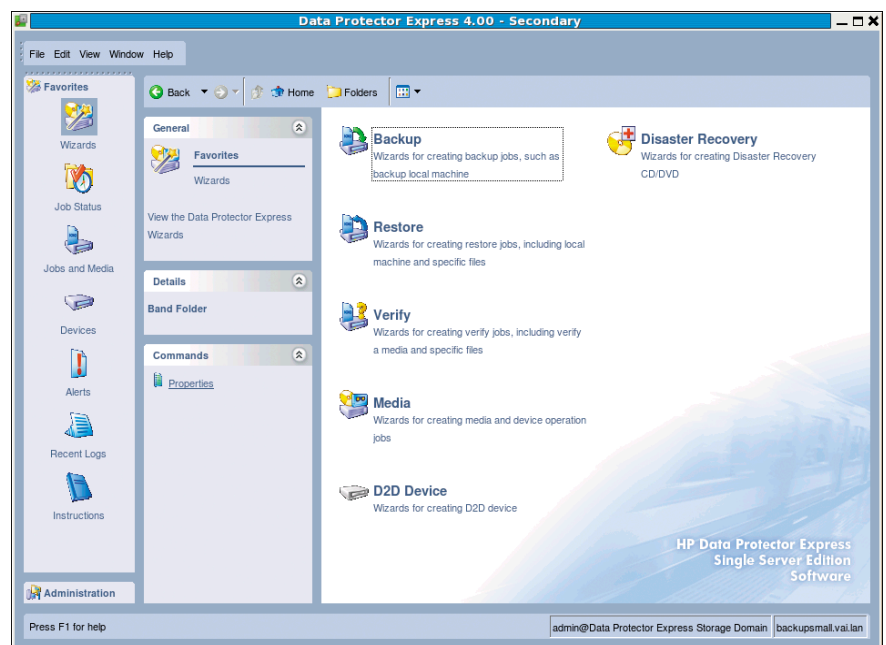


Рисунок 9. Основное окно программы



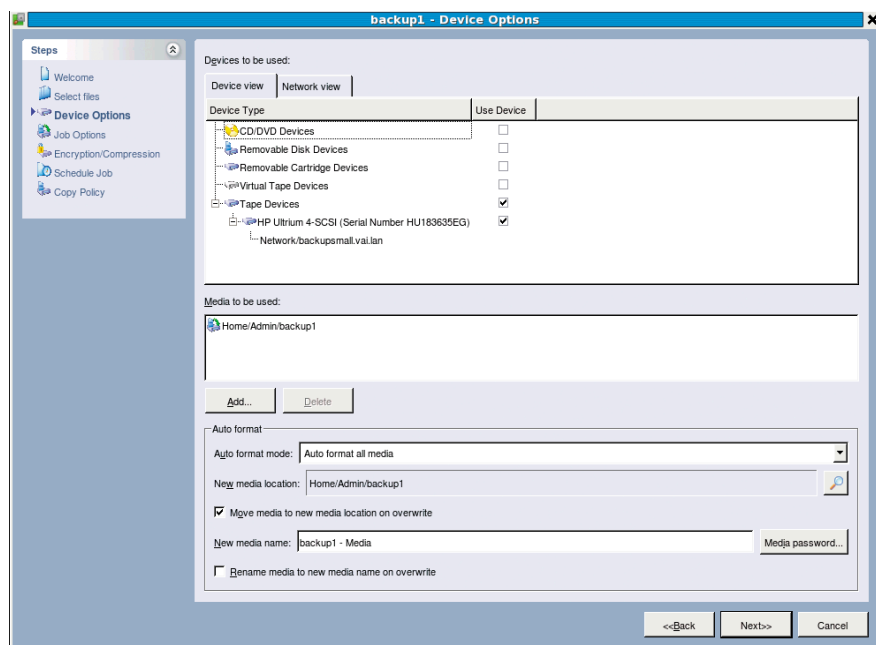


Рисунок 10. Окно Device Options

ем полную копию данных. Следует помнить, что для твердой уверенности в качестве записанной копии следует обязательно использовать режим Full verify).

- Span mode – Split file. В случае если файл слишком велик для использования на одном носителе, использовать несколько носителей. В другом случае, при выборе Restart file, программа будет просить поместить в накопитель другой носитель большего размера.
- Change mode – Prompt to another media. Если программа не обнаруживает требуемый носитель, она высылает предупреждение с просьбой загрузить искомым носитель в накопитель.

Окно Encryption/Compression появляется сразу после Job options. Здесь задаются параметры шифрования (encryption) и сжатия (компресии). Следует заметить, что заявленный объем для носителей LTO (1,6 Гб для LTO4, 800 Мб для LTO3 и т.д.) будет доступен только при включении аппаратного сжатия. (И то при условии, что информация на носителе может быть успешно сжата).

Предпоследнее окно – Shedule job, как и следует из названия, служит для планирования выполнения задания в нужное время. Так как мы собираемся всего лишь запускать Full backup в нужное время, при этом просто пе-

резаписывая вставленный носитель и не обращая внимания на дополнительные нюансы типа ротации носителей, то ограничимся самым простым расписанием.

Для этого выбираем:

- Shedule type – Run repeatedly. Для создания настроек расписания.
- Start time – 10:30. Время старта задания. К этому времени у нас в любом случае должен завершиться ночной Full backup с рабочих серверов на кэш-сервер.
- Start date – 15/05/2009. Дата начала бэкапа.

- Rotation type – No rotation. В нашем случае ротация носителей не требуется.

И в последнем окне Copy Policy остается нажать кнопку Finish.

Все, задание по резервному копированию создано. Осталось проконтролировать его выполнение, и, при необходимости, внести корректировки для обеспечения требуемой функциональности.

## Проверка возможности восстановления из резервной копии

Для проверки возможности восстановления поступим следующим образом. Скопируем на кассету один небольшой файл, а потом попробуем его восстановить.

Для этого снова перейдем в окно Wizards и выберем иконку Restore. Это приведет нас в следующее окно, где нам будет предложен всего один единственный метод восстановления Restore Specific. Жмем на одноименную иконку и переходим в окно Select files and folders. Здесь выбираются файлы, подлежащие восстановлению.

После нажатия кнопки Next мы переходим в окно Device options, в котором собственно и выбирается устройство и носитель, с которого будут восстанавливаться файлы.

Далее по кнопке Next перед нами появляется окно Job options. Основная

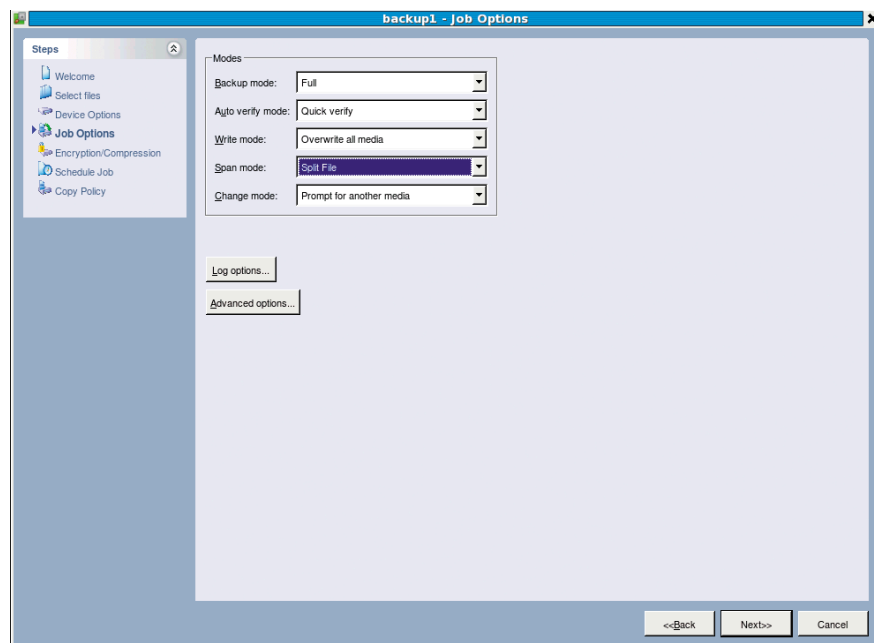


Рисунок 11. Окно Job options

деталь, на которую надо обратить внимание, – флажок *Restore files that are in use* (восстанавливать ли файлы, использующиеся в данный момент). Дополнительные параметры, устанавливаемые в окне *Advanced options*, вызываемом по нажатию одноименной кнопки, в большинстве случаев лучше оставить без изменения (см. рис. 12).

Ну и наконец уже знакомое нам окно планировщика *Schedule job*.

Все, далее после нажатия кнопки *Finish* начнется процесс восстановления выбранного нами файла.

Конечно, весьма огорчает тот факт, что программа лишена возможности восстанавливать файлы в другое место (как минимум, мне лично так и не удалось обнаружить данную функцию). Придется учитывать этот факт в работе и переименовывать файлы и каталоги, которые желательно не затирать при восстановлении из резервной копии.

## Настройка ntbackup

Несмотря на то что в мире существует довольно большое число программ резервного копирования для операционных систем семейства Windows, программа *ntbackup* продолжает пользоваться популярностью в первую очередь за бесплатность и простоту использования. Рассмотрим маленький пример по созданию тестового задания резервного копирования.

Для запуска программы достаточно в строке запуска «Выполнить» (*Run*) меню «Пуск» (*Start*) ввести имя программы *ntbackup* и нажать <Enter>.

Если программа запускается первый раз, она выдаст окно запуска мастера (*Wizard*). Пользоваться им не очень удобно, поэтому мы откажемся от его использования, сняв пометку «Всегда запускать в режиме мастера».

Далее в окне «Архивация и восстановление» мы выбираем пункт «Архивация файлов и параметров» и переходим к следующему окну: «Что следует архивировать». В зависимости от цели резервирования выбираем один из двух пунктов: «Всю информацию на данном компьютере» или «Предоставить возможность выбора объектов для архивации» (в нашем случае отмечаем второй пункт). Далее переходим в окно выбора объектов, подлежащих резервному копированию.

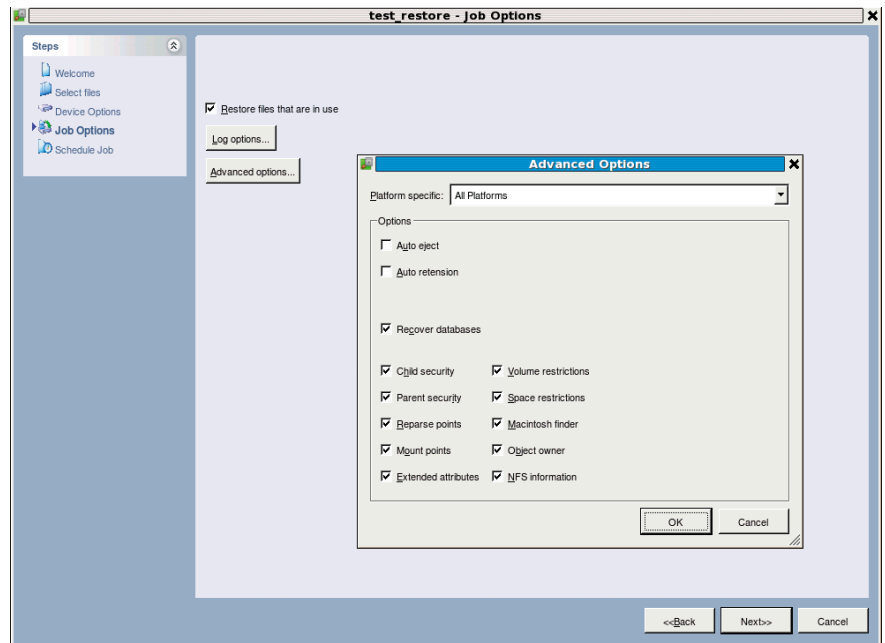


Рисунок 12. Окно *Job options* с открытым окном *Advanced options*

Отметив необходимые пункты, нажимаем кнопку «Далее» и переходим к следующему окну «Имя, тип и расположение архивации», где указывается ресурс, на который будет производиться копирование (мы указываем адрес и расшаренный ресурс нашего кэш-сервера).

Появится окно «Завершение мастера архивации и восстановления». В случае если больше ничего не надо настраивать, можно нажать кнопку «Финиш», и процесс резервного копирования сразу же запустится, при этом большая часть параметров будет установлена по умолчанию. Но так как мы хотим создать запланированное задание, мы нажимаем кнопку «Дополнительно» и продолжаем настройки.

В окне «Тип архива» выбираем какой архив мы будем делать: «Обычный» (*Full backup*), «Добавочный» (*Differential*), «Разностный» (*Incremental*) и т.д. Следующее окно предлагает выбрать «Способы архивации».

Назначить метод копирования и указать цель (файл или устройство). Далее задание можно либо запустить сразу, либо запланировать на определенное время. При планировании задания в «Планировщике» Windows (*Windows Scheduler*) появится задание в виде командной строки с длинным перечнем параметров. (Которую при желании можно вставлять в скрипты и т.д.). Помимо всего прочего, данная программа умеет корректно копи-

ровать открытые файлы. Как говорится – «дешево и сердито». Эту программу мы будем использовать для сбора информации с серверов, работающих под Windows.

## Завершающая настройка системы резервного копирования

После окончательной настройки кэш-сервера и системы записи на ленту осталось немного. Проверить доступность сетевых ресурсов на нашем сервере резервного копирования, настроить локальное ПО для создания резервных копий.

Еще нужно обязательно составить расписание резервного копирования, назначить ответственных лиц и передать им соответствующие полномочия.

## Заключение

Нет сомнения в том, что резервное копирование – важный аспект в работе ИТ-структуры любой компании. И несмотря на жесткие экономические условия, тем не менее возможно создать приемлемо работающую систему резервного копирования, затратив минимум средств на приобретение необходимых компонентов (ленточного накопителя и кассет). При этом созданная система позволяет делегировать полномочия другому лицу и при необходимости легко восстанавливать потерянные данные. ●



# Новые методы защиты и управления информацией

**Необходимость защиты информации – прописная истина для любого человека, связанного с компьютерными технологиями. Угрозы потери или порчи ценных данных остаются головной болью всех ИТ-специалистов, вне зависимости от размера обслуживаемого компьютерного парка. Эта статья рассказывает о способах и средствах решения нескольких из большого множества проблем, связанных с защитой информации.**

**П**римеры решения конкретных задач приведены с использованием решений компании Paragon Software. Как один из ключевых игроков рынка программного обеспечения, связанного с управлением и защитой цифровых данных, Paragon Software предлагает небольшим и средним по размеру компаниям несколько продуктов, обеспечивающих должный уровень защиты важной информации и с приемлемой стоимостью, что особенно важно во время трудной финансовой обстановки.

- **Paragon Drive Backup (DB)** – универсальное средство создания и управления секторными и файловыми архивами, с возможностью последующего восстановления информации как с работающей операционной системой, так и в случае её отсутствия или неработоспособности.
- **Paragon Adaptive Imaging Tools (PAIT)** – набор программ, позволяющих подготовить существующую программную среду на основе операционной системы семейства Microsoft Windows к перемещению на новое аппаратное обеспечение.
- **Paragon Remote Management (PRM)** – система дистанционного удаленного управления созданием резервных копий данных на компьютерах, подключенных к локальной сети.

Рассмотрим возможные проблемы, связанные с защитой данных, и варианты их решения с помощью вышеперечисленных приложений.

## Замена аппаратного обеспечения без подготовки нового программного окружения

Не секрет, что операционные системы Windows весьма чувствительны к смене оборудования, на котором они функционируют. Неполомки, скорее всего, возникнут при смене следующего аппаратного обеспечения: материнской платы компьютера, процессора, RAID- или SCSI-контроллера. В большинстве случаев система попросту откажется загружаться. Чаще всего с неработоспособной Windows можно столкнуться при восстановлении архивов жестких дисков компьютера после замены одного из вышеперечисленных компонентов или после решения о полной замене конкретных типов компьютеров, например замены сервера на более мощную машину.

Восстановление исходной конфигурации «с нуля», очевидно, требует больших затрат рабочего времени сотрудников, так как необходимо произвести множество нетривиаль-

ных операций. Кроме того, все архивные копии программного окружения со старой машины оказываются устаревшими и бесполезными.

Однако процесс миграции программного окружения на новый компьютер можно значительно ускорить, если воспользоваться архивной копией и произвести подготовку операционной системы к новому аппаратному обеспечению после восстановления данных. Обе эти операции легко выполнить в Paragon Drive Backup. Не имеет значения, какой именно программой были восстановлены данные; операционную систему можно быстро подготовить к запуску с помощью загрузочного диска от DB. Задача решается с помощью установки необходимых драйверов аппаратного обеспечения, которые отсутствуют в существующей ОС. Программа проверит компьютер на наличие нового оборудования и предложит добавить драйверы, если их нет в восстановленной операционной системе, либо автоматически активирует драйверы, если они отключены.

Эта операция так же эффективна при восстановлении работоспособности ОС после замены одного из ключевых аппаратных компонентов компьютера.

## Использование виртуальных сред

Системы виртуализации в настоящий момент применяются для более эффективного использования вычислительных ресурсов серверов, а также при необходимости использования нескольких разнотипных программных платформ. Компания может сократить затраты на аппаратные ресурсы за счет перемещения существующих программных сред с реальных компьютеров под управление виртуальной машины, установленной на один, но более мощный сервер. Этот процесс носит название миграции в виртуальную среду (P2V) и во многом схож с ранее рассмотренным процессом смены аппаратного обеспечения.

Затраты времени на создание виртуальной среды с нуля могут кардинально сказаться на работоспособности всей информационной системы компании. Более быстрое и эффективное решение задачи предоставляет программа Paragon Drive Backup. На первом этапе администратор создает пустую виртуальную среду. Затем в Drive Backup он создает виртуальный диск соответствующего типа и копирует на него всю необходимую информацию с существующего компьютера. На конечном этапе программа автоматически подготовит операционную систему к работе в виртуальной машине на новом оборудовании.

Аналогичным образом виртуальная среда может использоваться в качестве временной подмены реального сервера. Администратор просто восстанавливает с помощью DB один из существующих архивов сервера в виртуальную среду, а затем, после восстановления работоспособности сервера, восстанавливает архив виртуальной среды на реальной машине с добавлением драйверов при необходимости.

При работе с виртуальными средами может очень пригодиться одна из возможностей Drive Backup. Программа способна не только создавать но и открывать существующие файлы виртуальных дисков в режиме чтения и записи. При этом содержимое диска отображается в программе аналогично содержимому реального жесткого диска компьютера, и для виртуальных дисков доступны все операции, что и для их реальных аналогов.

## Обеспечение большого количества разнотипных компьютеров необходимыми программами

Перед информационным отделом компании поставлена задача быстрого развертывания операционной системы и программ на некотором количестве компьютеров. При этом среди них присутствуют машины с различными аппаратными компонентами. Решений у этой задачи несколько, рассмотрим некоторые из них. Наиболее очевидное – подготовка каждой машины в отдельности, включая установку операционной системы и программ вручную. По затратам времени это решение наиболее расточительное, особенно при необходимости обслужить большое количество компьютеров. Процесс можно несколько усовершенствовать, если после установки операционной системы и программ создать архивы данных каждой типовой конфигурации компьютеров. Несомненно, в этом случае выполнение поставленной задачи ускоряется, но только если типовых конфигураций небольшое количество, ведь даже при малейшем отклонении в аппаратном обеспечении могут возникнуть проблемы с работой Windows. Как бы то ни было, в обоих случаях сотрудникам компании, выполняющим развертывание данных, требуется выполнить значительное количество однотипных и повторяющихся операций. Рассмотрим решение проблемы с помощью программного обеспечения Paragon Software.

**Первый шаг:** при помощи набора программ Adaptive Imaging Tools IT специалист компании на каждом из типовых компьютеров выясняет и сохраняет информацию об аппаратном обеспечении.

**Второй шаг:** на одном из компьютеров устанавливаются операционная система и необходимые программы, затем опять же с помощью PAIT в операционную систему добавляются драйверы всех аппаратных компонентов, всех существующих типов компьютеров. Выполняется данная операция одной из программ набора, которая анализирует набор драйверов существующей операционной системы и сохраняет заранее информацию об аппаратном обеспечении всех остальных компьютеров.

**Третий шаг:** после добавления всех необходимых драйверов с помощью Drive Backup создается единый универсальный образ-архив операционной системы и программ, который затем используется для восстановления на всех без исключения компьютерах.

## Обеспечение комплексной защиты данных в локальной сети компании

Информационная система компании в данном примере состоит из следующих компонентов: серверы, рабочие станции пользователей, а также их персональные компьютеры, в том числе ноутбуки. Предполагается, что среда работы компании основывается на продуктах серии Microsoft Windows и Microsoft Windows Server. Требуется организовать централизованную систему создания и хранения архивных копий данных со всех компьютеров компании.

Для решения данной задачи можно воспользоваться программами Paragon Drive Backup и приложениями, входящими в пакет программ Paragon Remote Management. Администратор системы должен выбрать центральную машину для управления инфраструктурой резервного копирования. На эту центральную станцию устанавливаются Paragon Drive Backup Server и приложение PRM Console.


На серверные машины нужно установить соответствующие версии DB. Рабочие станции пользователей и их персональные компьютеры оснащаются приложениями Paragon Remote Management Client.

Хотя архивные копии могут храниться в нескольких местах, создание выделенного сетевого хранилища является наилучшим способом добиться надежного хранения резервных данных. Хранилище может располагаться как на отдельном сервере, так и на одном из дисков уже существующих серверов. В случае каких-либо затруднений в работе с сетевыми ресурсами либо сокращения нагрузки на сеть архивы могут храниться локально на клиентских машинах.

Управление резервным копированием всех компьютеров осуществляется администратором с машины, где установлено приложение PRM Console. Администратор должен создать Хранилище PRM – базу данных для хранения статистики по всем зарегистрированным клиентам, запланированным задачам, созданным группам и шаблонам задач, а также для хранения отчетов, отправляемых клиентами, и логов, отправляемых исполнителями.

После настройки системы дальнейшая задача администратора – создание задач резервного копирования. Задачи могут быть назначены для отдельного клиента, группы клиентов или всех клиентов, зарегистрированных в Хранилище PRM. Помимо этого, есть шаблоны задач для наиболее часто выполняемых операций. В случае необходимости внести изменения в процесс создания архивных копий администратору нужно либо исправить существующие задачи, либо создать новые.

## Заключение

В этой статье было рассмотрено несколько вариантов использования программных продуктов компании Paragon Software. Их основная задача заключается в обеспечении удобного и легкого способа защитить важные данные, помощи в быстром перемещении информации между реальными и виртуальными средами, обеспечении удобной миграции программного окружения между различными компьютерами. 

Сергей Соломатин



# Резервирование и восстановление объектов Active Directory в Windows Server 2008/2008 R2



**Сергей Яремчук**

**Служба Active Directory является стандартом в корпоративных сетях, работающих под управлением Windows. Обеспечивая администратора эффективными инструментами, внешне простая в использовании, она является тем не менее довольно сложной по своей структуре и составу. К тому же никто не застрахован от сбоев в работе операционной системы, программ, отказа «железа» или ошибки человека. Поэтому нужно быть всегда готовым к тому, что придется предпринять меры по восстановлению работы в целом или отдельных элементов.**

## **О необходимости резервного копирования**

В каждой новой версии Windows Server появляются новые инструменты, упрощающие и автоматизирующие процесс управления, с которыми может справиться даже начинающий администратор. Одним из распространенных мнений среди таких «специалистов» является вообще отказ от ре-

зервирования контроллеров доменов. Аргумент простой. В организациях среднего и крупного размеров используется несколько контроллеров доменов, это аксиома. Вероятность того, что в один день выйдут из строя все, практически равна нулю. Если только их не вынесут по постановлению прокурора или воспользовавшись ошибкой в организации охраны,

но этот случай, согласитесь, из ряда вон выходящий. Поэтому если выходит из строя один контроллер домена, все остальные работают в штатном режиме, а ему на замену подготавливается новый сервер. Отчасти они правы, но резервирование хотя бы двух контроллеров (на случай ошибки), имеющих роли FSMO (Flexible single-master operations, операции с одним испол-



нителем), все же обязательно. Так рекомендуют Microsoft и здравый смысл. Причем есть еще один главный довод в пользу резервирования. Простота управления приводит к росту процента ошибок. Удалить случайно объект Active Directory довольно просто. И необязательно это может быть умышленное действие, это может произойти, например, в результате ошибки при выполнении скрипта. И чтобы восстановить все настройки, потребуется приложить некоторые усилия.

Если ошибка обнаружена не сразу и изменение уже реплицировалось на другие контроллеры, в этой ситуации вам и понадобится резервная копия. Я уже не говорю о небольших организациях с одним контроллером домена.

Документом, показывающим возможности по резервированию и восстановлению данных в Windows Server 2008, является статья Джил Киркпатрика (Gil Kirkpatrick) «Резервное копирование и восстановление Active Directory в Windows Server 2008» в [1], которую и рекомендую к прочтению. Но если вопросы резервирования расписаны полностью, то восстановление показано, на мой взгляд, несколько поверхностно и не дает полной картины. Эта статья, собственно, и появилась из заметок, составленных на тот крайний случай.

## Система архивации данных Windows Server

В Windows Server 2008 на замену NT Backup пришел абсолютно новый компонент «Система архивации данных Windows Server» (Windows Server Backup, WBS), основанный на VSS (Volume Shadow Copy Service, сервис теневое копирования тома). WBS – довольно мощное приложение, позволяющее восстанавливать систему, в том числе и на другой компьютер, поддерживающее некоторые сервисы, в списке которых значится и AD.

Установить WBS просто, следует лишь активировать компонент «Возможности системы архивации данных в Windows Server» плюс подпункт «Система архивации данных Windows Server». Последний включает MMC-консоль управления и новое средство командной строки Wbadmin. Дополнительно доступен пункт «Программы командной строки», который включает сценарии PowerShell, позволяющие создавать и управлять резервными копиями.

В командной строке установка выглядит еще проще:

```
> servermanagercmd -install Backup-Features
```

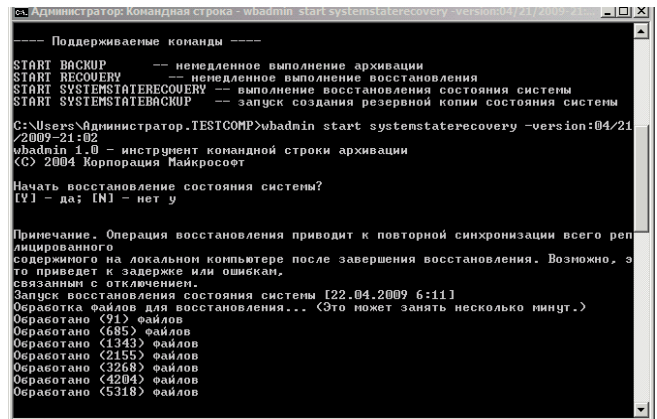
Или в Server Core:

```
> ocsetup WindowsServerBackup
```

Управлять резервированием можно из MMC-консоли или в командной строке. Так, чтобы создать резервную копию критичных томов, следует ввести:

```
> wbadmin Start Backup -backupTarget:E -allCritical
```

С полной копией, думаю, все понятно. В контексте статьи нас больше интересует резервное копирование состояния системы при помощи параметра SystemStateBackup.



Восстановление состояния системы из SystemState-копии

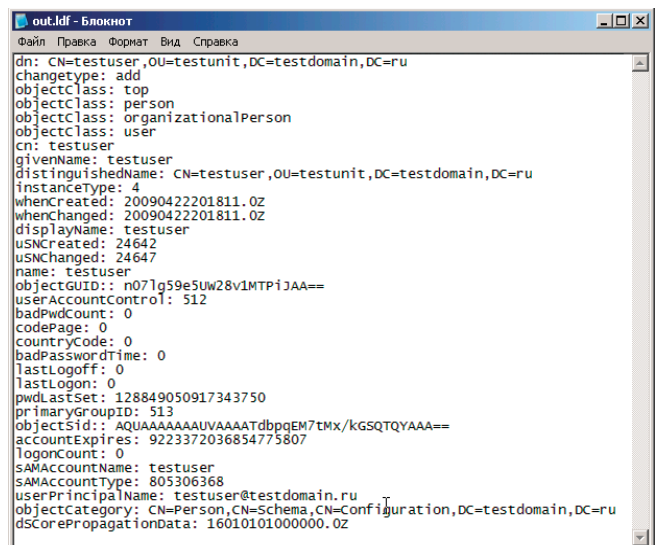
Кстати, в первых сборках Windows Server 2008 этой функции не было, а через MMC она недоступна:

```
> wbadmin Start SystemStateBackup -backupTarget:E:
```

В этом случае производится пофайловое копирование состояния системы и некоторых сервисов, в числе которых есть и AD. Самое неудобное в этом случае, что каждый раз приходится создавать полную копию (свежеустановленная система приблизительно 7 Гб), а процесс происходит несколько медленнее, чем обычное резервирование. Но зато восстановить такую копию можно на другой компьютер с идентичной конфигурацией.

В команде копирование производится на другой том. Но в KB944530 [2] рассказано, как разрешить возможность резервного копирования на любой том. Для этого нужно добавить параметр типа DWORD с именем AllowSSBToAnyVolume и значением 1 в ветку реестра HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\wbengine\SystemStateBackup.

С резервированием обычно здесь проблем не возникает, все просто и понятно, трудности начинаются, когда необходимо восстановить работоспособность AD или случайно удаленных объектов. Использование SystemState-копий позволяет обойтись без восстановления всей систе-



Созданный ldf-файл необходимо подправить



мы, а просто вернуть предыдущее состояние служб AD. Графическая консоль, предназначенная для восстановления данных, копий SystemState не видит (находятся на диске в другом каталоге SystemStateBackup). Если попробовать запустить процесс восстановления в рабочей системе, получаем сообщение о том, что так как архив содержит службу доменов Active Directory, операцию необходимо производить в режиме восстановления службы каталогов (Directory Services Restore Mode, DSRM). Это один из минусов, так как контроллер домена в это время будет недоступен.

Новый механизм загрузки BCD, появившийся в Windows, начиная с Vista, в котором убранны старый добрый boot.ini, заставляет нас произвести еще ряд действий, чтобы попасть в DSRM. В составе ОС имеется специальная утилита, предназначенная для редактирования параметров загрузчика (в Интернете можно найти графические утилиты, но я считаю им не место на сервере). Создаем новую копию записи:

```
> bcdedit /copy {default} /d "Directory Service Repair Mode"
```

```
Запись успешно скопирована в {df127c16-2ec7-11de-bc25-000c2971dfb5}
```

Теперь устанавливаем ее, указав в качестве параметра полученный ID:

```
> bcdedit /set "{df127c16-2ec7-11de-bc25-000c2971dfb5}" /safeboot dsrepair
```

Если команды вводятся с использованием PowerShell, то {ID} следует вводить в скобках «{ID}», иначе получаем ошибку:

```
The set command specified is not valid
```

По окончании проверяем:

```
> bcdedit /enum
```

В списке должен появиться новый пункт.

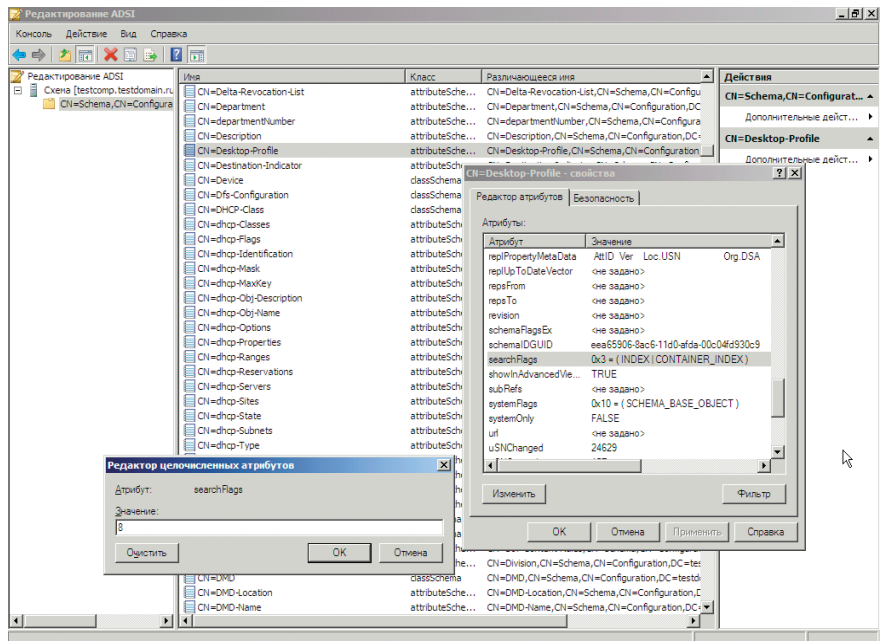
Перезагружаемся, выбираем пункт Directory Service Repair Mode и, нажав <F8>, отмечаем «Режим восстановления службы каталогов». Обратите внимание, что в этом режиме следует для входа использовать данные администратора локальной системы, а не доменную учетную запись.

Далее все просто. Получаем список резервных копий (команда wbadmin «видит» копии SystemState).

```
> wbadmin get versions
```

```
Время архивации: 22.05.2009 1:02
Идентификатор версии: 05/21/2009-21:02
Можно восстановить: Приложение (ия), Состояние системы
```

И восстанавливаем, используя в качестве параметра полученный идентификатор версии:



Установка searchFlags для нужного атрибута позволит сохранить его при удалении

```
> wbadmin start systemstaterecovery -version:05/21/2009-21:02
```

Если восстановление производится с локального диска, параметр BackupTarget, показывающий wbadmin, где взять резервную копию, указывать необязательно. Если копия находится на сетевом ресурсе, его прописываем так:

```
-BackupTarget: \\computer\backup -machine:server-ad
```

Несмотря на предупреждение о том, что:

Операция восстановления приводит к повторной синхронизации всего реплицированного содержимого на локальном компьютере после завершения восстановления. Возможно, это приведет к задержке и ошибкам.

Восстановление службы каталогов происходит обычно без проблем. После перезагрузки встречаем сообщение о том, что начатая операция по восстановлению успешно завершена.

Перейдя в консоль управления Active Directory, обнаруживаем, что все находится на своих местах... кроме новых объектов, созданных уже после того, как было произведено резервирование. В принципе такой результат ожидаем. А для восстановления отдельных объектов есть совсем другой путь (даже несколько).

## Принудительное восстановление объектов при помощи NTDSUTIL

В состав Windows Server входит утилита командной строки NTDSUTIL, предназначенная для обслуживания, управления и контроля Active Directory Domain Services (AD DS) и Active Directory Lightweight Directory Services (AD LDS). В системе утилита становится доступной после установки роли AD DS. В Windows Server 2008 ее функциональность несколько изменилась. Так, в Windows Server 2003 с ее помощью можно было восстановить всю базу данных, но в 2008 с этим отлично справляется wbadmin, наверное, поэтому ее возможности по восстановлению чуть подсо-

кратили. Теперь, используя NTDSUTIL, можно восстановить организационное подразделение со всем содержимым и отдельный объект.

Ее работа основана на мгновенных снимках Active Directory, сделанных при помощи службы VSS. Снимок представляет собой компактную резервную копию работающей службы Active Directory со всеми каталогами и файлами. Создание такой копии в отличие от SystemState происходит очень быстро и занимает несколько секунд.

```
> ntdsutil
```

Переходим в контекст snapshot:

```
ntdsutil: snapshot
```

Запускаем команду создания снимка (краткая форма – «as i ntds»):

```
снимок: activate instance ntds
```

```
Активный экземпляр "ntds".
```

```
снимок: create
```

Через некоторое время получаем информацию о созданном снимке, выходим:

```
снимок: quit
ntdsutil: quit
```

Теперь, чтобы восстановить базу Active Directory, достаточно ввести «ntdsutil files repair» в командной строке режима DSRM, но нас интересует отдельный объект.

Просмотреть список удаленных объектов можно при помощи LDP.exe, воспользовавшись командлетами PowerShell Get-ADObject и Restore-ADObject (есть и другие варианты).

В LDP, например, следует подключить к серверу, выбрать «Параметры (Options) → Элементы управления (Controls)» и в раскрывающемся списке «Предопределенная загрузка» (Load Predefined) установить параметр Return deleted objects. Затем переходим в «Вид → Дерево», выбираем контекст домена. В итоге в дереве справа появится объект CN=Deleted Object, где и находим все удаленные объекты.

Теперь важное – при удалении объект теряет большую и важную часть своих свойств (в частности, пароль, managedBy, memberOf), поэтому после его восстановления он будет не совсем в том виде, как нам хотелось. Это все хорошо видно в LDP. Но здесь есть несколько вариантов:

- увеличить количество атрибутов, которые не будут затерты при удалении объекта в хранилище удаленных объектов;
- восстановить объект и вернуть ему атрибуты;
- и самый лучший – заблокировать объект от случайного удаления.

Увеличить количество сохраненных при удалении атрибутов можно, установив параметр searchFlags для нужного атрибута в значение 8 (PRESERVE\_ON\_DELETE). Для этого следует запустить редактор интерфейса служб AD – ADSIEdit, подключиться к контексту наименования «Схема» (CN=Schema). Далее выбираем нужные параметры, например, Description (описание) и Unicode-PWD (пароль) и устанавливаем searchFlags в 8.

Восстановить удаленный объект можно несколькими способами. Самый удобный – утилита AdRestore Марка Руссиновича (Mark Russinovich) [3]. Скачиваем и вводим:

```
> adrestore -r user
```

Получаем объект с частью атрибутов.

Остальные методы расписаны в KB840001 [4], они не так просты, поэтому останавливаться на них не буду.

## Восстанавливаем атрибуты объектов

В снимке, полученном при помощи ntdsutil, есть объект и его атрибуты. Образ можно монтировать и подключать в качестве виртуального LDAP-сервера, экспортирующего объекты. Вызываем ntdsutil:

```
> ntdsutil
ntdsutil: snapshot
```

Смотрим список доступных снимков:

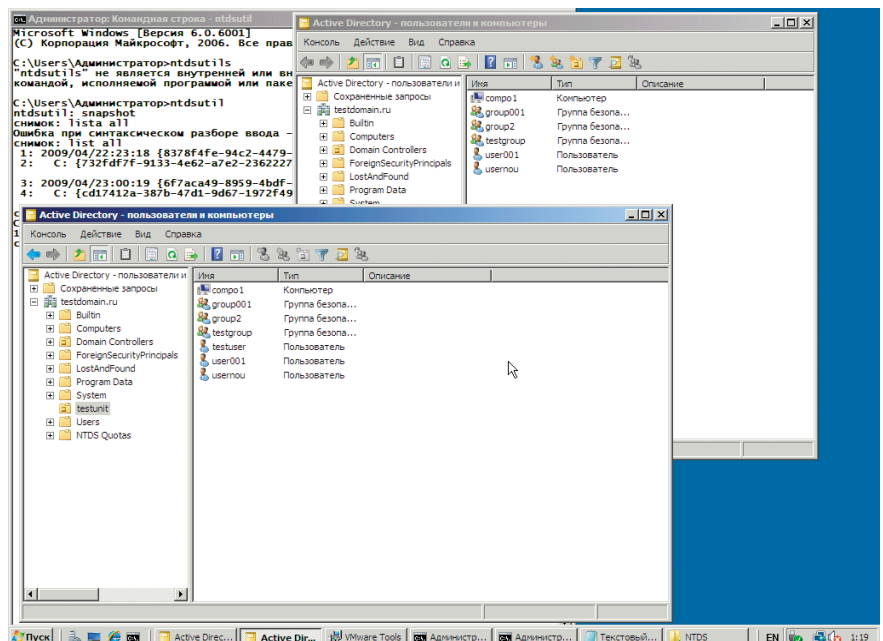
```
снимок: list all
```

```
1: 2009/04/22:23:18 {8378f4fe-94c2-4479-b0e6-ab46b2d88225}
2: C: {732fdf7f-9133-4e62-a7e2-2362227a8c8e}

3: 2009/04/23:00:19 {6f7aca49-8959-4bdf-a668-6172d28dde6}
4: C: {cd17412a-387b-47d1-9d67-1972f49d6706}
```

Монтируем командой mount с указанием номера или {ID}:

```
снимок: mount 4
```



Две консоли, подключенные к AD и виртуальному LDAP-серверу



Снимок {cd17412a-387b-47d1-9d67-1972f49d6706} установлен как  
C:\\$SNAP\_200904230019\_VOLUMECS\

Снимок смонтирован. Теперь можно перейти при помощи Проводника в указанный каталог и просмотреть, что находится внутри. Выходим из ntdsutil, введя дважды quit, образ по-прежнему будет смонтирован. Теперь, используя утилиту dsamain, создаем виртуальный LDAP-сервер, указав в качестве параметра путь к файлу ntds.dit, который находится в смонтированном снимке. В качестве порта LDAP-сервера я выбрал 10000:

```
> dsamain -dbpath C:\$SNAP_200904230019_VOLUMECS\ \
Windows\NT DS\ntds.dit -ldapPort 10000
```

EVENTLOG (Informational): NTDS General / Управление службой : 1000  
Завершен запуск доменных служб Active Directory (Майкрософт) версии  
6.0.6001.18000

Можно подключиться к виртуальному LDAP-серверу при помощи консоли «Active Directory – пользователи и компьютеры», указав в качестве параметра номер порта 10000, и просмотреть находящиеся внутри объекты.

Экспортируем параметры нужного объекта в ldf-файл, подробнее об ldifde написано в KB237677 [5].

```
> ldifde -r "(name=user)" -f export.ldf -t 10000
```

Установка связи с "testcomp.domain.ru"  
Вход от имени текущего пользователя с помощью SSP  
Экспорт каталога в файл export.ldf  
Поиск элементов...  
Записываются элементы.  
1 элементов экспортировано

В полученном ldf-файле следует изменить параметр changetype: add на changetype: modify и затем новый файл импортировать в каталог:

```
> ldifde -i -z -f import.ldf
```

Есть и другие варианты импорта/экспорта с использованием DSGET/DSMOD, PowerShell и так далее.

```
> dsget user cn=user,ou=ou1,dc=domain,ds=ru \
-s localhost:10000 -memberof | dsmof group \
-c -addmbr cn=user,ou=ou1,dc=domain,ds=ru
```

Другой метод основан на том, что каждый объект Active Directory имеет номер версии. При различии номеров версии на двух контролерах домена новым и правильным считается тот объект, у которого номер версии выше. Это и использует механизм «принудительного восстановления» (authoritative restore), когда восстановленному при помощи ntdsutil объекту присваивается номер выше и он принимается AD как новый. Для работы механизма принудительного восстановления сервер также перезагружается в DSRM.

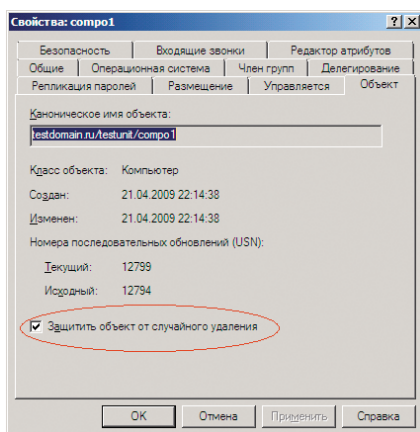
```
> ntdsutil "authoritative restore" \
"restore object cn=user,ou=group,dc=domain,dc=ru" q q
```

Аналогично восстанавливается подразделение:

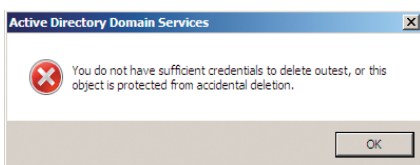
```
> ntdsutil "authoritative restore" \
"restore subtree ou=group,dc=domain,dc=ru" q q
```

## Защита объектов от удаления

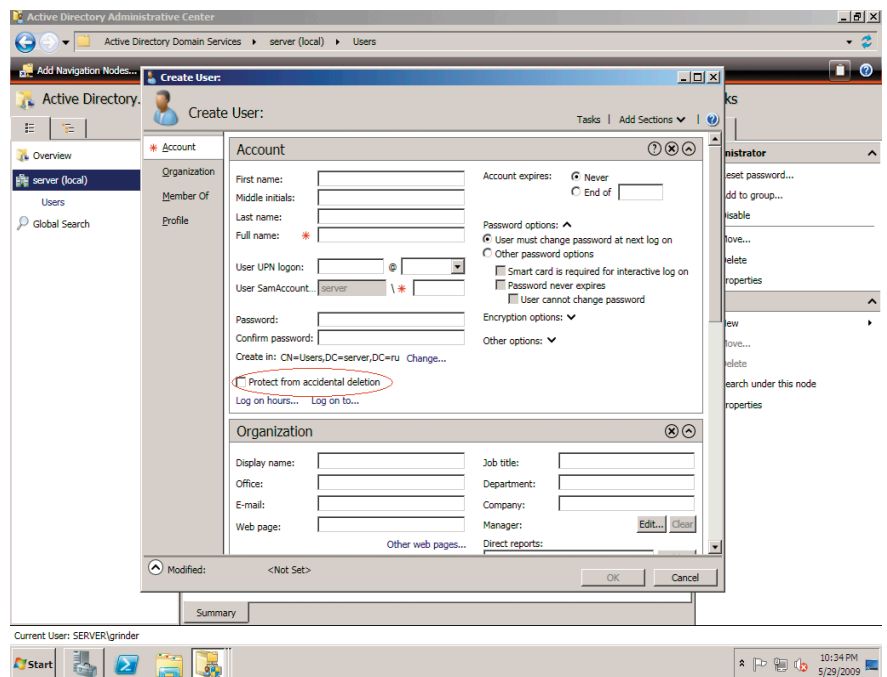
Начну с того, что вместе с Windows Server 2008 R2 [6] администраторы получили еще один функциональный уровень домена, и в итоге такой сервер может быть настроен в одном из четырех уровней – Windows 2000, Windows Server 2003, Windows Server 2008, Windows Server 2008 R2. Его можно указать на этапе установки при помощи dcpromo или повысить, если был выбран меньший уровень, используя меню Raise the domain (forest) functional level в Active Directory Admin Center, о котором чуть дальше. Причем возможна и обратная операция – понижение функционального уровня домена и леса, если они находятся на уровне Windows Server 2008 R2, его можно вернуть на уровень Windows



Защищаем объект от случайного удаления в Windows Server 2008



Объект защищен от случайного удаления



Защищаем объект от случайного удаления в Windows Server 2008 R2

Server 2008, ниже – на 2003 или 2000 – нельзя. Большинство из новых возможностей будут доступны только в том случае, если домен находится на уровне R2. Так, начиная с Windows Server 2008 в свойстве объекта появился дополнительный пункт, позволяющий его защитить от случайного удаления. Точнее, он был и раньше, но здесь его уже не приходится искать.

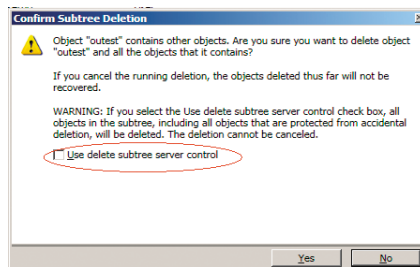
В Windows Server 2008 он доступен при создании подразделения (OU, Organizational Unit) и называется «Защитить объект (контейнер) от случайного удаления» (Protect object from accidental deletion). Такой флажок появляется только при создании нового OU. Для уже имеющихся OU, а также вновь создаваемых групп, компьютеров и учетных записей его можно активировать во вкладке «Объект» окна свойств (видно при активном «Вид → Дополнительные компоненты (Advanced)»).

В R2 нужный пункт Protect from accidental deletion имеется в свойствах отдельной учетной записи, компьютера, группы и подразделения, на самом видном месте. Достаточно установить здесь флажок и при попытке удалить объект, администратор получает предупреждение о невозможности произвести требуемую операцию. При этом нужно помнить, что флажок защищает от удаления лишь тот объект, в котором он установлен. То есть если он активирован для группы, на отдельные элементы, входящие в ее состав, эта установка никак не распространяется. То есть по-прежнему можно будет удалить любой объект внутри, если он не защищен персональным флажком. Чуть другая ситуация при удалении незащищенного OU. Если в его составе нет защищенных объектов, OU будет полностью удален. Но если такие объекты есть, то следует установить в появившемся окне флажок «Использовать элемент управления сервера «Удалить поддереву» (Use delete subtree server control). Иначе вместо удаления самого OU со всеми элементами будет фактически произведена попытка очистки OU от объектов, не имеющих защиты. Причем, как показывают эксперименты, очистка эта будет неполной, так как, столкнувшись с первым же защищенным объектом, программа прекращает работу, выдав предупреждение. Это характерно и для Windows Server 2008, и для R2 RC.

В Windows Server 2003 защитить объект от удаления можно, лишь установив в разрешениях запрет на «Удаление», «Удалить поддереву» и «Удалить все дочерние объекты» (Deny для Delete, Delete subtree, Delete All Child Objects). Такой подход не очень удобен, особенно если администрированием системы занимаются несколько человек и объекты все же нужно удалять.

## Active Directory Recycle Bin

В Windows Server 2008 R2 появилась новая функция Active Directory Recycle Bin (AD RB), автоматически активируемая, когда домен находится на уровне Windows Server 2008 R2. По своей сути она схожа с корзиной, используемой в Windows, в которую помещаются удаленные файлы, и случайно удаленный объект может быть быстро и без проблем восстановлен. Причем восстановленный из AD RB об-



При удалении дерева нужно подтвердить удаление всех объектов

ект сразу же получает и все свои атрибуты. По умолчанию время «жизни» удаленного объекта в AD RB составляет 180 дней, после этого переходит в состояние Recycle Bin Lifetime, теряет атрибуты и через некоторое время полностью удаляется. Изменить эти значения можно при помощи параметра msDS-deletedObjectLifetime. Если при установке AD был выбран уровень ниже R2, а затем был поднят командой:

```
PS C:\> Set-ADForestMode -Identity domain.ru -ForestMode Windows2008R2Forest
```

то AD RB следует активировать отдельно. Для этого используется командлет Enable-ADOptionalFeature PowerShell:

```
PS C:\> Enable-ADOptionalFeature -Identity 'CN=Recycle Bin Feature,CN=Optional Features,CN=Directory Service,CN=Windows NT,CN=Services,CN=Configuration,DC=domain,DC=ru' -Scope Forest -Target 'domain.ru'
```

Восстановить удаленный объект теперь очень просто:

```
PS C:\> Get-ADObject -Filter {displayName -eq "user"} -IncludeDeletedObjects | Restore-ADObject
```

Командлеты Get-ADObject и Restore-ADObject имеют большое количество параметров, например, позволяя найти OU, к которой принадлежала удаленная учетная запись, и затем восстановить весь OU. В документе Restore a Deleted Active Directory Object [7] все очень подробно изложено.

## Заключение

Несмотря на возможности новых серверных ОС от Microsoft, резервное копирование контроллеров Active Directory должно проводиться планомерно и постоянно, без этого невозможно восстановление отдельных объектов или OU. Причем помимо Windows Server Backup следует создавать снимки при помощи ntdsutil. Процесс резервирования упрощается, а объемы данных уменьшаются, если контроллер домена не выполняет других функций.

1. Джил Киркпатрик. Резервное копирование и восстановление Active Directory в Windows Server 2008 – <http://technet.microsoft.com/ru-ru/magazine/cc462796.aspx>.
2. Статья KB944530. Error message when you try to perform a system state backup in Windows Server 2008 – <http://support.microsoft.com/kb/944530>.
3. Утилита AdRestore – <http://technet.microsoft.com/ru-ru/sysinternals/bb963906.aspx>.
4. Документ KB840001. How to restore deleted user accounts and their group memberships in Active Directory – <http://support.microsoft.com/kb/840001>.
5. Документ KB237677. «Использование средства LDIFDE для импорта и экспорта объектов каталогов в Active Directory» – <http://support.microsoft.com/kb/237677/ru>.
6. Страница, посвященная Windows Server 2008 R2 – <http://www.microsoft.com/windowsserver2008/ru/ru/default.aspx>.
7. Документ Step 2: Restore a Deleted Active Directory Object – <http://technet.microsoft.com/en-us/library/dd379509.aspx>.



# Windows 7: продолжаем знакомство

Илья Рудь

**Разочарованы в Windows Vista? Считаете, что Windows 7 – это новая обертка старой операционной системы? Не торопитесь с выводами, Windows 7 есть чем удивить технического специалиста.**

**Н**а данный момент дата выхода новой операционной системы от Microsoft под названием Windows 7 уже не является секретом. Число обозначено, продукт поступит на полки магазинов в конце октября 2009 года. Партнерам и крупным корпоративным заказчикам он станет доступен во второй половине июля. Бытует мнение, что данная операционная система представляет собой доработанную Windows Vista, и это бесспорно так, но все же не стоит забывать и о новых возможностях преемницы Vista. Список изменений довольно широк и затрагивает многие компоненты операционной системы. Технические специалисты, пожалуй, первые, кому придется осваивать новый функционал, поэтому я предлагаю некоторый ликбез по ключевым изменениям в Windows 7.

## User Account Control

У специалистов и просто пользователей, знакомых с Windows Vista, после установки Windows 7 может возникнуть непреодолимое желание нарушить каноны безопасности и отключить технологию UAC (User Account Control). Советую все же не спешить, поскольку данный компонент Microsoft Windows в новой версии операционной системы был значительно доработан.

Первое, что можно заметить – это появление в панели управления апплета, позволяющего настроить активность контроля учетных записей. Для выбора предлагается 4 уровня защиты от наименее безопасного, когда UAC отключен, до максимального

уровня защиты, который использовался в Windows Vista.

Рассмотрим каждый из уровней:

- **Всегда оповещать при каждом изменении системы** – верхний и наиболее безопасный. Это поведение было в Vista, оповещение UAC появляется при внесении изменений на системном уровне (параметры Windows, установка ПО и т.д.)
- **Оповещать, только когда программа пытается внести изменения в компьютер** – уровень, установленный по умолчанию в Windows 7. Оповещения больше не появляются при работе в панели управления или при выполнении задач администрирования.
- **Третий уровень** – очень похож на второй, но имеет существенное отличие, оповещения UAC появляются на обычном рабочем столе, а не на заблокированном с использованием Secure Desktop. Данный уровень может быть полезен для систем с видеодрайверами, слишком медленно переключающимися на Secure Desktop. Но все же не следует забывать, что Secure Desktop является дополнительной преградой для ПО, пытающегося подделать ваш ответ.
- **Никогда не оповещать** – неркомендуемый уровень. При выборе этой опции UAC система полностью отключается. Отключение UAC нельзя сделать незаметно, пользователь получит предупреждение, и систему придется перезагрузить.

Расширенные настройки UAC по-прежнему находятся в параметрах локальной политики компьютера и представлены десятью параметрами. При использовании контроля учетных записей на корпоративных компьютерах будет правильней применить настройки UAC через групповую политику. К примеру, вы хотите добиться повышения безопасности работы путем конфигурирования UAC на всех компьютерах Windows 7 и соответствовать внутреннему стандарту безопасности вашей организации. Стандарт требует работы любых административных записей, в том числе встроенных администраторов с включенным UAC. И если администратор пытается выполнить какое-либо административное действие, он обязан еще раз ввести пароль для своей учетной записи. Обыкновенным же пользователям при попытке выполнения действия, требующего больших привилегий, система должна отвечать отказом. При этом любые запросы на повышение уровня доступа должны выводиться на безопасном рабочем столе. Довольно жесткий подход, который все же имеет место быть в компаниях, особенно серьезно относящихся к безопасности своих компьютеров (см. **рис. 1**).

Для решения данной задачи необходимо открыть параметры безопасности в разделе групповой политики «Конфигурация Компьютера».

Первый параметр, который необходимо настроить, называется «Контроль учетных записей: Все администраторы работают в режиме одобрения администратором». Перевод на русский язык

данного параметра неверный, этот параметр включает или отключает UAC для всех учетных записей, поэтому в нашем случае должен стоять в состоянии «Включен».

Второй параметр, подлежащий настройке «Контроль учетных записей: Режим одобрения администратором для встроенной учетной записи администратора». Включив его, мы задействуем работу UAC для встроенного администратора.

Теперь нужно описать действия системы при попытке администраторов или пользователей выполнить какие-либо действия, требующие повышения привилегий. Для этого в параметре «Контроль учетных записей: Поведение запроса на повышения прав для администраторов в режиме одобрения администратором» устанавливаем «Запрос учетных данных на безопасном рабочем столе», а в «Контроль учетных записей: Поведение запроса на повышения прав для обычных пользователей» выбираем «Автоматически отклонять запросы пользователей».

Для тех же, кто считает такие настройки излишне строгими, можно порекомендовать выбрать в параметре групповой политики «Контроль учетных записей: Поведение запроса на повышения прав для администраторов в режиме одобрения администратором» запрос согласия для двоичных данных не из Windows, тем самым установив на клиентах второй уровень работы UAC, описанный выше (см. **рис. 2**).

## Bitlocker

Безопасность — понятие комплексное, и компания Microsoft это прекрасно понимает, добавляя с каждой версией новый функционал, направленный на защиту компьютеров. Картина современного компьютерного парка показывает непрекращающийся рост доли мобильных ПК в квартирах пользователей. Технология Bitlocker, впервые появившаяся в Windows Vista, была направлена в первую очередь на защиту этого сегмента как самого уязвимого к краже и просто потери. Если рассматривать специалистов информационных технологий и бизнес-аудиторию, то на их ноутбуках, как правило, хранится ценная информация, и потеря ее может создать серьезную угрозу как личным финансам, так и существованию компании.

В первом выпуске Windows Vista до выхода SP1 присутствовала возможность зашифровать диск с операционной системой, для этого предварительно было необходимо создать специальный раздел размером 1,5 Гб, который оставался незашифрованным и хранил загрузочные файлы. Если же вы пропустили создание данного раздела, то при использовании версии Vista Ultimate вам была доступна утилита по подготовке диска перед включением Bitlocker. В противном случае приходилось переустанавливать операционную систему и разбивать жесткий диск заново.

В Windows 7 специальный служебный раздел для Bitlocker создается автоматически, без каких-либо вопросов при установке системы. Его размер был сокращен до 100 Мб, а сам раздел скрыт от глаз человека, работающего на компьютере. Если же вы захотите включить Bitlocker, дополнительные действия с диском вам не понадобятся, поскольку раздел уже существует.

С выходом SP1 для Windows Vista Bitlocker смог шифровать не только раздел с установленной системой, но и лю-

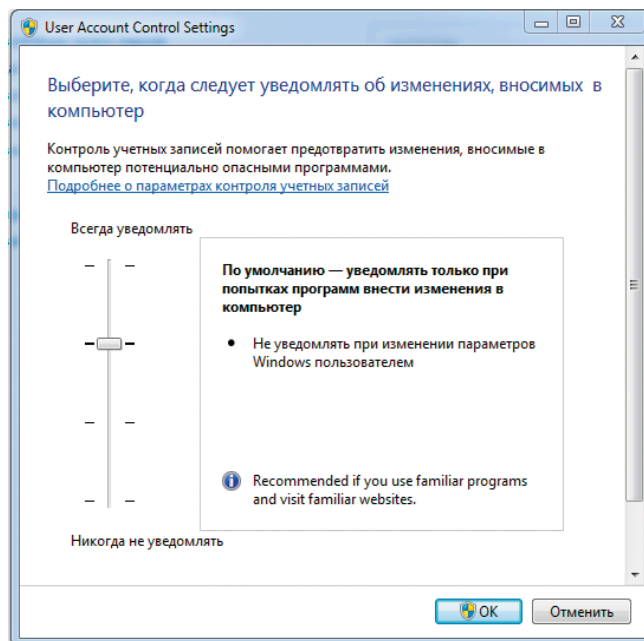


Рисунок 1. Настройки уровня UAC в панели управления Windows 7

бые другие. Присутствовало определенное ограничение, говорящее о том, что шифровать дополнительные разделы можно только после шифрования раздела с системой. В Windows 7 данное ограничение отсутствует. После установки системы вы можете зашифровать диск D: хранящий ваши документы, оставив при этом незашифрованным диск с самой Windows 7.

Основное изменение технологии Bitlocker связано с появлением нового функционала Bitlocker ToGo. Чтобы понять, нужен ли вам данный функционал, ответьте себе на два вопроса: Пользуетесь ли вы Flash-носителями? Забывали ли вы хотя бы раз свою флешку на работе, в интернет-кафе или у знакомых? Даже если вы ответили «да» только на первый вопрос, технология Bitlocker ToGo создана для вас.

Как вы уже догадались, Bitlocker ToGo позволяет шифровать Flash-носители и мобильные жесткие диски, подключенные через интерфейс USB. Осуществлена поддержка файловых систем NTFS, FAT, FAT32, ExFAT. После шифрования, время которого зависит от объема носителя, а не его наполненности, доступ будет предоставляться после ввода PIN-кода, указанного в процессе включения Bitlocker ToGo для конкретного носителя, либо возможно задействовать авторизацию с помощью смарт-карты. И если компьютеры, в которые будет вставлен этот носитель, работают под управлением Windows 7 или Windows 2008 R2, доступ к файлам произойдет абсолютно прозрачно для пользователя.

Менее радужно выглядит ситуация при работе с парком компьютеров под разными версиями Windows. Bitlocker ToGo создан для работы с Windows 7, но прочитать зашифрованный носитель с файловой системой FAT вы сможете и под Windows XP/Vista. К сожалению, только прочитать и только FAT. Для работы с зашифрованным носителем в Windows Vista вам понадобится ввести PIN-код и открыть приложение Bitlocker ToGo. Если вам нужно прочитать какой-либо файл, то предварительно его необходимо скопировать на текущий компьютер, вдобавок записать что-то на носитель из предыдущих версий ОС нельзя.



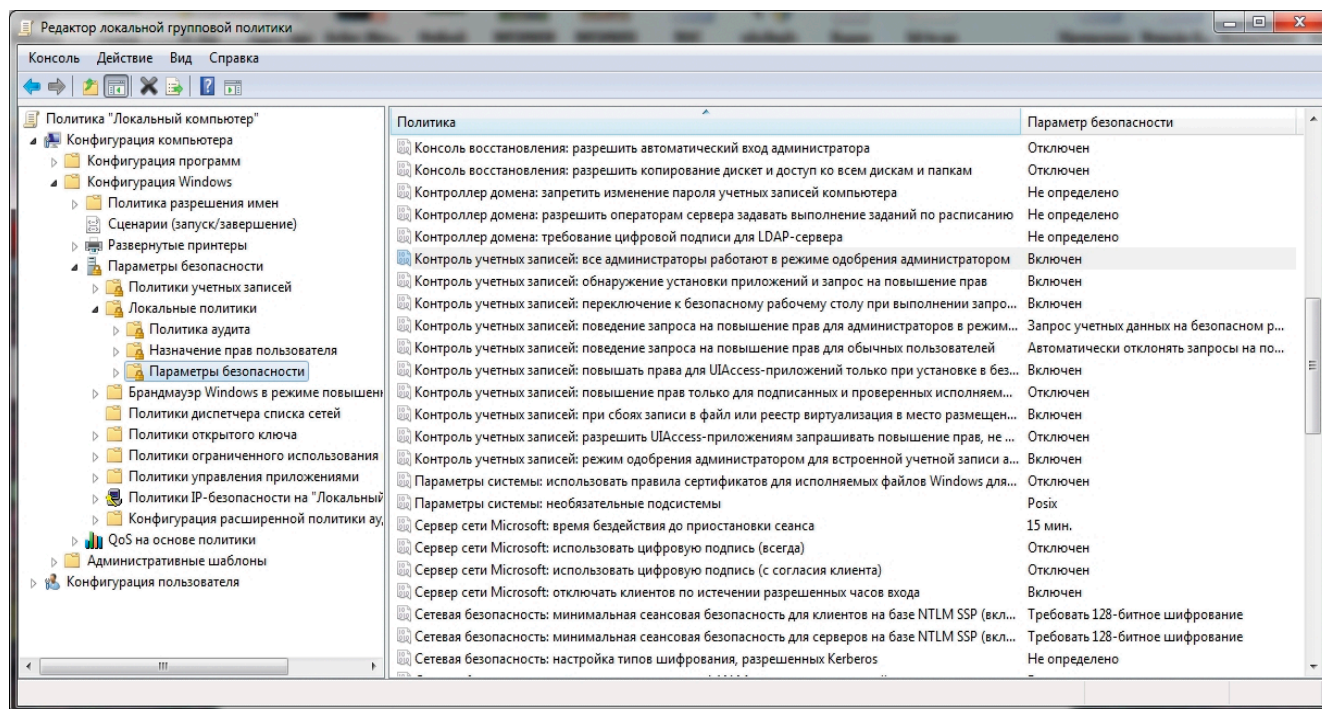


Рисунок 2. Настройка UAC через локальную политику Windows 7

Процесс включения BitLocker ToGo на мобильном носителе предельно прост и отдельного внимания не заслуживает, а вот расширенные параметры в групповой политике требуют более близкого знакомства.

Параметры, регулирующие BitLocker ToGo, находятся в ветке «Конфигурация Компьютера → Административные Шаблоны → Removable Data Drivers». К сожалению, на данный момент они не переведены на русский язык.

■ **Configure use of smart cards on removable data drives** – позволяет разрешить или запретить возможность использовать смарт-карты для аутентификации пользователя, использующего зашифрованный носитель.

■ **Deny write access to removable drives not protected BitLocker** – запрещает запись на носители, не зашифрованные BitLocker, соответственно любые принесенные незашифрованные носители будут доступны только для чтения.

■ **Allow access to BitLocker-protected removable data drives from earlier versions of Windows** – определяет, могут ли сменные диски, отформатированные под FAT, быть разблокированы и просмотрены на компьютерах под управлением Windows 2008, Windows Vista, Windows XP SP2.

■ **Configure password complexity requirements and minimum length** – влияет на длину и сложность пароля, создаваемого пользователем для получения доступа к носителю.

■ **Choose how BitLocker-protected removable drives can be recovered** – один из самых важных параметров, позволяющих настроить процедуру восстановления информации на носителе при потере PIN-кода.

Из вышесказанного можно сделать вывод, что в ближайшие годы у компаний, использующих компьютеры под управлением Windows, появится дополнительное средство контроля носителей информации, и наибольшее удобство при использовании BitLocker ToGo получат фирмы, полностью мигрировавшие свои клиентские компьютеры на Windows 7.

## Windows XP Mode

Одной из проблем при переходе на Windows Vista была совместимость приложений. Если практически все коммерческое ПО было обновлено и вышли новые версии, работающие под Vista, то самописные программы, созданные давно людьми, уже не работающими в вашей организации, по-прежнему мертвым грузом, не давая полноценно мигрировать на новую версию ОС. Как один из вариантов реше-

ния проблем был и остается Application Compatibility Toolkit, но, к сожалению, далеко не все программы можно приручить с помощью данного продукта. Компании, имеющие такие приложения, были вынуждены оставить часть компьютеров под управлением Windows XP, тем самым сохраняя платформу для запуска устаревших приложений.

В Windows 7 для совместимости с устаревшими приложениями предлагается новое решение, базирующееся на основе Windows Virtual PC, специальной версии под Windows 7, уже хорошо знакомой Virtual PC 2007. Сама по себе виртуализация не нова, и в Windows Vista вы могли поставить Windows XP в Virtual PC 2007 и запускать в ней старое приложение. Но в таком случае является неудобство использования нескольких рабочих столов и необходимость переключения между реальной и виртуальной ОС.

В Windows 7 же предлагается качественное улучшение под названием Windows XP Mode, в рамках этого улучшения предлагается скачать готовый образ операционной системы Windows XP SP3, установив на него нужное вам приложение. В виртуальной системе будет задействована опция «Публикации приложений», а это значит, что пользователю будет необходимо нажимать ярлык для запуска

ПО, а не запуска виртуальной машины. При этом на экране он увидит только окно приложения, без каких-либо признаков виртуальной Windows XP. Естественно, приложение будет выполняться в виртуальной среде, что потребует определенных дополнительных ресурсов системы, а первый запуск приложения займет гораздо больше времени, нежели то же приложение, установленное в реальной операционной системе (см. **рис. 3**).

К плюсам новой версии Windows Virtual PC можно отнести возможность установки Windows XP, Windows Vista, Windows Vista 7, Windows Server 2003/2008 и 2008R2, но только 32-битных версий. Поддержка виртуальными машинами USB-устройств также является новшеством в семействе продуктов Virtual PC, преград для подключения к виртуальной машине USB-принтеров и других USB-устройств больше не существует.

Серьезным препятствием на пути распространения данной технологии среди офисных компьютеров могут стать требования к оборудованию. В отличие от предшественни-

цы для Windows Virtual PC необходимо наличие у процессора аппаратной поддержки виртуализации (Hardware Virtualization Technology). Правила лицензирования Windows XP Mode пока точно не известны, но существует информация, что Windows XP Mode будет бесплатен для следующих версий Windows 7. Это Professional, Enterprise и Ultimate.

В любом случае ничто не мешает вам установить собственную виртуальную машину, естественно, лицензированную и задействовать функцию «Публикации приложений».

### AppLocker

Возвращаясь к технологиям обеспечения безопасности, нельзя обойти стороной новинку седьмой версии Windows – AppLocker, интересную в первую очередь корпоративному сегменту. Одной из причин, по которой пользовательский компьютер начинает отходить от внутренних стандартов, является установка дополнительного программного обеспечения. Пути проникновения такого ПО могут быть самые разные. Это и программы, прине-

сенные из дома, загруженные из Интернета или полученные по электронной почте. И даже при работе пользователя с минимальными привилегиями остается риск запуска портативных программ, не требующих установки. AppLocker – логическое продолжение политики ограниченного использования программ (SRP) в ОС Windows XP и Windows Vista, но более гибкое и удобное в администрировании.

Структура AppLocker проста и содержит три типа правил: разрешающие, запрещающие и исключения. Разрешающие правила дают возможность запускать только приложения из списка «благонадежных» и блокируют все остальные. Запрещающие правила, напротив, разрешают выполнение любых приложений, кроме тех, что в списке «неблагонадежных». Несмотря на то что существует возможность комбинаций, рекомендуется построение AppLocker только из разрешающих правил и исключений. AppLocker поддерживает ряд независимых политик: для исполняемых файлов, для установщиков, для сценариев и для библиотек DLL.



**СИСТЕМНЫЙ  
администратор**

**Второй ежегодный конкурс на звание  
«Самого системного администратора»**

**Ищу лучшего  
сисадмина!**

Отвечай на вопросы конкурса на сайте:  
[www.ideco-software.ru/company/sysadminday](http://www.ideco-software.ru/company/sysadminday)  
и получай призы:

- Портативный GPS-навигатор
- Интернет-шлюз Ideco ICS на 50 пользователей
- Подписку на журнал «Системный администратор»
- Футболку настоящего сисадмина

Конкурс проводится компанией «Айдеко» совместно с журналом «Системный администратор»

Реклама



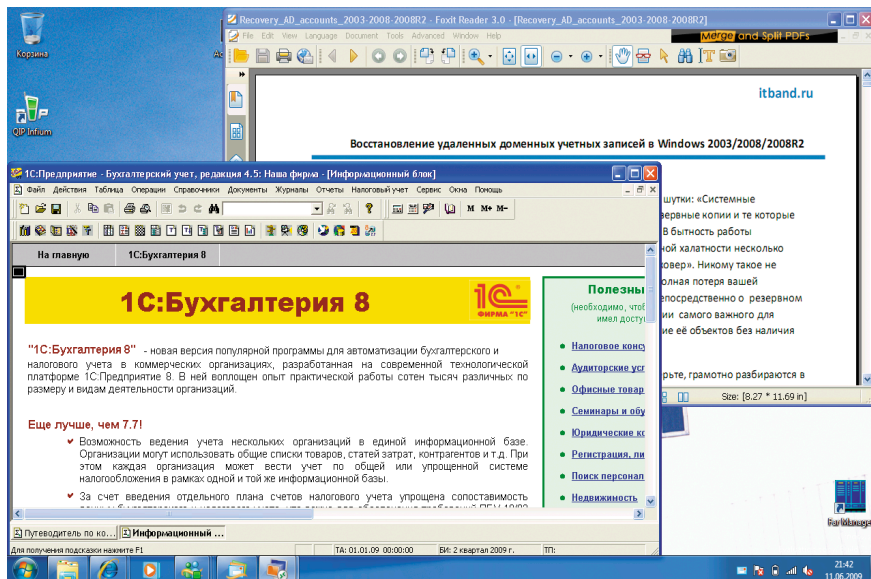


Рисунок 3. Приложения «1С:Предприятие» и Foxit Reader, запущенные в Windows XP Mode

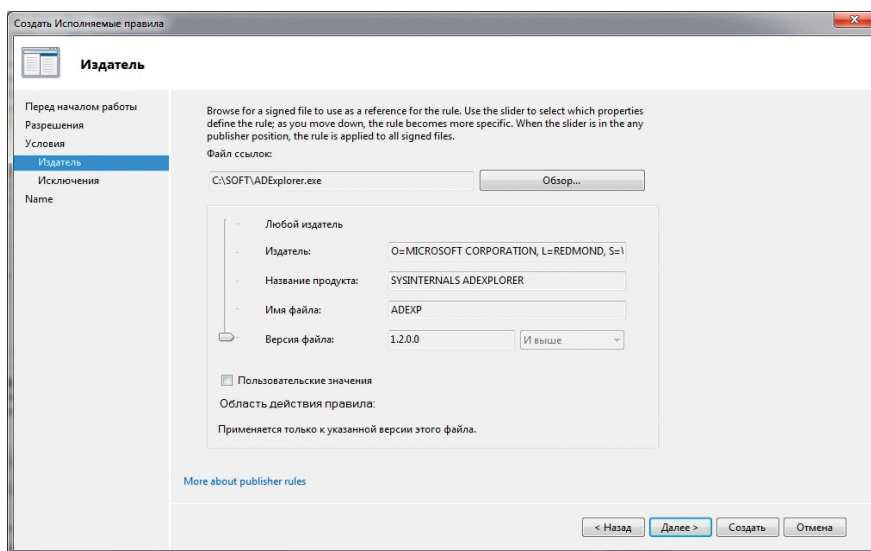


Рисунок 4. Создание правила типа «Издатель» в AppLocker

Нововведение AppLocker – правила на издателей, основанные на цифровых подписях приложений. Это дает возможность создавать правила, остающиеся в силе после обновления или установки новой версии приложения и достигается это за счет возможности указывать атрибуты приложения. Например, можно создать правило «разрешать запуск всех версий программы Microsoft Office Excel начиная с 2007, если они подписаны издателем Microsoft». При выходе новой версии Microsoft Office Excel можно просто обновить приложение, и создавать новое правило под него не потребуется.

Для того чтобы не получилось так, что созданные правила мешают работе системы и пользователям предусмотрены правила по умолчанию. Их три,

и действуют они на разрешение. Первое разрешает запуск приложений пользователям из папки Program Files, второе – из папки Windows и третье дает право администраторам запускать программы без ограничений. Даже задействовав только эти правила, вы будете уверены, что пользователи не смогут запустить несанкционированное приложение, точнее, смогут, если им удастся его положить в Program Files или Windows, но таких прав у них просто не будет.

Представим, что у пользователей на диске C: в папке SOFT находится необходимая для работы программа, но после применения разрешающих правил по умолчанию пользователи не смогут запускать из нее ПО. Если вы создадите еще одно разрешающее пра-

вило, дающее возможность запускать программы из C:\SOFT, то возникнет брешь в безопасности, т.к. любая скопированная в эту папку программа сможет быть запущена. Конечно, можно создать разрешающее правило, основанное на хэше программы, но тут существует своя тонкость, при каждом обновлении вашего приложения вам придется заново создавать правило, т.к. хэш будет меняться. В такой ситуации правила на издателей как раз будут самым эффективным решением, но только если приложение использует цифровую подпись.

На рис. 4 видно создание правила на издателя, где, перемещая ползунок детализации, разрешается использование только данной версии приложения, изменив детализацию можно добиться разрешения использовать любую версию приложения либо всех приложений от данного издателя. Для функционирования AppLocker необходимо запустить службу «Удостоверение приложения» и установить тип запуска «Автоматически», т.к. после установки Windows 7 данная служба находится в режиме запуска вручную.

В Windows 7 по-прежнему присутствуют политики ограниченного использования программ (SRP), и они могут быть задействованы. AppLocker – новая технология, которая будет доступна в версии Enterprise, в то время как устаревшие политики ограниченного использования программ останутся в младших редакциях операционной системы.

Количество новшеств Windows 7 на этом не заканчивается, за рамками данной статьи осталась технология DirectAccess, которая позволяет удаленным пользователям подключаться к корпоративной сети через Интернет без необходимости создания VPN-подключения. Возможность offline domain join, дающая ввести компьютер в домен без установки сетевого соединения с контроллером домена. Функция BranchCache, предназначенная для кэширования данных удаленных файловых и веб-серверов в локальной сети филиала, и много других. До первых поступлений Windows 7 осталось меньше месяца, а данного времени должно хватить на повышение квалификации и подготовки к пополнению семейства операционных систем.

# Решение давно наболевшей проблемы

## DYMO®

THE EASIER, THE BETTER

**Вы когда-нибудь считали, сколько времени вы тратите на то, чтобы определить, какой кабель к чему относится? А сколько раз вам приходилось бегать с прозвонкой из серверной в кабинеты и обратно, пытаясь разобраться с давно забытой розеткой?**

**Н**а днях ко мне обратился мой ИТ-директор, который поставил мне сложную задачу, а на решение дал всего пару дней. Его не устраивает, что в серверной вечный хаос с проводами и нужно тратить слишком много времени на определение, какой к чему относится. Рисовать схему долго, и, к тому же, ее необходимо постоянно обновлять. Как правило, такая схема через полгода уже неактуальна, а вспомнить сделанные изменения невозможно, следовательно, для её обновления придется проделать всю работу заново. Второе решение и, наверное, оно единственно правильное – это маркировка, но использовать маркеры или скотч ненадежно. Через короткое время сделанная ранее маркировка отваливается или стирается, оставляя за собой следы.

После пяти минут поиска в Интернете был найден сайт DYMO ([http://](http://www.dymo.ru)

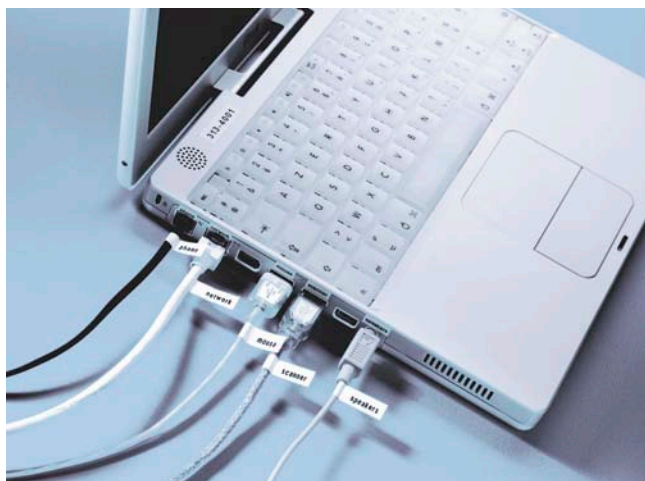
[www.dymo.ru](http://www.dymo.ru)), который предлагает специальные принтеры для маркировки. Изучив предлагаемый ассортимент, я выбрал новинку этого года LabelManager 210D. И сразу приступил к работе: то, что мог, маркировал по памяти, что-то по старым схемам, а остальное пришлось прозванивать. Я быстро оценил широкий экран принтера, на котором видна этикетка такой, какой она будет при печати. Познакомившись с принтером поближе, я нашел функцию, позволяющую печатать вертикальные наклейки. Я промаркировал стойки названиями серверных шкафов в соответствии с документацией компании, а также серверы и все активное сетевое оборудование, благодаря этикеткам разной ширины. Еще одно преимущество данного принтера заключается в том, что переключение алфавита с английского на русский и наоборот происходит всего лишь на-

жатием на одну кнопку. У нас в отделе исторически разношерстные стандарты наименований оборудования: часто используются как русские, так и английские аббревиатуры, так что я смог в полной мере оценить эту функцию. Названия самых старых серверов очень длинные, поэтому возможность печати в две строки пришлась очень кстати.

С помощью принтера LabelManager 210D можно легко подписывать диски, папки и прочее. Теперь во время инвентаризации можно забыть о вырезании бумаги и скотча. В общем, для меня этот принтер стал незаменимой вещью!

В итоге работу я закончил в срок, а директор теперь ставит нашу серверную в пример коллегам. 🌐

*Денис Староверов,  
старший системный инженер*





# Мониторинг Cisco IDS/IPS на примере модуля IDSM2 с помощью MRTG

## Часть 2

Андрей Дугин

Рано или поздно перед администратором систем обнаружения вторжений возникают вопросы рациональности использования ресурсов; соответствия официально заявленных производителем параметров реальным данным; возможности распределения сенсоров различной мощности по разным участкам сети. В первой части статьи я рассказывал о том, как можно использовать MRTG для своевременного определения сбоев в функционировании IDS или о реконфигурации сети. Для определения необходимости балансировки нагрузки на сенсоры и подобных задач также может пригодиться MRTG.

### Особенности создания конфигурационного файла

Если для мониторинга интерфейсов возможно использование стандартных MIB, то для контроля загрузки процессоров необходимо знать специфические для производителя Cisco OID.

Согласно официальной информации производителя [1], модули IDSM2 поддерживают следующие MIB, доступные на сайте <ftp://ftp-sj.cisco.com/pub/mibs/oid>:

- CISCO-CIDS-MIB;
- CISCO-PROCESS-MIB;
- CISCO-ENHANCED-MEMPOOL-MIB;
- CISCO-ENTITY-ALARM-MIB.

Cisco IDSM2 модуль является двухпроцессорным. Загрузка процессора напрямую зависит от количества и характера инспектируемого трафика. Показатели среднего значения загрузки за 5 минут CPU1 и CPU2 дают OID: 1.3.6.1.4.1.9.9.109.1.1.1.8.1 и 1.3.6.1.4.1.9.9.109.1.1.1.8.2 соответственно, относящиеся к CISCO-PROCESS-MIB. Конфигурационный файл в данном случае лучше создать на основе файла-шаблона. Пример можно найти в страницах инструкции `man cfmaker` и отредактировать под свои задачи.

Мой файл-шаблон после редактирования изначально-го варианта выглядит следующим образом:

```
$head_lines .= <<ECHO;
#-----
ECHO

my $target_name = $router_name . ".cpu";

$target_lines .= <<ECHO;
```

```
YLegend[$target_name]: CPU load, %
ShortLegend[$target_name]: %
Legend1[$target_name]: CPU1 load in %
Legend2[$target_name]: CPU2 load in %
Legend3[$target_name]: Max Observed CPU1 load
Legend4[$target_name]: Max Observed CPU2 load
LegendI[$target_name]: CPU1 Load:
LegendO[$target_name]: CPU2 Load:
WithPeak[$target_name]: ywm
MaxBytes[$target_name]: 100
Options[$target_name]: growright, gauge, nobanner,
Title[$target_name]: $router_name CPU load
Target[$target_name]:
    1.3.6.1.4.1.9.9.109.1.1.1.8.1&
    1.3.6.1.4.1.9.9.109.1.1.1.8.2:$router_connect
PageTop[$target_name]: <h1>$router_name CPU load</h1>
<div>
    <table>
        <tr>
            <td>System:</td>
            <td>$router_name in $html_syslocation</td>
        </tr>
        <tr>
            <td>Maintainer:</td>
            <td>$html_syscontact</td>
        </tr>
        <tr>
            <td>Description:</td>
            <td>$html_sysdescr</td>
        </tr>
        <tr>
            <td>Resource:</td>
            <td>CPU.</td>
        </tr>
    </table>
</div>
ECHO
```

Вкратце о параметрах в файле, которые пришлось отредактировать:

- **YLegend** – легенда оси Y графика;
- **ShortLegend** – единица измерения оси Y;
- **Legend1** – легенда графика зеленого цвета, в данном случае средней загрузки CPU1;

- **Legend2** – легенда графика синего цвета, в данном случае средней загрузки CPU2;
- **Legend3** – легенда дополнительного графика темно-зеленого цвета, в данном случае пиковой загрузки CPU1 за единицу времени;
- **Legend4** – легенда дополнительного графика фиолетового цвета, в данном случае пиковой загрузки CPU2 за единицу времени;
- **Legend1** – интерпретация параметра Legend1 на странице дополнительных графиков;
- **LegendO** – интерпретация параметра Legend2 на странице дополнительных графиков;
- **WithPeak** – использование пиковых значений в дополнительных графиках за неделю (w), месяц (m), год (y);
- **MaxBytes** – максимальное значение оси Y;
- **growright** – указывает направление оси X вправо;
- **gauge** – обработка параметров, значения которых не возрастают постоянно;
- **nobanner** – не добавлять баннер MRTG к страницам с дополнительными графиками;
- **unknaszero** – неизвестные значения отображать как нулевые, вместо повторения предыдущего значения – для более наглядной сигнализации о сбоях.

## Настройка

Конфигурационный файл создается командой:

```
# cfgmaker --nointerfaces \
--host-template=/etc/mrtg/templates/cpu-idsm \
--global "WorkDir: /var/www/mrtg/idsm" \
community_name@sensor1 \
community_name@sensor2 \
community_name@sensor3 \
community_name@sensor4 \
community_name@sensor5 > /etc/mrtg/idsm.cfg
```

В данном случае рассматривается автономный от интерфейсов вариант мониторинга загрузки CPU. Соответственно, кроме конфигурационного файла создается отдельная веб-директория:

```
# mkdir /var/www/mrtg/idsm
```

и, соответственно, index.html в ней:

```
# indexmaker --nolegend \
--title="IDSM CPU" \
/etc/mrtg/idsm.cfg > /var/www/mrtg/idsm/index.html
```

Создаем в /etc/cron.d/ отдельный файл, в котором указываем новые параметры конфигурации для запуска MRTG 1 раз в 5 минут, а также путь для записи ошибок в отдельный лог-файл:

```
# vim /etc/cron.d/idsm-mrtg
```

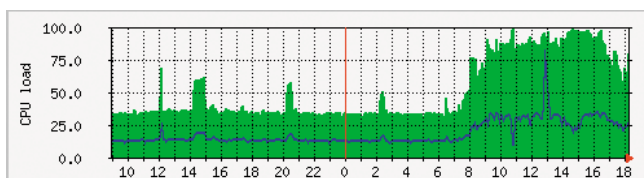


Рисунок 1. Сопоставление загрузки процессора и sniffер-порта модуля

и записываем:

```
* /5 * * * * root if [ -x /usr/bin/mrtg ] && \
[ -r /etc/mrtg/idsm.cfg ]; then env LANG=C \
/usr/bin/mrtg /etc/mrtg/idsm.cfg 2>&1 | \
tee -a /var/log/mrtg/idsm-mrtg.log ; fi
```

Веб-интерфейс мониторинга CPU будет находиться по адресу <http://yourserver/mrtg/idsm>.

Сопоставить загрузку процессора и sniffер-порта модуля можно на следующем примере. Зеленым цветом показана загрузка CPU1, синим – CPU2 сенсора (см. **рис. 1**).


На **рис. 2** показана загрузка интерфейса, принимающего SPAN, того же модуля в то же время. Сенсором контролируется пользовательский сегмент, можно заметить резкий рост трафика, а также соответствующей нагрузки на процессоры в понедельник после выходных.

## Практическое применение

После того как появилась возможность анализа загрузки и процессоров, и sniffер-порта, на основании выводимой информации можно принимать решение о:

- необходимости снятия части нагрузки с модуля путем исключения из SPAN-сессии некоторых интерфейсов либо VLAN в случае высокой загрузки модуля;
- возможности наращивания инспектируемого трафика в случае низкой нагрузки;
- целесообразности добавления дополнительного модуля в коммутатор – в случае перегрузок;
- целесообразности замены модуля в коммутаторе на более соответствующий поставленным задачам для данного участка сети сенсор другого производителя – как в случае чрезмерно высокой, так и низкой загрузки;
- возможности агрегации SPAN-сессий из разных коммутаторов для инспектирования на одном сенсоре любого производителя – при наличии такой необходимости;
- решения некоторых проблем, возникающих в ходе текущей эксплуатации.

## Заключение

Итого, сопоставляя полученные данные мониторинга систем, имеем, как минимум, дополнительный факт для принятия решения в зависимости от поставленной задачи. В ряде случаев показатели загрузки могут косвенно свидетельствовать о наличии аномалий сетевой активности, что ускорит процесс реагирования на инцидент информационной безопасности. Соответственно, в некоторых ситуациях MRTG еще и помогает системам IDS выполнять свои основные функции. 

1. [http://www.cisco.com/en/US/docs/security/ips/7.0/configuration/guide/cli/cli\\_snmp.html#wp1042408](http://www.cisco.com/en/US/docs/security/ips/7.0/configuration/guide/cli/cli_snmp.html#wp1042408).

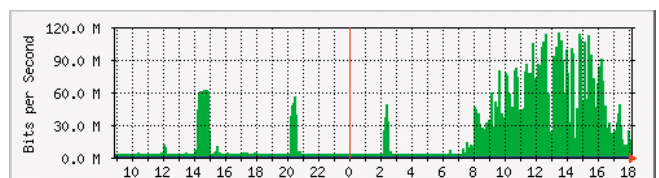


Рисунок 2. Загрузка интерфейса, принимающего SPAN, того же модуля в то же время



# Делегируем права на перемещение учетных записей пользователей в Active Directory

## Часть 4. Завершение надстройки

Вадим Андросов

В этой части статьи будет завершена разработка основного класса надстройки для Windows Server 2003, позволяющая разделить полномочия перевода пользователя из одного отдела в другой между локальными администраторами подразделений. Также рассмотрим использование регулярных выражений для упрощения обработки строк.

### Команда отказа принятия пользователя

Рассмотрим обработчик команды отказа принятия пользователя. Имеется в виду случай, когда администратор организационной единицы-назначения отказывает пользователю в приеме. Подробно данный сценарий описан в первой части статьи [1].

```
function dispatchDenyCommand(cmd)
dim comment, ou, who
```

При отказе принять пользователя может быть указана причина, которая сохранится в поле комментария команды. Если его нет – в поле помещается значение «пусто» (empty).

```
comment = cmd.userMoveComment
if comment = "" then comment = "empty"
```

Далее подключаемся к объекту менеджера – создателя команды, чтобы проверить, имеет ли он право управлять этой организационной единицей.

```
set who = getObject(cmd.userMoveExecutor)
```

Для этого нужно получить экземпляр текущей организационной единицы. Поле userMoveTarget содержит ссылку на перемещаемый объект пользователя. Пользователь ожидает приема, поэтому находится внутри объекта «Стул ожидания», который в свою очередь содержится в объекте «Комната ожидания». То есть текущее подразделение можно получить, поднявшись на три уровня вложенности вверх (первый родительский контейнер – стул, второй – комната ожидания, третий – организационная единица). Это делается с помощью функции получения контейнера на заданное количество уровней выше getAncestor. В качестве первого параметра ей передается исходный объект, второго – количество уровней, на которое нужно подняться.

```
set ou = getObject(getAncestor(cmd.userMoveTarget, 3))
if canHeManageOU(ou, who) then
```

С помощью метода canHeManageOU определяем, имеет ли право текущий пользователь «распоряжаться» в этой организационной единице и отдавать подобные команды.

Если необходимых прав нет, команда выполнена не будет. Но если выполнение дошло до этого места, – все в порядке.

```
dim chair, newChair, user
```

Подключаемся к объекту перемещаемого пользователя и его стула ожидания. Стул – контейнер первого уровня по отношению к ожидающему пользователю, для его получения используем функцию getParent. Она подобна getAncestor, но позволяет получить только непосредственный контейнер, что нам в данном случае и нужно.

```
set user = getObject(cmd.userMoveTarget)
set chair = getObject(getParent(cmd.userMoveTarget))
```

Дальше пользователя нужно вернуть в исходное подразделение. Окончательное возвращение – право менеджера этой организационной единицы, поэтому пользователь просто ставится в очередь. Для этого создается так называемый «зеркальный» стул в исходном отделе с помощью функции createMirroredChair.

```
set newChair = createMirroredChair(chair, cmd)
```

Затем пользователь перемещается, создается обратная ссылка. Текущий стул ожидания очищается с помощью clearEmptyChair, чтобы вернуть надстройке непротиворечивое состояние.

```
newChair.moveHere cmd.userMoveTarget, vbNullString
createBackLink getWaitingRoom(ou), "LDAP://" & _
    user.name & "," & newChair.distinguishedName
clearEmptyChair chair, cmd.userMoveTarget
end if
```

В конце обработанный объект команды удаляется.

```
ou.delete DENY_COMMAND_CLASS, "CN=" & cmd.cn
end function
```

Рассмотрим вспомогательные функции. Функция getParent возвращает путь к родительскому контейнеру, получив в качестве параметра путь к дочернему. В ее работе используются регулярные выражения, поэтому особенности ее использования я рассмотрю позже. На ее основе создана функция получения контейнера на заданное количество уровней выше. Вся ее работа сводится к вызову нужное количество раз функции getParent.

Листинг 1. Функция определения предка

```
function getAncestor(path, levels)
dim i
getAncestor = path
for i = 1 to levels
    getAncestor = getParent(getAncestor)
next
end function
```

Функция создания «зеркального» стула. Используется, когда пользователя необходимо «пересадить» из комнаты ожидания целевой организационной единицы в исходную.

```
function createMirroredChair(srcChair, denyCmd)
dim chairNumber, room
set room = getWaitingRoom(getObject(srcChair.userMoveFrom))
```

```
chairNumber = getNextNumber(room, CHAIR_CLASS)
```

Функция подключается к организационной единице-источнику (ее путь содержится в свойстве команды userMoveFrom) и создает там стул ожидания, копируя все свойства текущего. Изменяется только метка времени команды.

```
set createMirroredChair = _
    room.create(CHAIR_CLASS, "CN=chair_" & chairNumber)
createMirroredChair.userMoveFrom = _
    getAncestor(srcChair.ADSPath, 2)
createMirroredChair.userMoveWho = denyCmd.userMoveExecutor
createMirroredChair.userMoveComment = _
    denyCmd.userMoveComment
```

В первой части статьи [1] для поля со временем операции был выбран тип UTC Coded Time. Необходимые преобразования выполняет функция toUTC (см. Листинг 2).

```
createMirroredChair.userMoveWhen = toUTC(now)
createMirroredChair.userMoveDisabled = _
    srcChair.userMoveDisabled
createMirroredChair.setInfo
end function
```

Рассмотрим функцию приведения времени.

Листинг 2. Преобразование времени к типу UTC

```
Function toUTC(dat)
dim offsetMin
offsetMin = getTimeZoneOffset
toUTC= dateadd("n", offsetMin, dat)
end function
```

Собственно все преобразование сводится к смещению локального времени с учетом часового пояса. Смещение определяет функция getTimeZoneOffset, читая смещение из реестра (в минутах). То есть, скажем, если Киев находится в часовом поясе «+2», то смещение для получения времени по Гринвичу – минус 120 минут.

Понадобится еще функция обратного преобразования fromUTC. Ее реализация аналогична toUTC за исключением того, что полученное смещение нужно вычесть, а не добавить.

Листинг 3. Вычисление смещения времени для часового пояса

```
function getTimeZoneOffset()
if timeZoneOffset = "?" then
dim oShell, atb
set oShell = CreateObject("WScript.Shell")
atb = "HKKEY_LOCAL_MACHINE\System\CurrentControlSet\" & _
    "Control\TimeZoneInformation\ActiveTimeBias"
timeZoneOffset = oShell.RegRead(atb)
end if
getTimeZoneOffset = timeZoneOffset
end function
```

Наконец, рассмотрим функцию корректной очистки «опустевшего» стула ожидания. Передается ей два параметра: очищаемый стул и устаревший путь к объекту пользователя на этом стуле.

```
function clearEmptyChair(chairObj, whoWas)
dim srcOU
set srcOU = getObject(chairObj.userMoveFrom)
```

Сначала удаляется сам пустой стул ожидания.



```
chairObj.deleteObject(0)
dim room, li
set room = getWaitingRoom(srcOU)
room.filter = Array(LINK_CLASS)
```

Затем в организационной единице-отправителе находится и удаляется ссылка на отправленный объект, которая теперь указывает в никуда. Так что «подвисших» ссылок не остается.

```
for each li in room
  if li.userMoveLink = whoWas then
    li.deleteObject(0)
    exit function
  end if
next
end function
```

## Подтверждение перемещения

Менеджер также может подтвердить перевод пользователя в свою организационную единицу. Рассмотрим обработчик этой команды.

```
function dispatchAcceptCommand(cmd)
dim ou, chair, whom, ouFrom, who
```

По аналогии с прошлой командой сначала требуется подключиться к объектам создателя команды и организационной единице-получателю.

```
set who = getObject(cmd.userMoveExecutor)
set ou = getObject(getAncestor(cmd.userMoveTarget, 3))
if canHeManageOU(ou, who) then
```

Далее проверяем, имеет ли право пользователь, создавший эту команду, управлять текущей организационной единицей. Если имеет – выполняем завершение перевода.

```
set whom = getObject(cmd.userMoveTarget)
set chair = getObject(getParent(cmd.userMoveTarget))
```

Исходный статус пользователя (включен или нет) нужно восстановить.

```
whom.accountDisabled = chair.userMoveDisabled
whom.setInfo
```

После этого пользователь окончательно перемещается, а стул корректно очищается.

```
ou.moveHere cmd.userMoveTarget, vbNullString
clearEmptyChair chair, cmd.userMoveTarget
end if

ou.delete COMMAND_CLASS, cmd.name
end function
```

## Отмена перемещения

Также перемещение пользователя может быть отменено самим инициатором. Реализация метода никаких принципиальных отличий не имеет. Сначала происходит подключение ко всем объектам – участникам операции: перемещаемый пользователь, стул ожидания, инициатор перемещения, текущая организационная единица. Затем проверяются права создателя команды на ее выполнение. Если результаты проверки положительные, пользователь возвра-

щается в свое подразделение, а вспомогательные объекты (стул, обратная ссылка) удаляются.

### Листинг 4. Отмена перемещения

```
function dispatchRollbackCommand(cmd)
dim userMove, chair, srcPath, srcOU, who
set userMove = getObject(cmd.userMoveTarget)
set chair = getObject(userMove.parent)
set who = getObject(cmd.userMoveExecutor)
set srcOU = getObject(chair.userMoveFrom)
if (chair.class = CHAIR_CLASS) and _
  canHeManageOU(srcOU, who) then
  userMove.accountDisabled = chair.userMoveDisabled
  userMove.setInfo
  srcOU.moveHere userMove.ADSPPath, vbNullString
  clearEmptyChair chair, cmd.userMoveTarget
end if
srcOU.delete COMMAND_CLASS, cmd.name
end function
```

## Создание команд

Далее опишем функции подготовки команд, обработкой которых мы занимались ранее. Основная логика остается неизменной. Менеджер по персоналу создает объект команды в своей организационной единице. Сервер обрабатывает события появления команд, проверяет их на целостность и допустимость, выполняет и удаляет объект. То есть для пользователя работа серверной части надстройки остается полностью прозрачной. В случае невозможности выполнения команды она просто уничтожается.

Начнем с самой сложной и важной команды начала перемещения пользователя. Все подпрограммы подготовки команд будут также размещены в основном классе надстройки UserMove.Engine.

```
function move(whomPath, wherePath, comment)
```

Функции передается три параметра: кого перемещать, куда и с каким комментарием.

```
dim userMove, fromOU
if comment = "" then comment = "empty"
move = ""
set userMove = getObject(whomPath)
```

Ссылку на объект текущей организационной единицы можно получить, воспользовавшись свойством «родитель» (parent) перемещаемого объекта пользователя. Ведь пока он находится в своем подразделении.

```
set fromOU = getObject(userMove.parent)
if not canCurrentManageOU(fromOU) then
```

Если текущему пользователю не хватает прав для администрирования исходной организационной единицы, функция завершает работу, вернув сообщение об ошибке.

```
move = "Not enough right"
exit function
end if
```

Если прав достаточно, происходит окончательное перемещение.

```
move = transferUserTo(userMove, wherePath, fromOU, comment)
end function
```

Начало перемещения осуществляется в подпрограмме `transferUserTo`. Ей передаются следующие параметры: перемещаемый пользователь, путь к организационной единице-назначению, объект исходной организационной единицы и комментарий.

```
function transferUserTo(userMove, wherePath, fromOU, comment)
dim toOU
transferUserTo = ""
set toOU = getObject(wherePath)
```

Дальше производится проверка, не может ли менеджер по персоналу исходного отдела управлять еще и целевым. Если может (т.е. имеет достаточно прав в обоих отделах), то осуществляется простое перемещение пользователя сразу в целевую организационную единицу в обход надстройки. Это сделано, чтобы лишить менеджера необходимости сначала начинать перевод пользователя, а потом самому же его и подтверждать.

```
if canCurrentManageOU(toOU) then
toOU.moveHere userMove.ADSPath, vbNullString
transferUserTo = "User moved"
exit function
end if
```

Если же прав в целевом подразделении недостаточно, используется метод `enqueueHere`. Который ставит перемещаемый объект во входящую очередь организационной единицы.

```
enqueueHere userMove, fromOU, toOU, comment
transferUserTo = "User enqueued"
end function
```

Функция получает практически те же параметры, что и предыдущая, за исключением того, что целевая организационная единица теперь объект, а не путь к объекту, как раньше. Причина такой замены проста: к моменту вызова функции уже существует объект целевого подразделения. Поэтому лучше и дальше использовать его, чем плодить лишние сущности.

Следующий метод предельно прост. Он создает экземпляр класса команды и инициализирует его поля. Затем перемещаемый объект пользователя помещается внутрь команды. Команда сохраняется в организационной единице, откуда производится перемещение.

Листинг 5. Создание команды перемещения пользователя

```
function enqueueHere(whomObject, fromOU, toOU, comment)
dim cmd
set cmd = fromOU.create(START_MOVE_COMMAND_CLASS, _
"CN=cmd " & START_MOVE_COMMAND & " " & _
whomObject.samAccountName)
cmd.userMoveID = START_MOVE_COMMAND
cmd.userMoveExecutor = "LDAP://" & info.userName
cmd.userMoveFrom = fromOU.ADSPath
cmd.userMoveWho = "LDAP://" & info.userName
cmd.userMoveComment = comment
cmd.userMoveWhen = toUTC(now)
cmd.userMoveDisabled = whomObject.accountDisabled
cmd.userMoveTo = toOU.ADSPath
cmd.userMoveTarget = whomObject.ADSPath
cmd.setInfo
whomObject.accountDisabled = true
whomObject.setInfo
cmd.moveHere whomObject.ADSPath, vbNullString
end function
```

Формирование команды подтверждения перемещения еще проще, так как здесь достаточно проинициализировать основные поля (исполнитель, тип команды, объект) и сохранить ее в организационной единице, куда осуществляется перевод.

Листинг 6. Создание команды подтверждения перемещения

```
function accept(whomPath)
dim cmd, ou
set ou = getObject(getAncestor(whomPath, 3))
set cmd = ou.create(COMMAND_CLASS, _
"CN=cmd " & ACCEPT_COMMAND & " " & _
getObject(whomPath).samAccountName)
cmd.userMoveID = ACCEPT_COMMAND
cmd.userMoveExecutor = "LDAP://" & info.userName
cmd.userMoveTarget = whomPath
cmd.setInfo
end function
```

Команда отказа формируется аналогично, поэтому полный текст ее инициализации приводить не буду. Называется соответствующий метод `deny`. В качестве параметров ему передается путь к объекту команды и комментарий, содержащий причину отказа. То же касается и создания команды отката. Метод ее создания называется `rollback` и принимает один параметр – объект воздействия.

## Путь к родительскому контейнеру

В ходе описания реализации использовалась функция `getParent`, которая возвращает путь к родительскому контейнеру на основе пути дочернего объекта.

В чем заключается логика работы. Объекты в Active Directory упорядочены иерархически. На самом верху иерархии находится домен. Например, для домена с именем `marclar.ua` путь будет выглядеть так: `LDAP://DC=marclar, DC=ua`. Если в рамках домена существует подразделение с именем `department`, которое в свою очередь содержит сотрудника `ivanov`, то путь к объекту пользователя будет `LDAP://DN=ivanov,OU=department,DC=marclar,DC=ua`. То есть путь указывается от листового элемента дерева к корню. Для пользователей используется идентификатор DN (Distinguished Name или отличительное имя), для организационных единиц – OU (Organizational Unit), для элементов названия домена – DC (Domain Component). Получение пути к родительскому контейнеру заключается в отбрасывании от текущего значения первого элемента (в нашем примере это подстрока `DN=ivanov`).

Ранее я использовал примитивную версию этой функции [4], которая, однако, вполне пригодна и для этой надстройки. Она находит в пути первую запятую, вырезает подстроку после нее и добавляет в начало название протокола.

Листинг 7. Определение родительского подразделения без использования регулярных выражений

```
function getParent(path)
getParent = "LDAP://" & right(path, len(path) - _
instr(1, path, ",", vbTextCompare))
end function
```

Рассмотрим, как то же самое можно сделать с помощью регулярных выражений. Регулярное выражение позволяет задать правило, по которому можно опознать часть строки. Для этого используется ряд специальных символов. Рас-



смотрим только элементы, необходимые для понимания материалов статьи. Дополнительную информацию по регулярным выражениям можно без труда найти в MSDN [5].

Логика их использования напоминает маски для файлов, где знак вопроса обозначает один любой символ, а звездочка – любое количество произвольных символов. Регулярные выражения несколько сложнее. Рассмотрим необходимые специальные символы (см. **таблицу 1**).

Итак, напомним регулярное выражение для выделения пути родительского контейнера. Путь начинается с указания протокола LDAP://, если этой приставки нет, то соответствующая строка называется «Отличительное имя» (Distinguished Name). Чтобы наша функция работала с обоими типами строк, укажем приставку как необязательный элемент:

```
(?:LDAP:\/\/)?
```

С помощью «?:» мы сообщаем анализатору, что строка, соответствующая этому выражению, нам не понадобится, затем следуют символы «\|». Поскольку каждый из них является еще и специальным, все они экранированы с помощью обратной косой черты. В конце идет знак вопроса, т.е. эта подстрока может встретиться в пути один (ADSPATH) или ноль (Distinguished Name) раз.

Далее описываем первый элемент пути:

```
(?: (?:CN|OU)=[^,]*,)?
```

Здесь также везде используем группировку без захвата (?:) результата. Значит это буквально следующее. Подстрока, которая начинается с CN или OU, затем следует знак равенства, потом любое количество произвольных букв, кроме запятой, в конце находится запятая. Данный элемент может встретиться в пути один раз или не встретиться вовсе.

Ну и заканчивается выражение остальными символами.

```
(.*)
```

То есть любое количество любых символов. Здесь исполь-

Таблица 1. Специальные символы

Символ	Описание
[]	Несколько символов в квадратных скобках. Обозначает один любой из этих символов. Например [ab] обозначает a или b
^	Отрицание. То есть [^ab] обозначает любой символ, кроме a и b
()	Круглые скобки используются для группировки условий. Затем есть возможность получения частей строк, соответствующих каждой группе. То есть если требуется выделить несколько элементов строки, следует описание каждого из них взять в скобки. Если нужно просто выделить часть регулярного выражения без необходимости получения подстроки, нужно записать его в следующем виде: (?:выражение)
\	Обратная косая черта используется для экранирования спецсимволов. Например, если требуется указать круглую скобку именно как символ, следует записать так: \()
	Или. Например ab cde обозначает «подстрока abc или cde»
*	Обозначает, что выражение, стоящее до звездочки, может повториться 0 и более раз. Например, a* обозначает любое количество идущих подряд букв a (в том числе ни одной).
?	Говорит о том, что идущее перед ним регулярное выражение может повториться ноль или один раз
.	Точка. Любой символ, кроме перевода строки

зуются просто круглые скобки, потому что эта подстрока нас как раз и интересует.

Перейдем к реализации. Передается функции исходный путь к объекту:

```
function getParent(path)
dim matches
```

Сначала задаем шаблон регулярного выражения.

```
re.pattern = "(?:LDAP:\/\/)?(?: (?:CN|OU)=[^,]*,)?(.*)"
```

Затем происходит поиск соответствий.

```
set matches = re.execute(path)
```

В конце извлекаем результат. В нашем случае это подстрока, соответствующая выражению (.\*). Она и является путем к родительскому контейнеру.

```
getParent = "LDAP://" & matches(0).submatches(0)
end function
```

Используя этот подход, реализуем еще одну полезную функцию. Перевод пути к объекту в удобочитаемый для простого пользователя вид. Организация Active Directory подобна файловой системе с ее каталогами и вложенными файлами. В то же время путь здесь задается как бы «наизнанку», начиная не из корня иерархии, а от конкретного элемента.

Напишем функцию, которая представляет путь: LDAP://DN=ivanov,OU=department,DC=marklar,DC=ua в виде Marklar.ua/department/ivanov.

Функции передается путь к объекту в стиле Active Directory:

```
function ADSPATH2Readable(path)
dim matches, i, splitter
```

Сначала выделяем доменное имя. Оно может состоять из одного и более доменных компонентов через запятую, каждая часть имеет вид DC=<имя доменного компонента (ИДК)>.

```
re.pattern = "DC=([,]*)"
set matches = re.execute(path)
ADSPATH2Readable = ""
for i = 0 to matches.count - 1
```

Все совпадения затем собираются в строку вида <ИДК>.<ИДК>...<ИДК>

```
if i = 0 then
splitter = ""
else
splitter = "."
end if
ADSPATH2Readable = ADSPATH2Readable & splitter & matches(i).submatches(0)
next
```

С помощью следующего регулярного выражения выделяются остальные элементы пути – организационные единицы (OU) и остальные объекты (DN). В отличие от доменных компонентов эти элементы требуется собирать в строку в обратном порядке, поэтому массив совпадений пере-

бирается с конца. Между названиями добавляется прямая наклонная линия. Здесь все равно, какой символ использовать, поскольку единственное приложение данной функции – наглядное представление пути.

```
re.pattern = "(?:CN|OU)=[^,]*"
set matches = re.execute(path)
for i = matches.count - 1 to 0 step -1
    ADSPPath2Readable = ADSPPath2Readable & "."
    "/" & matches(i).submatches(0)
next
end function
```

## Основной класс надстройки

Наконец, можно перечислить все открытые методы основного класса надстройки. Все они были реализованы ранее (см. таблицу 2).

Когда класс создан, нужно не забыть зарегистрировать его в системе с помощью контекстного меню проводника «Установить (Register)». Можно сделать то же самое из командной строки:

- **Regsvr32 UserMove.Engine.wsc** – регистрация компонента;
- **Regsvr32 /u UserMove.Engine.wsc** – его удаление.

## Создание общих ресурсов домена

В конце вкратце хотелось бы рассмотреть вопрос размещения исходных файлов надстройки. Для этого удобнее всего будет воспользоваться механизмом DFS (Distributed File System) [6]. С его помощью можно обращаться к файлам, полностью игнорируя их физическое расположение. То есть, например, для домена marklar.ua можно пользоваться строкой следующего вида для обращения к файлам: \\marklar.ua\files\file.txt. При этом становится не важно, на каком компьютере хранится указанный файл (на самом деле он может быть расположен сразу на нескольких машинах для повышения надежности).

Для начала нужно создать корень DFS. Физически это должна быть обычная разделяемая (shared) папка. Пусть это будет UserMoveSupport. Корень создается с использованием специальной оснастки Distributed File System (см. рис. 1).

После выполнения команды «New Root...» будет запущен мастер создания корневого элемента распределенной файловой системы. Тип корня должен быть «Domain Root». Далее указываются название домена и сервера. Затем вводится имя корня – назовем его UserMoveSupport (см. рис. 2).

Когда создание корневого элемента будет завершено, нужно создать так называемые ссылки (команда «New link...», вызываемая из контекстного меню корня). Фактически нужно указать разделяемые (shared) папки, доступ к которым мы хотим обеспечить с помощью DFS (см. рис. 3).

Для окончательного создания ссылки нужно указать, имя, по которо-

Таблица 2. Интерфейс класса UserMove.Engine

Метод	Описание
dispatchCommand	Обработчик команд менеджеров по персоналу
canCurrentManagePath	Определяет, имеет ли текущий пользователь достаточное количество прав для управления организационной единицей
canHeManagePath	Определяет, имеет ли заданный пользователь достаточное количество прав для управления организационной единицей
delegateOU	Предоставление заданному пользователю прав для управления организационной единицей
undelegateOU	Лишения пользователя прав управления организационной единицей
move	Создать команду начала перемещения пользователя
accept	Создать команду подтверждения перемещения пользователя
Deny	Создать команду отказа в перемещении пользователя
Rollback	Создать команду отмены перемещения пользователя
getParent	Получить путь к родительскому контейнеру
ADSPPath2Readable	Преобразовать ADSI путь к объекту Active Directory в удобочитаемый вид
toUTC	Перевести местное время во время по Гринвичу
fromUTC	Получить из времени по Гринвичу местное время

му в дальнейшем нужно будет к ней обращаться (Link name), и путь к разделяемому ресурсу (Path to target (shared folder)). Обратите внимание, что эти имена не обязательно должны совпадать (см. рис. 4).

Все, теперь к папке можно обращаться без привязки к конкретной рабочей станции, указывая только имя домена.

```
"\\marklar.ua\UserMoveSupport\exec"
```

## Организация работы с приложениями

Для надстройки будет создан ряд вспомогательных hta-модулей, которые вызываются из контекстного меню оснастки Active Directory Users and Computers. HTA (HyperText Application) – особый вид приложений с графическим интер-

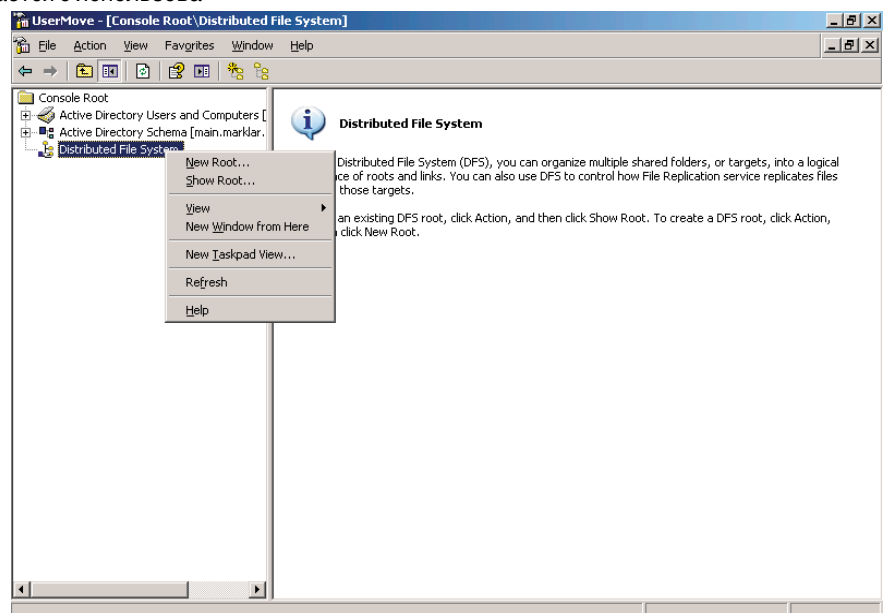


Рисунок 1. Создание корня DFS



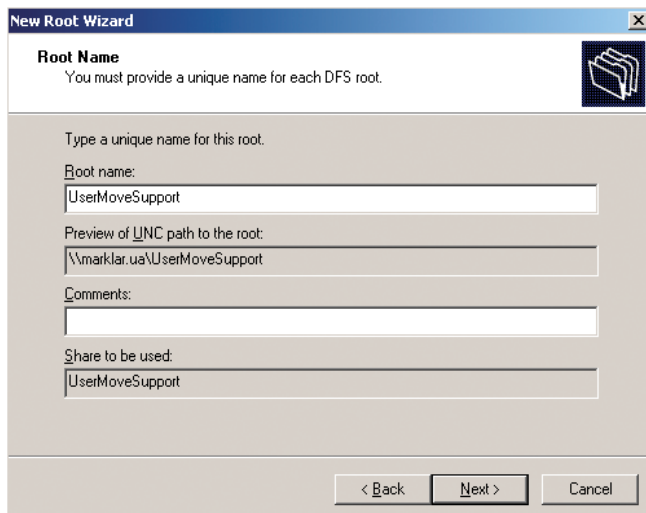


Рисунок 2. Имя корня

фейсом, основанным на HTML, подробно их создание будет рассмотрено в следующей части статьи. Рассмотрим общий механизм реализации такого подхода. В результате должно получиться так, как изображено на **рис. 5** (для наглядности контекстные меню надстройки начинаются с приставки UserMove:).

Следующая функция добавляет новое контекстное меню в оснастку. Для этого нужно создать специальную запись в Active Directory.

```
function installMenu(className, id, name, ↵
    scriptPath, action, locale)
```

Сначала подключаемся к корневому элементу Active Directory:

```
Set root= GetObject("LDAP://rootDSE")
```

Используя корневой элемент, получаем указатель на ветвь с настройками, которая называется configuration NamingContext, далее этот объект будет использоваться

при формировании полного пути (ADSPPath) необходимой конкретной настройки.

```
sConfig = root.Get("configurationNamingContext")
```

В полученной ветви настройки нас интересует раздел DisplaySpecifiers, в котором содержится список элементов – локалей (каждая локализация содержит настройки для определенного языка). В локали вложены элементы с настройками для каждого класса, например, для класса user соответствующий элемент будет называться user-Display. В этот элемент и помещаются специальным образом подготовленные настройки.

```
sPath = "LDAP://cn=" & className & ↵
        "-Display,cn=" & locale & ↵
        ",cn=DisplaySpecifiers," & sConfig
Set obj= GetObject(sPath)
```

Сначала нужно сформировать строку, состоящую из трех элементов, разделенных запятыми: идентификатора id (произвольное число, позволяющее упорядочивать добавляемые элементы меню, – разделы с меньшими номерами будут предшествовать разделам с большими), текста меню и пути к сценарию, который необходимо будет выполнить при выборе этого раздела.

```
sValue = id & "," & name & "," & scriptPath
```

Затем эта строка преобразуется в трехэлементный массив:

```
vValue = Array(sValue)
```

Наконец редактируется запись с надстройками. Изменить нужно ее свойство под названием adminContextMenu. Это массив, для которого мы будем использовать две операции (вид операции задается параметром action метода PutEx). Для добавления элемента используется константа ADS\_PROPERTY\_APPEND (3), для удаления ADS\_PROPERTY\_DELETE (4). Константы придется определить вручную, посмотрев их значения в MSDN [4].

```
obj.PutEx action, ↵
        "adminContextMenu", vValue
obj.SetInfo
end function
```

Рассмотрим параметры, передаваемые функции:

- **className.** Имя класса Active Directory, к которому будет привязываться создаваемый элемент контекстного меню. В этой надстройке – user или organizationalUnit.
- **id.** Числовой идентификатор, определяющий позицию пункта меню.
- **name.** Текст меню.
- **scriptPath.** Путь к сценарию, который необходимо выполнить при выборе элемента меню.

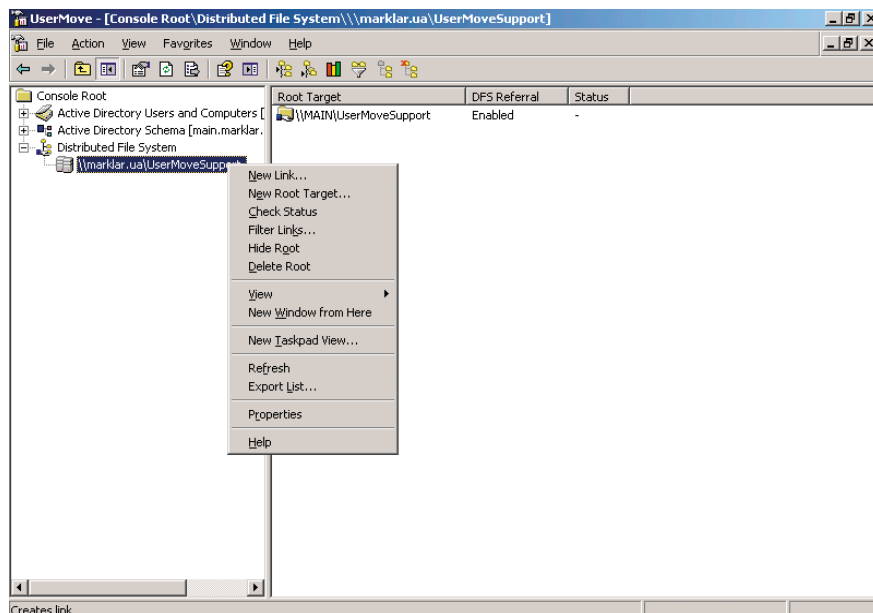


Рисунок 3. Создание ссылки

- **action.** Константа, определяющая, будет элемент меню добавлен или удален.
- **locale.** Локализация. Задается числом в шестнадцатеричной системе счисления. Для английского языка это 409, для русского – 419.

Необходимые настройки определим в виде констант.

Листинг 8. Константы инициализации надстройки

```
Const ADS_PROPERTY_APPEND = 3
Const ADS_PROPERTY_DELETE = 4
Const LOCALE_ENGLISH = "409"
Const LOCALE_RUSSIAN = "419"
Const prefix = "UserMove: "
Const path = "\\marklar.ua\UserMoveSupport\exec\"
```

Также создадим ряд функций-оберток:

- **installOUMenu** – установка раздела меню для организационной единицы;
- **installUserMenu** – установка раздела меню для пользователя;
- **uninstallOUMenu** – удаление раздела меню организационной единицы;
- **uninstallUserMenu** – удаление раздела меню пользователя.

Рассмотрим только одну из этих подпрограмм, все остальные отличаются только передаваемыми в installMenu константами.

Листинг 9. Создание дополнительных пунктов меню

```
function installOUMenu(id, name, scriptPath, locale)
installMenu "organizationalUnit", id, name, _
scriptPath, ADS_PROPERTY_APPEND, locale
end function
```

Всего будет три приложения. Одно будет привязано к объекту пользователя и позволит начать операцию его перемещения (приложение enqueue.hta). И два нужно прикрепить к организационным единицам: просмотр списков входящих (incoming.hta) и исходящих (outcoming.hta) пользователей.

Листинг 10. Создание пунктов меню для английской локали

```
function installEN
installUserMenu 100, prefix & _
"Start", path & _
"enqueue.hta", LOCALE_ENGLISH
installOUMenu 100, prefix & _
"Outcoming", path & _
"outcoming.hta", LOCALE_ENGLISH
installOUMenu 110, prefix & _
"Incoming", path & _
"incoming.hta", LOCALE_ENGLISH
end function
```

Функция installEN устанавливает все необходимые пункты меню для английской локализации. Аналогично создается подпрограмма для удаления этих пунктов uninstallEN а также соответствующие процедуры для русского языка uninstallRU и installRU.

Работу с двумя локализациями необходимо обеспечить, поскольку

в противном случае пользователи русских версий Windows новых пунктов меню просто не увидят.

## Заключение

Итак, создание основного класса надстройки и дополнительных сценариев завершено. Остается разработать графический интерфейс для ее комфортного использования. Он также будет создаваться средствами WSH. Этому и будет посвящена последняя часть статьи.

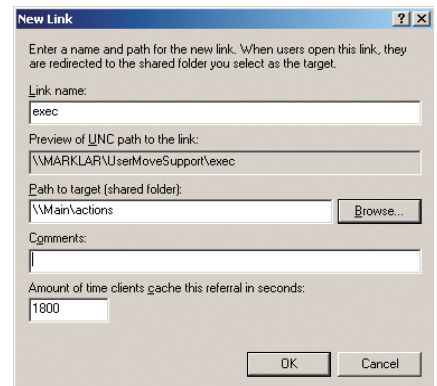


Рисунок 4. Настройки новой ссылки

1. Андросов В. Делегируем права на перемещение учетных записей пользователей в Active Directory. Часть 1. Постановка задачи. //Системный администратор, №3, 2008 г. – С. 16-21.
2. Андросов В. Делегируем права на перемещение учетных записей пользователей в Active Directory. Часть 2. Реализация основных функций. //Системный администратор, №4, 2008 г. – С. 24-30.
3. Андросов В. Делегируем права на перемещение учетных записей пользователей в Active Directory. Часть 3. Реализуем необходимые операции. //Системный администратор, №5, 2008 г. – С. 30-37.
4. Андросов В. Реализуем нестандартные правила управления доступом на основе архитектуры организации в Windows Server 2003. //Системный администратор, №10, 2007 г. – С. 48-58.
5. msdn.microsoft.com.
6. Чарли Рассел, Шарон Кроуфорд, Джейсон Джеренд. Windows server 2003 +SP1 и R2. Справочник администратора. – М.: Издательство «ЭКОМ», 2006 г. – 1424 с.

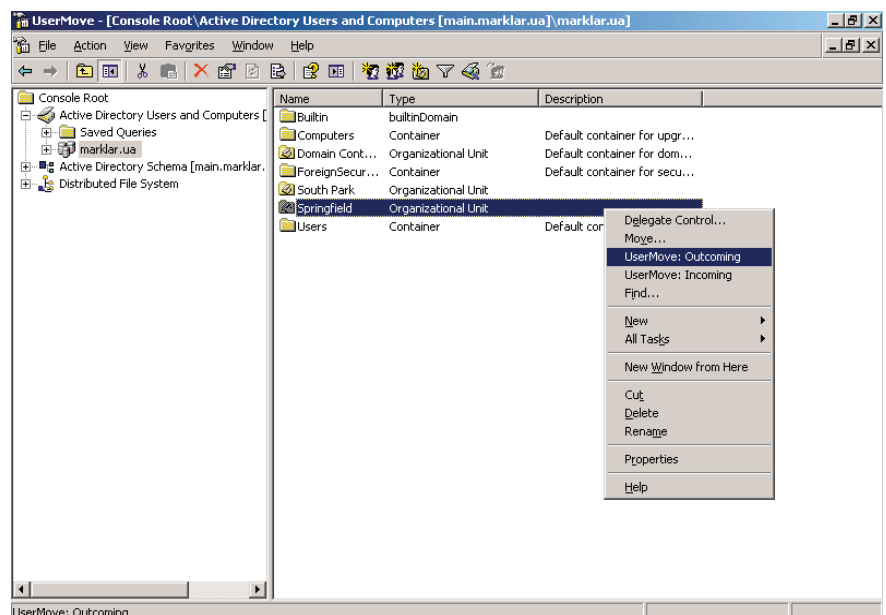


Рисунок 5. Контекстные меню надстройки



# Доступная виртуализация: Citrix XenServer 5.0

Андрей Панченко

В настоящее время все более популярной становится тема виртуализации, и об этом сказано уже достаточно много. Свою статью я хочу посвятить доступному решению по виртуализации вычислительных ресурсов на базе бесплатного программного продукта Citrix XenServer 5.0, который стал доступен 30 марта 2009 года.

Скачать дистрибутив можно по адресу [http://www.citrix.com/lang/English/lp/lp\\_1688615.asp](http://www.citrix.com/lang/English/lp/lp_1688615.asp). Следует упомянуть о том, что ранее было четыре редакции Citrix XenServer, отличающиеся набором функций: Express, Standard, Enterprise и Platinum. Хочу обратить внимание на то, что редакция Express была бесплатна, а остальные требовали оплаты за дополнительный функционал: возможность использования пула серверов, перемещения виртуальных машин между серверами пула, отказоустойчивый кластер и т.д.).

Не так давно компания Citrix приняла решение оставить только одну редакцию Citrix XenServer и распространять ее бесплатно. Теперь Citrix XenServer имеет практически весь набор функциональных возможностей бывшей Enterprise-редакции, кроме отказоустойчивого кластера (High Availability, HA). Редакции Enterprise и Platinum трансформировались в два дополнения для Citrix XenServer 5.0: Citrix Essentials for XenServer редакции Enterprise и Platinum соответственно. Эти дополнения стали доступны также и для Microsoft Hyper-V (Citrix Essentials for Hyper-V Enterprise Edition и Citrix Essentials for Hyper-V Platinum Edition), которые включают в себя:

- упрощенное управление различными системами хранения данных (технология Storage Link);
- динамическое управление виртуальными машинами (потокосная доставка операционных систем,

Citrix Provisioning Services). Бездисковая виртуальная машина может загружаться по сети из заранее созданного образа виртуального диска. Из одного образа может загружаться несколько виртуальных машин, причем добавление нового сервера с уже готовой операционной системой занимает всего несколько минут;

- автоматизированное управление лабораторной средой для разработчиков и тестировщиков, в которой часто приходится удалять и заново разворачивать множество виртуальных машин (Citrix LabManager), а также поддержку гипервизора XenServer.

Но речь сегодня пойдет не о них, а именно о бесплатном продукте Citrix XenServer 5.0.

## Функционал

Citrix XenServer 5.0 обладает богатым функционалом, достаточным для его использования не только в лабораторных целях, но и в ИТ-структуре действующего предприятия. Перечень основных функций и возможностей указан ниже:

- поддержка Windows и Linux в качестве гостевых операционных систем;
- поддержка до 8 виртуальных процессоров в виртуальной машине;
- поддержка до 7 виртуальных жестких дисков для гостевых машин;

- поддержка одного виртуального CD-ROM;
- поддержка до 7 виртуальных сетевых интерфейсов;
- поддержка до 6 физических сетевых интерфейсов на сервер (возможно использование 6 объединенных пар сетевых интерфейсов);
- поддержка виртуальных сетей (VLAN);
- поддержка неограниченного количества физических серверов в пуле, виртуальных машин и памяти;
- конвертер из физической среды в виртуальную для Windows и Linux-систем (P2V-конвертер);
- поддержка широкого спектра хранилищ данных (IDE, SATA, SCSI, SAS, DAS, Fibre Channel, iSCSI, NFS);
- централизованное управление пулом физических серверов из единой консоли управления;
- возможность перемещения виртуальных машин с одного физического сервера на другой без остановки виртуальной машины (XenMotion) при использовании сетевого хранилища данных;
- использование шаблонов для создания виртуальных машин;
- тонкая настройка использования процессорных мощностей;
- горячее подключение/отключение виртуальных жестких дисков и виртуальных сетевых адаптеров;
- создание мгновенных снимков виртуальных машин;

- возможность создания виртуальных машин из заранее подготовленных шаблонов и их клонирования.

## Поддерживаемые гостевые операционные системы

Citrix XenServer официально поддерживает все современные операционные системы Microsoft Windows, а также популярные Linux-системы:

- Windows 2000 SP4;
- Windows Server 2003/2008 (32/64 бит);
- Windows XP SP2/SP3;
- Windows Vista;
- Debian Sarge 3.1;
- Debian Etch 4.0 X;
- Red Hat Enterprise Linux 3.6-3.8, 4.5-4.7, 5.0-5.2 (32/64 бит);
- SUSE Linux Enterprise Server 9 SP1/2/3/4;
- SUSE Linux Enterprise Server 10 SP1/2 (32-bit/64-bit);
- CentOS 4.5, 4.6, 4.7, 5.0-5.2 (32/64 бит);
- Oracle Enterprise Linux 5.0-5.2 (32/ 64 бит).

## Архитектура

Citrix XenServer относится к программному обеспечению для виртуализации, устанавливаемому непосредственно на «железо» (bare-metal solutions), например, VMware ESX или Microsoft Hyper-V, в отличие от решений hosted solutions, которые устанавливаются на полноценную операционную систему, например VMware Workstation или Microsoft Virtual PC. Таким образом, Citrix XenServer практически не расходует ресурсы физического сервера на нужды собственной операционной системы и использует порядка 4-6% от его общей производительности.

Схематично архитектура Citrix XenServer представлена на **рис. 1**. Приведу краткие пояснения:

- **Hardware** – это, собственно, вычислительные ресурсы, т.е. сервер.
- **Hypervisor (Xen Hypervisor)** – это программное обеспечение, которое устанавливается непосредственно на физическое «железо», т.е. на сервер, и образует так называемый уровень абстракции (Abstraction layer), который обеспечивает виртуализацию вычислительных ресурсов (Virtualized Hardware) и позволяет запускать на одном физическом сервере несколько виртуальных, эффективно развязывая их, а также приложения внутри этих виртуальных машин. Hypervisor управляет оперативной памятью и процессорами (RAM/CPU).
- **Control Domain** – это виртуальная машина Linux с наивысшим приоритетом использования вычислительных ресурсов. Эта машина управляет остальным оборудованием, таким как сетевые адаптеры, устройства хранения данных, в том числе и локальные и т.д. (Drivers), кроме оперативной памяти и процессора. Так как используются обычные драйверы для Linux, поддерживается обширный перечень устройств (список всех протестированных устройств можно посмотреть здесь – <http://hcl.xensource.com>). Control Domain содержит пакет инструментов (Xen Tool Stack) для управления Citrix XenServer.
- **Linux** – это гостевая виртуальная машина Linux с поддержкой паравиртуализации. Доступ к устройствам хра-

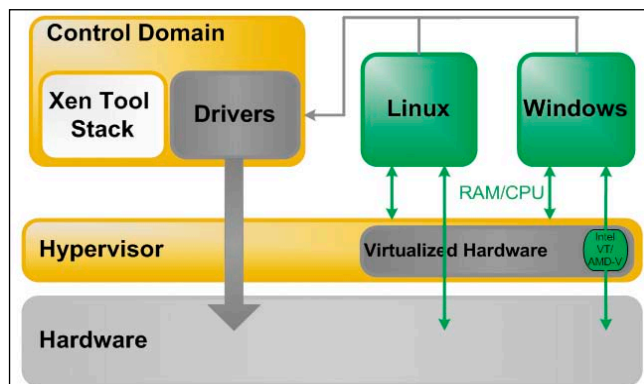


Рисунок 1. Архитектура Citrix XenServer

нения данных и к сетевым интерфейсам такая виртуальная машина получает через Control Domain, а к процессорам и оперативной памяти посредством Xen Hypervisor.

- **Windows** – гостевая виртуальная машина Windows. Доступ к устройствам хранения данных и к сетевым интерфейсам такая виртуальная машина, так же как и Linux, получает через Control Domain, а к процессорам и оперативной памяти посредством Xen Hypervisor, используя возможности аппаратной технологии виртуализации процессоров Intel VT и AMD-V, что позволяет увеличить производительность.

## Установка Citrix XenServer

В блоге Сергея Халяпина (<http://community.citrix.com/blogs/citrite/sergeyk>) есть отличный видеоролик, который наглядно демонстрирует процесс установки Citrix XenServer от начала до конца, а также есть описание процедуры активации бесплатного Citrix XenServer.

- **установка** – <http://community.citrix.com/download/attachments/60981422/XS-Install.mov>;
- **активация** – <http://community.citrix.com/pages/viewpage.action?pageId=68813643>.

В дополнение скажу лишь то, что процесс установки очень прост и занимает порядка 15 минут, а также приведу требования к аппаратной конфигурации сервера:

- один или более процессоров (до 32 процессоров) с поддержкой технологий виртуализации Intel VT или AMD-V 64-bit (необходимо только при использовании гостевых машин с операционной системой Microsoft Windows) с частотой не менее 1,5 ГГц;
- ОЗУ не менее 1 Гб;
- 100 Мбит/с сетевой интерфейс;
- локальный жесткий диск размером не менее 16 Гб.

## Консоль управления Citrix XenServer

Управление Citrix XenServer производится при помощи командной строки посредством SSH-клиента. Для администраторов, использующих операционные системы семейства Windows, предусмотрен специализированный графический инструмент Citrix XenCenter Console. Тем не менее довольно много операций выполняется исключительно из командной строки, например «снимки» виртуальных машин (snapshots). К счастью, все команды хорошо описаны в ру-



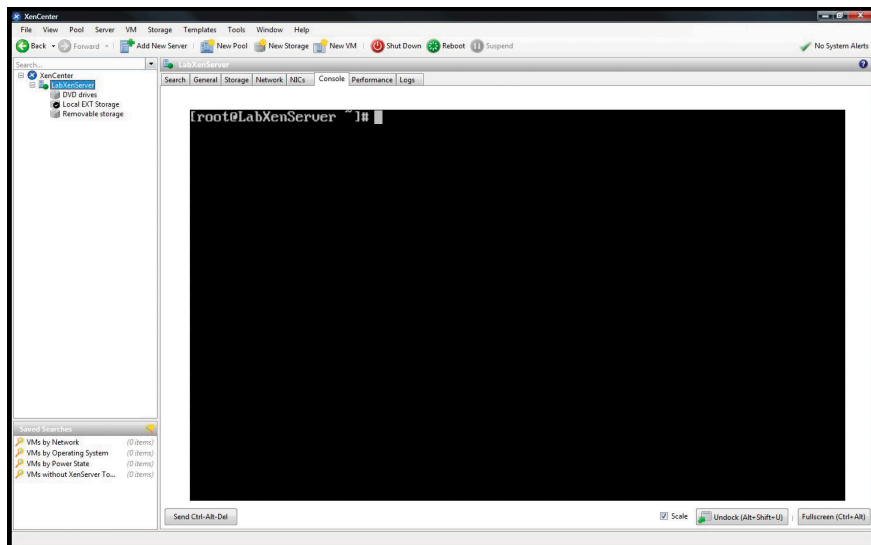


Рисунок 2. Консоль командной строки Citrix XenServer

ководстве администратора (XenServer Administrator's Guide), а также в базе знаний Citrix.

Для консоли управления Citrix XenCenter Console не нужно выделять специальный сервер. Она устанавливается на рабочую станцию администратора. Поддерживаются операционные системы Windows XP, Windows Server 2003 или Windows Vista. Данные о конфигурации пула серверов Citrix XenServer хранятся на всех серверах соответствующего пула, что обеспечивает сохранность конфигурации в случае выхода из строя одного из серверов пула Citrix XenServer.

## Репозиторий данных

Репозиторий данных (Storage Repository) – это хранилище, на котором располагаются диски виртуальных машин (Virtual Disk Images, VDI). Репозиторий может быть локальным (IDE, SATA, SCSI и SAS диски, подключенные локально), а также сетевым (iSCSI, NFS и Fibre Channel).

Если вы планируете использовать не более одного физического сервера в пуле, то вполне можно использовать локальный репозиторий. В качестве локального могут ис-

пользоваться два типа репозитория данных: LVM (Logical Volume Manager, создается по умолчанию при установке Citrix XenServer) и EXT (используется файловая система Ext3, можно создать после установки Citrix XenServer). Репозиторий EXT позволяет использовать диски виртуальных машин в формате Microsoft VHD (Virtual Hard Disk), что предоставляет возможность переносить на Citrix XenServer виртуальные диски из Microsoft Hyper-V либо Microsoft Virtual PC. Репозиторий EXT позволяет делать снимки (Snapshots) виртуальных машин, чего невозможно сделать при использовании репозитория LVM (см. ниже «Использованные источники», пункт 2 – «XenServer 5.0 Update 3 Administrator's Guide»).

Еще одним преимуществом репозитория EXT перед LVM является поддержка плавного роста виртуального диска. Например, если при создании виртуальной машины на базе Windows XP был создан виртуальный диск размером 30 Гб, а файлы операционной системы и приложений занимают 10 Гб, то на физическом жестком диске будет занято не 30 Гб, а всего лишь 10 Гб. Размер занимаемого физического дискового пространства будет постепенно расти до 30 Гб по мере заполнения виртуального диска. Такой же виртуальный диск, созданный на репозитории LVM, занял бы сразу 30 Гб на физическом жестком диске.

Однако конечный размер виртуального диска при использовании репозитория EXT изменить нельзя! Например, если был создан виртуальный диск размером 30 Гб, то увеличить его до 40 Гб уже не получится. А при использовании репозитория LVM поддерживается изменение конечного размера виртуального жесткого диска.

На мой взгляд, в качестве локального репозитория данных лучше всего использовать EXT и диски VHD, поэтому я расскажу, как удалить репозиторий LVM, который был создан при установке Citrix XenServer, и создать репозиторий EXT.

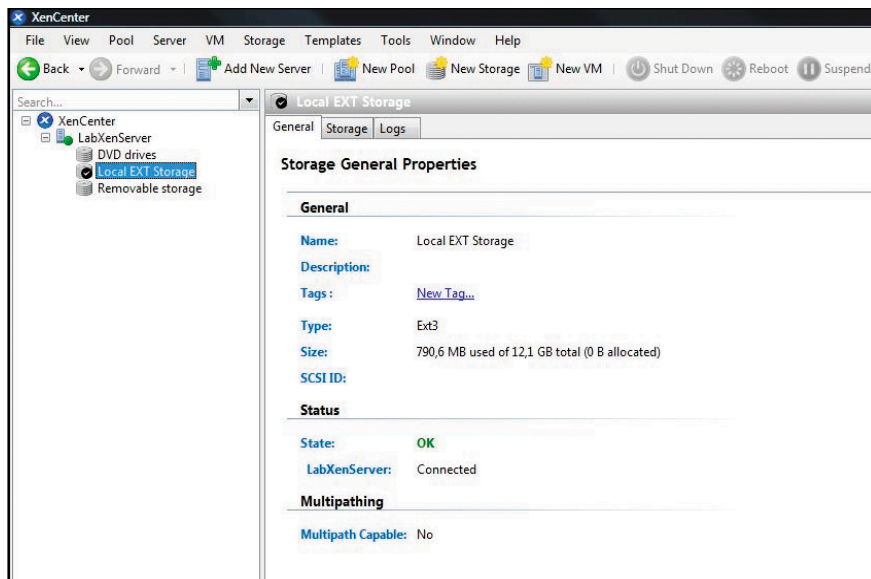


Рисунок 3. Консоль Citrix XenCenter с новым EXT-репозиторием

Все последующие операции выполняются в режиме командной строки из консоли управления Citrix XenServer. Для этого в Citrix XenCenter выделите соответствующий сервер, выберите вкладку Console, как показано на **рис. 2**. В этом случае команды выполняются непосредственно на сервере.

Этот вариант подходит для администраторов, использующих рабочую станцию под управлением Windows. Тем же, кто использует Linux, следует воспользоваться SSH-клиентом. Например, для операционных систем семейства UNIX, использующих в качестве SSH-клиента команду ssh, подключение производится при помощи команды `ssh -l root XenServer`, где root –

имя пользователя, а XenServer – имя или IP-адрес вашего сервера с установленным ПО Citrix XenServer. Когда будет запрошен пароль, введите тот, который вы назначили для пользователя root в процессе установки Citrix XenServer.

Перед тем как приступить к удалению существующего LVM-репозитория, экспортируйте все виртуальные машины, которые, возможно, уже созданы, на другой диск, например на USB-диск.

Экспорт производится следующим образом:

1) Определите имя подключенного USB-диска. Для этого используйте команду:

```
fdisk -l
```

В результате вы получите список дисковых устройств:

```
Disk /dev/sda: 160.0 GB 160000000000 bytes
255 heads, 63 sector track, 19452 cylinders
Units = cylinders of 16065*512 = 8225280 bytes
Device boot Start End Blocks Id System
/dev/sda1 * 1 499 4008186 83 Linux
/dev/sda2 500 998 4008217+ 83 Linux
/dev/sda3 999 19452 148231755 83 Linux
Disk /dev/sdb: 10.0 GB 10005037056 bytes
16 heads, 63 sector track, 19386 cylinders
Units = cylinders of 1008*512 = 516096 bytes
Device boot Start End Blocks Id System
/dev/sdb1 * 1 19385 9870008+ 7 HPFS/NTFS
```

где искомым USB-диск – это устройство /dev/sdb1.

2) Создайте каталог с именем «USB». Для этого используйте команду:

```
mkdir /mnt/usb
```

3) Смонтируйте устройство USB, определенное на этапе 1 в каталог, созданный на этапе 2, командой:

```
mount /dev/sdb1 /mnt/usb
```

4) Отформатируйте его при необходимости командой:

```
mkfs -t ext3 /dev/sdb1
```

5) Экспортируйте виртуальные машины на USB-диск командой:

```
xe vm-export vm=Debian filename=/mnt/usb/Debian.xva
```

где vm – это имя виртуальной машины, а filename – имя файла экспортированной виртуальной машины и путь к ней (расширение файла должно быть .xva).

6) Размонтируйте USB-диск, используя команду:

```
umount /mnt/usb
```

Теперь можно приступить к удалению LVM и созданию EXT-репозитория.

Последовательность действий следующая:

1) Определите, где находится необходимый репозиторий. Для этого используйте команду:

**Majordomo**  
Хостинг. Домены. Сервера.

(812) 335-35-45 (495) 727-22-78  
[www.majordomo.ru](http://www.majordomo.ru)

Входит в пятерку крупнейших хостинг-провайдеров России.  
На рынке с 2000 года. Полный комплекс услуг, связанных с размещением  
Вашего сайта в сети интернет.

Реклама



```
fdisk -l
```

чтобы увидеть список всех разделов:

```
/dev/sda1 *      1      499      4008186      83      Linux
/dev/sda2          500      998      4008217+      83      Linux
/dev/sda3          999     19452     148231755      83      Linux
```

где раздел /dev/sda1 используется операционной системой домена управления (Control Domain), /dev/sda2 – для резервного копирования, а оставшийся /dev/sda3 и есть искомый репозиторий, где размещаются диски виртуальных машин.

2) Определите универсальный уникальный идентификатор (Universally Unique Identifier, UUID) для существующего LVM-репозитория, а также для интерфейса между физическим сервером и репозиторием данных (Physical Block Device, PBD). Для этого используйте команду:

```
xe sr-list type=lvml params=uuid,name-label,PBDs
```

которая выводит следующий результат:

```
uuid ( RO)      : 45bab772-3aab-1a7f-33fb-3346b1ab379d
name-label ( RW): Local storage
PBDs (SRO) : e1b07204-6424-f95a-dedc-0ca6bfe2f286
```

где name-label – это наименование репозитория в том виде, в котором он отображается в консоли Citrix XenCenter.

3) Отключите PBD репозитория командой:

```
xe pbd-unplug uuid=e1b07204-6424-f95a-dedc-0ca6bfe2f286
```

где uuid – это идентификатор соответствующего PBD, полученного нами на этапе 2. Не обязательно вводить номер целиком, введите первые несколько символов, а далее нажмите клавишу TAB – номер будет подставлен автоматически.

4) Удалите LVM-репозиторий командой:

```
xe sr-destroy uuid=45bab772-3aab-1a7f-33fb-3346b1ab379d
```

где uuid – это идентификатор репозитория, полученный на этапе 2. Не обязательно вводить номер целиком, введите первые несколько символов, а далее нажмите клавишу <TAB> – номер будет подставлен автоматически.

5) Создайте новый репозиторий в формате EXT командой:

```
xe sr-create host-uuid=5d189b7a-cd5e-4029-9940-d4daaa34633d \
content-type=user name-label="Local EXT Storage" \
shared=false device-config:device=/dev/sda3 type=ext
```

где host-uuid – это идентификатор Citrix XenServer (выводится при нажатии клавиши TAB), content-type – тип содержимого раздела (наименование произвольное), name-label – наименование создаваемого репозитория (произвольное).

6) Определите уникальный идентификатор созданного репозитория командой:

```
xe sr-list type=ext params=uuid,name-label
```

которая выводит следующий результат:

```
uuid ( RO)      : 38525a18-7992-7905-ac73-468a03812ee5
name-label ( RW): Local EXT Storage
```

7) Установите его в качестве репозитория по умолчанию для размещения новых виртуальных машин:

```
xe pool-param-set default-SR=38525a18-7992-7905-ac73-468a03812ee5 \
uuid=6d87b954-db74-3414-cf64-d5568971069d
```

где default-SR – идентификатор созданного репозитория, полученный на этапе 6, а uuid – идентификатор пула серверов Citrix XenServer (выводится при нажатии клавиши <TAB>).

8) Далее установите его в качестве репозитория по умолчанию для размещения приостановленных виртуальных машин:

```
xe pool-param-set suspend-image-SR=38525a18-7992-7905-ac73-468a03812ee5 \
uuid=6d87b954-db74-3414-cf64-d5568971069d
```

где suspend-image-SR – идентификатор созданного репозитория, полученный на этапе 6, а uuid – идентификатор пула серверов Citrix XenServer (выводится при нажатии клавиши <TAB>).

В итоге вы увидите созданный EXT-репозиторий в консоли Citrix XenCenter, как показано на **рис. 3**.


Администраторы Linux могут получить информацию о созданном репозитории при помощи команды:

```
xe sr-list uuid=38525a18-7992-7905-ac73-468a03812ee5 params
```

где uuid – идентификатор созданного репозитория, который был определен выше.

Если вы планируете использовать не один Citrix XenServer в пуле, а несколько, то рекомендую использовать общий сетевой репозиторий, чтобы можно было использовать функцию XenMotion. В качестве такого репозитория можно использовать как коммерческие, например NetApp или Dell EqualLogic, так и бесплатные решения, например FreeNAS (<http://www.freenas.org>) или Openfiler (<http://www.openfiler.com>).

## Версия 5.5

В начале мая на конференции Synergy в Лас-Вегасе компания Citrix анонсировала Citrix XenServer версии 5.5, которая должна уже быть доступна на момент выхода этой статьи. Функциональные возможности несколько расширятся, но ничего принципиально нового с точки зрения архитектуры и управления не будет. Следовательно, все описанное выше будет актуально и для Citrix XenServer 5.5. 

1. XenServer 5.0 with Update 3 Installation Guide – <http://support.citrix.com/article/CTX120714>.
2. XenServer 5.0 Update 3 Administrator's Guide – <http://support.citrix.com/article/CTX120713>.
3. XenServer 5.0 Update 3 Virtual Machine Installation Guide – <http://support.citrix.com/article/CTX120715>.
4. База знаний по программному обеспечению компании Citrix – <http://support.citrix.com>.
5. Официальный учебный курс «CXS-200-1W Implementing Citrix XenServer Enterprise Edition 5.0».
6. Блоги Citrix – <http://community.citrix.com/blogs>.



**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)**

Реклама



# Построение каталога сервисов

noitulor

**Александр Башкиров**

**Первый вопрос, на который следует дать ответ перед тем, как приступить к построению каталога сервисов, – цель его построения. Как это ни странно, в большинстве случаев четкий ответ на этот вопрос получить довольно сложно, особенно от представителей бизнес-руководства. Туманные фразы про «повышение управляемости» и «гарантию улучшения качества обслуживания основных подразделений», безусловно, говорят о том, что произносящий их знаком или с ITIL, или с принципами сервисного обслуживания, но не дают конкретного ответа. Между тем именно от цели построения каталога сервисов зависят некоторые тонкие моменты, связанные с его построением и использованием.**

**Р**ассмотрим некоторые цели, которые может преследовать построение каталога услуг:

- каталог услуг строится для целей внедрения процесса управления уровнем сервисов в терминологии ITIL (например, для внутренних нужд – при внедрении рекомендаций ITIL или при подготовке к передаче части сервисов на аутсорсинг);
- каталог услуг строится для того, чтобы иметь возможность классифицировать поступающие инциденты в рамках процесса управления инцидентами для определения того, с каким конкретно сервисом связан тот или иной инцидент;
- каталог услуг строится для того, чтобы дать бизнес-руководству или ИТ-руководству представление об услугах, которые ИТ-отдел предоставляет бизнесу.

В любом случае вне зависимости от декларируемой цели каталог сервисов позволяет:

- производить классификацию сервисов;
- автоматически (или полуавтоматически) распределять работы между специалистами по критерию сервиса;

- классифицировать обращения по сервисам и, как следствие:

- ✓ получить информацию о возможных и имеющихся проблемах в инфраструктуре;
- ✓ выделить сервисы, уровень отказов по которым не соответствует требованиям бизнеса;
- ✓ спланировать модернизацию сервисов;
- ✓ получить статистические отчеты по сервисам.

Таким образом, построенный, эксплуатируемый и поддерживаемый каталог сервисов – это шаг к предвосхищению проблем, связанных с ИТ, и, как следствие, к снижению бизнес-рисков. В частности, при построенном каталоге услуг и внедренном процессе управления проблемами (в терминах ITIL) можно связать поступающие инциденты с конкретным сервисом и таким образом выявлять связанные с сервисом проблемы до их массового проявления.

Для того чтобы избежать непонимания, определим понятие «сервис» как конкретную услугу, предоставляемую пользователю, имеющую под собой конкретные инфраструктурные составляющие и обладающую опре-

деленной полезностью, как минимум, для одного пользователя.

## **Сервисы для ITIL (процесса управления уровнем сервиса)**

В случае когда каталог сервисов строится для целей внедрения процесса управления уровнем сервиса, необходимо проанализировать те сервисы, которые ИТ предоставляет бизнесу, в первую очередь с точки зрения пользователя. В частности, для построения подобного каталога рассматриваются типовые роли пользователей в организации (с точки зрения ИТ-сервисов – каждая роль должна обладать уникальным набором составляющих сервиса), и выделяются предоставляемые им сервисы. При этом сервис может быть представлен как конкретным программным, аппаратным или программно-аппаратным средством, так и их набором.

Рассмотрим пример. Предположим, что в процессе построения каталога сервисов были выделены следующие роли пользователей: директор, бухгалтер, менеджер (следует не путать понятие «роль» и «должность» – в рассмотренном примере роль «директор» может соответствовать дирек-

тору, его заместителям и помощникам, роль «бухгалтер» – сотрудникам бухгалтерии и экономистам, и т.д.). Предположим, что вся почта организации проходит через один почтовый сервер и используется один сетевой принтер. При этом каждая из ролей характеризуется определенным, уникальным в рамках организации, набором ПО и используемых аппаратных средств (этот критерий является основополагающим при проведении ролевого разделения пользователей).

Попробуем описать составляющие сервиса для роли «бухгалтер». Бухгалтер использует «1С» и ПО банк-клиент; он отправляет и получает электронную почту без доступа к ней через Интернет; он формирует отчеты для руководства и смежных подразделений, которые выкладывает в сетевую папку; он использует ПК под управлением Windows с пакетом офисных программ Microsoft Office. Кроме того, ему доступны сетевая печать, офисная телефония и факсимильная связь.

Для этой роли можно выделить следующие сервисы:

- сервис доступа к «1С»;
- сервис банк-клиент;
- сервис офисной электронной почты;
- сервис ПК с базовым набором ПО (Windows и Office);
- базовый сетевой сервис (то есть доступ к сети, возможность использования сетевых ресурсов);
- сервис сетевой печати;
- сервис офисной телефонии;
- сервис факсимильной связи.

Аналогично выделяются сервисы и для других ролей. После того как описаны все сервисы для всех ролей, их целесообразно свести в таблицу, которая будет давать представление о доступности того или иного сервиса для той или иной роли, а также о параметрах сервиса, то есть о некоторых его параметрах, характеризующих уровень, с которым данный конкретный сервис предоставляется данному конкретному сотруднику.

Возвращаясь к рассмотренному примеру, предположим, что основными инструментами работы для роли «бухгалтер» являются «1С», банк-клиент и, разумеется, ПК. В случае нарушения работоспособности этих сер-

висов в этой роли ее работа будет парализована; следовательно, в качестве параметров этих сервисов для этой роли должно стоять минимально возможное время восстановления, которое может гарантировать ИТ, а сами эти сервисы признаны критичными для данной роли. Кроме того, выделенные нами сервисы не могут функционировать без сервиса «ПК с базовым набором ПО», что в рассмотренных нами условиях также приравнивает этот сервис к выделенным ранее критичным сервисам.

## Сервисы для процесса управления инцидентами

В этом случае, так же как и в рассмотренном ранее случае, каталог сервисов может быть построен «с точки зрения пользователя», с тем отличием, что для каждого конкретного сервиса не определяются его метрики качества с точки зрения поддержки сервиса, и сами сервисы могут быть заменены на обеспечивающее ПО либо конфигурационную единицу, а роли пользователей быть либо не определены, либо совпадать с должностью. При этом под «метриками качества с точки зрения поддержки сервиса» понимаются не параметры, характеризующие качество предоставления сервиса (например, скорость доступа в Интернет, гарантированную пропускную способность локальной сети), а качество поддержания сервиса, т.е. время, в течение которого сервис при наличии внешних ситуаций будет гарантированно восстановлен. Такой подход противоречит ITIL, но хорошо работает в небольших организациях, когда во главу угла ставится не формализованное исполнение процедур поддержки, а баланс между эффективностью работы ИТ и усилиями, направленными на достижение этой эффективности.

Например, при подобном подходе в небольшой организации могут быть выделены следующие «сервисы»:

- **Windows на рабочих станциях** (вместо «сервис базового ПО с операционной системой»);
- **Linux на серверах** (вместо «сервис доступа в Интернет», «сервис файлового хранилища» и т.д.);
- **электронная почта thunderbird** (вместо «сервис электронной почты»);

- **почтовый сервер** (вместо «сервис электронной почты»);
- **OpenOffice** (вместо «сервис офисного ПО» или «сервис базового ПО с операционной системой»);
- **локальная сеть** (вместо «базовый сетевой сервис»);
- **Интернет** (вместо «сервис доступа в Интернет»).

С точки зрения ITIL подобное смешение недопустимо, но с точки зрения удобства работы конкретного исполнителя подобное разделение (до определенного объема инфраструктуры) выглядит оправданным.

Следует отметить, что в ITIL не сказано о том, какими принципами стоит руководствоваться при проектировании каталога сервисов для обеспечения процесса управления инцидентами – достаточно любым доступным способом идентифицировать проблему, возникшую у пользователя, например, описать ее произвольным виде, и все.

Рассмотрим пример. Предположим, что в организации работают 15 сотрудников, каждый из которых имеет доступ в Интернет, использует Windows и OpenOffice, два пользователя используют «1С». В организации имеются 2 сервера – шлюз и файловый под управлением Linux. В этом случае «каталог сервисов» может выглядеть либо так, как приведено в рассмотренном выше примере, либо вообще отсутствовать, а при обращении пользователя ИТ-специалист фиксирует проблему «со слов пользователя», после чего сервис не определяется, а просто исправляется повреждение.

С точки зрения управления ИТ-инфраструктурой этот случай является наихудшим, поскольку не дает возможности точно указать, какая именно услуга выведена из строя. Например, записанная со слов пользователя авария сервиса «электронная почта thunderbird» из рассмотренного выше примера может иметь причиной аварию на почтовом сервере под управлением Linux и затрагивать всех пользователей.

## Каталог услуг для бизнес-руководства

Построение каталога услуг для бизнес-руководства – это процесс, напоми-



нающий построение каталога для целей процесса управления инцидентами, с той разницей, что для бизнес-руководства имеет смысл иногда вводить более высокий уровень абстракции, поскольку его, как правило, интересуют обобщенные показатели. На практике при построении каталога сервисов обычно вводят двухуровневую модель сервиса. На первом уровне такой модели находится так называемый пользовательский сервис, на второй – обобщенный.

В примере, рассмотренном в подразделе «Сервисы для ITIL», обобщенными сервисами будут являться:

- **бухгалтерский сервис** (доступ к «1С» и доступ к банк-клиенту);
- **базовый сервис** (базовый сетевой сервис, доступ в Интернет, ПК с базовым набором ПО);
- **сервис Интернет** (электронная почта, доступ в Интернет);
- **телефония** (сервис телефонии и сервис факсимильной связи).

Подобный подход является несколько искусственным в том смысле, что для повседневной работы конкретного ИТ-специалиста он не имеет никакой практической ценности. Зато для целей предоставления бизнес-руководству сводных показателей по обобщенным сервисам он имеет, как минимум, одно весьма прагматическое применение: как правило, решения о материальном поощрении сотрудников ИТ принимаются руководством на основании отчета, построенного по обобщенному каталогу. В такого рода сводный отчет обычно включают обобщенные сервисы, количество отказов по ним и среднее время восстановления – плановое и фактическое. Кроме того, подобный отчет может являться обоснованием для введения в бюджет следующих периодов расходов на модернизацию инфраструктуры, поддерживающей сервис. Одновременно с таким отчетом для руководства ИТ, как правило, выпускается отчет, содержащий полный перечень всех сервисов, количество обращений и инцидентов по ним по каждому подразделению, среднее плановое и фактическое время восстановления.

Таким образом, получается достаточно логичная схема: руководство

каждого уровня получает соответствующий своему уровню интереса отчет, на основании которого принимаются управленческие решения.

## Параметры сервисов

Следующий шаг, который необходимо сделать после построения каталога сервисов, – определение для каждого сервиса его характеристик, или параметров доступности сервиса. При этом, разумеется, рассматривается лишь случай, при котором каталог сервисов строится для целей внедрения процесса управления уровнем сервиса в рамках ITIL и отчасти для случая, когда каталог сервисов строится для бизнес-руководства. Дело в том, что при внедрении каталога сервисов для процесса управления инцидентами параметры сервисов однозначно определить невозможно, поскольку сервисы в этом случае могут представлять собой не только «сервисы», но и абсолютно не относящиеся к ним сущности.

Рассмотрим пример, приведенный в разделе «Сервисы для ITIL», с точки зрения параметров сервиса. В примере мы выявили ряд сервисов для одной из ролей, определили, что часть из этих услуг является критичными.

Предположим, что отдел ИТ готов гарантировать для каждого конкретного сервиса следующее время его полного восстановления безотносительно к роли:

- **сервис доступа к «1С»** – 4 часа;
- **сервис банк-клиент** – 4 часа;
- **сервис офисной электронной почты** – 2 часа;
- **сервис ПК с базовым набором ПО (Windows и Office)** – 3 часа;
- **базовый сетевой сервис** – 8 часов;
- **сервис сетевой печати** – 2 часа;
- **сервис офисной телефонии** – 2 часа;
- **сервис факсимильной связи** – 2 часа.

Таким образом, для роли «бухгалтер» сервисы доступа к «1С» и «банк-клиент» будут иметь время восстановления 4 часа, а, например, для роли «менеджер» сервис доступа к «1С» будет иметь время восстановления 8 часов (а сервис «банк-клиент» может отсутствовать). Аналогично, ис-

ходя из технологических возможностей отдела ИТ и требований бизнеса, определяются параметры всех остальных сервисов.

Следует отметить следующее: время восстановления сервиса – это не время гарантированного простоя. Это то время, за которое отдел ИТ гарантирует полноценное восстановление сервиса. Таким образом, время восстановления, например, сервиса «1С» в 4 часа для конкретного сотрудника не означает того, что сотрудник, у которого неработоспособен «1С», может рассчитывать на то, что в течение 4 часов сервис не будет предоставляться. В зависимости от текущих задач специалисты ИТ могут восстановить сервис как через полчаса, так и через три. Возникает закономерный вопрос: если для различных ролей время восстановления, определяемое по возможностям ИТ, одинаковое, то почему тогда для разных ролей оно определяется различно? Ответ на этот вопрос лежит в требованиях бизнеса к параметрам конкретных сервисов – время восстановления сервиса будет тем меньше, чем больше необходимость роли в использовании этого сервиса для осуществления своих должностных обязанностей.

Типичная ошибка, которую допускают на этапе определения параметров сервисов, – при составлении каталога сервисов время восстановления сервиса определяют без оглядки на возможности ИТ выдержать это время. В результате при первом же серьезном сбое выявляется несостоятельность такого распределения: например, время восстановления в 1 минуту можно гарантировать, имея отказоустойчивый кластер, но не сервер с ежечасным бэкапом баз данных и т.д.

Определение, фиксация и выдерживание отделом ИТ заявленных параметров для каждого сервиса позволяет, во-первых, дать бизнес-подразделениям возможность планирования своих рисков, во-вторых, провести четкую взаимосвязь между инвестициями в ИТ и параметрами предоставляемых сервисов, в-третьих, предоставляет возможность оперативного планирования работы сотрудниками в случае нарушения какого-либо сервиса и, наконец, позволяет косвенно решить извечный вопрос об эффек-

тивности работы ИТ: параметры предоставляемых бизнес-подразделениям сервисов являются хорошим индикатором того, насколько оперативно способен работать отдел ИТ.

## Что дальше

Предположим, что в конкретной организации каталог сервисов построен и внедрен, т.е. выделены и описаны сервисы, определены роли пользователей и для каждой роли определены параметры всех предоставляемых ей сервисов.

Внедрение каталога сервисов может быть выполнено различными способами: от приказа по предприятию до декларации службы ИТ, зафиксированной, например, на внутреннем портале или в файле на общедоступном ресурсе – все зависит от размеров предприятия и ИТ-службы. При этом надо не забывать, что единственный критерий внедрения – то, что каталог используется в повседневной работе ИТ. При этом если используются автоматизированные средства для организации работы ИТ (системы класса helpdesk/servicedesk), то при наличии в них модуля SLA каталог сервисов может вестись и использоваться непосредственно в них, в противном случае для каждого конкретного случая время восстановления сервиса приписывается в каждый зарегистрированный инцидент вручную.

После того как каталог сервисов внедрен, дальнейшая работа службы ИТ будет строиться, во-первых, вокруг поддержки актуальной версии этого каталога, а во-вторых, вокруг улучшения самих сервисов. Не исключая при этом, разумеется, текущую работу ИТ-специалистов, ориентированную на выдерживание конкретных параметров конкретного сервиса и решение текущих задач.

Поддержка каталога сервисов включает в себя периодические ревизии каталога на предмет выявления уже непредоставляющихся сервисов или введения в него новых, неописанных сервисов. Подобные ревизии позволят поддерживать каталог сервисов в актуальном состоянии.

Текущая работа ИТ-специалистов в условиях жестких временных рамок, которые накладывает на решение того или иного инцидента уровень пре-

доставляемого пользователю сервиса, безусловно, будет отличаться от работы в «свободном стиле».

Во-первых, специалисты, задействованные на поддержке пользователей, обязаны будут выдерживать контрольные сроки, заявленные в качестве параметра сервиса. При этом скорее всего количество специалистов, обслуживающих тот или иной сервис (или ряд сервисов), не изменится, и они, работая, с одной стороны, над своей текущей работой, с другой – над поддержанием заявленного уровня сервисов, и с третьей – над улучшением сервисов, оказываются перед выбором – либо расширять свой коллектив, либо модернизировать инфраструктуру (одно, кстати, не исключает другое и связано обычно с ростом компании). В свою очередь модернизация инфраструктуры приведет к внедрению более прогрессивных технических решений, нацеленных на предоставление более качественного и отказоустойчивого сервиса пользователю: например, использование отказоустойчивого кластера сервера баз данных вместо RAID-массива дисков на одном сервере, онлайн бэкапирование всей почты и использование механизмов быстрого восстановления почтового сервера (DVD с образом системных разделов почтового сервера) вместо ежечасного копирования накопившейся за это время почты и т.д.


Отдельно стоит упомянуть такую вещь, как стимул специалистов ИТ к улучшению сервисов. В нарисованной выше картине улучшение происходило как бы само собой – следуя из логики развития событий. В реальной жизни все несколько иначе. В частности, у конкретных ИТ-специалистов в рамках нарисованной картины нет стимула к улучшению сервиса, поскольку такое улучшение банально не отражается на их заработной плате. Для того чтобы заинтересовать специалистов делать свою работу быстрее и качественнее, можно ввести «стимулирующие премии», т.е. поощрения за выполнение быстрее установленных параметров для тех или иных сервисов. Правда, встречаются случаи, когда основной бизнес вполне устраивает ситуация, при которой заданные параметры сервисов выдерживаются по граничным условиям – и в этом случае

обосновать премии «за перевыполнение» перед руководством бывает весьма проблематично. Кроме того, улучшение сервиса – это не только премии, но и определенный бюджет (оборудование, лицензии, работы), который необходимо получить от того же основного бизнеса. И в этом аспекте ситуация не отличается от ситуации с премированием: бизнес может выделить бюджет, а может и не выделить – все зависит от того, насколько его потребности в ИТ перекрыты текущим уровнем предоставляемых сервисов. Очень многое, если не все, зависит от позиции руководства по отношению к информационным технологиям.

Тем не менее позицию руководства можно (и нужно) попытаться изменить. ITIL в целом и каталог сервисов в частности позволяют вести учет таких параметров, как время решения инцидентов, соотнесенное с конкретным пользователем, группой пользователей (объединенных по какому-либо признаку: например, это могут быть сотрудники одного отдела или пользователи, играющие одну и ту же роль по отношению к ИТ) и предоставляемым сервисом. Такого рода показатели, предоставляемые руководству на регулярной основе в виде отчетов, позволят на основании фактов обосновать премирование сотрудников ИТ.

В любом случае когда проводится работа по улучшению сервисов, достигается двойной эффект: с одной стороны, улучшается сервис, предоставляемый пользователю, а с другой – повышается общая надежность ИТ-инфраструктуры. Кроме того, с улучшением сервиса повышается и общая удовлетворенность пользователей работой ИТ-службы.

## Вместо послесловия

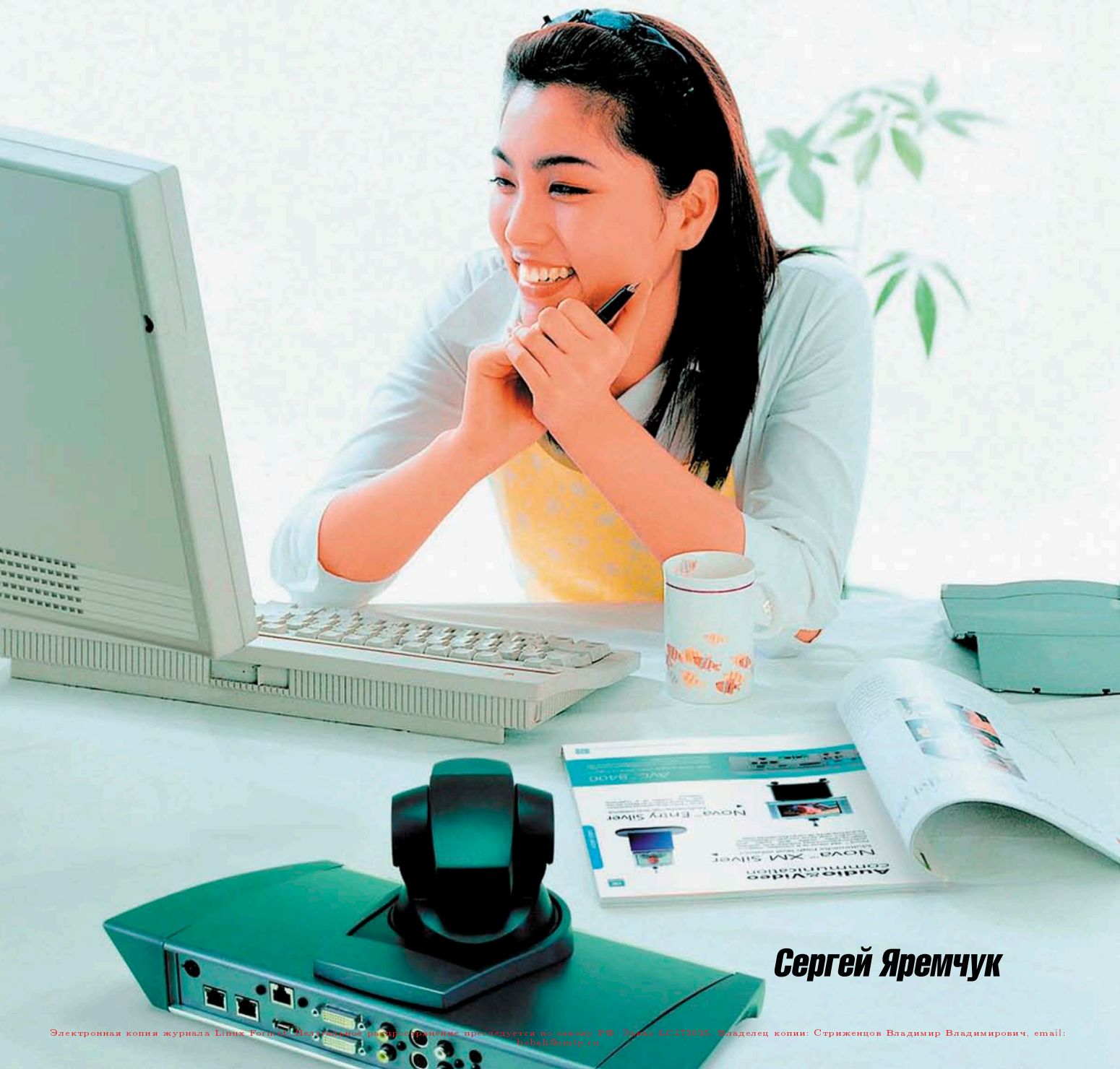
Тема построения и поддержки каталога сервисов практически неисчерпаема, и формат статьи не позволяет рассказать обо всех нюансах и тонких моментах, связанных с этими процессами, например, о планировании оборудования, резерве мощностей, связанных процессах ITIL, направленных на обеспечение поддержки уровня сервиса. Тем не менее приведенной информации вполне достаточно для того, чтобы сделать первые шаги. А там... дорогу осилит идущий. 



# Система видеоконференций OpenMeetings

*Лучше один раз увидеть,  
чем сто раз услышать.*

С развитием сетевой инфраструктуры в любой компании рано или поздно станет вопрос об увеличении ее возможностей за счет добавления новых сервисов. Учитывая, что некоторую часть времени сотрудники тратят на общение и обмен данными, актуальной становится применение систем конференц-связи, среди которых особую роль играют системы видеоконференций. В статье рассмотрим возможности и установку системы видеоконференций OpenMeetings.



**Сергей Яремчук**

Различные совещания, планерки, пятиминутки и так далее являются неотъемлемой частью процесса управления. На них руководство доводит свои требования выбранным исполнителям, а наличие большого количества участников позволяет обмениваться мнениями и выбрать эффективное решение. Даже если подразделения компании находятся в одном здании, районе, городе, все равно некоторую часть времени участникам приходится тратить на дорогу. Не говоря уже о том, что собирать людей из разных городов – дорогое удовольствие, и не только из-за больших финансовых расходов. Время, проведенное в дороге, также имеет свою цену, ведь успех в любом деле зависит от своевременного поступления информации и быстрого принятия решений. Именно поэтому системы, позволяющие объединять в процесс разговора несколько человек, всегда привлекали внимание бизнеса и занимают свою твердую нишу. Это и IRC, форумы, телефонные (селекторные) совещания, а с появлением доступных и широких каналов в эту группу добавились и системы видеоконференций. Последние весьма востребованы и наиболее популярны у руководства. И дело здесь не в их «крутости», а в физиологии человека. Ведь визуальную информацию мы воспринимаем намного лучше. А невербальное общение (мимика, жесты) часто дает больше данных, чем сказанное слово. При этом не следует воспринимать систему видеоконференций как веб-камеру с микрофоном, подключенную к компьютеру. Хотя, вероятно, это самая простая реализация. На самом деле это комплексное решение, позволяющее не только видеть и слышать друг друга, но и обмениваться данными, обрабатывая их в интерактивном режиме. Все должно выглядеть как будто бы человек находится рядом и сидит за одним столом.

В настоящее время существует большое количество решений для организаций видеоконференций, которые различаются по многим критериям: назначению (внутреннего, внешнего использования, вещания), типу (персональные или групповые (комнатные), виду (точка-точка и многоточечные), реализации (аппаратные, программные), протоколами, лицензиями, стоимостью

и так далее. Рыночная цена таких решений относительно высока, но применение свободного программного обеспечения поможет снизить затраты.

## Возможности OpenMeetings

Система веб-конференций Open Meetings распространяемая по лицензии GNU GPL. С ее помощью можно организовать проведение аудио- и видеосовещаний в многоточечном режиме, когда к серверу подключено несколько десятков человек. Обеспечивается несколько вариантов конференций:

- **Совещания** – от 4 до 16 участников, каждый может передавать аудио- и видеоданные.
- **Лекции** – до 200 участников, передача аудио и видео только у модератора (лектора).

Окно видео изначально маленькое, но его можно растянуть до требуемых размеров. Предусмотрена возможность записи и последующего проигрывания совещаний. Конференции могут быть открытыми (в пределах организации) и частными.

Предусмотрен импорт в конференцию документов в различных форматах (.tga, .xcf, .wpg, .txt, .ico, .tff, .pcd, .pcds, .ps, .psd, .tiff, .bmp, .svg, .dpx, .exr, .jpg, .jpeg, .gif, .png, .ppt, .odp, .odt, .sxw, .wpd, .doc, .rtf, .txt, .ods, .sxc, .xls, .xsi, .pdf). После импорта они будут доступны дру-

гим участникам текущей конференции без ограничений. Оригинальный файл и его pdf-версия доступны для скачивания всем участникам. С целью просмотра и редактирования на доске конференции файлы конвертируются в форматы png и pdf. Участники могут редактировать загруженный документ, вводя текст поверх оригинала, рисовать, отмечать нужные места стрелками. Реализовано два типа опросов («Да/Нет» и ввод числовой оценки 1-10).

Кроме видео, предусмотрен обмен текстовыми сообщениями в окне чата. Участник, организующий конференцию, сообщает о ней, отправив приглашение, включающее прямую ссылку на нужную страницу. Для рассылки задействуется внешний SMTP-сервер. У каждого пользователя имеется календарь событий с напоминанием о событиях (через электронную почту или iCal).

Реализовано три уровня доступа – пользователь, модератор и администратор. Для аутентификации пользователей (кроме администратора) возможно использование протокола LDAP, в том числе и Active Directory.

Встроенный менеджер создания резервных копий упрощает операции по резервированию и восстановлению работоспособности сервера и переносу в другую систему. При этом OpenMeetings очень прост в администрировании и после установки практически не требует к себе внимания.

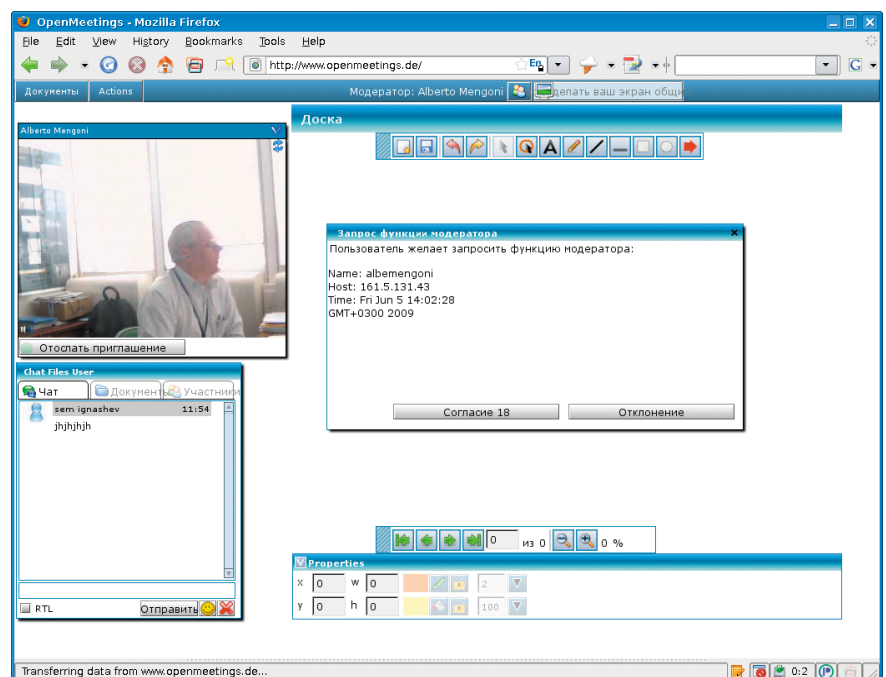


Рисунок 1. С работой OpenMeetings можно ознакомиться на демосайте проекта



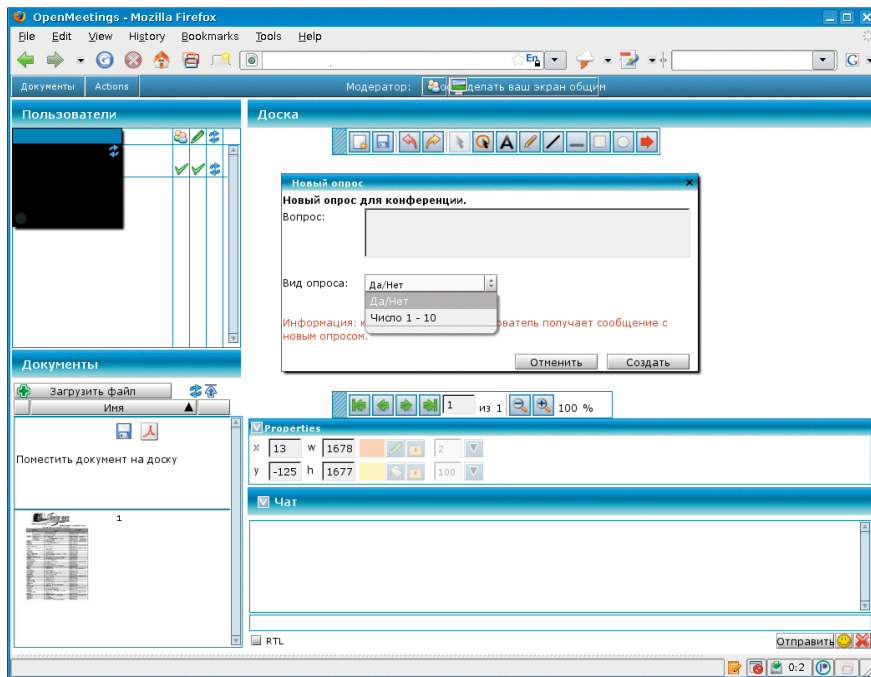


Рисунок 2. В конференции предусмотрена возможность создания опросов

Следует отметить, что отдельно проект предлагает и модуль для интеграции с системой управления обучения Moodle [2], позволяющий показывать видеолекции.

В настоящее время интерфейс OpenMeetings переведен на 19 языков, среди которых есть русский и украинский. Любой другой язык добавить довольно просто. Этот процесс упрощает встроенный редактор локализованных сообщений (LanguageEditor).

Построен OpenMeetings с использованием технологий Java и XML. Для организации сервера задействуются компоненты, распространяемые под свободными лицензиями: веб-сервер Apache Tomcat, Open Source Flash/RTMP Server Red5 [3], OpenOffice.org в качестве сервера документации. В качестве базы данных могут быть использованы MySQL, PostgreSQL, Microsoft SQL Server, Oracle, DB2, Sybase, Firebird и некоторые другие. Компоненты мультиплатформенные, поэтому в качестве сервера можно использовать как один из вариантов UNIX-систем, так и Windows.

Соединение с сервером осуществляется по протоколам HTTP (порт 5080), RTMP (порт 1935), RTMPT (порт 8088) и RTMPS (порт 8443).

При этом требования к оборудованию относительно невысоки. Минимальные требования к системе, которые указаны на сайте, – компьютер

с процессором 1 Гц CPU и 1 Гб ОЗУ. Но его можно использовать при условии, что не будут задействованы возможности по конвертированию документов, загрузки файлов и записи видео. В качестве рекомендуемых указан компьютер 2x/4x 2 Гц (32/64 бит) и 4 Гб ОЗУ. Для организации 100 соединений достаточно компьютера класса на Pentium 4 с 2 Гб ОЗУ.

Требования к пропускной способности определены более четко, каждое подключение к серверу требует

256 Кбит/сек. Хотя клиент может выбрать подключение с меньшим качеством, которое потребует меньшую ширину канала – 160 Кбит/сек.

В итоге для сервера нужно обеспечить (где N – количество участников):

- входящий канал –  $256 \times N$  Кбит/с;
- исходящий канал –  $256 \times N \times (N-1)$  Кбит/с.

Для клиентской системы:

- входящий канал –  $(256 \times (N-1))$  Кбит/с;
- исходящий канал – 256 Кбит/с.

И еще немаловажно, что для подключения клиентов к серверу не требуется установка дополнительного ПО, для этого используется веб-браузер с плагином для поддержки технологии Flash.

Познакомиться с работой и интерфейсом OpenMeetings можно на демо-сайте [4], создав для входа новую учетную запись.

## Подготовительные установки

В документации, доступной на сайте проекта, установка выглядит несколько запутанной, но на самом деле все просто и логично. В статье буду описывать установку на Ubuntu Server 8.04.1, хотя все сказанное за исключением особенностей использования APT будет актуально и для других UNIX-систем. Установка в Windows имеет

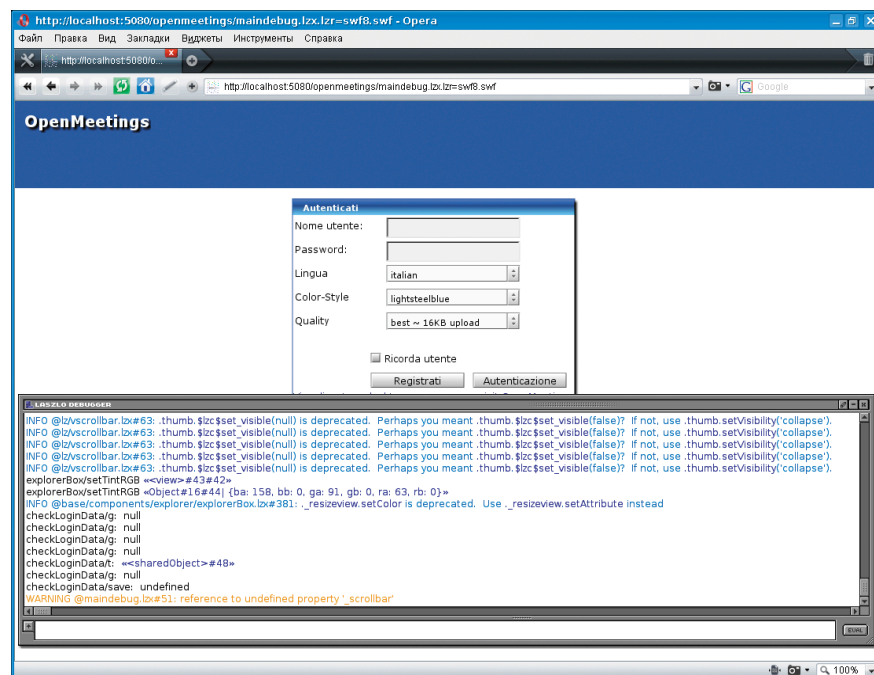


Рисунок 3. Запуск с выводом отладочной информации

свои отличия, но общий принцип остается аналогичным. Здесь я рекомендую файл `compilation.pdf`, который можно скачать с главной страницы группы Google – OpenMeetings User [5]. Он хоть и на французском, но по картинкам общий ход процесса понять можно. Также на сайте доступны и инструкции на русском языке [6], но в них подробно раскрыт лишь процесс администрирования и работы с OpenMeetings.

База данных должна поддерживать UTF8 и подключение через TCP/IP с локального узла. В Ubuntu 8.04 и многих других системах MySQL изначально настроен на работу только через сокет, не поддерживая TCP/IP. Для этого в `/etc/mysql/my.conf` следует добавить несколько строк.

```
[mysqld]
default-character-set=utf8
character-set-server=utf8
bind-address = 127.0.0.1
[client]
default-character-set=utf8
```

После чего перезапускаем MySQL.

```
$ sudo /etc/init.d/mysql restart
```

Проверяем, слушается ли порт 3306.

```
$ sudo /etc/init.d/mysql restart
```

```
tcp        0      0 127.0.0.1:3306      0.0.0.0:*        LISTEN
```

Устанавливаем OpenOffice Converter [7]. Для установки OpenMeetings он не нужен, но понадобится при конвертировании документов во время работы сервера. В Ubuntu должны быть подключены extra-репозитории.

```
$ sudo apt-get update
$ sudo apt-get install openoffice.org-headless \
openoffice.org-base openoffice.org-writer \
openoffice.org-calc openoffice.org-impress \
openoffice.org-draw openoffice.org-math \
openoffice.org-filter-mobiledev \
openoffice.org-filter-binfilter msttcorefonts \
pstoedit libpaper-utils ttf-dejavu
```

Для удобства запуска создаем скрипт `ooc.sh`:

```
unset DISPLAY/usr/bin/soffice"-accept=socket, \
host=localhost,port=8100;urp; \
StarOffice.ServiceManager" -nologo -headless \
-nofirststartwizard
```

И запускаем:

```
$ chmod +x ./ooc.sh
$ sudo ./ooc.sh
```

Проверяем, слушается ли 8100 порт и выполняется ли процесс с заданными параметрами:

```
$ netstat -an | grep 8100
```

```
tcp        0      0 127.0.0.1:8100      0.0.0.0:*        LISTEN
```

```
$ sudo /etc/init.d/mysql restart
```

```
root 11705 92.5 1.2 97024 25784 pts/5 S1 15:09 0:57
/usr/lib/openoffice/program/soffice.bin -accept=socket,
host=localhost,port=8100;urp;StarOffice.ServiceManager -nologo
-headless -nofirststartwizard -splash-pipe=
```

Устанавливаем приложения, необходимые для конвертирования файлов.

```
$ sudo apt-get install imagemagick ghostscript swftools \
xfonts-base
```

В документации упоминается и пакет `xvfb`, но он необходим был только для OpenOffice.org версией выше 2.3, последние версии OpenOffice.org умеют работать с `framebuffer`.

И наконец устанавливаем Java. Для Red5 минимально требуется Java 5 (1.5), оптимально Java 6 (1.6).

```
$ sudo apt-get install sun-java6-jre sun-java6-jdk
```

## Установка сервера Red5

Учитывая, что Red5 является основой для OpenMeetings, возможны 2 варианта установки:

- установка отдельно Red5 и OpenMeetings, при помощи архивов, взятых на сайтах проектов;
- установка Red5 и OpenMeetings, при помощи единого архива, взятого с сайта OpenMeetings.

Каждый вариант имеет свои плюсы и минусы. Так, в первом случае для установки можно выбрать любую доступную версию Red5 и OpenMeetings. На момент написания этих строк на сайте Red5 предлагались стабильные 0.6.3, 0.7.0 и тестовая 0.8.0 RC3. Для OpenMeetings последней версией является 0.8 RC2, есть еще 0.7 RC2 и стабильная 0.5.2, выпущенная в сентябре 2008 года. Для установки в Debian/Ubuntu проект Red5 предлагает `deb`-пакет, что упрощает обновление, и в подарок получаем набор стартовых скриптов. Кроме этого, пакет Red5 содержит ряд демонстрационных примеров. Например, зайдя после установки по ссылке [http://localhost:5080/demos/port\\_tester.swf](http://localhost:5080/demos/port_tester.swf), можно протестировать работу портов.

В актуальной на момент написания статьи версии единого архива находится Red5 0.8.3 RC3 и 0.8 RC2 OpenMeetings. Архивы, содержащие только OpenMeetings, подписаны как Webapp Only, но для тестовой версии 0.8.0 RC2 они не представлены. Поэтому как вариант можно установить Red5 с `deb`-пакета, а затем скопировать OpenMeetings из единого архива.

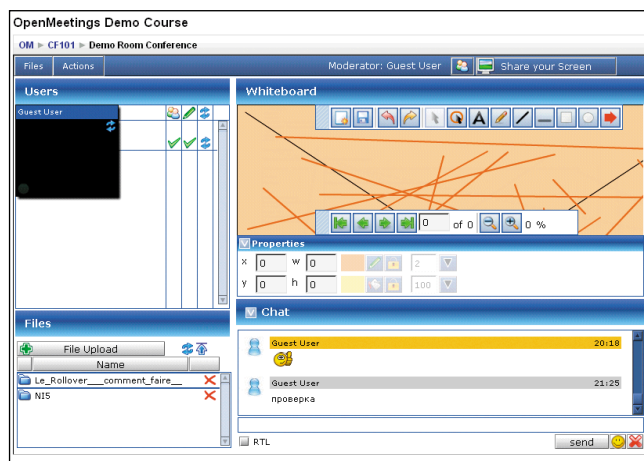


Рисунок 4. Доступен модуль для системы управления обучением Moodle



Дальше буду рассматривать установку OpenMeetings 0.8.0 RC2 при помощи единого архива.

Создаем учетную запись, от имени которой будет работать сервер, и назначаем права на каталог.

```
$ sudo adduser --group red5

Adding group `red5' (GID 1002) ...

$ sudo adduser red5 --gid 1002 --system \
--home /usr/lib/red5 --disabled-password

Adding system user `red5' (UID 115) ...
Adding new user `red5' (UID 115) with group `red5' ...

$ sudo chown -R red5:red5 /usr/lib/red5/
```

Скачиваем, распаковываем архив, копируем файлы на свое место:

```
$ wget -c http://openmeetings.googlecode.com/files/ \
openmeetings_0_8_rc2.zip
$ unzip openmeetings_0_8_rc2.zip
```

Домашний каталог /usr/lib/red5 создан при выполнении adduser, копируем в него файлы.

```
$ sudo mv -v \
red5-0.8.RC3-build-hudson-red5_jdk6_stable-79_2/* \
/usr/lib/red5/
```

Теперь файлы, относящиеся к Red5, будут находиться в корне /usr/lib/red5 (\$RED5-HOME), базовый каталог для OpenMeetings (\$OPENMEETINGS-HOME) – webapps/openmeetings. Именно этот каталог следует использовать при отдельной установке Red5 и Openmeetings. Но копировать его в таком случае нужно в каталог webapps/root, который является корневым для встроенного Tomcat, или самостоятельно изменить эти установки.

Теперь можно проверить работу Red5. Скрипты для запуска Red5 находятся в \$RED5-HOME.

```
$ ls /usr/lib/red5

conf lib red5.jar red5.sh webapps
```

Настройки портов, используемых Red5, указаны в файле \$RED5-HOME/conf/red5.properties:

```
$ grep -i port /usr/lib/red5/conf/red5.properties

http.port=5080
https.port=8443
rtmp.port=1935
rtmpt.port=8088
mrtmp.port=9035
proxy.source_port=1936
proxy.destination_port=1935
```

Если они не используются другими приложениями, нет необходимости в их изменении.

Попробуем запустить:

```
$ sudo /usr/lib/red5/red5.sh
```

Эксперименты показывают, что при попытке первого запуска происходит ошибка. Причина оказалась банальной, это первая строка в скрипте red5.sh:

```
if [ -z "$RED5_HOME" ]; then
    export RED5_HOME=`pwd`;
fi
```

Так как переменную RED5\_HOME никто не устанавливал, то запуск с другого каталога приводит к тому, что сервер не может найти своих файлов. Поэтому правильно сделать так:

```
$ cd /usr/lib/red5
$ sudo ./red5.sh
```

```
Starting Red5
Red5 root: /usr/lib/red5
Configuration root: /usr/lib/red5/conf
Root: /usr/lib/red5
Deploy type: bootstrap
Logback selector: org.red5.logging.LoggingContextSelector
Setting default logging context: default
Red5 Server 0.8.0-RC3 $Revision: 3568 $ (http://www.osflash.org/red5)
```

Последующие запуски с любого каталога происходят уже без проблем. Проверяем, слушаются ли порты:

```
$ netstat -an | grep 1935
```

```
tcp6      0      0 :::1935          :::*              LISTEN
```

```
$ netstat -an | grep 5080
```

```
tcp6      0      0 :::5080          :::*              LISTEN
```

Также работу Red5 можно проверить, зайдя при помощи веб-браузера на страницу <http://localhost:5080>.

Запуск во время отладки сервера лучше производить без перевода процесса в фон (&). В этом случае в консоли будут выводиться сообщения сервера, и мы получаем возможность сразу увидеть ошибку. В дальнейшем для запуска можно создать init-скрипт, скрипт, идущий в deb-пакете Red5 с некоторыми изменениями, можно скачать с сайта журнала [www.samag.ru](http://www.samag.ru) в разделе «Исходный код».

Еще одной возможной причиной неудачи при запуске может быть неустановленная переменная JAVA\_HOME. Обычно скрипт самостоятельно находит каталог с jvm, но если этого не происходит, то ее следует установить:

```
$ export JAVA_HOME=/usr/lib/jvm/java-1.6.0-sun/
```

Не забыв внести эту строку в /etc/profile.

## Настройка OpenMeetings

Теперь необходимо создать базу данных, учетную запись для управления, настроить подключение к базе сервера OpenMeetings.

```
$ mysql -uroot -p
mysql> create database openmeetings;
mysql> grant all on openmeetings.* \
to openmeetings@localhost identified by "om_user_pass";
```

База создана. Информация для подключения к базе данных находится в файле openmeetings/conf/hibernate.cfg.xml. В указанном каталоге имеется несколько шаблонов:

```
$ cd /usr/lib/red5/webapps/openmeetings/conf
$ ls

any_hibernate.cfg.xml  mysql_hibernate.cfg.xml
postgres_hibernate.cfg.xml  hibernate.cfg.xml  om_ldap.cfg
```

Так как мы используем MySQL, берем шаблон `mysql_hibernate.cfg.xml` и переименовываем в `hibernate.cfg.xml`:

```
$ cp mysql_hibernate.cfg.xml hibernate.cfg.xml
```

Соответственно для PostgreSQL выбираем `postgres_hibernate.cfg.xml`, для всех остальных – `any_hibernate.cfg.xml` (внутри есть шаблоны для нескольких баз данных).

Теперь следует отредактировать в `hibernate.cfg.xml` параметры доступа к базе данных.

```
<property name="connection.username"> ␣
    openmeetings</property>
<property name="connection.password"> ␣
    om_user_pass</property>
<property name="connection.driver_class"> ␣
    com.mysql.jdbc.Driver</property>
<property name="dialect"> ␣
    org.hibernate.dialect.MySQLMyISAMDialect</property>
```

Строка `connection.url` по умолчанию выглядит так:

```
<property name="connection.url"> ␣
    jdbc:mysql://localhost/openmeetings?autoReconnect= ␣
    true&useUnicode=true& ␣
    createDatabaseIfNotExist=true& ␣
    characterEncoding=utf-8</property>
```

Я ее привел к виду:

```
<property name="connection.url"> ␣
    jdbc:mysql://localhost/openmeetings</property>
```

Именно так рекомендует документация. После изменений в `hibernate.cfg.xml` следует перезапустить Red5.

Для дальнейшей работы потребуется установить на клиентских системах последнюю версию Flash Player 10 [8]. Несмотря на то что в репозитории Ubuntu имеется нужный пакет (с таким же номером версии), лучше взять Flash Player именно с сайта Adobe. Почему-то с убунтовским пакетом OpenMeetings не дружит.

Скачиваем его с сайта и ставим.

```
$ sudo dpkg -i install_flash_player_10_linux.deb
```

Теперь можно переходить к установке OpenMeetings, для этого переходим по адресу `http://localhost:5080/openmeetings/install`. Мастер установки состоит из двух шагов. На первом выводится краткая информация по компонентам и настройкам, необходимым для работы Open Meetings. На втором следует ввести учетные данные для входа в систему, вписать название организации. Затем заполнить данные в нескольких полях.

Поле Configuration:

- **Allow self-registering (allow\_frontend\_register)** – разрешить самостоятельную регистрацию пользователей (по умолчанию – Yes);
- **Send Email to new registered Users (sendEmailAt Register)** – отсылать почтовое сообщение новым пользователям (по умолчанию – Yes);
- **New Users need to verify their EMail (sendEmailWith VerificationCode)** – пользователи должны подтвердить указанный почтовый адрес (по умолчанию – No);
- **Mail-Referer (system\_email\_addr)** – системный почтовый адрес, который будет использоваться в сообщениях.

Указываем в полях SMTP-Server, SMTP-Server Port, SMTP-Username и SMTP-Userpass соответственно имя SMTP-сервера, порт и учетные данные, необходимые для отправки сообщения. Выбираем в Default Font for Export шрифт для экспорта (по умолчанию TimeNewRoman) и в раскрывающемся списке Default Language язык по умолчанию.

Теперь в поле Converters указываем путь к каталогу SWFTools (определяем `whereis pdf2swf`) и ImageMagick (определяем `whereis convert`).

Поле Crypt Type определяет стиль шифрования, возможны два варианта:

- **org.xmlcrm.utils.crypt.MD5Implementation** – MD5 как в PHP (по умолчанию);
- **org.xmlcrm.utils.crypt.MD5CryptImplementation** – BSD-стиль.

Если планируется использование для аутентификации LDAP-сервера, то в строке LDAP Config следует указать путь к файлу, в котором прописаны параметры подключения. В поставке имеется готовый шаблон такого файла – `openmeetings/conf/om_ldap.cfg`:

- **ldap\_conn\_url** – сервер:порт LDAP (`ldap://localhost:389`);
- **ldap\_admin\_dn** – DN (distinguished name) пользователя для обращения к серверу LDAP (`cn:ommanager, dc=localhost`);
- **ldap\_passwd** – пароль пользователя;

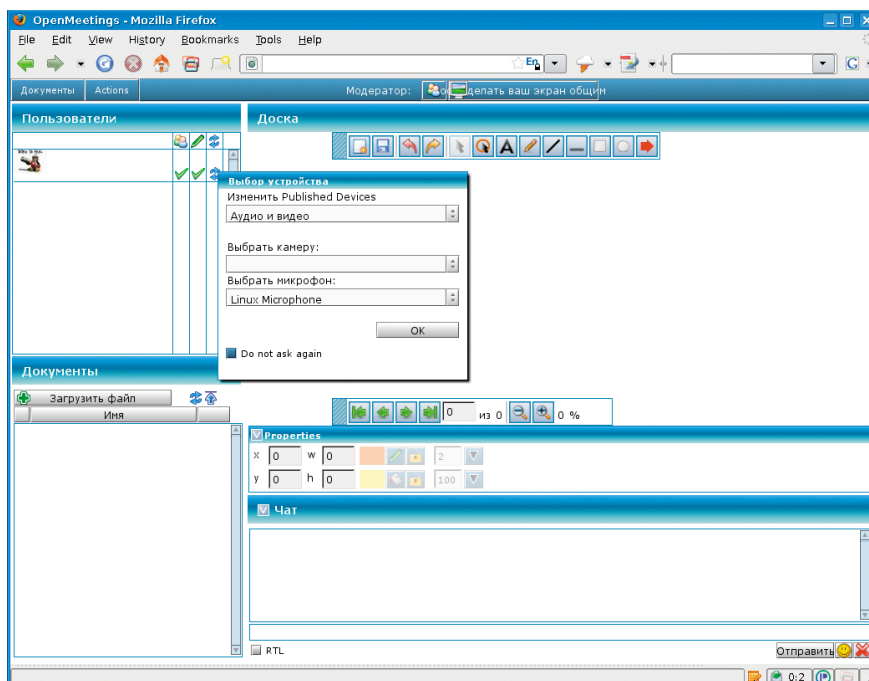


Рисунок 5. При подключении к конференции пользователь должен указать аудио- и видеопериферию



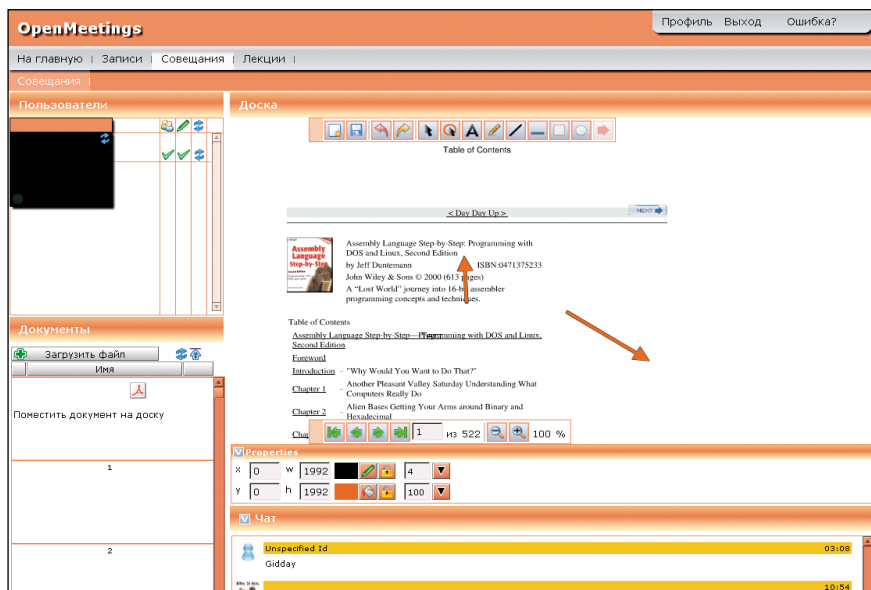


Рисунок 6. Поддерживается функция импорта документов с возможностью совместной работы с ними

- **ldap\_login\_base** – ветвь для поиска пользователя ldap\_admin\_dn (OU:...,OU:...,DC:...);
- **ldap\_search\_base** – ветвь для поиска данных (может совпадать с предыдущим);
- **field\_user\_principal** – поле сервера, с которым сравнивают введенные данные (uid).

Поле Screen Viewer позволяет выбрать вариант клиентского подключения. Под Standard Screenviewer, предлагаемым по умолчанию, понимается веб-браузер. Этот вариант оптимизирован для низкоскоростных каналов. В локальной сети можно использовать jrDesktop.

Многие установки затем можно будет изменить в окне администрирования OpenMeetings. Когда установки закончены, нажимаем INSTALL. На этом этапе может показаться, что приложение зависло. Чтобы убедиться, что что-то все-таки происходит, достаточно перейти в консоль, в которой запущен Red5. Сам процесс установки занимает некоторое

время, и, пока не получим сообщение в окне браузера Installation Complete, нажимать, что-либо в окне браузера не следует. Иначе придется весь процесс повторить сначала. По окончании вызываем <http://localhost:5080/openmeetings/> и регистрируемся с учетными данными, указанными на втором шаге. Если Red5 использует отличные от установок по умолчанию порты, их следует изменить в файле `openmeetings/config.xml`.

При возникновении проблем можно подключиться к серверу с выводом отладочной информации. Для этого необходимо использовать следующий адрес – <http://localhost:5080/openmeetings/maindebug.lzx.lzr=swf8.swf>.

Чтобы проверить работу конвертора документов, следует ввести такую команду:

```
$ java -jar /usr/lib/red5/webapps/openmeetings/jod/ jodconverter-cli-2.2.0.jar -p 8100 -f pdf test.ppt
```

где:

- **-f (--output-format)** – выходной формат файла;
- **-p (--port)** – порт, на котором принимает подключения OpenOffice.org Converter.

Инструкции для пользователя и администратора Open Meetings на русском языке можно найти в документации [6].

Если все сделано правильно и без ошибок, мы получим полностью готовую к работе и локализованную систему видеоконференций. Возможно, что после установки вместо надписей на русском будет выводиться Error и в чате нечитаемый текст. Это значит, что во время установки были допущены ошибки, следует удалить базы и повторить установку OpenMeetings сначала. Хотя, учитывая, что проект пока находится в состоянии активной разработки, никто не застрахован от вероятных ошибок. Единственная не решенная на данный момент проблема – вывод читаемого текста в чате при работе на клиентской Linux-машине. Вероятно, это связано с особенностями реализации Flash для этой системы.

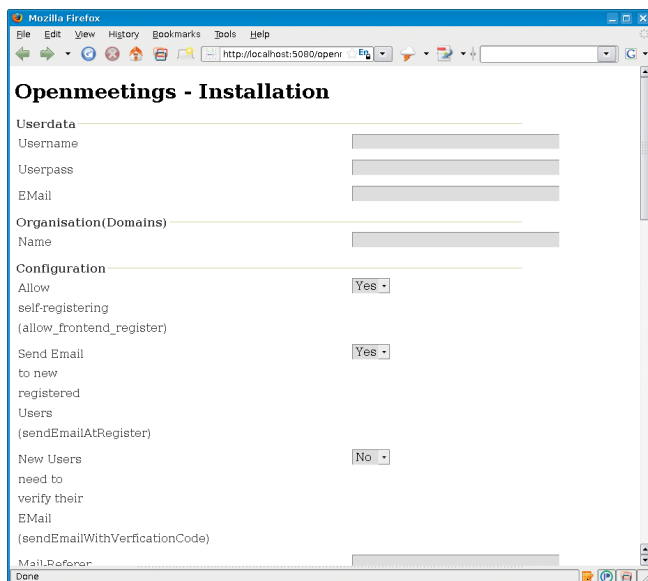


Рисунок 7. Заполняем параметры на втором шаге установки

1. Сайт проекта OpenMeetings – <http://code.google.com/p/openmeetings>.
2. Сайт системы дистанционного обучения Moodle – <http://www.moodle.org>.
3. Сайт проекта Red5 – <http://osflash.org/red5>.
4. Демосайт – <http://www.openmeetings.de>.
5. Группа Google OpenMeetings User – <http://groups.google.com/group/openmeetings-user>.
6. Русские инструкции – <http://code.google.com/p/openmeetings/wiki/RussianTranslatedInstructions>.
7. Страница OpenOfficeConverter – <http://code.google.com/p/openmeetings/wiki/OpenOfficeConverter>.
8. Страница Flash Player 10 – <http://labs.adobe.com/technologies/flashplayer10>.

## Переполнение буфера в Sendmail

**Программа:** Sendmail версии до 8.13.2.

**Опасность:** Высокая.

**Наличие эксплоита:** Да.

**Описание:** Уязвимость существует из-за ошибки проверки границ данных при обработке заголовков X-\*. Удаленный пользователь может с помощью специально сформированного e-mail-сообщения, содержащего слишком длинный заголовок X-\* (например, X-Testing), вызвать переполнение динамической памяти и выполнить произвольный код на целевой системе.

**Примечание:** Уязвимость была устранена в 2004 году, но о ней стало известно только сейчас.

**URL производителя:** [www.sendmail.org](http://www.sendmail.org).

**Решение:** Установите последнюю версию 8.13.2 или выше с сайта производителя.

## Множественные уязвимости в IBM WebSphere Application Server

**Программа:** IBM WebSphere Application Server версии до 6.0.2.35.

**Опасность:** Средняя.

**Наличие эксплоита:** Нет.

**Описание:** 1. Уязвимость существует из-за ошибки при доступе к защищенной странице через HTTP. Удаленный пользователь может произвести атаку «человек посередине» и получить доступ к важным данным.

2. Уязвимость существует из-за неизвестной ошибки в Configservice API. Удаленный пользователь может получить доступ к важным данным.

3. Уязвимость существует из-за ошибки в спецификации цифровых XML-подписей.

4. Уязвимость существует из-за неизвестной ошибки в wsadmin в компоненте System Management/Repository.

**URL производителя:** [www-306.ibm.com/software/webservers/appserv/was](http://www-306.ibm.com/software/webservers/appserv/was).

**Решение:** Установите последнюю версию 6.0.2.35 с сайта производителя.

## Множественные уязвимости в Sun Solaris

**Программа:** Sun Solaris 8, 9.

**Опасность:** Средняя.

**Наличие эксплоита:** Нет.

**Описание:** 1. Уязвимость существует из-за ошибки в демоне sadmind во время декодирования параметров запроса. Удаленный пользователь может с помощью специально сформированного RPC-запроса вызвать переполнение динамической памяти и выполнить произвольный код на целевой системе.

2. Целочисленное переполнение существует в демоне sadmind при выделении памяти на входящие sadmind запросы. Удаленный пользователь может с помощью специально сформированного RPC-запроса вызвать переполнение динамической памяти и выполнить произвольный код на целевой системе.

**URL производителя:** [www.sun.com](http://www.sun.com).

**Решение:** Установите исправление с сайта производителя.

## Переполнение буфера в NTP

**Программа:** NTP версии до 4.2.4p7.

**Опасность:** Высокая.

**Наличие эксплоита:** Нет.

**Описание:** Уязвимость существует из-за ошибки проверки границ данных в функции `crypto_recv()` в файле `ntpd/ntp_crypto.c`. Удаленный пользователь может с помощью специально сформированного пакета, отправленного ntpd демону, вызвать переполнение стека и выполнить произвольный код на целевой системе. Для успешной эксплуатации уязвимости требуется, чтобы Autokey Authentication была настроена через «crypto pw [password]» в файле `ntp.conf`.

**URL производителя:** [www.ntp.org](http://www.ntp.org).

**Решение:** Установите последнюю версию 4.2.4p7 с сайта производителя.

## Переполнение буфера в IBM WebSphere MQ

**Программа:** IBM WebSphere MQ версии до 6.0.2.7 и 7.0.1.0.

**Опасность:** Средняя.

**Наличие эксплоита:** Нет.

**Описание:** Уязвимость существует из-за неизвестной ошибки. Удаленный пользователь может с помощью специально сформированного запроса вызвать переполнение буфера и выполнить произвольный код на целевой системе.

**URL производителя:** [www-306.ibm.com/software/integration/wmq](http://www-306.ibm.com/software/integration/wmq).

**Решение:** Установите последнюю версию 6.0.2.7 или 7.0.1.0 с сайта производителя.

## Переполнение буфера в Cyrus SASL

**Программа:** Cyrus SASL версии до 2.1.23.

**Опасность:** Средняя.

**Наличие эксплоита:** Нет.

**Описание:** Уязвимость существует из-за небезопасного использования функции `sasl_encode64()` в файле `lib/saslutil.c`. Удаленный пользователь может при некоторых обстоятельствах вызвать переполнение буфера и скомпрометировать целевую систему.

**URL производителя:** [asg.web.cmu.edu/sasl/sasl-library.html](http://asg.web.cmu.edu/sasl/sasl-library.html).

**Решение:** Установите последнюю версию 2.1.23 с сайта производителя.

## Отказ в обслуживании в Quagga

**Программа:** Quagga 0.99.11 и более ранние версии.

**Опасность:** Средняя.

**Наличие эксплоита:** Нет.

**Описание:** Уязвимость существует из-за ошибки в bgpd при обработке AS-путей, содержащих множественные 4-байтные номера AS. Удаленный пользователь может анонсировать специально сформированные AS-пути и вызвать отказ в обслуживании приложения.

**URL производителя:** [www.quagga.net](http://www.quagga.net).

**Решение:** Установите последнюю версию 0.99.12 с сайта производителя.

Составил Александр Антипов

# Обзор проекта Gnash

*Свободный Flash, открытая медиа:  
это то, что нужно делать!*

*Призыв разработчиков Gnash*

Часто у проприетарных программ, имеющих большую популярность, появляется свободная реализация. Одним из таких продуктов и стал Gnash – альтернатива закрытому флеш-плееру компании Adobe. Кроме того, он привнес возможности и поддержку платформ, недоступные в последнем, входит в список приоритетных проектов Фонда свободного программного обеспечения и находится «в шаге» от реализации поддержки ActionScript 3 Class Library.

**Игорь Штомпель**



## История проекта

История проекта Gnash началась в 2005 году с разработки на заказ библиотеки GameSWF, над которой работал сегодняшний мейнтейнер проекта – Роб Савой (Rob Savoye). Как говорил разработчик в своем интервью Linux Format, он опирался на свободные проекты, которых оказалось немного [1].

Кстати, Gnash и сейчас разрабатывается на C++, что обусловлено активным использованием библиотеки GameSWF в ходе развития свободного плеера. Библиотека создана на языке C++, доступна по адресу <http://tulrich.com/textweb.pl?path=geekstuff/gameswf.txt>.

Сопоставив два интервью мейнтейнера и архитектора Gnash (одно, данное для ZDNet.com 16 ноября 2006 года [2], и другое – для Linux Format в июле 2008 года), можно прийти к выводу, что GameSWF был проектом по созданию пользовательского интерфейса для ТВ-приставок, который предложил реализовать Джон Гилмор (John Gilmore), друг Савоя. Используя имеющиеся свободные разработки, Роб Савой добавил в них ActionScript и создал интерфейс для стерео.

Через какое-то время Гилмор снова обратился к Савою и предложил на базе созданного Flash-плеера сделать плагин для Firefox. Но на тот момент последний уже уезжал на ликвидацию последствий урагана Катрина, который практически уничтожил Новый Орлеан. А вернувшись, он приступил к работе над данным плагином, что в конечном итоге привело к реализации Gnash таким, какой он есть сегодня.

В марте 2008 года было объявлено о создании некоммерческого фонда Open Media Now. Это произошло, после того как разработчики Gnash поняли, что необходимо создание «целостной инфраструктуры», т.е. реализации поддержки свободной флеш-технологии как на стороне клиента, так и на стороне сервера. Фонд был создан с целью оказания сервисных услуг как частным лицам, так и организациям в деле развития открытой инфраструктуры медиа (open media infrastructure). Gnash стал одним из проектов этого фонда.

В совет директоров Open Media Now сегодня входят: бывший глава компании RedHat – Боб Янг (Bob Young),

Джон Гилмор, Дэвид «Lefty» Шлезингер (David «Lefty» Schlesinger) и Роб Савой.

Читателям будет интересно узнать, что в ходе разработки свободного плеера сложилась определенная дискуссия вокруг принятия/не принятия условий EULA на Flash-инструменты от компании Adobe/Macromedia. Разработчики Gnash встали на позицию невозможности установки этих инструментов, тем самым не принимая данное лицензионное соглашение с конечным пользователем. Они, например, предпочитают использовать такие утилиты, как Ming для генерации testcases (набор тестов для тестирования ПО) Flash [3].

## Поддерживаемые платформы

Сегодня Gnash поддерживает платформы:

- Intel x86;
- Intel ia64;
- AMD x86\_64;
- AMD Geode;
- PowerPC (32 и 64-бита);
- Mips;
- Arm (7, 9 и 11);
- Hitachi SH.

Операционных системы, на которых будет работать свободный плеер:

- GNU/Linux (протестировано на базе Ubuntu, Fedora и Debian);
- BSD (протестировано на базе OpenBSD, NetBSD и FreeBSD);
- Open Embedded (различные дистрибутивы на основе Debian);
- Darwin;
- IRIX;
- Solaris;
- Windows.

Кроме того, имеются официально не поддерживаемые версии для операционных систем:

- RiscOS;
- OS/2;
- Syllable;
- Haiku.

Свободный Flash-плеер доступен и для встраиваемых устройств в рамках следующих проектов:

- OpenMoko;
- Ubuntu Mobile;
- Sharp Zaurus;
- Access Linux Platform;

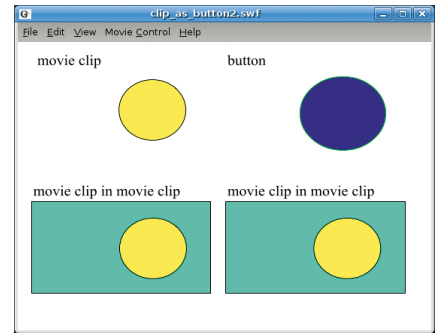


Рисунок 1. Работа тестового файла clip\_as\_button2.swf в плеере Gnash

- MobLin;
- OLPC XO;
- Intel Classmate PC;
- Studentmate.

## Возможности

Gnash обеспечивает поддержку, в первую очередь swf-файлов версии 7, реализация поддержки файлов версий 8 и 9 находится в активной разработке. Выпуск 0.8.2 (5 марта 2008 года [4]) принес первоначальную поддержку парсера swf (версий 8 и 9). Из классов ActionScript 2 поддерживаются часто используемые методы каждого класса. Поддержка остальных классов пока реализована частично. Кроме того, Gnash поддерживает большую часть кодов операций вплоть до версии 9 формата swf.

Свободный плеер позволяет автономно запускать флеш-файлы для просмотра. Например, на рис. 1 показана работа тестового файла clip\_as\_button2.swf в плеере Gnash (тестовые файлы поставляются вместе с исходным кодом программы – в версии gnash 0.8.5 они находятся в каталоге /testsuite/samples). Кроме того, свободный плеер может быть установлен в качестве плагина для браузеров Mozilla и Konqueror.

Поддержка видео появилась в Gnash в 2007 году, но стоит отметить, что многие сайты используют swf версии 8 и 9, реализация которых в свободном плеере находится на начальной стадии. Для воспроизведения видео используются кодеки ffmpeg (на этапе компиляции пользователь может выбрать использовать кодеки ffmpeg или GStreamer), которые позволяют проигрывать форматы SWF, FLV, VP6 (ON2), H.263, H.264, а также аудио MP3. Имеется поддержка Ogg Vorbis и Theora, а также Dirac.

```
apt-get install mozilla-plugin-gnash
```

## Ближайшие перспективы

В течение этого года в рамках развития проекта планировалось: продолжение работы по поддержке swf версии 9, реализация ActionScript 3 Class Library, развитие набора тестов и улучшение совместимости с другими плеерами, разработка свободных спецификаций swf и ActionScript, усовершенствование работы с памятью и процессором [5].

Но недавно стало известно, что разработчики хотят форсировать развитие проекта. Так, к концу лета 2009 года планируется выпуск Gnash 9.0. В данной версии будет включена поддержка библиотек классов ActionScript3, с целью обеспечения корректной работы свободного плеера с версиями swf – 9 и 10, и соответственно с образовательными, информационными и новостными порталами, а также большинством популярных сайтов, использующих данную технологию. Для реализации этих целей Open Media Now начала сбор средств в рамках проекта Gnash V9 Summer Bash.

Кроме того, планируется привлечение студентов в качестве стажеров – будет заключен контракт со студентами инженерных специальностей университета Колорадо, которые станут работать под непосредственным руководством Роба Савоя [7]. Как мне представляется, мы с большой долей вероятности увидим выпуск Gnash 9.0 в конце лета или с небольшой задержкой, так как такой проект, являющийся частью свободной альтернативы закрытым медиа в области Flash-технологии, не может оставить равнодушными власти различных стран, заинтересованные организации, разработчиков и студентов. ☺

1. Linux Format 107. Июль 2008. с. 26-27.
2. <http://blogs.zdnet.com/Stewart/index.php?p=177>.
3. <http://www.gnashdev.org/?q=node/25>.
4. [http://wiki.gnashdev.org/Release\\_0.8.2](http://wiki.gnashdev.org/Release_0.8.2).
5. <http://www.openmedianow.org/?q=node/14>.
6. <http://www.openmedianow.org/?q=node/39>.
7. <http://www.openmedianow.org/SummerBash/GnashSummerBash.pdf>.

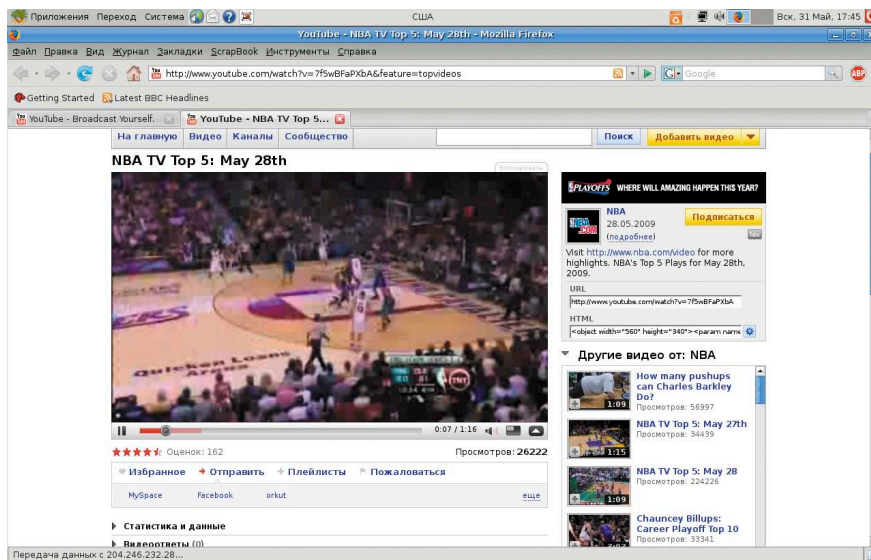


Рисунок 2. Просмотр видео на сайте [www.youtube.com](http://www.youtube.com) с использованием плагина Gnash для Mozilla Firefox 2

Официально заявлена поддержка потокового видео с таких популярных сайтов, как Lulu.tv и YouTube.com. Мне, как видно на рис. 2, при использовании плагина Gnash версии 0.8.2 (mozilla-plugin-gnash 0.8.2ubuntu3) для Mozilla Firefox 2 в операционной системе gNewSense GNU/Linux 2.2 удалось посмотреть видео с [www.youtube.com](http://www.youtube.com). Высокое качество вывода обеспечивается использованием OpenGL для рендеринга графики на настольных компьютерах и Anti-Grain Geometry (AGG) (свободная графическая библиотека, написанная на C++ и доступная по адресу <http://www.antigrain.com>) для встраиваемых устройств.

Еще одной возможностью, которой характеризуется свободный плеер, является поддержка основанной на XML системы сообщений, описанной в спецификации формата Flash.

Для работы на серверной стороне, в рамках проектов Open Media Now, развивается Cygnaal (на сегодняшний день еще не готов и представляет собой прототип). Продукт призван стать совместимым с Flash Media Server от компании Adobe. Он будет иметь возможность обрабатывать тысячи сетевых соединений и несколько потоков с различным содержанием, и работать на крупных кластерах GNU/Linux.

Cygnaal должен будет работать с RTMP (Real Time Messaging Protocol, протокол потоковой передачи данных – видео, аудио). Уже сегодня разработчики усовершенствовали производительность сервера (http) и поддержку пре-

рванных закачек (uploads). Вся сетевая работа свободного сервера на сегодняшний день основывается на очереди сообщений, что позволит ему осуществлять маршрутизацию пакетов между сетевыми соединениями или RTMP-каналами.

Из-за патентных угроз, связанных с форматами MP3, FLV и ON2, Cygnaal будет использовать свободные кодеки для их воспроизведения. Например, будет использоваться плагин ffmpeg с поддержкой FLV, а также ON2 (VP6 и VP7) для Gstreamer. Также свободный сервер получит возможность конвертации данных (потоков аудио/видео), сжатых с использованием закрытых технологий в свободные форматы, например, в Ogg Theora и в Ogg Vorbis. Узнать о текущем состоянии проекта Cygnaal можно по адресу <http://wiki.gnashdev.org/Cygnaal>.

Все, что было сказано о Gnash выше – это была «теория». Испытать свободный плеер на практике можно, либо установив его с помощью программы управления пакетами вашего дистрибутива, либо загрузив и установив с этой страницы <http://www.getgnash.org/packages/releases>.

Например, для установки плеера в gNewSense GNU/Linux 2.2 нужно дать команду:

```
apt-get install gnash
```

А если необходимо установить Gnash в качестве плагина для браузера mozilla, то надо выполнить:

# Mandriva Linux

## Сертифицированная ФСТЭК версия

Дружественный и удобный интерфейс, Простота работы и настройки, Большой спектр поддерживаемого оборудования, Гарантия безопасности: дистрибутивы сертифицированы ФСТЭК.\*

### Офисная рабочая станция

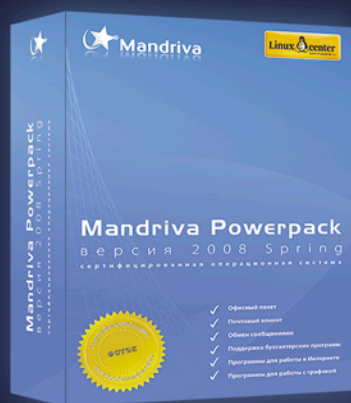
Mandriva Powerpack 2008 Spring — надежное решение для рабочей станции. Включает в себя офисный пакет OpenOffice.org: текстовый редактор, электронные таблицы, редактор презентаций, конструктор баз данных, почтовый клиент, браузер, другие интернет-приложения, графические редакторы, приложения для работы со звуком и видео, другое ПО для офисного компьютера.

### Мобильное рабочее место

Mandriva Flash — защищенное рабочее место для мобильных сотрудников. Mandriva Flash загружается и работает прямо с USB-накопителя. Mandriva Flash содержит необходимые офисные приложения и достаточно места для хранения ваших настроек и данных. Все, что нужно для загрузки защищенного рабочего места — это любой компьютер, поддерживающий загрузку с USB-носителя.

### Надежный сервер

Mandriva Corporate Server 4 Update 3 — надежное решение для сервера. На базе Mandriva Corporate Server можно создать: интернет-сервер, почтовый сервер, сервер баз данных, сервер приложений, сервер печати, и т.д.



\* Сертификат ФСТЭК по 5 классу для СВТ и 4 уровню контроля НДВ.

Сертифицированные ФСТЭК продукты рекомендуются к использованию в государственных организациях и организациях, обрабатывающих персональные данные граждан.

Приобрести сертифицированные ФСТЭК продукты вы можете в ГНУ/Линуксцентре.

[www.linuxcenter.ru](http://www.linuxcenter.ru) | Телефон в Москве: (499)271-49-55 | Телефон в Санкт-Петербурге: 8(812) 309-06-86

Реклама



# Защита данных с помощью Active Directory Rights Management Services



**Андрей Бирюков**

**Служба AD RMS была выпущена несколько лет назад, но до сих пор не получила широкого распространения. В этой статье я расскажу о функционале, архитектуре и возможностях данного программного продукта.**

## Постановка вопроса

Как известно, информация нуждается в защите. В основном защита является эшелонированной, то есть мы предотвращаем несанкционированный доступ к конфиденциальным данным на нескольких уровнях: на сетевом, закрывая доступ по различным портам и протоколам, на уровне приложений, запрещая пользователям доступ к определенным ресурсам, или с помощью шифрования. Применяем антивирусные системы, средства обнаружения и предотвращения вторжений.

С недавних пор определенное развитие получили технологии контроля подключаемых к сети устройств (Network Admission Control), которые по-

зволяют контролировать эти устройства на актуальность антивирусных баз, пакетов обновлений и других критически важных компонентов.

Не стоит забывать и об обеспечении безопасности на физическом уровне, ведь во многих учреждениях на проходной не то что ноутбук нельзя внести, но даже флеш-носители и КПК приходится сдавать.

Разнообразные средства защиты, описанные выше, способны при грамотной настройке свести к минимуму вероятность несанкционированного проникновения и последующей утечки конфиденциальных данных.

Но что делать, если злоумышленнику куда-то проникать не нужно по той

простой причине, что он сам является сотрудником организации и у него по долгу службы есть доступ ко всем корпоративным данным. Типичным «злоумышленником» является сотрудник, собравшийся сменить работу и решивший забрать с собой конфиденциальные документы. То есть данный сотрудник может без труда скопировать любой документ себе на флешку и передать, например, конкурентам, что может привести к серьезным экономическим последствиям для организации.

Решить проблему с помощью стандартных средств шифрования нельзя, так как сотрудник должен иметь доступ к данным документам. Запрет доступа к USB-порту тоже не являет-

ся полноценным решением, так как во многих компаниях USB-устройства используются для производственных нужд.

## Существующие решения

На данный момент существует ряд продуктов, предназначенных для решения проблемы. Однако я предлагаю рассмотреть средство, входящее в состав операционной системы Windows 2003/2008, не требующее каких-либо дополнительных финансовых затрат и позволяющее создавать системы защиты данных различного уровня сложности.

Промышленными решениями, предназначенными для предотвращения утечек данных, получившими распространение, являются Rights Management Services (RMS, служба управления правами) от Microsoft и Information Rights Management. Собственно, эти два продукта являются дополнением друг друга.

RMS представляет собой технологию защиты информации, которая используется с такими приложениями, как Microsoft Office 2003. RMS обеспечивает защиту данных от ее неправомерного использования независимо от того, где и как она используется: автономно, в закрытой брандмауэром сети или за пределами этой сети.

Служба управления правами на доступ к данным IRM расширяет возможности использования службы RMS в приложениях Microsoft Office 2003, а также в обозревателе Microsoft Internet Explorer. Служащие, работающие с информацией, теперь могут указывать тех, кому разрешено использовать документ. Также они могут определять действия, которые разрешено производить с документом. Например, они могут предоставить права на открытие, внесение изменений, печать, пересылку документа, а также на выполнение ряда других действий. Подробнее о работе связи RMS и IRM вы можете прочесть в статье [1].

## Подробнее об RMS

Теперь мы рассмотрим более детально службу RMS, а затем поговорим о нововведениях в Windows Server 2008.

RMS появилась в 2003 году в качестве службы, позволяющей предотвратить несанкционированное обращение к электронной информации в онлайн-режиме и автономном режиме. Основой технологии RMS является Extensible Rights Markup Language (XrML, расширяемый язык разметки прав доступа) версии 1.2.1. (К слову, в настоящее время доступна версия 2.0.) Разметка XrML позволяет серверному и клиентскому компонентам, которые работают совместно с приложениями RMS, обеспечивать проверку правомочности доступа и защиту документов, электронной почты и даже контента интернет-сайтов.

Служба RMS плотно интегрирована в Active Directory, поэтому перед началом проектирования внедрения необходимо продумать ряд вопросов. В частности, будет ли RMS работать только внутри организации или же будет взаимодействовать с другими компаниями-партнерами.

RMS позволяет указывать для каждого сервера по два URL: один для использования в корпоративной сети предприятия, другой – для предоставления услуг внешним пользователям через Интернет. Адрес URL для корпоративной сети указывается в момент установки, и изменить его потом достаточно сложно. Значение локатора URL для внешней сети, которое определяется после завершения установки, можно изменить в любое время.

Серверная часть RMS представляет собой веб-службу, использующую для работы Windows .NET Framework, она может взаимодействовать с любой версией Windows Server 2003; для работы требуется установить Microsoft IIS 6.0, ASP .NET и службу очередей сообщений Microsoft Message Queue Services (MSMQ).

Клиентский компонент RMS может выполняться на любой версии Windows, начиная с Windows 98 Second Edition; для коммуникаций с серверным компонентом RMS использует стандартные протоколы – HTTP и HTTPS (HTTP Secure), при этом коммуникации являются защищенными вне зависимости от того, используется HTTPS или HTTP.

Для работы сервера RMS требуется ADO-совместимая база данных, например, Microsoft SQL Server 2000 (жела-

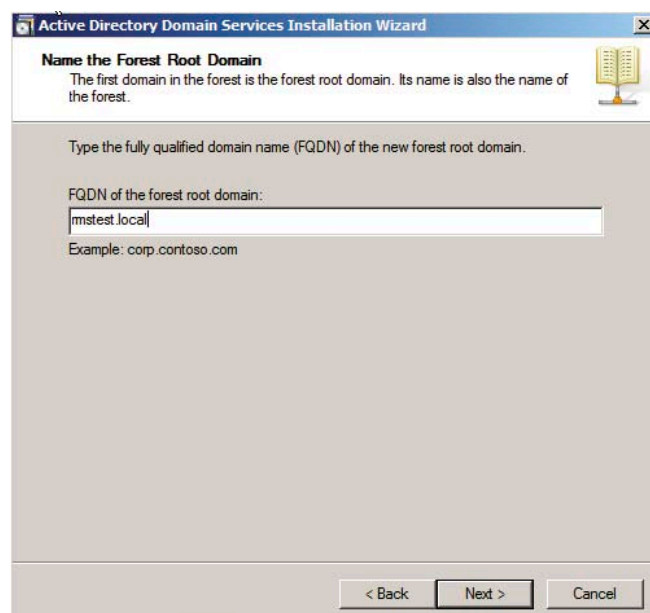


Рисунок 1. Создание домена Active Directory

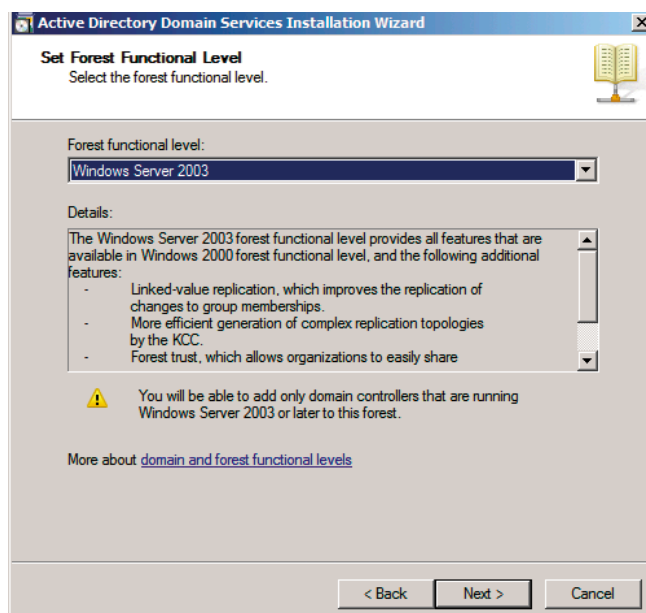


Рисунок 2. Функциональный уровень леса

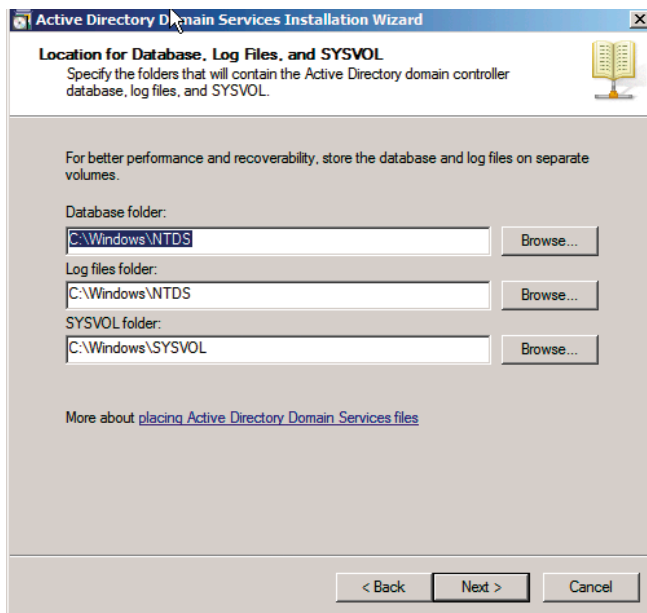


Рисунок 3. Пути к файлам Active Directory

тельно с пакетом обновлений SP3 или более новым). База данных служит для хранения конфигурации и журналов, а также для кэширования расширенных списков рассылки DL (distribution list). RMS и сервер баз данных должны принадлежать одному и тому же домену Active Directory.

Клиенты обращаются к серверу сертификации при активации и в момент получения RAC (Rights Management Account Certificate). При аутентификации пользователей сервер сертификации RMS обращается к серверу глобального каталога GC, к службе Microsoft Enrollment Service при развертывании и обновлении собственного сертификата издателя лицензий и к службе активации для клиентов RMS.

Таким образом, сервер RMS должен быть помещен в центральное, физически защищенное от доступа посторонних место и находиться в одном сетевом сегменте с сервером глобального каталога GC и сервером баз данных, имеющих хорошие соединения с клиентами по локальной сети и через Интернет. Специалисты Microsoft рекомендуют размещать службу RMS на отдельном сервере [3].

Посмотрим, что происходит при открытии защищенного RMS документа. При попытке открытия защищенного контента в RMS-приложении производится обращение к серверу RMS, указанному в лицензии публикации, для получения разрешения на использование этих данных. Далее приложение использует полученную лицензию для предоставления конкретному лицу возможности работать с контентом в соответствии с правами, описанными в лицензии на использование. Для ее получения необходимо сначала получить действующий сертификат учетной записи управления доступом XrML RAC (Rights Management Account Certificate). Этот сертификат выдает особый сервер сертификации RMS (RMS certification server) – впрочем, функции лицензирования и сертификации могут быть объединены на одном физическом сервере.

ре. Все действия по получению сертификата доступа RAC, если пользователь еще не имеет собственного сертификата, направляются RMS-приложением. Если на компьютере пользователя отсутствуют приложения, поддерживающие технологию RMS, можно установить модуль расширения RMA (Rights Management Add-on) для Internet Explorer. Эта бесплатная надстройка позволяет просматривать защищенный документ без возможности редактирования.

Из приведенного выше описания работы RMS очевидно, что, если организация планирует взять на вооружение RMS, до начала внедрения системы необходимо тщательно спланировать и проработать все аспекты использования технологии.

## RMS в Windows Server 2008: подготовка Active Directory

Прежде чем приступить непосредственно к установке Rights Management Service, необходимо подготовить доменную среду Active Directory. Так как в качестве рабочей операционной системы у нас используется Windows Server 2008, то я вкратце опишу развертывание контроллера домена Active Directory и создание необходимой для работы RMS учетной записи. Итак, в целом процесс развертывания Active Directory в Windows Server 2008 похож на аналогичный процесс в Windows Server 2003. Но есть и некоторые изменения.

Для запуска процесса установки можно воспользоваться командой `dsiproto`.

Далее выбираем создание нового домена в новом лесу. Указываем имя домена (см. **рис. 1**).

На следующем шаге нам необходимо указать функциональный уровень леса. Здесь необходимо выбрать уровень Windows 2003. Если в вашем каталоге Active Directory находятся только контроллеры домена под управлением Windows Server 2008, то вы можете указать уровень Windows 2008, однако тогда вы не сможете добавить в домен контроллеры под управлением Windows 2003 (см. **рис. 2**).

Далее указываем, где будут храниться файлы хранилища и журналы событий. Для тестового развертывания можно использовать пути по умолчанию. Однако для реальных промышленных систем рекомендуется под хранилище и log-файлы использовать разные диски (см. **рис. 3**).

На следующем шаге начинается непосредственно установка. По завершении установки вы получите соответствующее сообщение.

Теперь необходимо создать учетную запись для RMS. Для этого в Administrative Tools выбираем Active Directory Users And Computers. После этого Action → New → User (см. **рис. 4**).

При создании доменного пользователя для RMS необходимо учесть тот факт, что данная учетная запись должна отличаться от используемой для установки данной службы.

Что касается прав, необходимых данной учетной записи, то членства в группе Domain Users будет вполне достаточно.

Теперь все готово для установки службы RMS.

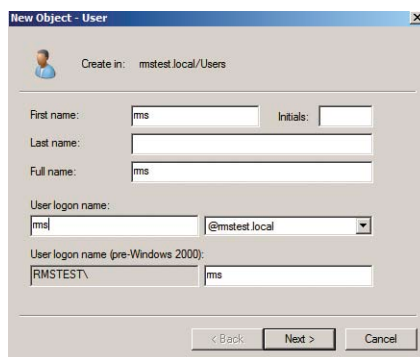


Рисунок 4. Создание пользователя RMS



## RMS в Windows Server 2008: установка и настройка

В отличие от предыдущих версий Windows Server, в 2008 компонента RMS интегрирована в операционную систему. Поэтому для установки RMS достаточно добавить серверную роль в окне Server Management в разделе Roles Summary (см. **рис. 5**).

Как видно, при выборе роли RMS автоматически указывается роль веб-сервера IIS. Как уже упоминалось ранее, данный компонент является необходимым для работы RMS. После выбора RMS на экран выводится полный список необходимых компонентов, которые должны быть установлены (см. **рис. 6**).

На следующем шаге нам необходимо выбрать, какие дополнительные компоненты RMS требуется установить. Как видно из **рис. 7**, выбор у нас невелик. Компонент Identity Federation Support необходим для взаимодействия со сторонними организациями. Сейчас он нам не потребуется, так что предлагаю оставить настройки по умолчанию.

После этого нужно определиться с хранилищем данных. В случае если вам не нужно разворачивать кластерную систему, будет вполне достаточно использования внутреннего хранилища RMS. Тогда все данные будут храниться на этом сервере. В случае если вам необходимо развернуть кластер RMS, содержащий несколько серверов, луч-

ше использовать внешнее хранилище. Для тестового разворачивания RMS нам будет вполне достаточно первого варианта (см. **рис. 8**).

На следующем шаге нам необходимо указать учетную запись, под которой будет работать RMS. Выбираем учетную запись, которую мы создали ранее (см. **рис. 9**).

Прежде чем мы пойдем далее, я хотел бы остановиться на одном странном сбое, который может проявиться на этом шаге установки RMS. После указания учетной записи и введения правильного пароля мы получаем сообщение о том, что пароль неправильный (The password could not be validated). Для решения данной проблемы необходимо включить пользователя, используемого для RMS (в нашем случае это пользователь rms), в группу Administrators. После этого установка продолжится без проблем. По окончании инсталляции RMS пользователя можно удалить из группы администраторов.

После этого нужно указать, как мы хотим хранить ключи, используемые для создания сертификатов. Можно использовать AD RMS-хранилище или же внешний криптографический провайдер (CSP). Будем использовать первый режим (см. **рис. 10**).

Теперь нам необходимо указать настройки веб-сервера RMS. Для соединения можно использовать http или https. Также нужно указать имя веб-сервера. (см. **рис. 11**).

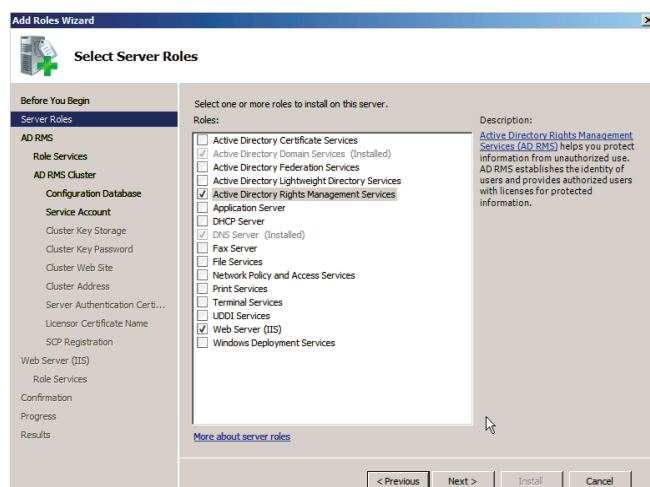


Рисунок 5. Добавление роли RMS

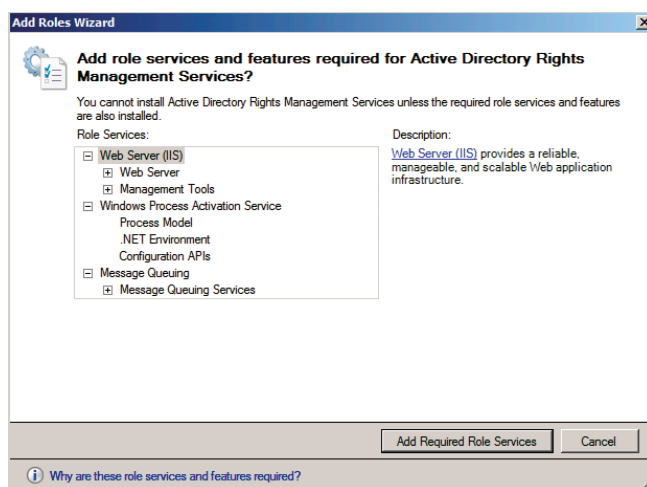


Рисунок 6. Компоненты, необходимые для работы RMS

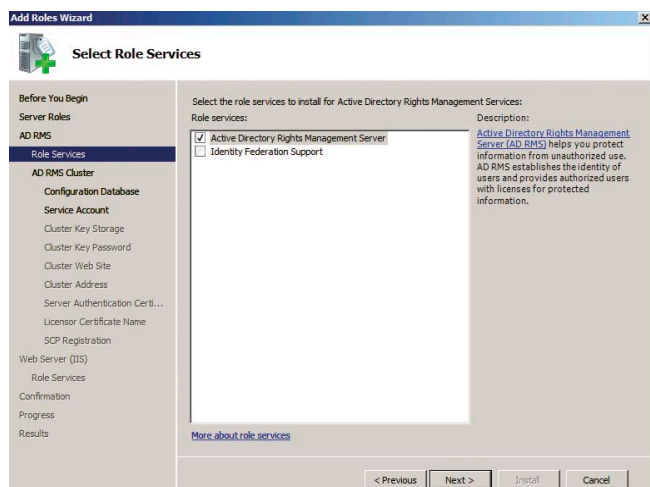


Рисунок 7. Компоненты RMS

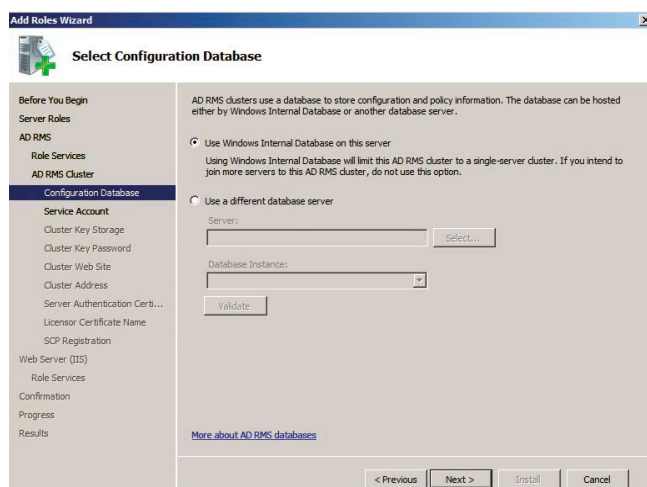


Рисунок 8. Выбор хранилища

После этого нам остается только подтвердить правильность указанных настроек для установки RMS и запустить процесс установки.

## Настройка RMS

Теперь проверим работоспособность компонентов RMS и произведем дополнительные настройки. Для этого в консоли Administrative Tools откройте Active Directory Rights Management Services (см. рис. 12). В административном интерфейсе присутствуют шесть основных разделов:

- Trusted Policies;
- Rights Policy Templates;
- Rights Account Certificate Policies;
- Exclusion Policies;
- Security Policies;
- Reports.

В Trusted Policies содержатся Trusted User Domains, в которых находятся списки пользователей из других доменов, которым доверяет данный сервер RMS. Также в этом разделе присутствует Trusted Publishing Domains, в котором приводятся списки доменов в других лесах, которым доверяет данный RMS. Для того чтобы добавить новые данные в каждый из этих разделов, можно воспользоваться средствами экспорта.

Раздел Rights Policy Templates содержит шаблоны, которые определяют Права пользователей для работы с теми или иными документами (Word, Excel). Здесь также можно указать, какое время должны действовать эти правила.

Следующий раздел – Rights Account Certificate Policies – определяет правила для сертификатов. В частности, здесь определяется срок, в течение которого сертификат может использоваться.

Exclusion Policies представляет собой политики для исключений. В частности, здесь можно определить исключения для приложений, к которым применяется RMS, также можно исключить определенных пользователей и версии операционной системы.

Политики Security Policies определяют, какие действия могут производить пользователи. Например, кто является суперпользователем, кто может изменять свой пароль на документы и т.д.

Раздел Reports предназначен для настройки отчетов, в которых содержится информация об учетных записях, использованных сертификатах, а также об использовании федеративных отношений.

## Клиентская часть RMS

Теперь поговорим о том, что должно быть установлено на клиентской рабочей станции для функционирования RMS. Клиент службы AD RMS входит в стандартную поставку ОС Windows Vista. Предыдущие версии этого клиента, предназначенные для других операционных систем семейства Windows, можно загрузить из Интернета. После этого для обеспечения доступности шаблонов политик прав необходимо провести дополнительную настройку рабочей станции клиента службы AD RMS. Для этого необходимо скопировать шаблоны политик прав службы AD RMS на клиентский компьютер и создать параметр реестра, указывающий на расположение этих шаблонов.

Клиент службы AD RMS сможет находить шаблоны политик прав службы AD RMS только после создания параметра реестра и локальной копии шаблонов. Для решения этих задач перед организацией защиты документа необходимо выполнить следующие изменения в реестре. Чтобы автоматизировать процесс, можно подготовить reg-файл для внесения изменений в следующий раздел реестра. В ветке HKEY\_CURRENT\_USER\Software\Microsoft\Office\12.0\Common\DRM необходимо добавить параметр AdminTemplatePath. В этом параметре нужно указать значение %UserProfile%\AppData\Microsoft\DRM\Templates, где %UserProfile% является псевдонимом пути C:\Users\<имя\_пользователя>. После этого убедитесь, что все папки, указанные в данном пути, существуют. Затем с сервера \имя\_сервера\_RMS\ADRMSTemplates необходимо скопировать в указанную выше папку созданные шаблоны политик.

## RMS в работе

В качестве примера создадим тестовый шаблон и проверим его работу на тестовой рабочей станции.

В консоли администрирования Active Directory Rights Management Services выберите запись LocalHost. В секции Tasks (задачи) области результатов выберите пункт Manage

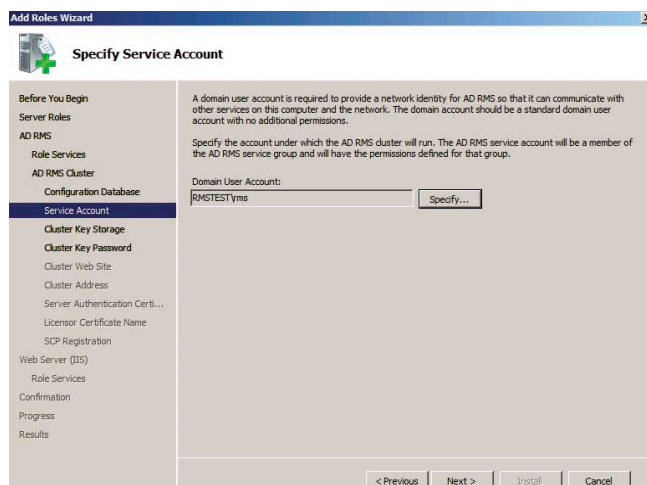


Рисунок 9. Выбор учетной записи

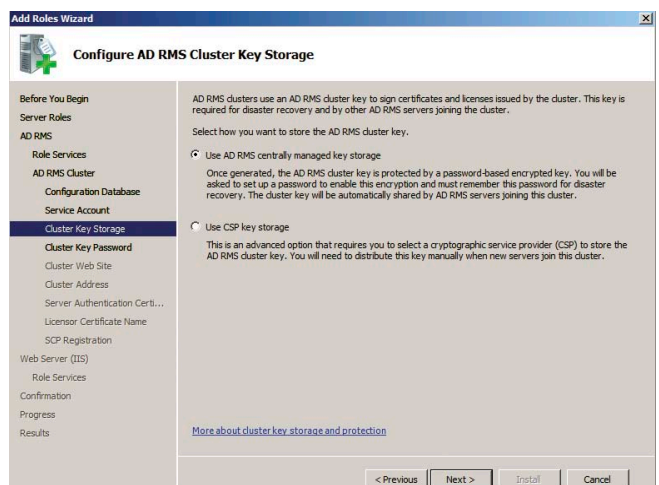


Рисунок 10. Хранилище ключей



2009  
www.infosecuritymoscow.com

infosecurity



RUSSIA

6-я международная  
специализированная  
выставка-конференция  
по информационной  
безопасности

**29 сентября – 1 октября 2009**  
**МОСКВА, Экспоцентр на Красной Пресне**  
**Павильон №7**

Одновременно  
на одной площадке  
с Infosecurity Russia:

**STORAGE  
EXPO**

**DOCUMENTATION**

## РАЗДЕЛЫ ВЫСТАВКИ

- Антиспам
- Антивирусы
- Безопасность приложений
- Биометрические системы
- Непрерывность бизнеса/ восстановление бизнеса после катастроф
- Соответствие требованиям регуляторов и стандартам
- Системы мониторинга и фильтрации контента
- E-mail безопасность / Безопасность средств оперативной пересылки сообщений или Безопасность мгновенного обмена сообщениями (систем типа ICQ)
- Шифрование, PKI (инфраструктура открытых ключей), Цифровые сертификаты
- Межсетевые экраны (брандмауэры)
- Управление идентификацией и доступом
- Безопасность Интернет/ сетевая безопасность
- Выявление и предупреждение вторжений
- Расследование компьютерных инцидентов
- Техническая поддержка/системы helpdesk
- Законодательство и стандарты/BS7799/Сертификация
- Сертификационные центры
- Управление внесением исправлений
- Тестирование безопасности системы путем имитации атак / Оценка риска и уязвимости
- Физическая безопасность
- Удаленный доступ
- Безопасность хранения данных
- Политика безопасности
- Маркеры доступа
- Обучение и повышение осведомленности в области безопасности
- Безопасность Веб-сервисов
- Система «Доступ за один шаг» (Single Sign-On)
- Смарт-карты
- Системы унифицированного управления защитой от угроз
- Безопасность IP телефонии
- VPN (виртуальные частные сети)
- Безопасность мобильных/беспроводных систем

ВЫСТАВОЧНОЕ ОБЪЕДИНЕНИЕ  
**РЕСТАЭК**™

 **Reed Exhibitions**®

**Дирекция выставки:**

Санкт-Петербург, Петрозаводская ул., д.12

Тел.: +7 (812) 320-8098, факс: +7 (812) 320-8090, E-mail: itcom@restec.ru

Реклама



rights policy templates (управление шаблонами политики прав). Для того чтобы разрешить экспорт шаблонов политик прав службы AD RMS, нажмите кнопку Properties в области Actions (действия). После этого необходимо установить флажок Enable export (разрешить экспорт), введите путь \\имя\_сервера\_RMS\ADRMSTemplates в поле Specify templates file location (расположение файла шаблонов (UNC)), после чего нажмите кнопку OK.

Чтобы открыть мастер создания распространяемых шаблонов политик прав, нажмите кнопку Create Distributed Rights Policy Template (создать распространяемый шаблон политики прав) в области Actions. Нажмите кнопку Add и выберите язык шаблона политики прав в списке Language (язык). Укажите название домена DOMAIN.COM CC в поле Name (имя). Введите строку DOMAIN.COM Company Confidential в поле Description (описание), после чего нажмите кнопку Add. Нажмите кнопку Next. Нажмите кнопку Add, введите почтовый адрес employees@domain.com в поле The e-mail address of a user or group (адрес электронной почты пользователя или группы), а затем нажмите кнопку OK.

Чтобы предоставить группе EMPLOYEES@DOMAIN.COM доступ на чтение ко всем документам, созданным с помощью данного шаблона политики прав службы AD RMS, установите флажок View. Нажмите кнопку Finish.

После этого нужно осуществить доступ на рабочую станцию под учетной записью пользователя. Далее запустить Microsoft Word, ввести в документе какой-либо текст. Далее нажмите кнопку Microsoft Office, выберите Finish, затем Restrict Permission (ограничить разрешение) и, наконец, Restrict Permission as (ограничить разрешение как). Указав адрес имя\_пользователя@domain.com в диалоговом окне Select User (выбор пользователя), нажмите кнопку OK. После открытия диалогового окна Permission установите флажок Restrict permission to this document (ограничить разрешения на работу с документом), выберите пункт Read и введите имя пользователя или группы, которой предполагается предоставить выбранный вид разрешения. В нашем случае следует ввести адрес имя\_пользователя@domain.com, а затем дважды нажать кнопку OK. После этого сохраните созданный файл.

Проверим защищенность нашего документа. Для этого необходимо зайти на ту же рабочую станцию под дру-

гой учетной записью и попытаться открыть созданный ранее документ. На экране появится следующее сообщение: «Permission to this document is currently restricted. Microsoft Office must connect to https://adrms-srv.domain.com/\_wmcs/licensing to verify your credentials and download your permission» («Разрешение на работу с данным документом ограничено. Microsoft Office необходимо подключиться к https://adrms-srv.domain.com:443/\_wmcs/licensing для проверки ваших учетных данных и загрузки сведений о ваших разрешениях»). Затем будет произведена проверка учетных данных. После этого документ откроется, печать будет недоступна. Если открыть View Permissions, то можно увидеть, что к данному документу применен шаблон политики RMS.

## Заключение

В этой статье я постарался подробно описать Active Directory Rights Management Services, основные функции и компоненты данной службы. Стоит отметить, с помощью RMS можно строить различные решения, позволяющие, к примеру, осуществить интеграцию с MS Exchange для контроля за распространением сообщений электронной почты. Также RMS имеет SDK, позволяющий дорабатывать данный продукт под свои нужды.

К сожалению, пока RMS по различным причинам не получил широкого распространения. Но стоит отметить, что проблема утечки информации и ее несанкционированного распространения инсайдерами становится все острее, и поэтому в будущем технологии, аналогичные RMS, получат более широкое распространение. ●

1. Защита информации с помощью служб RMS и IRM – [http://4win.ru/2006/11/24/zashhita\\_informacii\\_v\\_microsoft\\_office\\_2003\\_s\\_pomoshhju\\_sluzhb\\_rms\\_i\\_irm.html](http://4win.ru/2006/11/24/zashhita_informacii_v_microsoft_office_2003_s_pomoshhju_sluzhb_rms_i_irm.html).
2. Р. Моримото, Р. Ноэл. Microsoft Windows Server 2008. Полное руководство.
3. Описание службы RMS – [http://www.osp.ru/win2000/2006/03/1156376/\\_p1.html](http://www.osp.ru/win2000/2006/03/1156376/_p1.html).
4. AD RMS Step-by-Step Guide – <http://technet.microsoft.com/en-us/library/cc753531.aspx>.
5. Windows Server 2008. Пошаговое руководство по созданию и развертыванию шаблонов службы управления правами Active Directory.

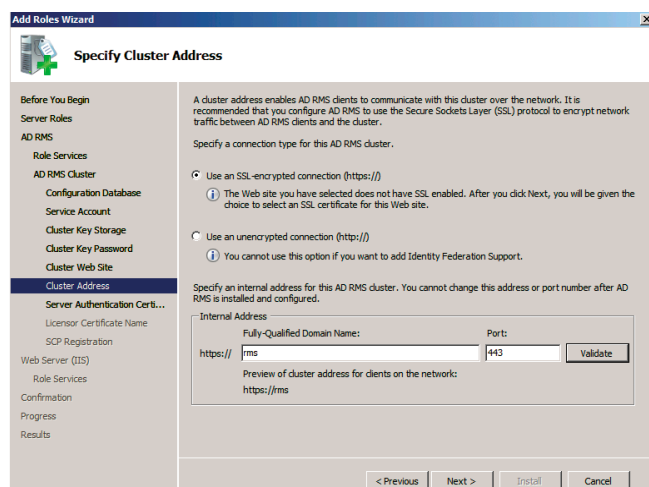


Рисунок 11. Настройки WEB для RMS

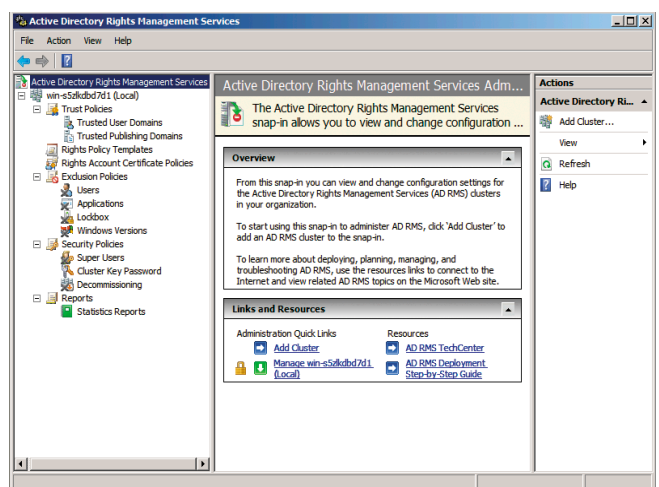


Рисунок 12. Интерфейс администрирования RMS

# «Доктор Веб» дал старт первому российскому антивирусу для Mac OS X

Долгие годы «маки» считались неуязвимыми для злоумышленников. Многие эксперты утверждали, что для Mac OS X и вовсе не существует каких-либо вирусных угроз. Безусловно, это стало поводом для некоторой беспечности пользователей данной операционной системы.

Тем не менее причины отсутствия на определенном этапе вредоносных программ, функционирующих в Mac OS X, заключаются, скорее, в низкой популярности этой системы, нежели в ее неприступности.

Киберпреступность ставит перед собой много разных целей. Однако неизменным остается одно – стремление заработать как можно больше денег. Чем больше сторонников ОС Windows, тем выгоднее создавать вредоносные программы, направленные против них. Однако число пользователей Mac OS X также с каждым годом растет, что вынуждает злоумышленников присмотреться к ней внимательнее. Первые вирусы под Mac OS X – черви Mac.Lear и Mac.Inqtana – появились в 2006 году. А в начале 2009 года, к примеру, много шума наделала троянская программа Mac.Iservice, заразившая компьютеры, впоследствии объединенные бот-сетью компьютеров-зомби iBot.

На сегодняшний день на рынке уже есть несколько зарубежных антивирусных продуктов для «маков». Однако российские разработчики до сих пор ничего аналогичного не предлагали.

Первый российский антивирус для Mac OS X появился в июне 2009 года. Создала его компания «Доктор Веб», известная своими передовыми решениями по обеспечению информационной безопасности как в корпоративном сегменте, так и среди домашних пользователей.

К разработке Dr.Web для Mac OS X специалисты «Доктор Веб» приступили еще в 2008 году. В декабре была представлена первая бета-версия продукта, весной 2009 года –

вторая, и наконец в середине июня 2009 года появился первый полноправный российский антивирус для Mac OS X.

## Каковы особенности данного продукта?

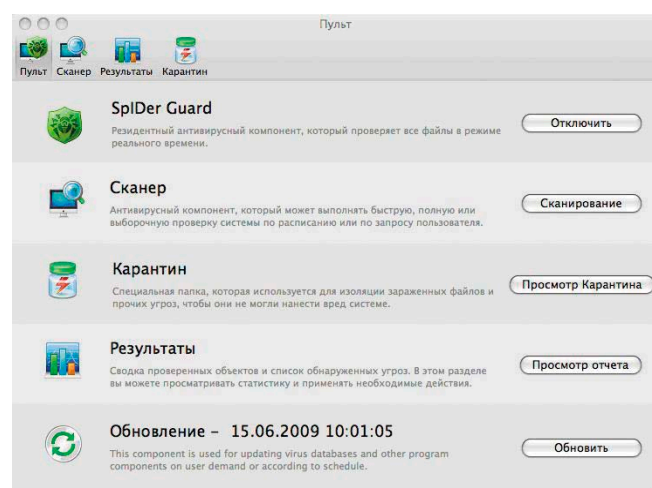
Прежде всего отличная скорость сканирования и минимальная нагрузка на систему, что делает Dr.Web для Mac OS X практически незаметным. Его русифицированный интерфейс полностью соответствует современному «мак»-дизайну, обеспечивая пользователям массу удобств.

В состав Dr.Web для Mac OS X входит сразу несколько важных компонентов. Прежде всего это сканер Dr.Web и монитор Spider Guard, который отвечает за многостороннюю проверку состояния защищаемой системы в режиме реального времени, здесь и сейчас.

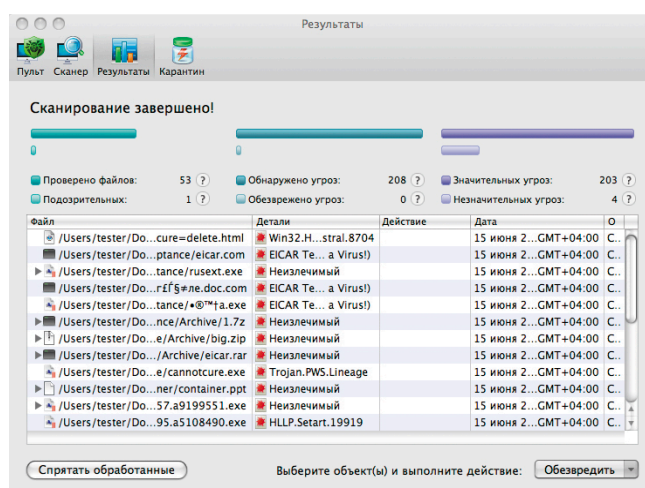
Чрезвычайно удобный управляемый карантин позволяет владельцу «мака» изолировать зараженные или подозрительные файлы, если он решил их не удалять при невозможности вылечить. Среди других важных компонентов Dr.Web для Mac OS X – утилита обновления, менеджер лицензий, а также планировщик.

Таким образом, Dr.Web для Mac OS X надежно защищает «мак» (с процессором Intel) от троянцев, шпионского и рекламного ПО, разнообразных хакерских утилит, программ-шуток. Что важно – написаны они могут быть не только для Mac OS, но и для других операционных систем. Тем не менее Dr.Web спасет вас даже в этой ситуации.

Валерий Ледовской



Dr.Web для Mac OS X



Результаты сканирования Dr.Web для Mac OS X

# ***Корпоративные VPN на базе Cisco***

В статье рассматривается несколько технологий построения VPN-туннеля: IPSec VPN Site-to-Site, Easy-VPN и DMVPN на базе маршрутизаторов Cisco. Преимущества и недостатки, топологии и конфигурации.



***Иван Панин***



## IPSec VPN Site-to-Site

Первый способ Site-to-Site или Intranet VPN представлен на **рис. 1**, используется для объединения в защищённую сеть нескольких распределённых филиалов одной организации, обменивающихся данными по открытым каналам связи. В основе решения лежит сеть VPN с предварительно настроенными в каждой точке входа в сеть туннелями для передачи защищаемого трафика. Таким образом, все политики доступа и параметры взаимодействия конфигурируются отдельно для каждого устройства доступа и каждой удаленной подсети.

В данном примере топология представляет собой звезду, маршрутизатор А расположен в центральном офисе компании, В и С – в дополнительных.

### Настройка RouterA

Создаем политику ISAKMP (Internet Security Association and Key Management Protocol) с приоритетом 1 (приоритет от 1 до 10000, 1 является самым высоким) и входим в режим конфигурации ISAKMP. Здесь устанавливаем общие параметры для установки туннеля. Указываем алгоритмы хэш-функции и шифрования.

Метод аутентификации. Определяем схему обмена ключами Диффи-Хеллмана [1] (group 2 – 1024 бита, Cisco IOS (Interwork Operating System) также поддерживает 1 и 5 группы) для протокола IKE (Internet Key Exchange). IP-адреса и крипто-ключи должны совпадать с соответствующими на удаленных маршрутизаторах. При смене ключа необходимо очистить крипто-сессию командой:

```
clear crypto session
```

Также здесь можно указать время жизни туннеля, команда «lifetime <60-86400>» в секундах.

```
crypto isakmp policy 1
 hash md5
 encryption 3des
 authentication pre-share
 group 2
 crypto isakmp key cisco123 address 172.16.2.1
 crypto isakmp key cisco124 address 172.16.3.1
```

Далее определяется список выполняемых операций (transform – изменений) для установки подлинности данных, конфиденциальности и сжатия. В нашем примере протокол шифрования сетевого трафика ESP (Encapsulation Security Payload) использует DES (Data Encryption Standard) и MD5 (Message Digest 5).

```
crypto ipsec transform-set rtpset esp-des esp-md5-hmac
```

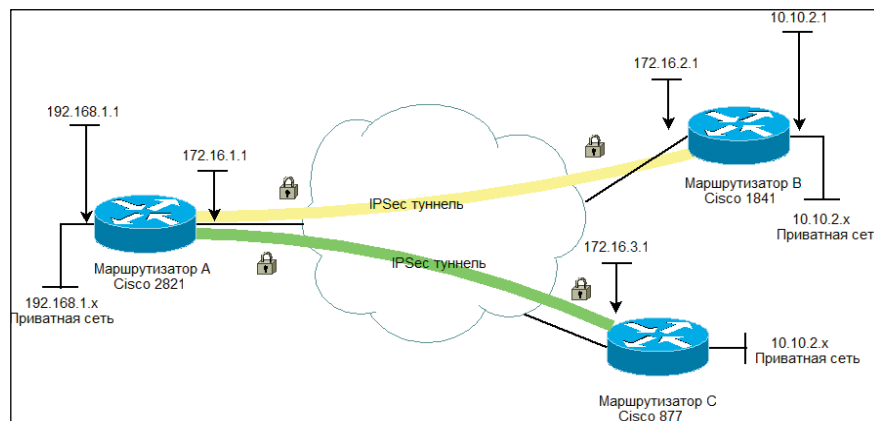


Рисунок 1. VPN Site-to-Site

Создаем расширенные списки контроля доступа acl (Access Control List) 102 и 103. В них указываем подсети, трафик между которыми будем шифровать.

```
access-list 102 permit ip 192.168.1.0 0.0.0.255 10.10.2.0 0.0.0.255
access-list 103 permit ip 192.168.1.0 0.0.0.255 10.10.3.0 0.0.0.255
```

Создаем крипто-карты для удаленных VPN-маршрутизаторов В и С. Указываем соответствующие IP-адреса, определенный ранее transform-set и списки доступа.

Здесь также можно задействовать классификацию качества обслуживания QoS (Quality of Service), до того как пакет попадет в туннель.

```
crypto map rtp 2 ipsec-isakmp
 set peer 172.16.2.1
 set transform-set rtpset
 match address 102
 crypto map rtp 3 ipsec-isakmp
 set peer 172.16.3.1
 set transform-set rtpset
 match address 103
 exit
```

Теперь назначаем внешнему интерфейсу созданную крипто-карту rtp. И указываем максимальный размер сегмента MSS (Maximum Segment Size) [2].

```
interface GigabitEthernet0/1
 ip address 172.16.1.1 255.255.255.0
 ip tcp adjust-mss 1400
 crypto map rtp
```

### Настройка RouterB

```
crypto isakmp policy 1
 hash md5
 encryption 3des
 authentication pre-share
 group 2
 crypto isakmp key cisco123 address 172.16.1.1

crypto ipsec transform-set rtpset esp-des esp-md5-hmac
```

## О технологии

VPN (Virtual Private Network – виртуальная частная сеть) – логическая сеть, создаваемая поверх другой сети, например Интернета. За счёт шифрования создаются закрытые каналы, позволяющие объединить территориально разрозненные подразделения организации, надомных и мобильных работников в единую сеть. Учитывая современный ритм бизнеса, VPN является незаменимой технологией.

```
access-list 101 permit ip 10.10.2.0 0.0.0.255 ┘
192.168.1.0 0.0.0.255

crypto map rtp 2 ipsec-isakmp
set peer 172.16.1.1
set transform-set rtpset
match address 101

fastEthernet0/1
ip address 172.16.2.1 255.255.255.0
ip tcp adjust-mss 1400
crypto map rtp
```

RouterC настраивается аналогично RouterB.

## Резюме

Наиболее распространенная технология, основанная на открытых стандартах, поддерживается наибольшим числом производителей оборудования и программного обеспечения. Идеальна для построения гетерогенных VPN-сетей.

Однако отсутствует возможность динамической маршрутизации между узлами сети (поддержка только IP-трафика) и установки соединения между отдельными узлами компании без участия центрального маршрутизатора. Отсутствует механизм автоматического переключения на резервный канал. Нет возможности назначить отдельную QoS-политику для каждого туннеля.

## EasyVPN

В основе решения стоит размещение всех параметров взаимодействия и политик безопасности на центральном сервере сети VPN (Easy VPN Server) [5], к которому подключаются удаленные устройства VPN – аппаратные (Easy VPN Remote) и программные (VPN Client) клиенты. Перед установкой зашифрованного соединения клиент сети Easy VPN проходит процедуру проверки подлинности с последующей загрузкой политик безопасности с сервера.

В случае использования VPN Client на удаленный компьютер устанавливается клиентское программное обеспечение Cisco VPN Client, на текущий момент доступна версия 5.x для Windows 2000/XP/Vista.

На рис. 2 представлена логическая схема подключения, при которой удаленный компьютер становится полноценным участником корпоративной сети.

Трафик от VPN Client, адресованный сети 192.168.1.x, направляется через туннель, а остальное движение может быть настроено по трем вариантам:

- через маршрутизатор A;
- напрямую через линк клиента;
- или вообще запрещен на время сеанса работы.

Авторизация клиента может быть настроена двумя способами: predeterminedный ключ Pre-Shared Keys (PSK) – набор символов, далее рассматривается в примере или по сертификату X.509: Public Key Infrastructure (PKI).

При реализации с небольшим числом дополнительных офисов можно выбрать PSK, однако когда их число растет, управлять индивидуальными PSK становится проблематично и лучше выбрать PKI.

## Настройка VPN Server (маршрутизатор A) для подключения EasyVPN Client

Задействуем модель аутентификации, авторизации и учета AAA (Authentication, Authorization, Accounting)<sup>[1]</sup>.

```
aaa new-model
aaa authentication login local
aaa authorization networkt authgroup local
```

Создаем политику с приоритетом 1, которая будет использоваться при подключении клиентов, и входим в режим конфигурации ISAKMP.

Определяем группу Diffie-Hellman, указываем алгоритмы хэш-функции и шифрования, а также пул динамического назначения IP-адресов<sup>[2]</sup>.

```
crypto isakmp policy 1
authentication pre-share
group 2
hash md5
encryption 3des
crypto isakmp client configuration address-pool ┘
local easy-vpn-group-dynpool
```

Создаем групповую политику IKE, содержащую атрибуты для удаленных клиентов. Указываем имя группы (логин), пароль, первичный сервер имен, домен, пул, маску сети, дополнительно можно указать WINS-сервер. А также разрешаем клиенту работу в его локальной сети на время работы VPN-туннеля.

```
crypto isakmp client configuration group authgroup
key easyvpnpassword
dns 192.168.1.254
```

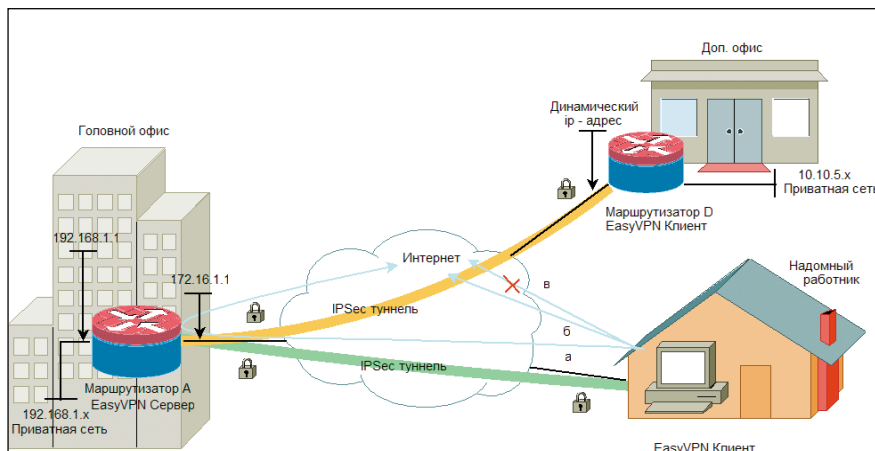


Рисунок 2. EasyVPN

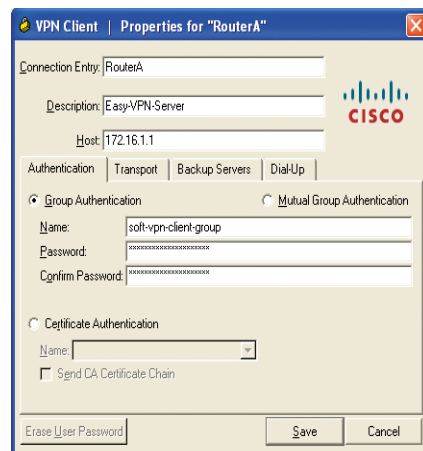


Рисунок 3. Настройки подключения

```
domain company.ru
pool easy-vpn-group-dynpool
include-local-lan
netmask 255.255.255.0
```

Далее определяется список выполняемых операций (transform – изменений) для установки подлинности данных, конфиденциальности и сжатия<sup>[3]</sup>.

```
crypto ipsec transform-set rtpset esp-des esp-md5-hmac
```

Создаем динамическую криптокарту rtp с порядковым номером 100, указываем transform-set и RRI (Reverse Route Injection) чтобы вещать маршруты на удаленные сети<sup>[3]</sup>.

```
crypto dynamic-map rtp 100
set transform-set rtpset
reverse-route
```

Применяем метод поиска ключей (IKE-запросы) для установления подлинности и разрешений группы. Настраиваем маршрутизатор для ответов на запросы удаленных клиентов<sup>[4]</sup>.

```
crypto map rtp isakmp authorization list authgroup
crypto map rtp client configuration address respond
```

Создаем профиль криптокарты:

```
crypto map rtp 100 ipsec-isakmp dynamic rtp
```

Ведение журнала подключений:

```
crypto logging session
```

Создаем пул адресов для группы VPN-клиентов:

```
ip local pool easy-vpn-group-dynpool 10.10.1.2 10.10.1.5
```

Список доступа для внешнего сетевого интерфейса. Открываем порты для VPN-клиентов: Authentication Header Protocol(AHP), ESP и UDP ISAKMP:

```
access-list 101 permit udp any host 172.16.1.1
eq non500-isakmp
access-list 101 permit udp any host 172.16.1.1 eq isakmp
access-list 101 permit esp any host 172.16.1.1
access-list 101 permit ahp any host 172.16.1.1
access-list 101 permit icmp any any echo
access-list 101 permit icmp any any echo-reply
access-list 101 deny ip any any log
```

Не забываем про инспектирование сессий:

```
ip inspect name FW isakmp
ip inspect name FW tcp
ip inspect name FW udp
ip inspect name FW icmp
```

Дополнительные протоколы выбираем, исходя из потребностей.

Конфигурирование сетевых интерфейсов: назначаем криптокарту (включить VPN-сервер), список доступа, входящий и исходящий интерфейсы для процесса трансляции сетевых адресов NAT.

```
interface GigabitEthernet0/1
ip address 172.16.1.1 255.255.255.0
ip access-group 101 in
ip nat outside
crypto map rtp
ip inspect FW out

interface GigabitEthernet0/0
ip address 192.168.1.1 255.255.255.0
ip nat inside
ip inspect FW in
exit
```

Исключаем VPN-трафик из процесса NAT между внутренней подсетью 192.168.1.0/24 и удаленной 10.10.1.0/24 (VPN-клиенты):

```
access-list 110 deny ip 192.168.1.0 0.0.0.255
10.10.1.0 0.0.0.255
access-list 110 permit ip 192.168.1.0 0.0.0.255 any

route-map ISP permit 10
match ip address 110

ip nat inside source route-map ISP interface gi0/1 overload
```

С чем пришлось столкнуться. За маршрутизатором А спрятан почтовый сервер, IP: 192.168.1.2. На внешнем DNS-сервере в записи «А» для mx-записи указан IP 172.16.1.1, а на внутреннем DNS указан 192.168.1.2. С внешнего интерфейса настроено перенаправление 25 порта.

```
ip nat inside source static tcp 192.168.1.2 25
172.16.1.1 25 extendable
```

Однако VPN-клиенты не могли отправлять почту через внутренний почтовый сервер.

В качестве решения можно использовать дополнительную карту маршрутизации для исключения трафика из процесса NAT, тем самым направить его через туннель.

```
access-list 111 deny tcp 10.10.1.0 0.0.0.255
host 192.168.1.2 eq smtp
access-list 111 permit tcp any host 172.16.1.1 eq smtp

route-map smtp-for-vpn permit 10
match ip address 111

ip nat inside source static tcp 192.168.1.2 25
172.16.1.1 25 route-map smtp-for-vpn extendable
```

## Настройка VPN Client

Программный VPN-клиент доступен для загрузки на веб-сайте компании Cisco Systems по адресу [4]. После установки в операционной системе автоматически будет создан виртуальный сетевой интерфейс, MTU установлено значение 1300. На **рис. 3** представлен интерфейс создания нового подключения.

После успешного соединения с VPN-сервером в трее появится «замок» (см. **рис. 4**).

Состояние текущих подключений можно посмотреть при помощи команды: «show crypto session», очистить текущие: «clear crypto session».



Рисунок 4.  
Соединение  
установлено

## Блок конфигурации VPN Server для подключения VPN Remote

Заделяем аутентификацию для локальных пользователей, авторизация групп – см. выше {1}.



```
aaa authentication login authuser local
```

Создаем пользователя для удаленного подключения:

```
username ezvpn privilege 0 password cisco120
```

Настройка политики isakmp выполнена выше {2}.

Настраиваем групповую политику для удаленного подключения. Задаем ключ и разрешаем клиенту сохранять пароль в конфигурации:

```
crypto isakmp client configuration group easy-vpn-conn
key cisco121
save-password
```

Набор преобразования для протоколов безопасности IPSec и динамическая карта созданы выше {3}.

Задействуем расширенную аутентификацию XAUTH (Extended Authentication) для криптокарты (имя и пароль пользователя cisco сохранили в конфигурации маршрутизатора VPN Remote):

```
crypto map rtp client authentication list authuser
```

Авторизация групп для криптокарты задействована ранее {4}.

По аналогии с VPN Client необходимо исключить VPN-трафик из процесса NAT и разрешить доступ на внешнем интерфейсе. В списки доступа 110 и 101 добавляем:

```
access-list 110 deny ip 192.168.1.0 0.0.0.255 ┘
10.10.5.0 0.0.0.255
access-list 101 permit ip 10.10.5.0 0.0.0.255 ┘
192.168.1.0 0.0.0.255
```

## Настройка VPN Remote

Указываем параметры подключения: автоматическое поднятие IPSec-туннеля, имя и ключ для соответствующей группы на VPN-сервере, IP-адрес сервера.

Расширенная аутентификация (Xauth) является дополнительной опцией, для включения которой на стороне сервера необходимо настроить криптокарту см. выше {4}. Аутентификация через Xauth может быть настроена в трех вариантах, интерактивная – через командную строку (CLI), веб-интерфейс и сохранение имени и пароля – в конфигурации, как показано ниже:

```
crypto ipsec client ezvpn easy-vpn-conn
connect auto
group ez-remote-group key cisco121
mode network-extension
peer 172.16.1.1
username cisco password cisco120
xauth userid mode local
```

Назначим конфигурацию Easy VPN внешнему интерфейсу:

```
interface vlan 1
ip address 172.16.1.4 255.255.255.0

crypto ipsec client ezvpn easy-vpn-conn
```

Определяем интерфейс, который получит доступ и будет доступен на VPN-сервере:

```
interface Vlan 2
ip address 10.10.5.1 255.255.255.0
crypto ipsec client ezvpn easy-vpn-conn inside
```

Также необходимо добавить маршрут для внутренней подсети за RouterA, на нем маршрут до подсети 10.10.5.0 создается автоматически при поднятии туннеля:

```
ip route 192.168.1.0 255.255.255.0 172.16.1.1
```

## Резюме

Объем настроек оборудования в удаленных офисах сводится к минимуму и состоит в подготовке универсального шаблона на конфигурации. В дальнейшем этот шаблон может быть легко тиражирован на все устройства сети VPN без ущерба для уровня безопасности. В случае программного VPN Client, кроме установки на ПК, затрат вообще никаких не требуется. Таким образом, технология Easy VPN значительно минимизирует затраты на сопровождение благодаря автоматической загрузке конфигураций и политик с центрального узла. Существует возможность переключения на резервный канал, статические политики QoS для каждого узла.

К недостаткам можно отнести: ограничения динамической маршрутизации и отсутствие поддержки мобильных устройств.

Альтернативой является Cisco AnyConnect Client – новое поколение VPN-клиента Cisco, работающего по протоколу SSL. Отличительной особенностью является возможность его автоматической загрузки на компьютер, который до этого не имел VPN-клиента, а также поддержка Windows Mobile версий 5.0 и 6.0. Однако полная поддержка данного клиента реализована лишь в Cisco Adaptive Security Appliances (ASA).

## Dynamic Multipoint VPN (DMVPN)

В основе технологии лежит механизм динамического установления соединений между узлами сети. Cisco DMVPN может быть развернут как совместно с системами безопасности Cisco IOS Firewall и Cisco IOS IPS, так и вместе с такими необходимыми в современных сетях механизмами, как QoS, IP Multicast, Split Tunneling. Используя возможности Cisco DMVPN, можно создавать крупные VPN-сети с десятками и сотнями узлов с возможностью балансировки загрузки каналов и резервирования.

В основе DMVPN [6] лежат несколько технологий:

- mGRE-туннели (Multiple Generic Routing Encapsulation);
- протокол NHRP [7] (Next Hop Resolution Protocol);
- протоколы динамической маршрутизации;
- профили IPsec (IPsec profiles).

На рис. 5 представлена Dual-DMVPN[8] топология с двумя центральными маршрутизаторами Hub 1 и 2, настроенными с одним mGRE-туннелем, а удаленные Spoke 1, 2 и 3 настроены с двумя mGRE-туннелями, подключенными к DMVPN-1 и 2 сетям (желтые облака).

NHRP – клиент-серверный протокол преобразования адресов, позволяющий всем хостам, которые находятся

в NBMA (Non Broadcast Multiple Access) сети, динамически найти физические адреса друг друга, обращаясь к next-hop серверу (NHS). После этого хосты могут обмениваться информацией напрямую.

### Алгоритм работы DMVPN

- Hub-маршрутизатор работает как NHS, а spoke-маршрутизаторы – клиенты.
- Hub-маршрутизатор хранит и обслуживает базу данных NHRP, в которой хранятся соответствия между физическими адресами и адресами mGRE-туннелей spoke-маршрутизаторов.
- На каждом spoke-маршрутизаторе, hub-маршрутизатор статически указан как NHS и задано соответствие между физическим адресом и адресом mGRE-туннеля hub-маршрутизатора.
- При включении каждый spoke-маршрутизатор регистрируется на NHS и при необходимости запрашивает у сервера информацию об адресах других spoke-маршрутизаторов для построения туннелей spoke-to-spoke.
- Для взаимодействия между собой все маршрутизаторы должны принадлежать одной сети NHRP, принадлежность к сети определяется идентификатором сети (network ID).
- По средствам протокола EIGRP (Enhanced Interior Gateway Routing Protocol) распространяется информация о маршрутах к внутренним подсетям за hub- и spoke-маршрутизаторами.
- При потере связи с активным NHS, spoke-клиент использует альтернативный туннель.

mGRE-туннель позволяет одному GRE-интерфейсу поддерживать несколько IPsec-туннелей и упрощает количество и сложность настроек по сравнению с GRE-туннелями точка-точка. Также mGRE-интерфейс позволяет использовать динамически назначенные IP-адреса на spoke-маршрутизаторах.

### Настройка DMVPN на Hub-1

- IP subnet: 10.10.1.0/24
- NHRP network ID: 100001
- Tunnel key: 100001
- Dynamic routing protocol: EIGRP

Создаем политику ISAKMP, указываем ключ и разрешаем аутентификацию с любого IP-адреса:

```
crypto isakmp policy 1
authentication pre-share
crypto isakmp key cisco119 address 0.0.0.0 0.0.0.0
```

Определяем список выполняемых операций (transform) для установки подлинности данных, конфиденциальности и сжатия. Возможны два варианта: туннельный режим – инкапсуляция и защита всей IP-дейтаграммы и транспортный режим – инкапсулирует или защищает только полезную часть, что делает его подверженным атакам, но более экономичным за счет отсутствия дополнительного IP-заголовка ~ 20 байт на пакет.

```
crypto IPsec transform-set rtpset esp-des esp-md5-hmac
mode transport
crypto IPsec profile vpnprof
set transform-set rtpset
```

Создание туннельного интерфейса:

```
interface Tunnel1
! Полоса пропускания 1000 Кбит
bandwidth 1000
ip address 10.10.1.1 255.255.255.0
! Так как GRE добавляет дополнительные заголовки к IP-пакету,
! необходимо изменить значение MTU[2] на интерфейсе
ip mtu 1400
no ip next-hop-self eigrp 1
! Включаем NHRP с указанием идентификатора сети
ip nhrp network-id 100001
! Аутентификации (опционально)
ip nhrp authentication cisco118
! Автоматическое добавление соответствия между адресами
! spoke-маршрутизаторов
ip nhrp map multicast dynamic
! NHRP NBA-адреса действительны в течении 10 минут
ip nhrp holdtime 600
no ip split-horizon eigrp 1
! Необходимо изменить значение MSS[2]
ip tcp adjust-mss 1360
! Задержка пропускной способности интерфейса
! (десятки микросекунд)
delay 1000
! Настройка соответствия между туннельным интерфейсом
! и физическим
! В качестве адреса отправителя в пакете выходящем
! из mGRE-интерфейса будет использоваться IP-адрес
! физического интерфейса, а адрес получателя будет
! выучен динамически с помощью протокола NHRP
tunnel source Vlan1
```

Включаем mGRE-туннель, задаем идентификатор, профиль IPsec:

```
tunnel mode gre multipoint
tunnel key 100001
tunnel protection IPsec profile vpnprof

interface Vlan1
ip address 172.16.1.1 255.255.255.0

interface Vlan2
ip address 192.168.1.1 255.255.255.0
```

Динамическая маршрутизация:

```
router eigrp 1
network 10.10.1.0 0.0.0.255
network 192.168.1.0 0.0.0.255
no auto-summary
```

### Настройка DMVPN на Hub-2

Конфигурация Hub-2 аналогична Hub-1, отличия лишь в DMVPN:

- IP subnet: 10.10.2.0/24
- NHRP network ID: 100002
- Tunnel key: 100002

### Настройка DMVPN на Spoke-1

```
crypto isakmp policy 1
authentication pre-share
crypto isakmp key cisco119 address 0.0.0.0 0.0.0.0

crypto IPsec transform-set rtpset esp-des esp-md5-hmac
mode transport

crypto IPsec profile vpnprof
set transform-set rtpset
```

```

interface Tunnel1
 bandwidth 1000
 ip address 10.10.1.101 255.255.255.0
 ip mtu 1400
 ip nhrp authentication cisco118
 ! Статическое соответствие между адресом mGRE-туннеля
 ! и физическим адресом hub-маршрутизатора
 ! (первый адрес- адрес туннельного интерфейса,
 ! второй – адрес внешнего физического интерфейса)
 ip nhrp map 10.10.1.1 172.16.1.1
 ! Адрес внешнего физического интерфейса hub-маршрутизатора
 ! указывается как получатель multicast-пакетов от локального
 ! маршрутизатора
 ip nhrp map multicast 172.16.1.1
 ip nhrp network-id 100001
 ip nhrp holdtime 300
 ! Адрес туннельного интерфейса hub-маршрутизатора
 ! указывается как next-hop-сервер
 ip nhrp nhs 10.10.1.1
 ip tcp adjust-mss 1360
 delay 1000
 tunnel source Vlan1
 tunnel mode gre multipoint
 tunnel key 100001
 tunnel protection IPsec profile vpnprof shared

interface Tunnel2
 bandwidth 1000
 ip address 10.10.2.101 255.255.255.0
 ip mtu 1400
 ip nhrp authentication cisco118
 ip nhrp map 10.10.2.1 172.16.1.2
 ip nhrp map multicast 172.16.1.2
 ip nhrp network-id 100002
 ip nhrp holdtime 300
 ip nhrp nhs 10.10.2.1
 ip tcp adjust-mss 1360
 delay 1000
 tunnel source Vlan1
 tunnel mode gre multipoint
 tunnel key 100002
 tunnel protection IPsec profile vpnprof shared

interface Vlan1
 !ip address dhcp hostname Spoke1
 ip address 172.16.1.101 255.255.255.0
interface Vlan2
 ip address 192.168.101.1 255.255.255.0

router eigrp 1
 network 10.10.1.0 0.0.0.255
 network 10.10.2.0 0.0.0.255
 network 192.168.101.0 0.0.0.255
 no auto-summary

```

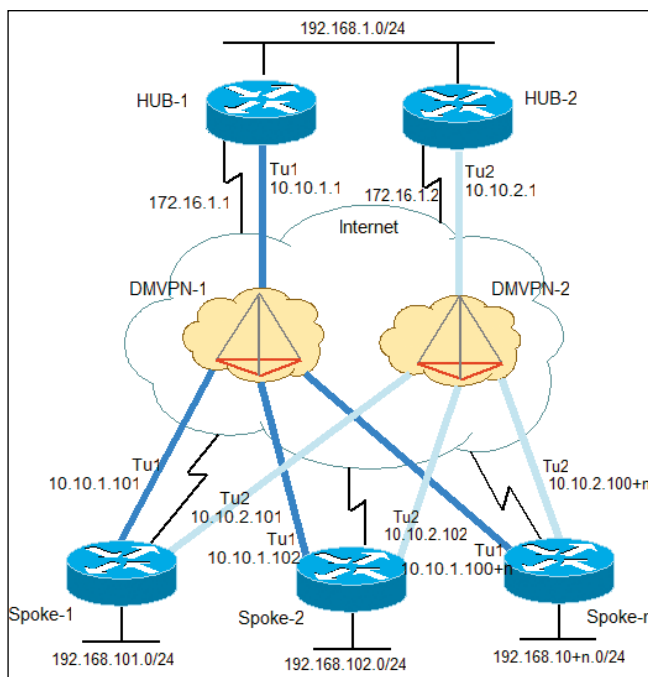


Рисунок 5. Dual-hub Router, Dual-DMVPN Topology

## Настройка DMVPN на Spoke-2, Spoke-n

Конфигурация аналогична Spoke-1, отличия лишь во внутренних IP-подсетях согласно рис. 5.

## Резюме

Сеть может быть построена как с использованием одного, так и нескольких центральных узлов для обеспечения резервирования устройств и каналов связи. Пересылка информации об IP-сетях осуществляется по зашифрованным туннелям между подразделениями компании при помощи протоколов динамической маршрутизации. Добавление нового узла в сеть VPN не требует изменений в конфигурации как соседних узлов сети VPN, так и центрального узла сети. Отдельные узлы смогут устанавливать соединения VPN между собой без участия центрального узла. Возможна реализация политик QoS с различным приоритетом для разных узлов сети.

Недостатком выступает отсутствие возможности назначить отдельную QoS-политику для каждого туннеля, альтернативными технологиями в данном случае являются Point-to-Point GRE over Ipsec [9] и Virtual Tunnel Interface (VTI) [9].

## Заключение

Рассмотренные способы настройки VPN применимы и вполне достаточны для большого числа современных компаний, однако в данной статье рассмотрены далеко не все технологии. Также на базе маршрутизаторов Cisco Systems могут быть реализованы такие технологии, как GRE VPN, MPLS VPN, VTI VPN и Web VPN, обладающие дополнительными преимуществами и недостатками, но это уже темы для следующих статей.

Перечень VPN-платформ на базе маршрутизаторов Cisco, поддерживающих рассмотренные технологии, доступен по адресу [9].

1. Алгоритм Диффи-Хеллмана – <http://ru.wikipedia.org/wiki/Diffie-Hellman>.
2. Resolve IP Fragmentation, MTU, MSS – [http://www.cisco.com/en/US/tech/tk827/tk369/technologies\\_white\\_paper09186a00800d6979.shtml](http://www.cisco.com/en/US/tech/tk827/tk369/technologies_white_paper09186a00800d6979.shtml).
3. Site-to-Site Tunnel Between IOS Routers – [http://www.cisco.com/en/US/tech/tk583/tk372/technologies\\_configuration\\_example09186a0080223a59.shtml](http://www.cisco.com/en/US/tech/tk583/tk372/technologies_configuration_example09186a0080223a59.shtml).
4. Software VPN Client – <http://www.cisco.com/kobayashi/sw-center/sw-vpn.shtml>.
5. Easy VPN – [http://www.cisco.com/en/US/products/sw/secursw/ps2308/products\\_configuration\\_example09186a008032b637.shtml](http://www.cisco.com/en/US/products/sw/secursw/ps2308/products_configuration_example09186a008032b637.shtml).
6. Dynamic Multipoint VPN – [http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN\\_and\\_MAN/DMVPN\\_1.html](http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/DMVPN_1.html).
7. Configuring NHRP – [http://www.cisco.com/en/US/docs/ios/ipaddr/configuration/guide/iad\\_cfg\\_nhrp\\_ps9587\\_TSD\\_Products\\_Configuration\\_Guide\\_Chapter.html](http://www.cisco.com/en/US/docs/ios/ipaddr/configuration/guide/iad_cfg_nhrp_ps9587_TSD_Products_Configuration_Guide_Chapter.html).
8. Sharing IPsec with Tunnel Protection – [http://www.cisco.com/en/US/docs/ios/security/configuration/guide/share\\_ipsec\\_w\\_tun\\_protect.html](http://www.cisco.com/en/US/docs/ios/security/configuration/guide/share_ipsec_w_tun_protect.html).
9. IPsec VPN WAN Design Overview – [http://www.cisco.com/application/pdf/en/us/guest/netso1/ns130/c649/ccmigration\\_09186a0080685ce6.pdf](http://www.cisco.com/application/pdf/en/us/guest/netso1/ns130/c649/ccmigration_09186a0080685ce6.pdf).



## Обход каталога в CiscoWorks

**Программа:** Cisco Unified Service Monitor версии 1.0, 1.1, 2.0 и 2.1; CiscoWorks QoS Policy Manager версии 4.0 и 4.1; CiscoWorks LAN Management Solution версии 2.5, 2.6, 3.0 и 3.1; Cisco Security Manager версии 3.0, 3.1 и 3.2; Cisco TelePresence Readiness Assessment Manager версия 1.0; CiscoWorks Voice Manager версии 3.0 и 3.1; CiscoWorks Health и Utilization Monitor версии 1.0 и 1.1; Cisco Unified Operations Manager версии 1.0, 1.1, 2.0 и 2.1; Cisco Unified Provisioning Manager версии 1.0, 1.1, 1.2 и 1.3.

**Опасность:** Средняя.

**Наличие эксплоита:** Нет.

**Описание:** Уязвимость существует из-за ошибки проверки входных данных в службе TFTP. Удаленный пользователь может с помощью символов обхода каталога загрузить и изменить произвольные файлы за пределами корневой директории TFTP-сервера.

**URL производителя:** [www.cisco.com](http://www.cisco.com).

**Решение:** Установите исправление cwcs3.x-win-CSCsx07107-0.zip с сайта производителя.

## Множественные уязвимости в IBM Tivoli Storage Manager Client

**Программа:** IBM Tivoli Storage Manager Client версии до 5.1.8.3, 5.2.5, 5.5.2, 5.3.6.6 и 5.4.2.7.

**Опасность:** Средняя.

**Наличие эксплоита:** Нет.

**Описание:** 1. Уязвимость существует из-за ошибки проверки границ данных при обработке строк в IBM Tivoli Storage Manager Agent Client (dsmagent.exe). Удаленный пользователь может с помощью специально сформированного пакета, содержащего строку более 1025 символов, вызвать переполнение стека и выполнить произвольный код на целевой системе.

2. Уязвимость существует из-за ошибки проверки границ данных при копировании NodeName из полученного пакета в IBM Tivoli Storage Manager Agent Client (dsmagent.exe). Удаленный пользователь может с помощью специально сформированного пакета, содержащего строку более 65 символов, вызвать переполнение стека и выполнить произвольный код на целевой системе.

3. Уязвимость существует из-за ошибки проверки границ данных в WebGUI-клиенте. Удаленный пользователь может вызвать переполнение буфера и выполнить произвольный код на целевой системе.

4. Уязвимость существует из-за неизвестной ошибки в Java GUI-клиенте. Удаленный пользователь может получить неавторизованный доступ к системе и просмотреть, изменить, скопировать и удалить произвольные файлы.

5. Уязвимость существует из-за неизвестной ошибки при использовании Secure Socket Layer (SSL) в клиентах для платформ AIX и Windows. Удаленный пользователь может произвести атаку человек посередине и просмотреть или скопировать файлы с клиентской системы.

**URL производителя:** [www.ibm.com](http://www.ibm.com).

**Решение:** Установите последнюю версию с сайта производителя.

## Обход ограничений безопасности в Apache

**Программа:** Apache 2.2.11 и более ранние версии.

**Опасность:** Низкая.

**Наличие эксплоита:** Нет.

**Описание:** Уязвимость существует из-за ошибки при обработке AllowOverride директив и некоторых Options-аргументов в .htaccess-файлах. Локальный пользователь может выполнить произвольные команды посредством Server Side Includes.

**URL производителя:** [www.apache.org](http://www.apache.org).

**Решение:** Установите исправление из SVN-репозитория производителя.

## Множественные уязвимости в IBM DB2

**Программа:** IBM DB2 версии до 9.1 Fixpak 7 и 9.5 Fixpak 4.

**Опасность:** Низкая.

**Наличие эксплоита:** Нет.

**Описание:** 1. Уязвимость существует из-за неизвестной ошибки при обработке IPv6-адресов в корреляционных токенах. Удаленный пользователь может аварийно завершить работу приложения.

2. Уязвимость существует из-за ошибки при использовании LDAP-аутентификации.

**URL производителя:** [www-306.ibm.com/software/data/db2/9](http://www-306.ibm.com/software/data/db2/9).

**Решение:** Установите последнюю версию 9.1 Fixpak 7 или 9.5 Fixpak 4 с сайта производителя.

## Обход ограничений безопасности в pam\_krb5

**Программа:** pam\_krb5 2.2.14 и более ранние версии.

**Опасность:** Низкая.

**Наличие эксплоита:** Нет.

**Описание:** Уязвимость существует из-за того, что приложение возвращает различные сообщения об ошибке в зависимости от корректности введенного имени пользователя. Удаленный пользователь может узнать имена учетных записей.

**URL производителя:** [fedorahosted.org/pam\\_krb5](http://fedorahosted.org/pam_krb5).

**Решение:** В настоящее время способов устранения уязвимости не существует.

## Уязвимость в NFSv4 в ядре Linux

**Программа:** Linux kernel 2.6.x.

**Опасность:** Низкая.

**Наличие эксплоита:** Нет.

**Описание:** Уязвимость существует из-за некорректной проверки привилегий MAY\_EXEC в функции nfs\_permission() в файле fs/nfs/dir.c. Злоумышленник может выполнить произвольные сценарии на NFSv4-разделе без надлежащих привилегий. Для успешной эксплуатации уязвимости сервер должен поддерживать atomic open.

**URL производителя:** [www.kernel.org](http://www.kernel.org).

**Решение:** В настоящее время способов устранения уязвимости не существует.

Составил Александр Антипов

## Отказ в обслуживании в Wireshark

**Программа:** Wireshark версии 0.8.20 по 1.0.7.

**Опасность:** Средняя.

**Наличие эксплоита:** Нет.

**Описание:** Уязвимость существует из-за ошибки в PCNFSD-диссекторе. Удаленный пользователь может с помощью специально сформированного PCNFSD-пакета аварийно завершить работу приложения.

**URL производителя:** [www.wireshark.org](http://www.wireshark.org).

**Решение:** Установите последнюю версию 1.0.8 с сайта производителя.

## Выполнение произвольного кода в HP OpenView Network Node Manager

**Программа:** HP OpenView Network Node Manager версии 7.01, 7.51 и 7.53.

**Опасность:** Средняя.

**Наличие эксплоита:** Нет.

**Описание:** Уязвимость существует из-за неизвестной ошибки, которая позволяет удаленному пользователю скомпрометировать целевую систему. Подробности уязвимости не сообщаются.

**URL производителя:** [www.openview.hp.com/products/nnm](http://www.openview.hp.com/products/nnm).

**Решение:** Установите исправление с сайта производителя.

## Уязвимости при конвертации CIFS-строк в ядре Linux

**Программа:** Linux kernel версии до 2.6.29.4.

**Опасность:** Низкая.

**Наличие эксплоита:** Нет.

**Описание:** Уязвимость существует из-за ошибок при конвертации строк. Удаленный пользователь может вызвать переполнение буфера и скомпрометировать целевую систему.

**URL производителя:** [www.kernel.org](http://www.kernel.org).

**Решение:** Установите исправление из GIT-репозитория производителя.

## Отказ в обслуживании в rpc.nisd в Sun Solaris

**Программа:** Sun Solaris 8, 9, 10.

**Опасность:** Низкая.

**Наличие эксплоита:** Нет.

**Описание:** Уязвимость существует из-за неизвестной ошибки в rpc.nisd. Удаленный пользователь может запретить серверу NIS+ отправлять ответы клиентам NIS+.

**URL производителя:** [www.sun.com](http://www.sun.com).

**Решение:** Установите исправление с сайта производителя.

## Отказ в обслуживании в fstat() в Sun Solaris

**Программа:** Sun Solaris 9.

**Опасность:** Низкая.

**Наличие эксплоита:** Нет.

**Описание:** Уязвимость существует из-за неизвестной ошибки в системном вызове fstat(). Локальный пользователь может вызвать панику ядра системы.

**URL производителя:** [www.sun.com](http://www.sun.com).

**Решение:** Установите исправление с сайта производителя.

## Обход ограничений безопасности в Sun Solaris

**Программа:** Sun Solaris 8, 9, 10.

**Опасность:** Низкая.

**Наличие эксплоита:** Нет.

**Описание:** Уязвимость существует из-за неизвестной ошибки в механизме управления сохраненными в кэше учетными данными Kerberos. Локальный пользователь может с помощью Kerberos без авторизации получить доступ к NFS-точкам монтирования.

**URL производителя:** [www.sun.com](http://www.sun.com).

**Решение:** Установите исправление с сайта производителя.

## Обход ограничений безопасности в FreeBSD

**Программа:** FreeBSD 6.3, 6.4, 7.1, 7.2.

**Опасность:** Низкая.

**Наличие эксплоита:** Нет.

**Описание:** Уязвимость существует из-за отсутствия проверки привилегий к SIOCSIFINFO\_IN6 IOCTL. Локальный пользователь может с помощью специально сформированного SIOCSIFINFO\_IN6 IOCTL-запроса изменить некоторые настройки IPv6-интерфейса или полностью отключить IPv6-интерфейс.

**URL производителя:** [www.freebsd.org](http://www.freebsd.org).

**Решение:** Установите исправление с сайта производителя.

## Повышение привилегий в IBM AIX

**Программа:** IBM AIX 5.3.0, 5.3.7, 5.3.8, 5.3.9, 6.1.0, 6.1.1 и 6.1.2.

**Опасность:** Низкая.

**Наличие эксплоита:** Нет.

**Описание:** Уязвимость существует из-за ошибки состояния операции в компоненте отладки MALLOCDEBUG в malloc-подсистеме в libc.a. Локальный пользователь может при выполнении setuid-приложений перезаписать произвольные файлы на системе и выполнить произвольный код с привилегиями учетной записи root.

**URL производителя:** [www.ibm.com](http://www.ibm.com).

**Решение:** Установите исправление с сайта производителя.

## Отказ в обслуживании в ядре Linux

**Программа:** Linux kernel версии до 2.6.29.4.

**Опасность:** Низкая.

**Наличие эксплоита:** Нет.

**Описание:** 1. Уязвимость существует из-за ошибки в реализации KVM. Локальный пользователь гостевой ОС может получить доступ к порту 80h основной системы и вызвать зависание основной ОС. Уязвимость распространяется на определенные AMD-платформы.

2. Уязвимость существует из-за ошибки блокировки в реализации системного вызова splice() в файле fs/ocfs2/file.c. Локальный пользователь может заблокировать другие приложения на системе.

**URL производителя:** [www.kernel.org](http://www.kernel.org).

**Решение:** Установите последнюю версию 2.6.29.4 с сайта производителя.

Составил Александр Антипов

# Очередное собрание ошибок

Прочитай и не делай так

Андрей Луконькин

## Непосредственное удаление

Чаще всего ошибка встречается в «самописных» (не типовых) конфигурациях. Несмотря на имеющуюся возможность, которую предлагает платформа, я бы рекомендовал отключать у пользователей права на непосредственное (интерактивное) удаление справочников и документов, даже у роли «Полные права». Не всегда пользователь точно знает, что удаляемый объект не связан ни с какими другими объектами базы данных (если не произведет поиск ссылок на объект). Поэтому в базе могут появляться некорректные записи, нарушающие целостность данных. Например, записи такого вида:

```
<Объект не найден> (103:ad3d0015176230fe11de4a92be828136)
```

**Важно!** Если у роли убраны также права «Удаление» и «Интерактивное удаление помеченных», то станет невозможным использование штатного механизма удаления помеченных объектов.

## Ошибочное указание в проводке счета, являющегося группой

Актуально для «1С:Предприятия 7.7». При описании проводок документа иногда ошибочно указывает не счет, а группу счетов, что не допустимо.

Например:

```
Операция.НоваяПроводка();
Операция.Дебет.Счет=СчетПоКоду("23");
Операция.Дебет.Затраты=Затраты;
Операция.Кредит.Счет=СчетПоКоду("10");
Операция.Кредит.Материалы=Материалы;
Операция.Кредит.МестаХранения=МестаХранения;
Операция.Количество=Количество;
Операция.Записать();
```

Здесь счет по кредиту задан 10-й (материалы). Правильно было бы указать счет, корреспондирующий со счетом, не являющимся группой – 10.1 или 10.6.

В «1С:Предприятие 8» ситуация с проводками несколько иная. У каждого счета есть признак «Запретить использовать в проводках», которым может управлять сам пользователь. Поэтому ограничением для использования счета в проводках является только данный признак.

## Ошибся – повтори ввод снова

Интересную ситуацию я обнаружил в вопросе пользователя на одном из форумов. Оказывается, не всегда платформа корректно обрабатывает ввод текста программы. Приведу конкретный пример.

```
Отбор = Новый Структура("Номенклатура", ЭлементНоменклатуры);
```

Видим явную ошибку, после оператора «Новый» по ошибке пропущен пробел. Казалось бы, куда уж проще вставить пробел. Но нет, добавление пробела не приводит к нужному результату! Получаем строку кода, написанную корректно с точки зрения синтаксиса, но платформа не воспринимает оператор «Новый» как зарезервированное слово.

```
Отбор = Новый Структура("Номенклатура", ЭлементНоменклатуры);
```

Синтаксический контроль выдаёт ошибку:

```
Отбор=Новый<<>>Структура("Номенклатура", ЭлементНоменклатуры);
```

Остаётся только удалить и набрать снова вручную «Новый», и только после этого получаем желаемый результат:

```
Отбор = Новый Структура("Номенклатура", ЭлементНоменклатуры);
```

## Платформа должна быть однообразной

Не раз я слышал фразы вроде «Да какая разница, какая платформа, ведь работает же!». В «1С:Предприятии 8» этот вопрос практически закрыт, т.к. отслеживаются версии платформы при подключении к одной базе данных. В «1С:Предприятии 7.7» иногда используют одновременно 25 и 27 релиз платформы. Чем это чревато?

В принципе сюрпризов можно ждать где угодно. Начиная от внезапного пропадания документов и заканчивая невозможностью использования отчетов, созданных на 27-й платформе, на клиентах с установленной 25-й платформой. Кроме того, различие платформ неблагоприятно сказывается при работе с распределенными базами данных:

```
DistUplErr 5 "SQL State: 23000 Native: 2601 Message:
[Microsoft] [ODBC SQL Server Driver] [SQL Server]
Невозможно вставить повторяющуюся ключевую строку в объект
"dbo.CJ5959" с уникальным индексом "ID".
SQL State: 01000 Native: 3621 Message:
[Microsoft] [ODBC SQL Server Driver] [SQL Server]
Выполнение данной инструкции было прервано.
```

Если вы не желаете видеть подобные ошибки, то не поленитесь, установите на всех компьютерах одинаковые платформы. 🍎



# Романтик

С Дмитрием Курашевым,  
совладельцем и CEO  
компании Entensys,  
приятно поговорить  
даже виртуально.



**К**огда общаешься с людьми по долгу службы, но при этом любишь свою профессию и находишь удовольствие в таком общении, начинаешь задумываться о философии коммуникации. Почему иногда после интервью с человеком обретаешь крылья, хочется летать и никакой усталости? Словно не работу выполнил, а с лучшим другом за чашкой чая посидел... А порой – наоборот. Недолгое общение, пустяковый комментарий «по поводу», а чувство – будто вагон с углем разгрузил (хотя и не знаю точно, что испытывают люди, разгрузившие вагон, но могу догадаться...). В просторечии «тяжелых» в общении людей называют «энергетическими вампирами». Самое интересное, что «кровушку» твою такой собеседник может выпить, даже общаясь с тобой виртуально, на форуме или по электронке... А может доставить интеллектуальную радость.

## Ключ к собеседнику

Задаю вопросы Дмитрию Курашеву дистанционно. Пишу письмо. Захожу в почту, прикрепляю файл... Кнопка «Отправить» – сообщение ушло. Принимаю ответное послание и... неожиданно с удовольствием читаю наш виртуальный диалог. Проскальзывает мысль, удивляющая меня своим самодовольством: «А кажется, неплохие вопросы задала... интересный получил разговор».

Ну восхищение собой быстро прошло: слава богу, я вспомнила высказывание одного французского философа-моралиста. Погодите, сейчас не поленюсь его вам процитировать, где-то была книжка... Вот – Жан де Лабрюйер: «Талантом собеседника отличается не тот, что охотно говорит сам, а тот, с кем охотно говорят другие; если после беседы с вами человек доволен собой и своим остроумием, значит, он вполне доволен и вами. Люди хотят не восхищаться, а нравиться, не столько жаждут узнать что-либо новое или даже посмеяться, сколько желают произвести хорошее впечатление и вызвать всеобщий восторг; поэтому самое утонченное удовольствие для истинно хорошего собеседника заключается в том, чтобы доставлять его другим». Вампиризмом и не пахнет...

Но любопытно другое – а сам Дмитрий любит общаться? Должность CEO в одной компании, то бишь «Фаматеке», теперь в другой – Entensys – предполагает, что с клиентами, партнерами, журналистами – приходится взаимодействовать часто и помногу.

– Вы получаете удовольствие от общения или просто «надо»?

– Как правило, да. Уверен, беседуя с любым человеком, можно найти интересную тему.

– Умение общаться, заключать договоры, налаживать долгосрочные отношения и дружить с пиар-агентствами и СМИ рождается после изучения психологии?

– Если говорить о пиар-агентствах, то дружба с ними возникает, прежде всего, при наличии денег. Это шутка, но...

«...очень близка к истине», – добавляю я мысленно.

– А если серьезно, то академическое изучение психологии уж точно не имеет ничего общего с успехами в бизнесе. Это не квантовая физика и не запуск баллистических ракет, так что глобальной научной основы нет и быть не может. Все на инстинктах.

Ну теперь понятно, откуда у Дмитрия интерес к изучению языков. Они – ключ к общению. Вот почему в арсенале Курашева и английский, и французский. Дмитрий подтверждает мою версию...

– Интерес к лингвистике у меня возник в 16 лет, когда я первый раз побывал за границей. Тогда, имея стандартное советское школьное языковое образование, я почувствовал себя жутко некомфортно – не мог выразить свои мысли. Сразу по приезде на Родину серьезно занялся английским языком, потом, когда надоело заниматься именно им, временно переключился на французский. Оказалось, это очень интересное занятие! Стал читать книги, новости и прочее. Лет пять не занимался французским, почти забыл, но потом посчастливилось вспомнить благодаря моей супруге. Она, кстати, знает французский лучше меня. Сейчас пытаюсь найти время освоить немецкий, надеюсь, это тоже удастся.

Даже не сомневаюсь, что нашему герою это удастся!

## Магия МГУ

У нас с Дмитрием нет почти ничего общего, кроме одного – мы выпускники Московского университета и, похоже, оба с удовольствием вспоминаем студенческую жизнь. Знаете, когда я захожу на «Одноклассниках» в группу «МГУ», всегда с удовольствием заглядываю на форум под названием «Самые счастливые моменты студенческой жизни», кажется, так он называется. У всех такая ностальгия... И всегда есть что вспомнить – хорошее!

«Ощущение счастья нескончаемого осталось от всего – все было счастьем. Но вот пение соловьев под утро на Воробьевых горах... а ты их после целой ночи трепа с друзьями в прокуренной комнате слушаешь... а потом подходишь к окну, и у твоих ног – вся Москва! (18-й этаж, окна на смотровую площадку – для неудачников с нижних этажей и с видом во двор поясню.) Вот это была романтика высокого полета!»

И еще, чтобы усилить впечатление: «Самых счастливых моментов просто не перечислить, потому что на эти годы пришлись и любовь, и замужество, и рождение первого ребенка – это из личного счастья. А еще был первый по порядку счастливый момент – поступление (приняли!), второй – удачные соседи по комнате (вот повезло с соседками!), много друзей всех мыслимых и немыслимых национальностей, отличный научный руководитель».

Ну и... погодите... там еще есть стихи...

*Ближе к расцвету сирени  
слаще тоска ожиданий,  
тоньше становятся тени,  
горше обвалы желаний.  
Выйдешь к Университету –  
город раскинется голый,  
ласковый и недопетый,  
выстраданный и новый...*

Не иронизируйте. Я не смеюсь... так, немного сентиментально улыбаюсь. Ввела вас в атмосферу? Вот и представьте, что такой ностальгией были проникнуты воспоминания о студенческих годах родителей Дмитрия Курашева, которые не только оба учились в МГУ, но и встретились там. Когда ощущаешь огромный университет точкой отсчета... собственной жизни, конечно, испытываешь к нему особые чувства. И конечно, нет выбора после

школы – куда идти учиться. Тем более что Дмитрий в школьные годы был победителем различных олимпиад по физике и математике, мог выбрать любой физико-математический вуз. Атмосфера студенческого городка оправдала ожидания...

А вообще-то выбор вуза, реалистично размышляет Курашев, «происходит в 16 лет, когда невозможно ясно представить, чем хочешь заниматься, какие есть устремления...». Элемент случайности присутствовал и когда школьник Дима выбирал профессию:

– Мое детство все-таки прошло во времена Советского Союза, когда не было слов «Интернет», «информационные технологии», «бизнес», когда никто не мыслил создание проектов вне государственной структуры. Так что я, как и многие мои сверстники, постепенно переключился с фундаментальной науки на информационные технологии».

Вот это самое «переключение» – уже достаточно осознанный этап, и выбор второго высшего – магистратуры экономического факультета – «был связан, естественно, с тем, чем я стал заниматься в своей взрослой жизни. Там я, кстати, встретил очень хороших людей, которые стали моими друзьями».

МГУ – альма-матер и Дмитрия Зноско, некогда партнера Дмитрия Курашева в фирме «Фаматек». Так что все же случайным выбор университета называть нельзя... Все ложится в «масть»...

О «Фаматеке» – разговор особый, правда, в прошедшем времени. Но опять-таки воспоминания приятные, потому что получалось почти все...

– Что подвигло на создание собственной компании «Фаматек»? Не пугало, что можете оказаться в финансовом проигрыше? Не проще было устроиться в какую-нибудь крупную фирму?

– Честно говоря, в финансовом проигрыше я никогда не оказывался. Так получилось, что дела пошли в гору очень быстро, так что дилеммы, зани-

маться ли своим делом или идти куда-либо работать, у меня практически никогда не было.

Компания действительно оказалась крепкой, а ее продукт – средство удаленного доступа Radmin (Remote Administrator) – востребованным. Это объяснять не надо...

– Она успешно продолжает свою деятельность и по сей день, но без меня. Я получил колоссальный опыт, ведь у нас получилось продвинуть Radmin буквально по всему миру. Было очень приятно осознавать, что удалось создать программный продукт, востребованный по всей планете. Мы экспортировали высокие технологии в чистом виде, не нефть или газ, а именно продукт интеллектуального творчества!

Гордость Дмитрия Курашева вполне понятна и очень даже оправдана. И тревога тоже:

– Меня очень беспокоит вопрос, почему у нас в стране при наличии мощных интеллектуальных традиций возникает так мало международно известных продуктов именно интеллектуального творчества.

– Что вы хотели бы изменить в этой сфере, чтобы ИТ развивались в правильном направлении?

– Прежде всего хотелось бы, чтобы влияние России в ИТ было не меньше, чем в шахматах или фигурном катании. Главная проблема, на мой взгляд, – это наш разрыв между разработкой технологий и их внедрением, бизнесом. В России много программистов, но мы пока не являемся центром ИТ-технологий.

## Новая жизнь в Городке

С января этого года у Дмитрия Курашева началась новая жизнь, о которой было объявлено во всеуслышание и на сайте «Фаматека», и по всему Интернету ИТ-сообществу. Он продал свою долю в «Фаматеке» партнеру Дмитрию Зноско (при этом моих коллег, конечно, весьма интересовало, сколько «зеленых» составила сделка)

и «продолжил свою карьеру в качестве совладельца и CEO компании Entensys, занимающейся разработкой популярного прокси-сервера UserGate».

Конечно, мой вопрос Дмитрию: что дал ему этот переход, почему отошел от собственного дела? У меня, честно говоря, есть свой ответ. Но об этом позже...

– От собственного дела я ни в коем случае не отошел. Просто мне хотелось развить именно Большой проект. А компания Entensys, на мой взгляд, несет в себе огромный потенциал. Мы стараемся развивать разработки, технологии и создать реально крупный и значимый проект. С моим будущим партнером Сашей Левченко я познакомился в 2004 году. Спустя какое-то время я в первый раз приехал в офис в Академгородке Новосибирска, где разрабатывался наш основной продукт – UserGate Proxy & Firewall. Несмотря на то что тогда это был маленький офис и маленькая компания, я был просто очарован атмосферой, средой и обстановкой. Сразу возникла уверенность в потенциале проекта, перспективе и возникло желание способствовать развитию проекта. Сейчас компания выросла до 35 человек, разработка ведется уже по нескольким направлениям – разрабатывается UserGate Mail Server, альтернатива MS Exchange для малого и среднего бизнеса, создается продукт для предотвращения утечек конфиденциальной информации. Кроме того, за последние три года UserGate стал мощным средством, позволяющим обеспечивать полный контроль доступа в Интернет, управление трафиком, а также сетевую безопасность.

О технологиях, разработках и новом партнере – это все вполне искренне. Но я улавливаю даже в виртуальном монологе Дмитрия нотки восхищения средой общения, обстановкой Академгородка. И думаю: не это ли главный фактор? Ведь новосибирский Академгородок – уникальное место. Когда

**RUSONYX**  
лучший VPS хостинг  
для системных администраторов!

WWW.RUSONYX.RU/SAMAG  
+7 (495) 799-00-18

**20%**  
скидка  
читателям  
журнала



он возник, его заселили удивительные люди – ученые, романтики, энтузиасты. Их воспоминания можно найти в сети, в книгах. Просто не могу удержаться, чтобы не процитировать Людмилу Прокуруину, которая была старшеклассницей, когда в 1959 году ее семья переехала в Академгородок из Новосибирска: «Первые годы в Городке даже милиции не было, пьяных не видели никогда. В основном население составляли научные сотрудники, приехавшие из Москвы, Ленинграда, Киева, Минска, высококвалифицированные рабочие, инженеры и учащаяся молодежь. Двери не запирались, велосипед можно было прислонить к дереву около дома, никто не боялся, что его украдут... Всех контролеров и продавцов знали по имени, некоторых я и сейчас встречаю на улицах Городка».

Сейчас, конечно, времена другие и многое изменилось, но, собственно, перемены лишь материальные – не хватает жилья, обветшала материальная база... Человеческие отношения остались во многом прежние – доверие друг к другу, дружелюбие, стремление к самосовершенствованию, но не в одиночку, а в компании таких же, как ты, людей. И вот это все Дмитрию Курашеву, по-моему, очень близко. Ведь его фраза: «Я стараюсь постоянно учиться, развиваться» – это не для красного словца, это принципиальная жизненная позиция.

Здесь, в новосибирском Академгородке, ему будет комфортно и трудиться...

– На мой взгляд, главное – это понимание того, как работает компания, как используются продукты, как действуют партнеры. Очень важно вникать во все это и постоянно думать о том, что можно улучшить.

...и отдыхать:

– Настоящий отдых получается, когда на время забываешь о долгосрочных планах. Можно путешествовать, кататься на лыжах, играть в футбол, теннис, делать что-то еще – главное, чтобы это нравилось, и все.

Нестоличный ритм жизни этому способствует...

Ну и, конечно, найдется больше времени для семьи. Жена и дочка Анечка для Дмитрия Курашева – особая тема. Мне всегда интересно, как в семье, особенно такой, где есть ма-



ленький ребенок и где папа очень занят на работе, распределяются обязанности, какие проблемы возникают. Но, получается, проблем-то и нет.

– Семейная жизнь вдохновляет и стимулирует на дальнейшие свершения. Я не могу представить себе жизни без детей, без той радости, которую они дают, без осознания преемственности, которое возникает вместе с ними. Бытовые проблемы для настоящего мужчины не должны являться препятствиями. Что касается распределения обязанностей – на мой взгляд, не так важно, кто конкретно чем занимается. Главное, что детей должны воспитывать оба, и мама и папа, а все бытовые вопросы всегда можно решить. Моя супруга, кстати, кроме домашних дел и воспитания ребенка, занимается собственным проектом в сфере не подвижности, а также учится.

– Сколько лет вашей дочке? У вас есть какие-то особые взгляды на воспитание ребенка? Собираетесь отдать ее в музыкальную, художественную школу?..

– Дочке почти полтора года. Она еще очень маленькая, но уже вызывает отцовскую гордость своим развитием, энергией и дружелюбием. Думаю, взгляды на воспитание еще будут складываться, но главное – это развитие личности, воспитание лучших качеств, которые заложены природой. Буду рад, если дочка захочет заниматься спортом, теннисом, фигурным катанием.

Наверное, именно таким и должно быть гармоничное развитие наследницы идей и «высокой романтики».

Оксана Родионова,  
фото из архива  
Дмитрия Курашева

## Друзья!

В этом году нашему журналу исполняется семь лет. Благодаря Вашей поддержке это были интересные и незабываемые годы. Мы старались быть Вам полезными и надеемся, что нам это нередко удавалось. С каждым годом тираж «Системного администратора» заметно увеличивался. Росли Вы, а мы росли вместе с Вами. Пора двигаться дальше, покорять иные вершины. Но чтобы мы по-прежнему хорошо понимали друг друга, давайте сверим часы перед новой дорогой.

Просим Вас ответить на вопросы нашей анкеты. Нам очень важно узнать мнение каждого читателя – ведь мы работаем для Вас! Заполнить электронную версию анкеты Вы можете на сайте журнала [www.samag.ru](http://www.samag.ru).

**1. Какова, на Ваш взгляд, главная функция журнала «Системный администратор» (расставьте по местам в соответствии с важностью: 1 – самая важная, 9 – самая неважная):**

- ☐ обзор актуальных тенденций ИТ-рынка,
- ☐ анализ самых острых проблем индустрии ИТ,
- ☐ знакомство с новейшими решениями в области ИТ, применяемыми в России и за рубежом,
- ☐ рассказ о лучших системных администраторах и программистах,
- ☐ интервью с CIO известных компаний на актуальные темы, связанные с развитием компьютерных технологий,
- ☐ опыт ведущих компаний – наиболее значимые наработки и достижения в разных направлениях ИТ-рынка,
- ☐ кейсы успешных проектов,
- ☐ все важно – обойдемся без приоритетов,
- ☐ другая функция (пожалуйста, сформулируйте):

- ☐ Программирование.
- ☐ WEB.
- ☐ Тенденции.
- ☐ Документация.
- ☐ Интервью.
- ☐ Человек номера.
- ☐ Ретроспектива.
- ☐ BUGTRAQ.
- ☐ Хобби.
- ☐ Книжная полка.

**2. Кого бы Вы хотели видеть в качестве наших авторов (нужное отметить):**

- ☐ Представителей властных структур (федерального и регионального уровней).
- ☐ CIO.
- ☐ Руководителей ИТ-компаний и ИТ-департаментов в компаниях.
- ☐ Российских аналитиков и консультантов.
- ☐ Зарубежных экспертов и консультантов.
- ☐ Представителей науки.
- ☐ Самого себя.

**3. Пожалуйста, сформулируйте свои варианты главной «проблемы номера». Какие проблемы отрасли кажутся вам наиболее актуальными?**

**4. Какие рубрики в журнале Вас интересуют больше всего?**

- ☐ Администрирование.
- ☐ Безопасность.
- ☐ Сети.
- ☐ Программирование.
- ☐ WEB.
- ☐ Тенденции.
- ☐ Документация.
- ☐ Интервью.
- ☐ Человек номера.
- ☐ Ретроспектива.
- ☐ BUGTRAQ.
- ☐ Хобби.
- ☐ Книжная полка.

**5. Какие рубрики Вы считаете ненужными (если такие есть)?**

- ☐ Администрирование.
- ☐ Безопасность.
- ☐ Сети.

**6. Какие материалы в нашем журнале Вам хотелось бы читать чаще?**

- ☐ Обзоры (новых технологий, программных продуктов, другое).
- ☐ Сравнение (новых технологий, программных продуктов, другое).
- ☐ Оригинальный опыт решения задач администрирования.
- ☐ Тонкие настройки сервисов и серверов.
- ☐ Готовые решения в настройке программных продуктов.
- ☐ Аналитические статьи.
- ☐ Статьи по безопасности.
- ☐ Материалы по базам данных.
- ☐ Различные how-to, FAQ, tips.
- ☐ Творчество сисадмина.
- ☐ Ретроспектива.
- ☐ Собственные материалы.

**7. Какие новые рубрики Вы бы хотели увидеть в журнале?**

**8. Какие темы, на Ваш взгляд, освещаются пока недостаточно?**

**9. От каких тем, на Ваш взгляд, следует отказаться?**

**10. Ваши любимые авторы в журнале?**

**11. Как давно Вы читаете журнал?**

- ☐ Все номера, начиная с пилотного.
- ☐ Более 3-х лет.
- ☐ 1-2 года.
- ☐ Меньше года.
- ☐ Прочитал анкету и узнал.

**12. Как Вы узнали о журнале?**

- ☐ Увидел на выставке (укажите, какой):
- ☐ От друзей/коллег.
- ☐ Из листовки в коробке дистрибутива ALT Linux/ASPLinux (укажите дистрибутив):

☐ Из прессы (укажите издание):

☐ Из анонсов Linuxcenter.ru, Nixp.ru, Opennet.ru, Securitylab.ru, Sysadmins.ru / увидел ссылку на сайте (укажите сайт):

☐ Прочитал анкету и узнал.

**13. Используете ли Вы какие-либо советы и рекомендации из журнала?**

- ☐ Да, часто. ☐ Нет.  
☐ Да, иногда. ☐ Я и сам могу давать советы.

**14. Оцените журнал по пятибалльной шкале:**

- а) Информативность:  
 б) Актуальность:  
 в) Полезность:  
 г) Интересность:  
 д) Оформление:  
 е) Популярность:  
 ж) Доступность:

**15. Сколько коллег (в среднем) читают Ваш экземпляр «Системного администратора»?**

- ☐ Только я.  
☐ 1-3.  
☐ 4-5.  
☐ Да все, кому он попадется.

**16. Собираетесь ли Вы оформить подписку на следующее полугодие?**

- ☐ Да.  
☐ Нет.  
☐ Уже оформил.

**17. Укажите Вашу профессию/должность:**

---

**18. Сколько лет работаете (работали) системным администратором:**

---

**19. Ваше образование:**

- ☐ Среднее.  
☐ Среднее специальное.  
☐ Неоконченное высшее.  
☐ Высшее.  
☐ Два и более высших.

**20. Сколько системных администраторов в вашем ИТ-отделе:**

---

**21. Численность компьютерного парка Вашей организации:**

- ☐ 10 и менее. ☐ 501-1000.  
☐ 11-50. ☐ 1001-2000.  
☐ 51-100. ☐ Более 2000.  
☐ 101-500.

**22. Численность серверного парка Вашей организации:**

- ☐ 1-2. ☐ 21-50.  
☐ 3-10. ☐ Более 50.  
☐ 11-20.

**23. С какими операционными системами Вы работаете?**

- ☐ Windows.  
☐ Linux.  
☐ FreeBSD.  
☐ OpenBSD.  
☐ Solaris.  
☐ Netware.  
☐ Другие:

---

**24. Какие компьютерные издания Вы читаете?**

---

**25. Какие сайты, связанные с Вашей рабочей деятельностью, Вы посещаете?**

---

**26. Повышаете ли Вы свою квалификацию на различных семинарах, курсах?**

- ☐ Да, часто.  
☐ Да, иногда.  
☐ Нет.  
☐ Я сам преподаю.

**27. Какие профессиональные выставки посещаете?**

---

**28. Как Вы приобретаете журнал?**

- ☐ Оформляю подписку через компанию.  
☐ Подписываюсь самостоятельно.  
☐ Покупаю в интернет-магазинах.  
☐ Покупаю в розницу.  
☐ Беру у друзей.

**29. Довольны ли Вы работой службы доставки? (если Вы получаете журнал по подписке)**

- ☐ Да.  
☐ Нет.

**30. Укажите Ваш пол:**

- ☐ Мужской.  
☐ Женский.

**31. Укажите Ваш возраст:**

---

**32. В каком городе Вы живете?**

---

**33. Читаете ли Вы электронное приложение журнала?**

- ☐ Да, я на него подписан.  
☐ Да, я периодически его скачиваю.  
☐ Нет.

**34. Оцените электронное приложение по пятибалльной шкале:**

---

**35. Оставьте Ваши общие пожелания, рекомендации:**

---



# Редакционная подписка для физических лиц

- Вы можете оформить подписку только на **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.
- Журнал высылается почтой заказной бандеролью только после поступления денег на расчетный счет и **копии заполненного и оплаченного бланка, отправленной в редакцию по факсу: (495) 628-82-53 (доб. 120) или на электронный адрес: subscribe@samag.ru.**

<b>ИЗВЕЩЕНИЕ</b>	<div style="text-align: right; font-size: small;">Форма № ПД-4</div> <p> <b>ООО "С 13"</b>              ИНН 7708654814 / КПП 770801001              Р.сч. 40702810300080001868 К.сч. 30101810100000000787              ОАО «УРАЛСИБ» г. Москва БИК 044525787              Коды: по ОКПО 84027582, по ОКОПФ 65           </p> <hr style="border-top: 1px dashed black;"/> <p style="text-align: center;"><b>Вид платежа: Редакционная подписка на журнал "Системный администратор" за 2009 г.</b></p> <table border="1" style="width: 100%; text-align: center; font-size: x-small;"> <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>X</td><td>X</td><td>X</td><td>X</td><td>X</td><td>X</td><td>X</td><td>X</td><td>X</td><td>X</td><td>X</td><td>X</td></tr> </table> <p>Дата _____ Сумма платежа: <b>2400</b> руб. <b>00</b> 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 style="text-align: right;">Подпись _____</p>	01	02	03	04	05	06	07	08	09	10	11	12	X	X	X	X	X	X	X	X	X	X	X	X
01	02	03	04	05	06	07	08	09	10	11	12														
X	X	X	X	X	X	X	X	X	X	X	X														
Кассир _____																									
<b>КВИТАНЦИЯ</b>	<div style="text-align: right; font-size: small;">Форма № ПД-4</div> <p> <b>ООО "С 13"</b>              ИНН 7708654814 / КПП 770801001              Р.сч. 40702810300080001868 К.сч. 30101810100000000787              ОАО «УРАЛСИБ» г. Москва БИК 044525787              Коды: по ОКПО 84027582, по ОКОПФ 65           </p> <hr style="border-top: 1px dashed black;"/> <p style="text-align: center;"><b>Вид платежа: Редакционная подписка на журнал "Системный администратор" за 2009 г.</b></p> <table border="1" style="width: 100%; text-align: center; font-size: x-small;"> <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>X</td><td>X</td><td>X</td><td>X</td><td>X</td><td>X</td><td>X</td><td>X</td><td>X</td><td>X</td><td>X</td><td>X</td></tr> </table> <p>Дата _____ Сумма платежа: <b>2400</b> руб. <b>00</b> 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 style="text-align: right;">Подпись _____</p>	01	02	03	04	05	06	07	08	09	10	11	12	X	X	X	X	X	X	X	X	X	X	X	X
01	02	03	04	05	06	07	08	09	10	11	12														
X	X	X	X	X	X	X	X	X	X	X	X														
Кассир _____																									

## Российская Федерация

- Подписной индекс: годовой – **20780**, полугодовой – **81655**  
Каталог агентства «Роспечать»
- Подписной индекс: годовой – **88099**, полугодовой – **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 администратор

Стои-мость	по каталогу	руб.	коп.	Количество комплектов:
	за доставку	руб.	коп.	

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\*

+ диск с архивом статей 2008 года

# 81655\*\*

без диска

по каталогу агентства «Роспечать»

# 88099\*

+ диск с архивом статей 2008 года

# 87836\*\*

без диска

по каталогу агентства «Пресса России»

\* Годовой  
\*\* Полугодовой  
\*\*\* Диск вкладывается в февральский номер журнала, распространяется только на территории России

**УЧРЕДИТЕЛИ**

Частные лица

**РЕДАКЦИЯ**

Генеральный директор

Владимир Положевец

Ответственный секретарь

Наталья Хвостова

sekretar@samag.ru

Технический редактор

Владимир Лукин

Главный редактор

электронного приложения

«Open Source»

Дмитрий Шурупов

osa@samag.ru

**Внештатные редакторы**

Алексей Барабанов

Александр Емельянов

Кирилл Сухов

Алексей Бережной

Андрей Бешков

Андрей Бирюков

Олег Щербаков

**РЕКЛАМНАЯ СЛУЖБА**

тел./факс: (495) 628-8253 (доб. 120)

Дарья Зуморина

reclama@samag.ru

Евгения Тарабина

expro@samag.ru

**Верстка и оформление**

maker@samag.ru

**Дизайн обложки**

Дмитрий Репин

**По вопросам распространения  
обращайтесь по телефону:**

Светлана Зобова

(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**

ООО «С 13»

**Отпечатано типографией**

ООО «Периодика»

Тираж 17000 экз.

Тираж электронной версии 62000 экз.

Журнал зарегистрирован в Министерстве РФ  
по делам печати, телерадиовещания и средств  
массовых коммуникаций (свидетельство ПИ  
№ 77-12542 от 24 апреля 2002 г.).

За содержание статьи ответственность несет  
автор. Мнение редакции может не совпадать  
с мнением автора. За содержание рекламных  
материалов ответственность несет рекламо-  
датель. Все права на опубликованные мате-  
риалы защищены.



Вы знаете, как бороться  
с «Просачивающейся Адварью»?  
Применяете «Чарующий скрипт»?

Редакция журнала «Системный администратор» представляет  
вам новый админский сувенир для истинных знатоков своего дела –  
карточную игру «**АУТСОРСЕР**».

В ходе игры участники тянут из колоды карты «Проблем», с которыми  
им предстоит бороться один на один или с помощниками, используя  
подручные средства. Успешное решение «Проблемы» добавляет игроку  
уровни. Если вы не считаете себя добрым и милым, то для вас в игре  
предусмотрена специальная возможность – сделать гадость другому  
участнику и обойти его в потоне за уровнями.

Победителем становится тот, кто быстрее всех  
доберется до 10 уровня. Остальные подробности об игре,  
«Чарующем скрипте», «МегаУтилите» и «Клановом коктейле»  
вы сможете узнать из правил игры.

«**АУТСОРСЕР**» – это пародия на жизнь, которая позволит вам  
ошутить всю прелесть аутсорсинга... но без всей словесной мишуры,  
типа, «утром стулья, вечером деньги...»!

Приобретайте игру «**АУТСОРСЕР**» в редакции.

