Так видит журнал читатель, который забыл оформить подписку:

НОВОГОДНИЕ КАНИКУЛЫ ЗАТЯНУЛИСЬ

БЫСТРО РАСКУПИЛИ ТИРАЖ

УЕХАЛ В ОТПУСК

ПОСЛЕ ОТПУСКА АВРАЛ НА РАБОТЕ

НЕОЖИДАННО ЗАКОНЧИЛИСЬ ДЕНЬГИ

Так видит журнал читатель, оформивший подписку:

ПОДПИШИТЕСЬ И ЧИТАЙТЕ!

Роспечать – 20780, 81655

Пресса России – 88099, 87836

Интер-почта – тел. (495) 500-00-60

системный администратор

№5(78) май 2009 подписной индекс 20780 www.samag.ru

№5(78) май 2009 системный администратор

ISSN 1813-5579

9 771813 557005 09005

OCS Inventory NG и GLPI: проводим учет оборудования

Устанавливаем Windows XP с помощью SCCM 2007 R2

Доступный WiMAX

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

Настраиваем хранение логов в базе данных MySQL

PowerShell: поиск объектов в каталоге Active Directory

Работаем с FTP-сервером из «1С»

Портал в стиле Web 2.0

Python: сложные аспекты

Sun Tech Days 2009: кризис не помеха

Ф.СП-1

Министерство связи РФ

АБОНЕМЕНТ на журнал ______ (индекс издания)

Системный администратор

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.; за доставку ______руб.______коп.

Количество комплектов: ______

на 200 год по месяцам

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

Куда (почтовый индекс)

Кому (адрес)

(фамилия, инициалы)

ИЗВЕЩЕНИЕ

Форма № ПД-4

ООО "С 13"
ИНН 7708654814 / КПП 770801001
Р. сч. 40702810300080001868 К. сч. 30101810100000000787
ОАО «УРАЛСИБ» г. Москва БИК 044525787
Коды: по ОКПО 84027582, по ОКОПФ 65

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

Форма № ПД-4

ООО "С 13"
ИНН 7708654814 / КПП 770801001
Р. сч. 40702810300080001868 К. сч. 30101810100000000787
ОАО «УРАЛСИБ» г. Москва БИК 044525787
Коды: по ОКПО 84027582, по ОКОПФ 65

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

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 рассказики 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 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!

Open Source разветвляется: Nagios – ICINGA, MySQL – ODA

На май пришлась точка кипения сообществ сразу двух известных Open Source-проектов: Nagios и MySQL. Энтузиасты настолько устали от давления со стороны главных коммерческих компаний, занимающихся развитием этих продуктов, что решили запустить альтернативные ветки.

Так, в начале мая у популярного средства мониторинга Nagios появилось ответвление ICINGA. Авторы форка объяснили причины появления нового проекта на сайте www.icinga.org. Если вкратце, то компания Nagios Enterprises LLC, обеспечивающая коммерческую поддержку Nagios, в последнее время стала всерьез докучать любым сторонним инициативам, действующим в отношении к Open Source-проекту Nagois. В частности это проявляется в постоянной медлительности в принятии патчей сообщества к базовому коду Nagios, а также в регулярных запретах использования названия Nagios и требованиях переименовывать сайты/проекты. В ICINGA намерены устранить эти проблемы, поддерживая классическую модель разработки приложения всем Open Source-сообществом. Авторы обещают полную совместимость с Nagios, а свой первый релиз – уже в конце мая. Первую стабильную версию ICINGA стоит ожидать 28 октября 2009 года.

А в середине месяца компании Monty Program Ab и Percona, специализирующиеся на СУБД MySQL, объявили о создании консорциума Open Database Alliance (ODA) для обеспечения независимой поддержки MySQL. Open Database Alliance намерен собрать вокруг себя компании, заинтересованные в дальнейшем развитии открытой СУБД и предоставлении различных услуг на ее базе. Что интересно, среди главных инициаторов ODA оказался Михаэль Видениус (Michael «Monty» Widenius) – автор оригинальной версии СУБД MySQL, покинувший Sun более полугода назад и ныне руководящий своей компанией Monty Program Ab. Последняя работает над MariaDB – ответвлением СУБД MySQL, использующим в качестве движка хранения Maria.

Вот как Видениус прокомментировал появление ODA: «Наша цель с Open Database Alliance – предоставить главный информационный центр для разработки MySQL, поддержать по-настоящему открытую экосистему разработки с непосредственным участием сообщества, обеспечить высокое качество кода MySQL. Участники альянса на данный момент будут обладать значительным голосом при решении вопросов о том, какой должна быть структура организации, и мы заинтересованы в сотрудничестве со всеми в индустрии, кто зависит от MySQL или работает над ней».

Сооснователем ODA стал Петр Зайцев (Peter Zaitsev) – наш соотечественник, являющийся исполнительным директором хорошо известной в сообществе MySQL компании Percona Inc.

В Open Source-телефонии очередные подвижки – с новым проектом oFono

Компании Intel и Nokia объявили о запуске нового Open Source-проекта, призванного разработать открытое решение, реализующее возможности телефонии, – oFono.

Аки Ниеми (Aki Niemi) из подразделения Maemo Software компании Nokia так анонсировал новый проект: «oFono.org – это место, которое соберет разработчиков для совместного проектирования инфраструктуры для создания приложений для мобильной телефонии (GSM/UMTS). Наработки oFono.org лицензированы под GPLv2 и включают высокоуровневый D-Bus API, который может использоваться телефонными приложениями, распространяемыми под любыми лицензиями. Кроме того, в oFono.org входит низкоуровневый подключаемый API для интеграции как с Open Source-, так и со сторонними телефонными стеками, сотовыми модемами и бэкендами хранения. Функциональность этого API основана на общедоступных стандартах – в частности, 3GPP TS 27.007 AT command set for User Equipment (UE)».

Поддержкой проекта занимаются Intel и Nokia – при этом компании приглашают всех заинтересованных разработчиков для присоединения к проекту. Исходный код наработок oFono доступен на ofono.org/downloads.

Незадолго до этого Intel уже совместно с Novell объявила о начале сотрудничества в области развития мобильной Linux-платформы Moblin и ее продвижения среди производителей аппаратного обеспечения (OEM). Одновременно Novell также анонсировала намерение разработать свой программный Linux-продукт на базе Moblin, ориентированный на использование на нетбуках.

Более того, в Novell собираются учредить лабораторию Open Labs в Тайване, которая будет сотрудничать с центром Taiwan Moblin Enabling Center (MEC) – совместной инициативой Intel и Тайваньского института информационной промышленности (Taiwan Institute for Information Industry). Заявляется, что в Novell Open Labs займутся «развитием адаптации» Moblin при содействии и участии MEC.

Linux.com обновился и стал социальным

Некоммерческая организация Linux Foundation, занимающаяся продвижением свободной операционной системы GNU/Linux, объявила о запуске новой версии сайта Linux.com.

Ресурс был создан в результате достигнутого в марте соглашения с SourceForge по дальнейшему развитию Linux.com под руководством Linux Foundation. Помимо традиционной информации вроде новостей, статей и документации на сайте представлена интересная особенность – система оценки знатоков Linux («Linux Guru Rankings»). По задумке авторов, такая система будет способствовать эффективному взаимодействию пользователей и разработчиков, которые будут обмениваться своими знаниями, накапливая баллы.

По итогам каждого года редакция Linux.com будет награждать главных знатоков. Так, первый гуру получит Linux-ноутбук, на котором поставит свой автограф создатель ядра Linux Линус Торвальдс (Linus Torvalds). Еще 5 лучших будут приглашены на Linux Foundation Collaboration Summit и займут почетные места «представителей сообщества» на собраниях по планированию развития Linux.com. Наконец, 50 лидеров попадут в ежегодно публикуемый Linux Foundation список главных знатоков.

Подготовил Дмитрий Шурупов по материалам www.nixp.ru

Sun Tech Days 2009: кризис не помеха

8-10 апреля в Санкт-Петербурге прошла очередная конференция Sun Tech Days.

В этом году традиционная встреча разработчиков, использующих технологии Sun Microsystems, проходила на Васильевском острове в павильонах выставочного центра «Ленэкспо».

Хотелось этого или нет, но фоном конференции был кризис и связанные с ним тревожные слухи о судьбе корпорации. Несмотря на это на самом мероприятии о тяжестях, переживаемых мировой экономикой, хотелось думать меньше всего – столько интересного было показано. К экономическим реалиям вернули только сами сотрудники Sun, но об этом позже.

Первый день начался пленарным докладом Джита Коула (Jeet Kaul), вице-президента подразделения клиентского программного обеспечения (Client Software Group). Джит много говорил о приверженности Sun открытым технологиям и о причинах этой приверженности. Были озвучены достижения корпорации в таких направлениях, как OpenSolaris, VirtualBox, MySQL, GlassFish и других. Не были обойдены стороной средства разработки – NetBeans и SunStudio, а также концепция Cloud Computing.

Большое внимание в пленарном докладе было посвящено Rich Internet Applications и вообще клиентским технологиям, в первую очередь платформе JavaFX. Рассказ сопровождался эффектными демонстрациями, из которых наиболее запомнилось применение технологии Sun SPOT в проекте «Сенсомоторный интерфейс управления пользователя».

После пленарного доклада пришлось буквально разрываться – разумеется, присутствовать на всех докладах и пресс-конференциях я не смог, посему обо всех последующих событиях рассказываю не в хронологическом порядке, а по основным темам конференции.

Кризис и социальная ответственность

Работе корпорации и её технологических партнёров в условиях непростого состояния моровой экономики была посвящена существенная часть первой пресс-конференции.

По словам Джита Кола, понимание того, что условия могут измениться, пришло ещё три-четыре года назад, и тогда же были предприняты шаги для работы. В первую очередь это развитие многоядерных вычислительных систем, открытых систем хранения данных, инвестиции в новые, перспективные технологии. Всё это дало свои результаты – к кризису Sun подошли с некоторым заделом. Как объяснил Джит, деньги можно зарабатывать различными путями, и если тот сегмент бизнеса корпорации, который опирался на традиционные технологии, разработанные десятилетие назад, сейчас и в самом деле испытывает заметный спад, то сегмент новых технологий вполне продолжает развиваться.

Боб Поррас (Bob Porras), вице-президент подразделения Solaris Data, Availabiliy, Scalability и HPC, заявил, что одним из важных последствий кризиса стало ускорение перехода ряда ведущих компаний на открытые платформы, на программное обеспечение с открытым исходным кодом. Поэтому компания Sun твердо намерена воспользоваться кризисом к своей выгоде, опираясь на стратегию продвижения открытого ПО.

Григорий Лабзовский, директор Санкт-Петербургского центра разработки программного обеспечения, заявил, что компания намерена активно заниматься продвижением идеи открытого ПО на всех уровнях, и это сейчас особенно актуально с учетом того, что правительство с недавних пор прониклось идеей Open Source. Sun уже вступила в недавно созданную Российскую ассоциацию свободного программного обеспечения (РАСПО) и активно взаимодействует с Минкомсвязи по вопросам внедрения открытого ПО.

Последней инициативой Sun в этой области в России стал состоявшийся 7 апреля 2009 года ввод в эксплуатацию переданного в дар физическому факультету Санкт-Петербургского государственного университета (СПбГУ) вычислительного комплекса, включающего счетный кластер и учебный класс на 20 рабочих станций Sun Ultra 24.

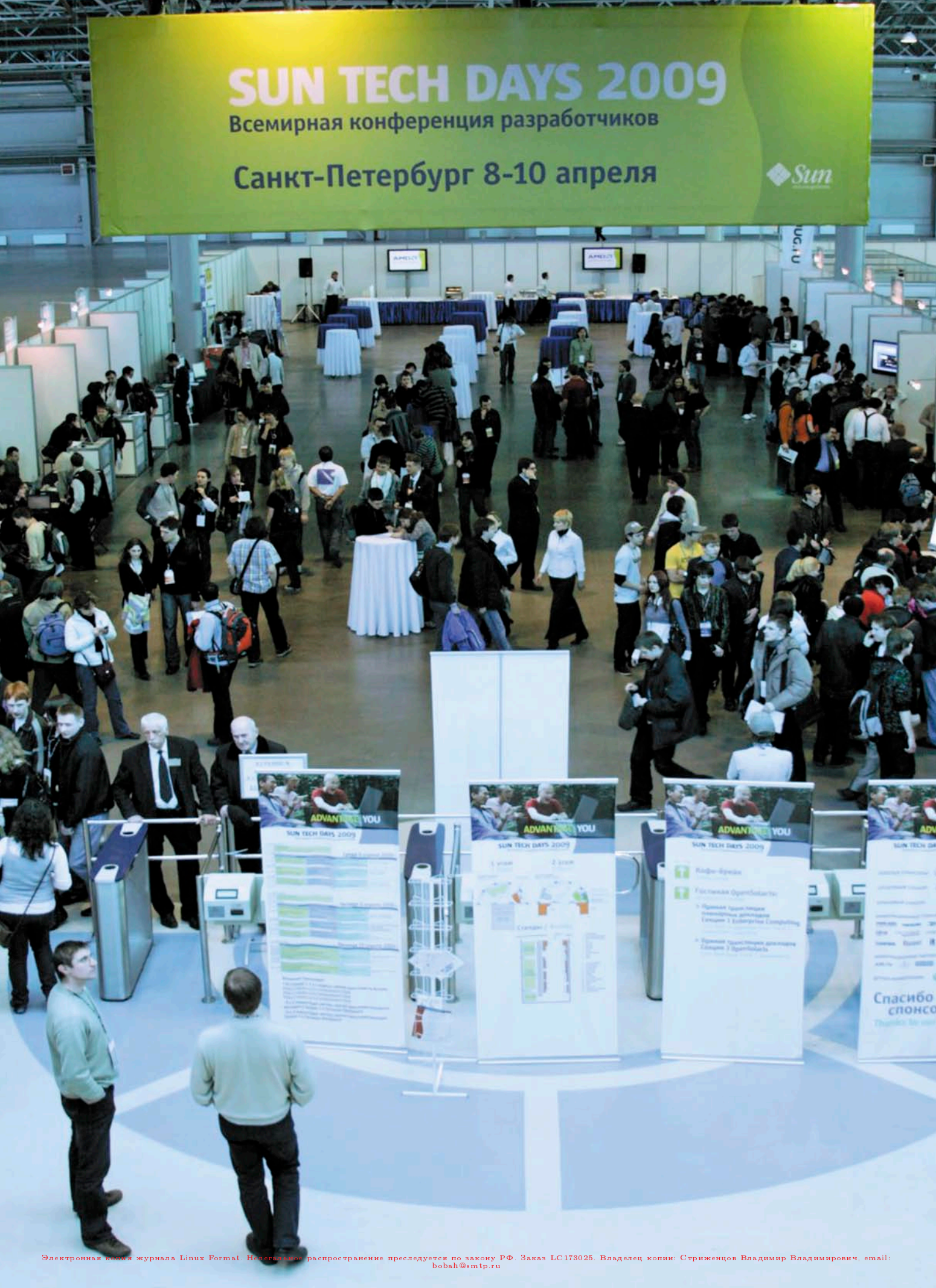
Ранее, 7 февраля, компания Sun объявила об открытии центра компетенции по программным продуктам и решениям с открытым исходным кодом на базе Центра высоких технологий Sun Microsystems в Санкт-Петербурге. Эта инициатива представляет собой демонстрационную и тестовую площадку для партнеров, нынешних и потенциальных партнёров Sun, а также студентов.

Интерес Sun к нашей стране не случаен. Россия сегодня является одной из трех стран (наряду с США и Индией) с самым большим сообществом разработчиков. По данным Григория Лабзовского (директора Санкт-Петербургского центра разработки Sun Microsystems), у нас существует около 50 000 активных разработчиков, поддерживающих регулярную связь с центром, среди них свыше 10 000 студентов.

В связи с этим ожидаемой новостью стало объявление о начале действия в нашей стране программы Sun Startup Essential, предоставляющей начинающим российским компаниям особые, благоприятные условия для приобретения и сопровождения оборудования и программного обеспечения Sun Microsystems.

Кому-то это может показаться странным, но, по уверению Боба Порраса (Bob Porras), вице-президента подразделения Solaris Data, Availability, Scalability и HPC, для Sun Microsystems потенциал роста экономики России представляется очевидным. Руководствуясь этим, Sun планирует продолжать вкладывать сюда средства как за счет участия в разработке ПО с открытым кодом, так и при помощи прямых инвестиций.

Возвращаясь к положению корпорации в свете мирового экономического кризиса, следует заметить, что всё это происходило в свете недавних упорных слухов о несостоявшейся сделке по покупке компании IBM. Я задал воп-



Роман Штробл

рос об этом одному из сотрудников Sun после окончания пресс-конференции и получил ответ, что такие переговоры и правда имели место. А ещё услышал спасибо за то, что не задал подобного вопроса на пресс-конференции.

Впрочем, сейчас, когда я пишу эти строки, мы уже знаем, чем всё закончилось (см. врезку «Солнечное затмение»), и оптимистичные слова Джита Коула, естественно, не кажутся теперь такими убедительными. Впрочем, безнадёжный бизнес, наверное, никого бы не заинтересовал. Мне кажется, что то, что произошло, далеко не худший выход для компании.

Технология JavaFX

JavaFX была посвящена чуть ли не половина «клиентской» секции конференции. Эта платформа провозглашена флагманской технологией компании.

В своей статье о JavaFX в №4 за 2009 год я, как выяснилось, допустил ряд неточностей, и тут самое время их исправить.

Прежде всего JavaFX – это среда, в основе которой лежит платформа Java, и работающая там, где есть Java. Принцип write once run anywhere здесь воплощён в том, что одна и та же программа предназначена для настольного ПК, мобильника, а в будущем и для TV.

Что особенного в JavaFX? Это модель разработки за счёт декларативности языка, позволяющая отделить дизайнеров от программистов.

Это потенциально широчайший, не имеющий аналогов рынок распространения приложений. В общем, выражаясь лозунгами, JavaFX – единая платформа для разработки и распространения программ для всех экранов вашей жизни.

В день открытия конференции Sun Microsystems представила платформу JavaFX Mobile – средство для создания на базе Java решений для беспроводной связи, которые в полной мере используют многофункциональные контент-сервисы и в то же время сохраняют весь потенциал Java Platform Micro Edition (JavaME).

В докладе «JavaFX: платформа для привлекательных интерактивных интернет-приложений» Александров Зуев рассказал о концепции Rich Internet Application и обосновал необходимость нового средства разработки для их реализации (почему не Java?). Затем был рассказ об особенностях платформы JavaFX и языка JavaFX Script с многочисленными примерами кода. Были показаны примеры реализации различных графических и фотоэффектов, анимации, встраиваемого видео и многого другого. При этом любого скептика бы поразило, как легко с применением новой технологии может быть реализовано то или иное графическое/мультимедиа решение.

Продолжил рассказ о JavaFX Вячеслав Баранов в докладе «JavaFX: анимация и медиа», в котором подробно осветил технологию реализации медиаконтента и анимации.

Платформе JavaFX была целиком посвящена и вторая пресс-конференция, Джит Кол отвечал на вопросы курируемой им разработки. Лично меня интересовали сроки выхода JavaFX SDK для платформы Linux (пока есть только под Windows), и я не преминул воспользоваться служебным положением. Был получен вполне определённый ответ – в июне, после проведения конференции JavaOne.

Напоследок сотрудники Sun заинтриговали слушателей проектом JavaFX TV, но детали прояснить отказались. Прямая цитата: «Я знаю, что это такое, но не скажу».

OpenSolaris

Это, естественно, была самая популярная тема конференции, которой было посвящено больше всего докладов и практических занятий.

Начало было положено Крисом Армесом (Chris Armes) докладом «Что такое OpenSolaris и чем он хорош?». Затем, логически развивая неизбежное, последовали два доклада Романа Штробла (Roman Strobl) «Как эффективно перейти на OpenSolaris» и «Эффективная работа в OpenSolaris» и Игоря Никифорова «Как перенести приложение с открытым кодом в OpenSolaris?»

Далее в докладах, проходивших в секции «OpenSolaris», обсуждались вопросы оптимизации, виртуализации, применения средств разработки. Отдельное выступление было посвящено реализации концепции OpenStorage.

Завершалась секция докладом Кристофа Скубы (Christoph Schuba) «Обеспечение безопасности при разработке и внедрении».

Всюду раздавали диски с различными вариантами дистрибутива. Проходили мастер-классы по различным аспектам применения системы (ZFS, DTrace, виртуализация сетевых интерфейсов Crossbow).

MySQL

В докладе «MySQL: взгляд в будущее» Константин Осипов рассказал о новых возможностях СУБД, появившихся в версии 5.1 (partitioning, row-based replication (RBR), event scheduler, поддержка XML/XPath, диспетчер событий и др.). При этом докладчик постарался развеять слухи о неготовности проекта 5.1 и всякие мрачные домыслы, свя-

занные с уходом из проекта MySQL её основателей.

После рассказа об изменении в процессе и цикле разработки СУБД (внедрена Bazaar) был сделан обзор возможностей ветки 5.x в целом, а также будущих возможностей MySQL 6.x.

Было интересно послушать про форки MySQL (XtraDB, OurDelta, Drizzle), также про движки сторонних производителей, а это, кроме давно привычного InnoDB, ещё и PrimeBase XT, Sphinx SE и Maria.

DTrace

Технологии DTrace было посвящено несколько выступлений. В докладе «DTrace: наблюдение за приложениями на Java и на языках сценариев в OpenSolaris» Саймон Ритер (Simon Ritter) в очередной раз представил технологию (хотя, по-моему, она давно не нуждается в представлении), показал основы её применения с примерами кода на языке D, рассказал о возможностях применения в технологии скриптовых языков (Python, PHP и т.д.). Закончил Саймон рассказом о применении DTrace для диагностирования приложений MySQL, и эта тема была подхвачена на следующий день коротким, но очень познавательным докладом Алексея Копылова «Поддержка DTrace в MySQL: способы решения типичных проблем с производительностью».

Закрепление материала на практике состоялась в конце первого дня конференции, в мастер-классе Филиппа Торчинского «Глубокое изучение приложений на языке Java с помощью Dtrace».

Второй день

Второй день открывал пленарный доклад Боба Порраса, посвящённый вопросам разработки, Open Solaris, концепции Open Storage и виртуализации (xVM Virtual Box). Был представлен российский портал, посвящённый OpenSolaris, – http://ru.opensolaris.org. Также Боб рассказал о Sun Cloud – публичной сервис-ориентированной сети, создаваемой специально для разработчиков, компаний-стартапов и студентов.

В докладе Константина Золотникова и Сергея Трошина «Мобильная Java: что дальше» рассказывалось о перспективах развития технологий, основанных на Java, в мобильных устройствах. Цифры, приведённые в начале этого выступления, впечатляли – «мобильная Java» используется более чем в шести миллиардах различных устройств, в том числе в двух с половиной миллиардах телефонов. В этом безобразии задействованы 180 миллионов разработчиков. Очевидно, чтобы занять разработчиков ещё больше, в Sun на достигнутом не останавливаются, технология непрерывно развивается.

Рассказывалось о новой платформе JavaFX Mobile, о релизе MIDP 3.0 (Mobile Information Device Profile), о концепции Mobile Services Architecture v2. Также было уделено внимание спецификации JSR 290 (Language & XML User Interface Markup Integration lu-ray.

В секции клиентских технологий Василий Исаенко рассказывал о том, что нового произошло в технологии JavaCard. Сама технология представляет собой открытую и не зависящую от производителя платформу для смарт-карт и прочих «умных» устройств с ограниченными ресурсами. JavaCard совместима с существующими стандартами для смарт-карт.

При изучении стендов больше всего заинтересовали проекты:

Project Kenai – проект Sun по хостингу открытых проектов. На стенде проекта сотрудники подчёркивали, что он предназначен для разработок, не обязательно использующих технологии Sun. Основное условие – проект должен быть иметь лицензию, одобренную Open Source Initiative (OSI).

Project Kenai включает все основные сервисы для подобных площадок, как то: форумы, списки рассылок, Wiki. Большое внимание уделено возможностям совместной работы – системы контроля версий представлены Subversion, Mercurial и любимым Торвальдсом Git. Для отслеживания ошибок предусмотрена возможность использования систем Jira и Bugzilla. Впрочем, на прямой вопрос, чем данный проект принципиально отличается от, скажем, от SourceForge, особо подчеркивалось наличие «On-line-поддержки» пользователей. Вот только в детали оной меня не посвятили, откупившись бейсболкой.

Стенд **Cloud Computing** оставил несколько странное впечатление. Два американца показывали на мониторе нечто не вполне внятное (что, в общем, неудивительно, что там может быть наглядно) и много говорили про «облачные» вычисления, но без всякой конкретики. Очевидно, что данной темой Sun занимается, но, по-видимому, показывать результаты ещё рановато.

Также на стендах были представлены другие продукты и технологии компании – SunStudio, JavaME, JavaFX, OpenSolaris, проект BlackBox (Sun MD S20).

University Day

Третий день конференции – «University Day» был организован специально для студентов и преподавателей. На нём демонстрировались различные академические программы Sun, программы

Григорий Лабзовский

Солнечное затмение

«Горе! Горе! Крокодил
Солнце в небе проглотил!»
Наступила темнота.
Не ходи за ворота:
Кто на улицу попал -
Заблудился и пропал.

К.И. Чуковский

20 апреля 2009 года корпорации Sun Microsystems и Oracle объявили о достижении договоренности, согласно которой Oracle приобретает Sun Microsystems. Общая сумма сделки составит около 7,4 млрд долларов, из которых 1,8 млрд составляют финансовые обязательства Sun.

Исполнительный директор Oracle Ларри Эллисон (Larry Ellison), комментируя соглашение, сказал: «Oracle станет единственной компанией, которая сможет создавать полностью интегрированные системы, в которых все компоненты максимально эффективно работают друг с другом. Наши заказчики получат дополнительные конкурентные преимущества, поскольку затраты на системную интеграцию снизятся, а производительность систем, их надежность и безопасность – повысятся». Ему вторит президент компании Сафра Кэтц (Safra Catz): «Мы ожидаем, что в результате данной сделки корпорация Oracle в течение первого полного года после закрытия увеличит свою прибыль, как минимум, на 15 центов на акцию... Приобретение этой корпорации уже в первый год принесет больше прибыли в расчете на одну акцию, чем приобретение компаний BEA, PeopleSoft и Siebel вместе взятых».

Слухи о финансовых проблемах у Sun ходили уже довольно давно, журналисты чуть не «продали» корпорацию IBM, но эта новость всё равно прозвучала неожиданно. Нас, конечно, больше интересует не увеличение капитализации или прибыли Oracle, а судьба технологий и наработок компании Sun, судьба многих из них теперь под вопросом.

Разумеется, таким ключевым продуктам, как Java и операционная система Solaris, ничто не угрожает – продукция Oracle давно и прочно интегрирована с этими технологиями, и, в общем, ради них всё и затевалось. По некоторым данным, можно также не переживать за архитектуру Sun SPARC и технологию Open Storage, уже заявлено о дополнительных инвестициях в них наряду с Java и Solaris. Также не стоит сильно переживать за судьбу СУБД MySQL – её развитие будет продолжено, об этом, а также о том, что Java останется открытой технологией, заявил президент Oracle на совещании с руководством Sun.

По-иному обстоят дела с OpenOffice.org. Пока высказываются намерения сделать его независимым проектом, организовав для курирования разработки некоммерческую организацию наподобие Linux Foundation.

Системы виртуализации VirtualBox и распределённая кластерная файловая система по всем признакам также не должны пропасть, так как востребованы и применяются в Oracle.

Собственно, это всё, что известно на настоящий момент. Какая судьба ожидает OpenSolaris, OpenSparc, OpenJDK, NetBeans, GlassFish, JavaFX и многие другие продукты? Будем надеяться на лучшее, перспективные технологии не должны пропасть. Для некоторого оптимизма приведу слова Скотта Макнили (Scott McNealy), председателя совета директоров корпорации Sun Microsystems: «Oracle и Sun были пионерами ИТ-отрасли и тесно сотрудничают уже более 20 лет. Объединение является естественным развитием этих взаимоотношений и событием, которое изменит ИТ-отрасль».

Источники:

- ☑ Пресс-релиз компании Sun Microsystems – http://ru.sun.com/news/press/2009/april/pr200409.html.
- ☑ Ответы на часто задаваемые вопросы, касающиеся соглашения от Oracle – http://www.oracle.com/sun/sun-faq.pdf.

сотрудничества с вузами, а также материалы по сертификации и трудоустройству студентов. Число студентов, которых и так немало присутствовало на конференции, увеличилось до подавляющего большинства.

Давались конкретные советы по различным аспектам трудоустройства: составление резюме, прохождение собеседования. Много говорилось про программы стажировок студентов, правда, с оговорками, что в период кризиса с ними есть некоторые ограничения. Впрочем, было показано, что и сейчас у студентов есть много возможностей для развития.

Активно обсуждался проект OSUM (Open Source University Meetup) – система университетских клубов, объединяющих людей, интересующихся свободным ПО. Sun активно поддерживает идею открытого исходного кода, и вкладывает много сил в развитие этого сообщества. Под эгидой компании на сайте osum.sun.com фактически создаётся своеобразная социальная сеть для разработчиков.

Студенческой аудитории также пришлось выслушать свою порцию материалов по JavaFX и OpenSolaris в докладах Александра Щербатого и Филиппа Торчинского.

Параллельно с докладами и «круглыми столами» для преподавателей вузов, работающих с технологиями Sun Microsystems, проводились мастер-классы по созданию приложений с использованием JavaFX и OpenSolaris. Последний был сосредоточен на программе сертификации знаний и вызвал повышенное количество вопросов.

Далее следовали доклады представителей Sun в вузах и выступления преподавателей. Особый интерес вызвал проект Wonderland, представленный Евгением Бугровым. Этот инструмент для создания виртуальных интерактивных миров сразу же вызвал среди публики разговоры о Лукьяновском Диптауне.

Конференция закончилась. К сожалению, разорваться, как я ни старался, не получилось, и многое из того, что там происходило, здесь не освещено. Это OpenESB, GlassFish 3.0, ZFS, Zembly – среда разработки для социальных сетей, проект Blackbox (модульный центр хранения данных) и другие интересные вещи. Всем заинтересованным предлагаю ознакомиться с презентациями докладов, которые выложены на странице конференции (http://developers.sun.ru/techdays2009/index.phpoption=com_content&task=view&id=62&Itemid=66).

Что ещё можно сказать? К хорошему очень быстро привыкаешь, и уже не хочется представлять весну без питерских Sun Tech Days. Надеюсь, и не придется, и, несмотря на все экономические проблемы нашего времени, мы, разработчики, системные администраторы, инженеры, встретимся на Неве в следующем году.

Текст: Кирилл Сухов,
фото: Лика Чекалова

31 июля – 2 августа

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

Четвёртый 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 info@sletadminov.ru

Организаторы Слёта

softline® @mail.ru

Партнёр Слёта

symantec.

Информационный спонсор

СИСТЕМНЫЙ администратор

Учет оборудования с OCS Inventory NG и GLPI

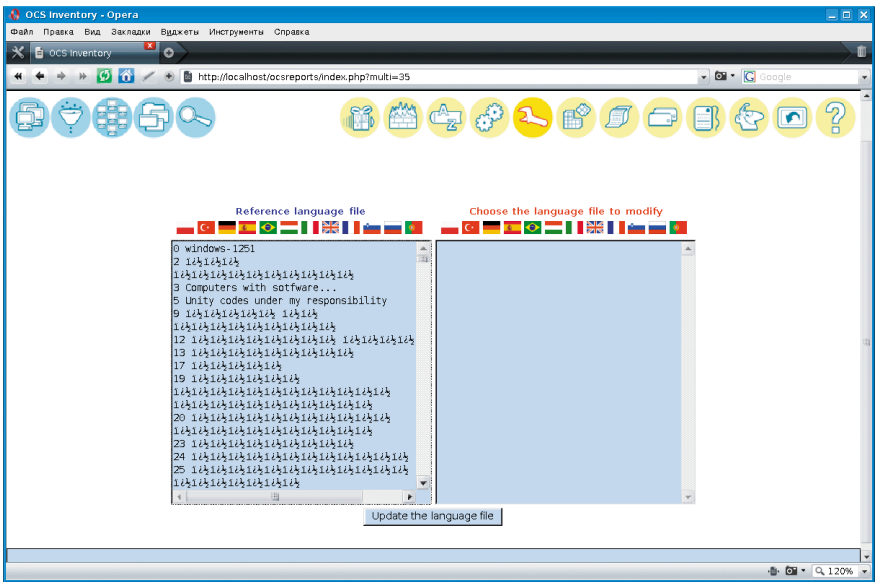
Сегодня в любой организации много компьютерной техники и прочего оборудования, учет которого, а также прочих связанных затрат часто входит в обязанности администратора. Применение специализированных систем может значительно упростить эту задачу. В статье рассмотрим решения OCS Inventory NG и GLPI, которые являются хорошей альтернативой проприетарным продуктам.

Сергей Яремчук

Возможности OCS Inventory NG и GLPI

Система OCS Inventory NG (OCSNG, Open Computers and Software Inventory New Generation) [1] предназначена для инвентаризации компьютеров в локальной сети, комплектующих и программного обеспечения. Также с ее помощью можно удаленно разворачивать программы на рабочих местах и получать информацию о сетевой конфигурации.

GLPI (Gestion Libre de Parc Informatique) [2] кроме задач по учету компьютеров и входящих в их состав комплектующих, позволяет инвентаризировать прочее оборудование, включая расходные материалы (например, картриджи), а также организовать службу технической поддержки, автоматизируя обработку обращений пользователей. Теперь пользователь, вместо того чтобы бежать или звонить админу, заполняет, зайдя по адресу ресурса, заявку. Обращения обрабатываются с учетом их важности или в порядке очередности. Администратор выигрывает вдвойне – все обращения документируются, и можно спокойно отчитаться перед начальством о проделанной работе и затраченном времени, пользователи по этой же причине перестанут обращаться по мелочам. Не говоря уже о том, что звонки обычно отвлекают от выполнения текущей работы.



Файл локализации OCSNG требует замены

Также с его помощью можно сформировать базу знаний, которая будет состоять из заметок, статей и ЧаВО, вести учет поставщиков, договоров. Доступно большое количество отчетов (по договорам, финансовая, за год) и статистик (по заявкам, оборудованию, элементам).

Поддерживается синхронизация календаря по протоколам Ical, Webcal. Функциональность GLPI можно расширить при помощи большого набора плагинов от сторонних разработчиков!

Обе системы русифицированы (с некоторыми оговорками) и распространяются по лицензии GNU GPL.

В GLPI, как и в Kwok Information Server [2], изначально все данные вводятся вручную и сохраняются в базе данных MySQL. Затем администратор при помощи веб-формы может отобрать любую интересующую его информацию. Начиная с версии 0.65 GLPI поддерживает синхронизацию данных с базами OCSNG, причем для этого не требуется никаких дополнительных модулей. Хотя если в сети уже есть сервер Nagios или Cacti, то данные о компьютерах и прочем оборудовании можно импортировать и оттуда.

Основным плюсом OCS Inventory NG является то, что для сбора информации об установленном оборудовании с клиентских компьютеров и серверов используется программа-агент. Все собранные данные агенты отсылают на сервер управления (management server) в виде XML-потока, сжатого при помощи Zlib, для передачи используется стандартный протокол HTTP/HTTPS.

Сервер OCSNG состоит из 4 компонентов, которые могут быть установлены на одном или нескольких компьютерах:

- **база данных** – используется для хранения информации, поддерживается MySQL от 4.1;
- **служба связи** – обеспечивает связь по протоколу HTTP между сервером базы данных и программами-агентами, требуется Apache Web Server 1.3.X/2.X с интегрированным Perl (в Debian/Ubuntu пакет libapache-dbi-perl);
- **служба развертывания** – предназначена для хранения установочных файлов программ-агентов, подходит любой веб-сервер с поддержкой SSL;
- **консоль управления** – просмотр собранных данных в браузере, требуется веб-сервер с поддержкой PHP (с активированными ZIP и GD).

Серверная часть OCSNG может быть установлена на компьютер, работающий под управлением Windows 2000 Professional/Server, XP Professional Edition и 2003, а также Linux, FreeBSD, OpenBSD, NetBSD, Solaris, IBM AIX и MacOS X.

Агент доступен для клиентских и серверных версий Windows от 95 до Server 2008 R2, а также перечисленных Linux (2.4/2.6, x86, x86_64/AMD64, Sparc64, ARM, PowerPC), MacOS X (10.3-10,5), FreeBSD/OpenBSD/NetBSD (x86/Sparc), Solaris 8, 9, 10 (x86/Sparc), IBM AIX (5.1-5.3) и HP-UX.

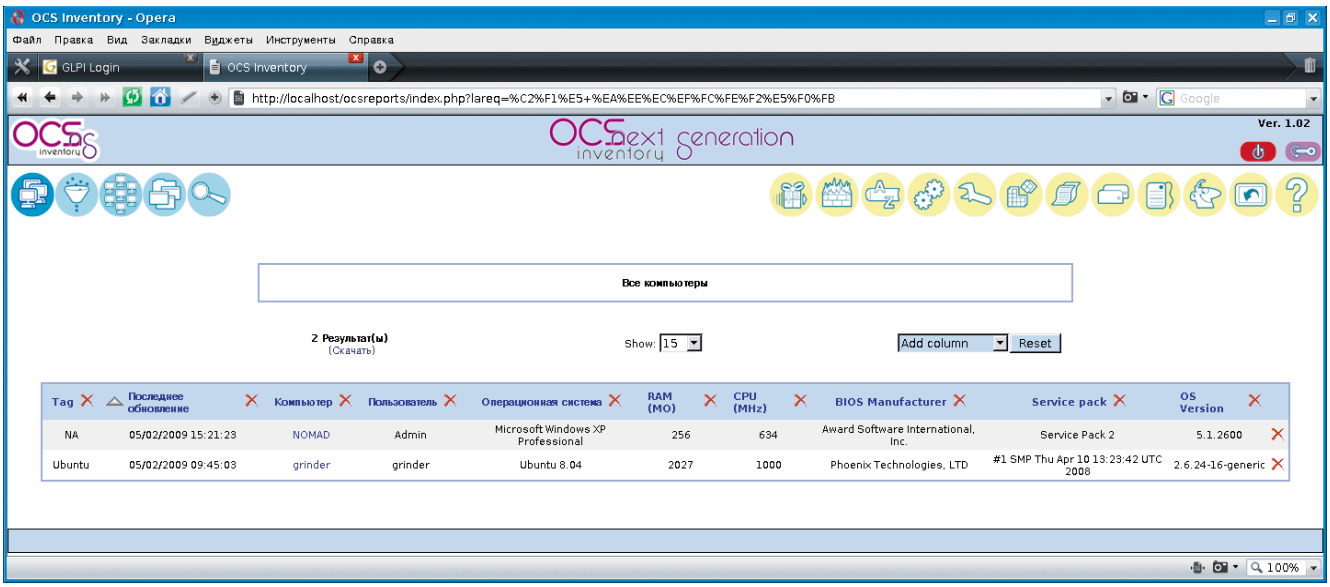
Следует отметить, что одним из недостатков как данного проекта, так и проекта GLPI является малое количество документации. Хотя, понимая суть процесса, разобраться со всеми нюансами довольно просто.

Установка OCS Inventory в Ubuntu

В середине апреля, после более чем года разработки, вышла новая версия 1.02 OCSNG, о которой и пойдет речь далее. Пакет с OCSNG имеется в репозиториях многих дистрибутивов. Для примера в качестве сервера и клиента выберем Ubuntu 8.04 LTS.

Проверяем, что есть в репозитории Ubuntu.

```
$ sudo apt-cache search ocsinventory
ocsinventory-reports - Hardware and software inventory tool
(Administration Console)
```



После установки агентов данные автоматически появляются в консоли управления OCSNG

```
ocsinventory-server - Hardware and software inventory tool
(Communication Server)
ocsinventory-agent - Hardware and software inventory tool
(client)
```

Хотя это не самая актуальная версия на данный момент:

```
$ sudo apt-cache show ocsinventory-server | grep -i version
Version: 1.01-3

$ sudo apt-cache show ocsinventory-agent | grep -i version
Version: 1:0.0.8-1
```

Поэтому будем устанавливать, используя исходные тексты. В зависимостях пакета ocsinventory-server, полученных при помощи команды:

```
$ sudo apt-cache depends ocsinventory-server
```

указаны Apache2 и некоторые модули Perl, утилита для изменения файлов настроек ucf и dbconfig-common. Пакет MySQL указан в качестве необязательных зависимостей, поэтому его устанавливаем отдельно:

```
$ sudo apt-get install mysql-server
```

Команда:

```
$ sudo apt-get build-dep ocsinventory-server
```

в данном случае бесполезна, поэтому устанавливаем все, что необходимо, вручную:

```
$ sudo apt-get install libapache2-mod-perl2 libdbi-perl ↵
      libapache-dbi-perl libdbd-mysql-perl ↵
      libsoap-lite-perl libxml-simple-perl ↵
      libnet-ip-perl libcompress-zlib-perl php5-gd
```

Скачиваем с сайта проекта OCSNG архив OCSNG_UNIX_SERVER-1.02.tar.gz и устанавливаем:

```
$ tar xzfv OCSNG_UNIX_SERVER-1.02.tar.gz
$ cd ./OCSNG_UNIX_SERVER-1.02/
$ sudo ./setup.sh
```

По ходу установки следует ответить на ряд стандартных вопросов: расположение сервера баз данных, исполняемого и конфигурационного файла веб-сервера, пользователь, от имени которого запускается веб-сервер и так далее.

В большинстве случаев скрипт сам находит все необходимое и достаточно просто подтвердить параметр. Единственное, с чем он не разобрался, это с пользователем и группой, от имени которых запускается Apache. Поэтому вместо предложенного [${APACHE_RUN_USER}] указываем www-data.

Далее производится проверка установленных модулей Perl. И в случае, если нужный не будет найден, выдается соответствующее сообщение. Так в зависимостях Ubuntu не указан модуль XML::Entities.

```
Checking for XML::Entities PERL module...
*** Warning: PERL module XML::Entities is not installed !
```

В репозитории пакета, обеспечивающего функции XML::Entities, нет, поэтому его следует установить самостоятельно из CPAN:

```
$ sudo cpan -i XML::Entities
```

И повторяем установку. По окончании скрипт предложит инсталлировать консоль администрирования.

В процессе установки в каталоге /etc/apache2/conf.d/ будут созданы конфигурационные файлы для веб-сервера – ocsinventory-server.conf и ocsinventory-reports.conf.

Сами PHP-скрипты, обеспечивающие функции OCSNG, будут скопированы в /usr/share/ocsinventory-reports/ocsreports и подключены к веб-серверу с использованием директивы Alias:

```
$ cat ocsinventory-reports.conf | grep -i alias

# Alias used to put Administration Server static page
# (typically PHP) outside
```

```
Alias /ocsreports /usr/share/ocsinventory-reports/ocsreports
# Alias to put Deployement package files outside Apache
# document root directory
Alias /download /var/lib/ocsinventory-reports/download
```

Поэтому при необходимости управления доступом все изменения следует производить в упомянутых конфигурационных файлах, иначе назначенные на корень права не будут наследоваться.

Кроме этого создается файл, обеспечивающий ротацию журналов раз в неделю.

```
$ cat /etc/logrotate.d/ocsinventory-server

# Rotate OCS Inventory NG Communication server logs daily
# Save 7 days old logs in compressed mode
/var/log/ocsinventory-server/*.log {
        daily
        rotate 7
        compress
        missingok
}
```

По окончании следует перезапустить веб-сервер:

```
$ sudo /etc/init.d/apache2 force-reload
```

Некоторые пакеты, распространяемые при помощи OCSNG, могут иметь размер больше 8 Мб, поэтому, чтобы не было проблем с их загрузкой, следует установить большее значение переменных post_max_size и upload_max_filesize в файле /etc/php5/apache2/php.ini, например в 10 Мб (по умолчанию – 8 и 2 Мб):

```
php_value post_max_size          10m
php_value upload_max_filesize    10m
```

Эти же установки надо изменить в файле ocsinventory-reports.conf.

Набираем в браузере http://localhost/ocsreports/install.php и в появившемся окне вводим логин и пароль для доступа к MySQL. По умолчанию в процессе установки для доступа к базе ocsweb будет создана учетная запись ocs с паролем ocs. Если только доступ к базе не ограничен локальной системой, то в целях безопасности пароль следует изменить:

```
$ mysql -uroot -prootsecret
mysql> UPDATE mysql.user SET Password = ↵
    PASSWORD('ocspasswd') WHERE User = 'ocs';
mysql> FLUSH PRIVILEGES;
mysql> exit
```

Новое значение пароля следует прописать в файле /usr/share/ocsinventory-reports/ocsreports/dbconfig.inc.php:

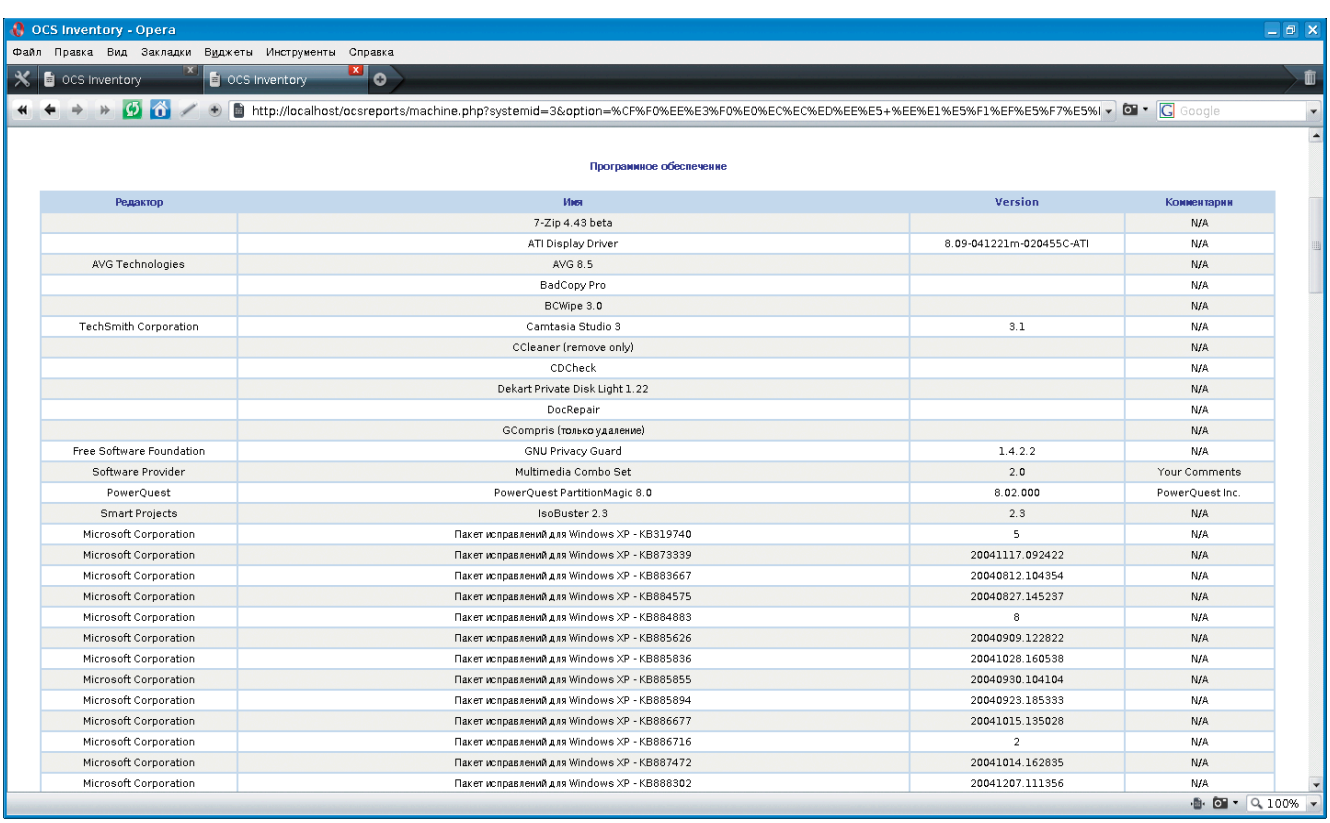
```
$_SESSION["PSWD_BASE"]="ocspasswd"
```

И в ocsinventory-server.conf:

```
PerlSetVar OCS_DB_PWD ocspasswd
```

Локализация

Переходим на страницу http://localhost/ocsreports, для регистрации используем логин admin с паролем admin. Щелкнув здесь же по флагу, можно активировать русский язык интерфейса, но сразу после установки это привело к появлению нечитаемых символов. Единственным материалом по локализации интерфейса OCS Inventory является статья Евгения Бражко [5], но она относится к версии 1.02RC1, вышедшей в марте 2008 года, и многие вопросы, которые в ней описа-



После всех правок информация об установленном ПО на кириллице выводится корректно

ны, в текущей версии уже решены. Так, анализ HTML-кода страницы показал, что она выдается в нужной кодировке:

```
<META HTTP-EQUIV="Content-Type" CONTENT="text/html; ↵
      charset=windows-1251;">
```

Интерфейс локализуется при помощи языкового файла russian.txt, расположенного в /usr/share/ocsinventory-reports/ocsreports/languages. В меню Configurations есть отдельный пункт Language file, позволяющий его редактировать. Но открыв файл russian.txt в текстовом редакторе, поддерживающем CP1251, обнаруживаем только набор нечитаемых символов.

Вывод команды file:

```
$ file russian.txt
russian.txt: UTF-8 Unicode English text
```

Задает еще больше вопросов. При этом:

```
$ file english.txt
english.txt: ASCII English text
```

А первая строка файла явно указывает на нужную кодировку.

```
$ head -n 1 russian.txt
0 windows-1251
```

Из этого делаем вывод – что-то не то с самим файлом, поэтому берем аналогичный с RC1 или другого источника (например, на сайте журнала www.samag.ru в разделе «Исходный код») и подменяем его, не забыв установить нужные права доступа.

```
$ sudo chown root:www-data russian.txt
```

После этого все надписи выводятся на русском.

Чтобы корректно выводились названия программ, установленных на Windows-системах, следует в файле /usr/share/ocsinventory-reports/ocsreports/preferences.php установить в «1» значение UTF8_DEGREE:

```
// 0 For non utf8 database, 1 for utf8
define("UTF8_DEGREE", 1 );
```

Далее в файле machine.php, который находится в этом же каталоге, правим функцию print_softwares. После установки она будет иметь такой вид:

```
echo "$td3".htmlentities(textDecode($item->PUBLISHER))."</td>
$td3".htmlentities(textDecode($item->NAME))."     </td>
$td3".textDecode($item->VERSION)."  </td>
$td3".(htmlentities(textDecode($item->COMMENTS))? ↵
      htmlentities(textDecode($item->COMMENTS)): "N/A")." ↵
           </td>";
```

Меняем на:

```
echo "$td3".textDecode($item->PUBLISHER)."</td>
$td3".textDecode($item->NAME)."     </td>
$td3".textDecode($item->VERSION)."  </td>
$td3".(htmlentities(textDecode($item->COMMENTS))? ↵
      textDecode($item->COMMENTS):"N/A")."     </td>";
```

После этого список программ, установленных на конкретном компьютере, будет выводиться корректно. Страница в PDF, создаваемая при помощи кнопки «Напечатать эту страницу», которая расположена в самом низу, также выглядела корректно. Хотя в общем списке ПО по-прежнему будет нечитаемый текст.

Установка агента

Агент для Windows написан на C++, его можно установить вручную, при помощи logon скрипта или правил GPO. Агент для Linux написан на Perl и C. Для его установки потребуется наличие некоторых модулей Perl (XML и Zlib) и dmidecode [4] (обеспечивает сбор данных из BIOS об оборудовании в соответствии со стандартами SMBIOS/DMI). В Linux агент устанавливается вручную. Сначала рассмотрим этот вариант.

Если клиент устанавливается на том же компьютере, что и сервер, практически все необходимые пакеты для удовлетворения зависимостей уже будут. Иначе устанавливаем:

```
$ sudo apt-get install libcompress-zlib-perl ↵
      libnet-ip-perl libnet-ssleay-perl libwww-perl ↵
      libxml-simple-perl po-debconf ucf dmidecode pciutils
```

Далее скачиваем и ставим агента:

```
$ tar xzvf OCSNG_UNIX_AGENT-1.02.tar.gz
$ cd Ocsinventory-Agent-1.0.1
$ perl Makefile.PL
$ make
$ sudo make install
```

После ввода последней команды поступит запрос на настройку агента.

```
Do you want to configure the agent
Please enter 'y' or 'n'?> [y]
```

Отмечаем «y» и при помощи цифровых клавиш отвечаем на вопросы, где должен располагаться конфигурационный файл:

```
Where do you want to write the configuration file?
 0 -> /etc/ocsinventory
 1 -> /usr/local/etc/ocsinventory
 2 -> /etc/ocsinventory-agent
```

Далее указываем адрес или имя сервера, создаем тег (с его помощью можно собрать системы в целевую группу, например, по принципу размещения) для агента, активируем задачу для cron, каталог для хранения файлов и так далее. По окончании выдается запрос на отсылку собранных данных о компьютере на сервер:

```
Do you want to send an inventory of this machine?
Please enter 'y' or 'n'?> [y]
[info] Accountinfo file doesn't exist. I create an empty one.
   -> Success!
```

В итоге в /var/lib/ocsinventory-agent будет создан подкаталог с файлами, содержащими текущую конфигурацию компьютера. Например, в ocsinv.adm содержатся тег и название системы, под которым она будет видна в консоли управления.

```
$ cat /var/lib/ocsinventory-agent/http\: ↵
      __localhost_ocsinventory/ocsinv.adm
```

```
<ADM>
  <ACCOUNTINFO>
    <KEYNAME>TAG</KEYNAME>
    <KEYVALUE>Ubuntu</KEYVALUE>
  </ACCOUNTINFO>
</ADM>
```

Практически сразу после установки агента сведения о новой системе появятся в консоли управления во вкладке «Все компьютеры».

При возникновении проблем можно запустить агента в режиме отладки:

```
$ ocsinventory-agent -l /tmp -debug ↵
      --server http://localhost/ocsinventory
```

По умолчанию во вкладке «Все компьютеры» выводятся 7 характеристик клиентских машин, но при помощи раскрывающегося списка Add column можно добавить еще 23 поля. Хотя в некоторых случаях замечены ошибки в определении параметров. Так, на системе с такими характеристиками:

```
$ dmesg | grep -i processor
[   97.725563] powernow-k8: Found 1 AMD Athlon(tm) 64 X2 Dual
Core Processor 3600+ processors (2 cpu cores) (version 2.20.00)
[    0.000000] Detected 2010.408 MHz processor.
```

В консоли OCS Inventory было выведено – 1000 Мгц, но при необходимости данные можно скорректировать вручную. По разным причинам в базу компьютер может быть занесен несколько раз, для удаления дубликатов существует одноименная вкладка, в которой одинаковые системы можно отобрать по нескольким характеристикам (имя, MAC-адрес, серийный номер).

Текущая версия агента для Windows 4.0.5.4, архив OCSNG_WINDOWS_AGENT_1.02.zip с установочными файлами можно скачать с сайта проекта. Судя по всему, в нем уже исправлена ошибка, которая приводила к тому, что русские буквы, начиная с 'x'(0xF4) заменялись английским иксом. Во всяком случае, на тестовых системах все работало правильно. Как вариант можно использовать специальную сборку OCSNG_WINDOWS_AGENT_1.02_RC2_OTEA.zip (версия агента 4.0.4.9) [5].

Самым простым вариантом установки является запуск исполняемого файла OcsAgentSetup.exe, в этом случае будет произведена стандартная установка, по окончании которой агент будет прописан в качестве сервиса. На последнем этапе указываем имя или IP-адрес OCSNG сервера и устанавливаем флажок Immediatly launch inventory, чтобы сразу же отправить отчет.

Все настройки будут сохранены в файле service.ini каталога, в который установлен агент.

В Vista следует открыть его и добавить параметр /DEBUG в строку запуска:

```
Miscellaneous= ↵
      /SERVER:192.168.0.10 ↵
      /PNUM:80 /DEBUG
```

При изменении оборудования или ПО агента вызвать принудительно, набрав в командной строке:

```
> "C:\Program Files\OCS Inventory Agent\OCSInventory.exe" ↵
      /SERVER:ocsng_server /PNUM:80 /NOW
```

Также агента (файл ocsagent.exe, являющийся zip-архивом) можно импортировать в базу OCSNG, выбрав во вкладке «Агент» и указав место расположения файла. В этом случае он будет доступен с любого компьютера сети.

Кроме функций сетевой инвентаризации, OCSNG имеет возможность развертывания пакетов и запуска команд, записанных в файле (например, bat/vbs) на клиентских компьютерах (кроме Vista), информация о которых находится в инвентаризационной системе. При необходимости установки одного приложения на большое количество систем такая функциональность очень выручает.

Для начала пакет нужно создать. Переходим в меню Deployment → Build и заполняем поля New package building. Название пакета должно быть уникальным, и желательно отражать его назначение. Параметр Priority определяет порядок размещения пакетов. Что, собственно, делать с пакетом, определяет поле Action.

Здесь три возможных значения:

- **Store** – копировать на целевую систему;
- **Execute** – копировать и выполнить с командой;
- **Launch** – копировать и запустить.

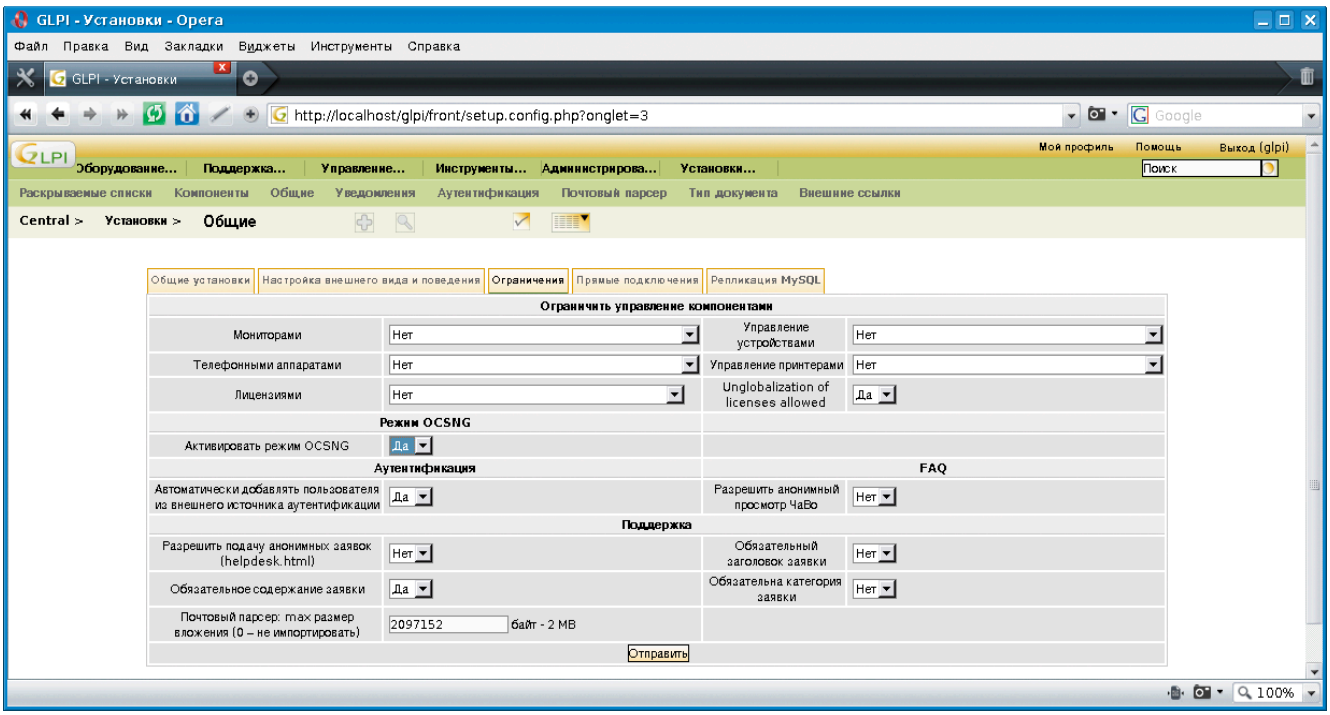
Параметры в User notifications позволяют вывести соответствующее предупреждение пользователю, разрешить ему отмену выполнения задачи. Созданный пакет загружается в каталог /var/lib/ocsinventory-reports/download/timestamp.

При этом timestamp получается уникальным.

```
$ ls /var/lib/ocsinventory-reports/download/
1241705351  1241722723

$ ls 1241722723
1241722723-1  info
```

При установке GLPI следует выполнить все рекомендации программы



Окно активации режима OCSNG

Файл info содержит настройки пакета, а 1241722723-1 является собственно программой.

Переходим в меню Deployment → Activate, выбираем нужный пакет и нажимаем ссылку Activate. Вводим в появившемся окне адрес вида https://server/download/, при этом timestamp к URL будет добавлен автоматически, нажимаем «Отправить». В ответ должны получить сообщение:

```
Package activated, it can now be deployed.
```

Теперь выбираем компьютер, на котором хотим установить пакет, переходим в меню Customization, в самом низу выбираем ссылку add package, указываем на пакет и нажимаем в поле Affect. Подтверждаем свой выбор. В Customization появится информация о состоянии задачи, а в таблице в Activate будет выводиться статистика.

По умолчанию агент подключается к серверу раз в сутки, тогда и будет произведена установка. Можно ускорить этот процесс, вызвав подключение принудительно, как это показано выше. После подключения агента к серверу состояние пакета должно измениться с WAITING_NOTIFICATIONS на NOTIFIED, а затем Success. Пакет будет сохранен в каталоге C:\Program Files\OCS Inventory Agent\download\TIMESTAMP. А все связанные сообщения можно найти в файле download.log.

Кроме выдачи информации о «своем» компьютере, агенты в разных подсетях сканируют сеть в поисках MAC-адресов, принадлежащих других системам. Такая функция называется IP discovery и позволяет находить другие устройства, на которые нельзя установить агент (например, свитчи, принтеры и так далее).

Установка GLPI

Установка GLPI достаточно проста. В репозиториях дистрибутивов нужный пакет есть, но его версия обычно сильно отстает.

```
$ sudo apt-cache search glpi
glpi - IT and Asset management software

$ sudo apt-cache show glpi | grep -i version
Version: 0.68.3.2-1
```

Актуальной на момент написания статьи является версия 0.71.5, вышедшая в январе 2009 года. Кроме этого, на странице загрузки доступен предрелиз 0.72-RC2 и срез CVS-архива.

Для установки просто распаковываем скачанный архив в корневой каталог веб-сервера:

```
$ sudo tar xzvf glpi-0.71.5.tar.gz -C /var/www
$ cd /var/www/glpi
```

Устанавливаем для некоторых каталогов владельца и группу-владельца:

```
$ sudo chown www-data:www-data config files files/* inc
```

Далее набираем в браузере http://localhost/glpi выбираем язык (в списке есть русский), принимаем условия GPL и следуем указаниям мастера установки. Самый главный этап – «Проверка окружения на совместимость с GLPI», где следует внимательно прочитать и выполнить все рекомендации.

Например, по указанию мастера параметр memory_limit в php.ini следует установить в значение, большее чем 32 Мб:

```
$ grep -i memory_limit /etc/php5/apache2/php.ini

memory_limit = 128M
```

Выполняем все требования, проверяем повторно и, если все нормально, нажимаем Continue. Теперь собственно

установка – вводим данные для доступа к MySQL, название базы данных, и все.

Чтобы GLPI автоматически проверял почту, отправлял уведомления, следует создать задание для пользователя, от имени которого работает веб-сервер (нужен пакет php5-cli):

```
$ sudo crontab -u www-data -e

*/5 * * * * /usr/bin/php5 ↵
     /var/www/glpi/front/cron.php &>/dev/null
```

По умолчанию в GLPI создаются четыре учетные записи с разными правами и возможностями (через дробь указан пароль):

- **glpi/glpi** – администратор;
- **tech/tech** – технический специалист;
- **normal/normal** – обычная учетная запись (возможность просмотра данных);
- **post-only/post-only** – только обращение в службу поддержки.

GLPI поддерживает импорт учетных данных из AD или другой LDAP.

Регистрируемся в системе как glpi. Для локализации интерфейса в меню Setting → Select Language выбираем русский язык, после этого все новые учетные записи будут использовать по умолчанию выбранный язык. Новые пользователи добавляются в одноименной вкладке, там несколько некорректный перевод. Так, логину соответствует поле «Имя пользователя», это иногда сбивает с толку. Чтобы не было путаницы, можно изменить значение в файле /var/www/glpi/locales/ru_RU.php:

```
$LANG["setup"][18]="Имя пользователя";
```

Далее переходим в меню «Установки (Setup) → Общие (General setup)» и устанавливаем «Активировать режим OCSNG (Activate OCSNG mode)» в «Да». После этого появится новая вкладка «Режим OCSNG» (OCSNG Mode).

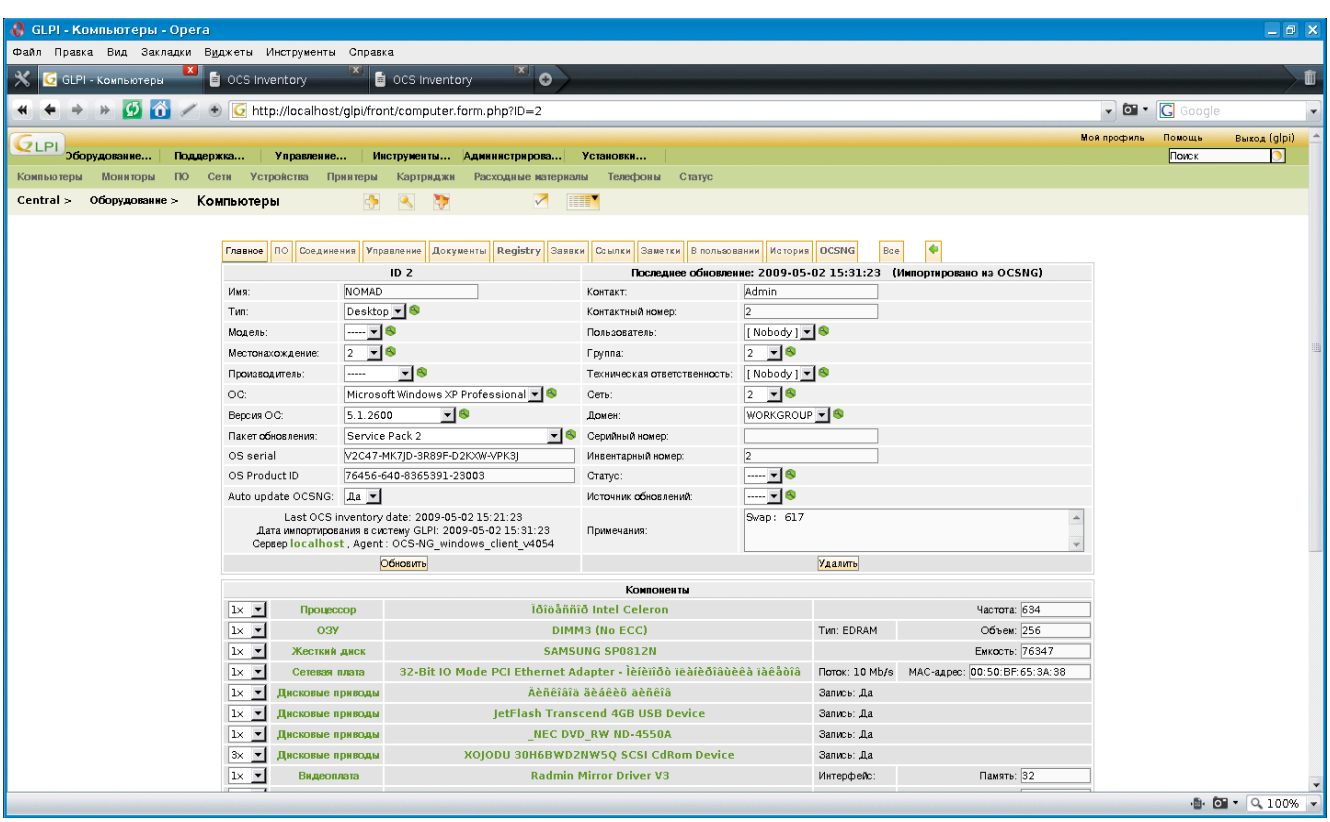
Если OCSNG и MySQL установлены на локальной машине, то данные для подключения к OCSNG будут найдены автоматически. Иначе необходимо будет заполнить информацию о сервере OCSNG вручную.

По умолчанию синхронизируется только часть параметров, чтобы в базу данных GLPI были перенесены и компоненты компьютеров, следует разрешить их синхронизацию, установив флажок напротив нужного в положение «Глобальный импорт».

Кроме этого, во вкладке «Инструменты» появится пункт OCSNG, при помощи имеющихся здесь ссылок можно производить синхронизацию и импортирование компьютеров между OCSNG и GLPI.

Полученные данные появляются во вкладке «Оборудование». Здесь несколько подпунктов, переход в некоторые из них позволяет получить список некоторых компонентов, входящих в компьютер («Мониторы», «Принтеры»), отдельного оборудования («Картриджи», «Телефоны»), а также ПО. Импортированные компьютеры доступны в одноименном подпункте.

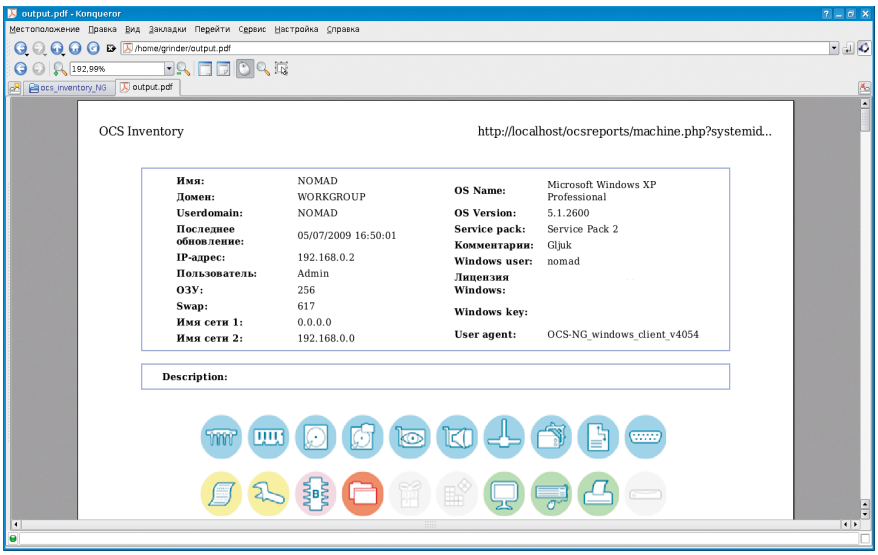
Выбрав компьютер или устройство, мы получаем доступ к 12 вкладкам, в которых можно просмотреть и скорректировать данные об оборудовании, сопоставить ответственного, просмотреть заявки, добавить заметки, сделать отметку о выдаче во временное использование, просмотреть историю и так далее.



Информация об оборудовании, импортированная с OCSNG в GLPI, отображается некорректно

К сожалению, на данный момент список импортированных с OCSNG компонентов компьютера, написанный на русском языке, выводится нечитаемым текстом.

Пользователей GLPI можно объединить в группы, кроме этого существует более глобальное понятие – «Организация». Сразу после установки создается «Основная организация», в которую и будут включены все компоненты. Предусмотрено создание других организаций с установлением подчиненности между ними (структуры). Но работа с организациями реализована неудобно, так перенос техники в другую организацию усложнен и неудобен. Предусмотрен экспорт данных в PDF, CVS и SLK (Symbolic Link).



Файл PDF, сгенерированный в OCSNG, с информацией о системе

По умолчанию при экспорте в PDF вместо русских букв выводятся знаки вопросов, это происходит по двум причинам: стандартная функция экспортирует данные в кодировке ISO-8859-1, которую и поддерживает используемый по умолчанию шрифт. Подсказка была найдена на форуме OPENNET [6]. Заменяем в скрипте /var/www/glpi/inc/export.function.php вызов функции utf8_decode на utf8_decode_cyr:

```
$ sudo perl -p -i -e 's/utf8_decode/utf8_decode_cyr/g' ↵
      export.function.php
inc/export.function.php:
```

И добавляем в export.function.php описание самой функции utf8_decode_cyr:

```
function utf8_decode_cyr($value){
        return iconv("UTF-8","Windows-1251",$value);
}
```

По умолчанию для экспорта используется шрифт Helvetica, его бы я и рекомендовал оставить. Если заменить шрифт другим, его имя придется править не только в двух местах файла export.function.php:

```
$ cat export.function.php | grep -i selectFont
$pdf->selectFont(GLPI_ROOT."/lib/ezpdf/fonts/ ↵
      Helvetica.afm");
```

Но и в двух файлах, находящихся в lib/ezpdf.

Теперь шрифт. Для конвертирования TTF-шрифта в Postscript type 1 потребуется утилита ttf2pt1.

```
$ sudo apt-get install ttf2pt1
```

Запускаем:

```
$ ttf2pt1 -l cyrillic -A Helvetica.ttf Helvetica
```

Теперь копируем файлы вместо старых, не забыв подправить права:

```
$ sudo cp -v Helvetica* /var/www/glpi/lib/ezpdf/fonts/
```

```
`Helvetica.afm' -> `/var/www/glpi/lib/ezpdf/fonts/Helvetica.afm'
`Helvetica.t1a' -> `/var/www/glpi/lib/ezpdf/fonts/Helvetica.t1a'
`Helvetica.ttf' -> `/var/www/glpi/lib/ezpdf/fonts/Helvetica.ttf'
```

Исправленный вариант шрифтов, можно найти в разделе «Исходный код» сайта журнала www.samag.ru . После этого PDF будет выводиться корректно.

Установка плагинов для GLPI производится простой распаковкой в подкаталог glpi/plugins, после чего плагин будет доступен для настройки в меню «Установки → Плагины». С сайта проекта можно скачать приблизительно 50 самых разнообразных плагинов.

Заключение

Интерфейсы, как OCSNG, так и GLPI, достаточно просты для освоения, нужно потратить полчаса, и вы будете хорошо ориентироваться. К сожалению, до конца вопрос локализации так и не решен. Так, для Windows в OCSNG неправильно отображаются кириллические наименования установленных программ и компонентов оборудования. Обсуждение всех вопросов по локализации можно найти на форумах проекта OCSNG и OPENNET [6], некоторым они помогают, у некоторых не получается все решить.

1. Сайт проекта OCS Inventory NG – http://www.ocsinventory-ng.org.
2. Сайт проекта GLPI – http://glpi-project.org.
3. Яремчук С. Учет оборудования с Kwok Information Server. //Системный администратор, №10, 2008 г. – С. 40-43.
4. Страница проекта dmidecode – http://www.nongnu.org/dmidecode.
5. Инвентаризация компьютерной и оргтехники. OCS Inventory – http://eugene-online.blogspot.com/2008/04/ocs-inventory.html.
5. Архив с исправлениями для агента Windows – http://switch.dl.sourceforge.net/sourceforge/ocsinventory/OCSNG_WINDOWS_AGENT_1.02_RC2_OTEA.zip.
6. Обсуждение проблем локализации OCSNG – http://www.opennet.ru/openforum/vsluhforumID3/14092.html и http://forums.ocsinventory-ng.org/viewtopic.php?id=603.
7. Страница Wiki проекта GLPI на русском – http://glpi-project.org/wiki/doku.php?id=ru:welcome.

Партнерская сеть компании Fast Reports охватывает весь мир. Среди партнеров Fast Reports есть фирмы-разработчики отчётов и дополнительных возможностей к генераторам отчетов FastReport, системные интеграторы средств автоматизации бизнеса, консалтинговые компании.

Devrace SOFTWARE DEVELOPMENT

Компания Devrace разрабатывает программное обеспечение для Delphi и C++ Builder программистов. Работает над созданием с различных библиотек компонент (общего и специального назначения) и дополнительных утилит, которые позволяют повысить качество и скорость разработки. Компания Devrace специализируется на разработке программного обеспечения для специалистов, которые используют продукты для разработки Embarcadero CodeGear® Delphi™, CodeGear ® C++ Builder и CodeGear ® InterBase®, Fast Reports.

www.devrace.com

FS FrontSoft
software development

ООО "ФронтСофт" занимается индивидуальной разработкой, внедрением и сопровождением: программного обеспечения, программно-аппаратных комплексов с использованием программных разработок Fast Reports для формирования и печати документов.

www.frontsoft.ru

POLE SOFT Technologies Group

Автоматизация учёта и управление торговлей, "БОЛЬШИЕ" технологии для малого и среднего бизнеса с использованием технологий Fast Reports для Business Intelligence

www.polesoft.ru

Компания «Паритет Софт» занимается:
- разработкой, распространением, внедрением и поддержкой программного обеспечения для бухгалтерского учёта «Главный бухгалтер» с использованием программных разработок Fast Reports для формирования и печати отчётности;
- полным сопровождением бухгалтерского учета с созданием отчетности.

www.paritetsoft.ru

RuNetSoft

Основные направления деятельности компании RuNetSoft - разработка ПО (программного обеспечения) на заказ и внедрение готовых программных продуктов сторонних производителей. Высококвалифицированные разработчики реализуют проекты любой степени сложности, которые могут быть ориентированны на любую сферу бизнеса в диапазоне от Интернет-проектов до бизнес-приложений многоуровневой клиент-серверной архитектуры с использованием разработок Fast Reports для Business Intelligence.

www.rns-soft.ru

Fast Reports
Reporting must be Fast!

Компания Fast Reports предлагает программное обеспечение для организации отчетности. Программный комплекс включает в себя наборы компонентов для разработчиков отчетов, решения для бизнес пользователей, аналитиков и системных администраторов.

www.fastreport.ru

FASTREPORT® 4 VCL - генератор отчётов для Delphi / C++Builder.

FastReport® 4 VCL - это набор компонентов для построения отчетов. Представляет собой сочетание дизайнера, генератора и Preview отчетов. FastReport написан на 100% Object Pascal и может быть установлен в Delphi 4-2009 и C++Builder 4-2009.

FASTCUBE - инструмент оперативного анализа данных

FastCube позволит Вам без лишних затрат сил и времени проанализировать данные, получить сводные таблицы (срезы данных), построить отчеты и графики. Это удобное средство оперативной аналитической обработки больших массивов данных.

FASTREPORT®.NET

Генератор отчетов с широчайшими возможностями для Windows Forms и ASP.NET. Совместим с Microsoft Visual Studio 2005 и 2008, .NET Framework 2.0 и выше. Любые .Net-среды разработки. Самостоятельный визуальный дизайнер отчётов.

FASTREPORT® STUDIO - генератор отчётов для бизнес-пользователей

Вам нужен универсальный генератор отчётов?
Генератор отчётов FastReport Studio Business Edition включает в себя мощный дизайнер отчётов, средства для разработки и множество демонстрационных отчётов.

FASTREPORT® SERVER - сервер отчётов

FastReport Server дополняет комплекс программ Fast Reports.
FastReport Server - мощное и полнофункциональное решение для организации корпоративной отчётности, содержащее все инструменты для создания и доставки отчётов.

Полный список партнёров, продуктов и услуг - на сайте www.fastreport.ru

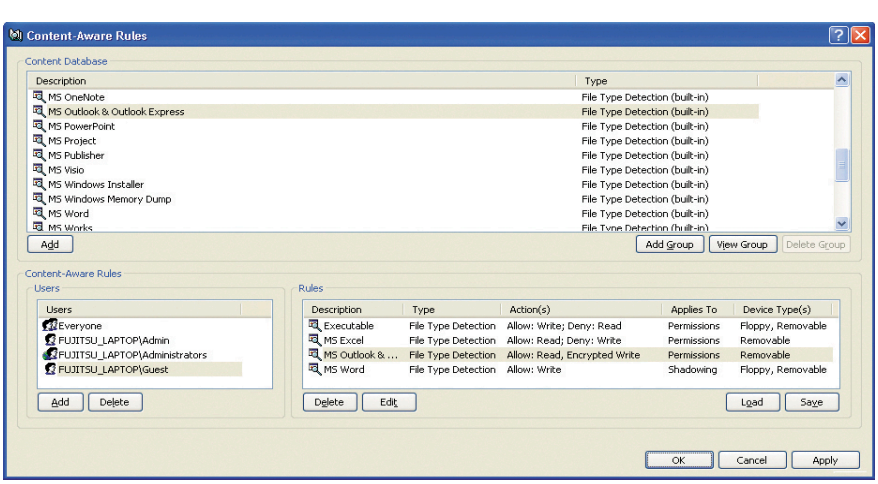
«Облачные» перспективы защиты корпоративных endpoint-компьютеров

Подлинными изобретателями и первыми «промышленными» внедренцами столь популярных сегодня технологий «облачных» вычислений (Cloud Computing) были не Amazon, IBM или Sun, а кибер-криминальные технологи, которые уже 10 лет назад эксплуатировали пиринговые «варезные сети», представлявшие, по сути, прототипы современных распределенных сетей Cloud Computing – такой, на первый взгляд, парадоксальный, но, если вдуматься, небезосновательный вывод сделал в своем блоге [1] Рювен Коэн (Reuven Cohen), основатель и главный технолог компании Enomaly, разработчика программных Cloud-платформ.

Столь же небезосновательно сразу после анонса Microsoft их Cloud Computing технологии Live Mesh главный редактор по технологиям еженедельника eWeek Insider Channel Франк Олхорст (Frank Ohlhorst) предупреждал о ее деструктивном влиянии на корпоративную информационную безопасность (ИБ). В своей статье «Microsoft Live Mesh – следующая большая угроза бизнесу» [2] он назвал Live Mesh «антитезой управления сетевым доступом и информационной безопасности endpoint-компьютеров». Причиной опасений Олхорста послужила уникальная способность технологии Live Mesh преодолевать периметры частных корпоративных сетей вне зависимости от политик защищающих их межсетевых экранов (МЭ) и NAT-шлюзов. Прообразом Live Mesh, по его мнению, была система IP-телефонии Skype, всепроникающую «силу» которой уже в полной мере ощутили практически все ИТ-организации.

Подобные комментарии, очевидно, не добавляют оптимизма в отношении завтрашних перспектив внедрения Cloud Computing со стороны руководителей и главных специалистов служб ИБ организаций финансового сектора экономики.

Равно как и сегодня, когда невиданные доселе «вычислительные тучи» только собираются на далеком заморском горизонте, ситуация с обеспечением ИБ оконечных вычислительных устройств (рабочих станций, десктопов и ноутбуков) организаций далека от безоблачной, о чем свидетельствует свежая статистика организации Ponemon Institute, которая в феврале опубликовала результаты исследований размера ущерба от утечек данных в организациях США и Великобритании за 2008 год. Согласно этим отчетам, угрозы корпоративной ИБ со стороны инсайдеров в Америке не уменьшаются (прирост 2-5%), а в Европе – существенно возрастают (прирост 22-28%), причем подавляющая часть случаев утечек данных связана с нарушением ИБ компьютеров сотрудников.



Новый функционал в DeviceLock 6.4 – «контентно-зависимые» правила на уровне файловых операций

Поэтому без преувеличения можно сказать, что для специалистов в области ИБ кредитно-финансовых организаций один из важнейших вопросов завтрашнего дня состоит в том, как на уровень инсайдерских угроз и, прежде всего, защищенность endpoint-компьютеров повлияет внедрение в корпоративные ИТ-технологий Cloud Computing.

В технологической интерпретации это вопрос о том, сможет ли индустрия ИБ использовать уникальные внутренне присущие архитектурам Cloud Computing характеристики – глобальную распределенность, динамическую масштабируемость и оперативную связность – для повышения эффективности и надежности работы средств защиты информации (СЗИ) множества оконечных вычислительных узлов?

Следует отметить, что в последние три года наблюдается постепенный прогресс участников отрасли ИБ в этом направлении.

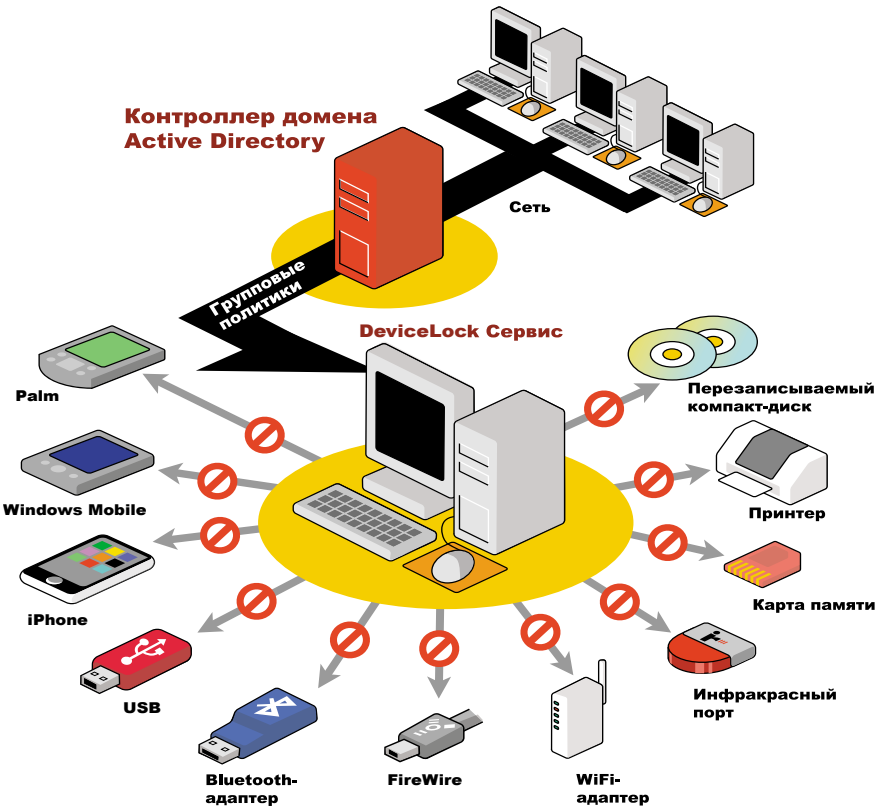
Исторически, первым реальным примером использования преимуществ Cloud Computing – еще до выделения этой технологии в отдельный отраслевой сегмент – стало предоставление услуг аутсорсинга ИБ для корпоративных клиентов. Один из пионеров этого движения – «Лаборатория Касперского», услуга Hosted Security Services [3] которой пользуется популярностью как в России, так и за рубежом. В качестве другого – недавнего по времени – примера следует отметить анонс в октябре 2008 года трехлетнего плана [4] компании Symantec по предоставлению всех своих продуктов ИБ в виде услуг SaaS.

Следующим значительным шагом отрасли ИБ стало использование вы-

сокого уровня взаимосвязности сред Cloud Computing для ускорения процессов сбора и проверки сигнатур вредоносных программ. В 2008 году были введены в эксплуатацию системы Smart Protection Network от компании Trend Micro и Artemis от McAfee. В упрощенном виде идея работы этих систем состоит в том, что исполнительные агенты на компьютерах не ждут обновления базы сигнатур с сервера, а по каждому подозрительному объекту считают хэш-сумму и отсылают ее в Cloud-сеть производителя, после чего эти хэш-суммы в онлайн-режиме сравниваются со всеми имеющимися в Cloud сигнатурами и результат возвращается агенту. В результате как скорость выявления сигнатур вредоносных кодов, так и оперативность реагирования на них возрасли на порядок – причем без увеличения вычислительной нагрузки на защищаемые компьютеры.

Наконец, самой современной тенденцией использования Cloud Computing в отрасли ИБ стало использование супер-инфраструктур «вычислительная платформа как услуга» (Platform-as-a-Service или PaaS) в качестве платформ, на которые небольшие вендоры программных СЗИ портируют свои продукты и предоставляют своим клиентам доступ к ним как к услугам. Иначе говоря, они используют платформы PaaS для создания собственных услуг аутсорсинга ИБ и предоставления их в виде Software-as-a-Service. В конечном итоге, это выгодно пользователям, поскольку состав провайдеров услуг ИБ не ограничивается только крупнейшими игроками типа Symantec, McAfee и Trend Micro, а появляется выбор между множеством услуг мелких, но более заботливых для клиентов суб-провайдеров. Примером такой трансформации продукта в услугу ИБ служит портирование компанией FullArmor своей программы PolicyPortal [5] на платформу Windows Azure, в результате чего этот продукт стал доступен для клиентов FullArmor непосредственно через Интернет как экономичная услуга централизованного управления политиками ИБ и конфигурирования endpoint-компьютеров.

Очевидно, не каждый продукт ИБ рационально использовать в виде отдельной услуги – например, из-за специфики его функционала. Тем не менее, если продукт качественный, он может оказаться весьма полезным как один из компонентов функционально полного набора интегрированных сервисов аутсорсинга ИБ. Приятно радуют в этом отношении популярные российские программные СЗИ. Например, немецкий провайдер аутсорсинга ИБ Logica Managed Services Deutschland в качестве одного из компонентов своих услуг по информационной защите компьютеров клиентов использует программный комплекс DeviceLock производства компании «Смарт Лайн Инк», мирового технологического лидера в этой области.



DeviceLock контролирует все типы внешних устройств посредством групповых политик

DeviceLock – это система централизованного контроля доступа пользователей к периферийным устройствам и портам ввода-вывода персональных компьютеров и серверов под управлением ОС Microsoft Windows. DeviceLock позволяет контролировать все типы локальных каналов утечки на компьютерах пользователей в корпоративной ИС и полный спектр портов и внешних устройств. В новой версии DeviceLock 6.4 принципиально повышена гранулированность контроля за привилегиями и действиями пользователей за счет поддержки функции детектирования и фильтрации типов файлов для любых операций файловой системы. Обеспечиваются перехват, экстракция, детектирование типа и блокирование файловых объектов во всех локальных каналах утечки данных защищаемого компьютера, при этом администраторы безопасности могут дополнительно задавать гибкие правила событийного протоколирования операций и теневого копирования данных с точностью до типов файлов.

В планах компании «Смарт Лайн Инк» – дальнейшее развитие решений и услуг по информационной защите endpoint-компьютеров на базе DeviceLock.

Алексей Лесных,
менеджер по развитию бизнеса
компании «Смарт Лайн Инк»

1. http://www.elasticvapor.com/2008/11/fraud-as-service-did-criminals-invent.html.
2. http://blogs.channelinsider.com/tech_tidbits/content/new_products/microsoft_live_meshthe_next_big_security_threat_for_business_1.html.
3. http://www.kaspersky.ru/hosted_security.
4. http://www.zdnetasia.com/news/security/0,39044215,62046931,00.htm.
5. http://www.fullarmor.com/products-policyportal.htm.

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

Андрей Дугин

Если ваши системы обнаружения вторжения вызывают беспокойство тем фактом, что не сигнализируют своевременно о сбоях в функционировании или реконфигурации сети, не спешите искать дорогостоящие решения. Возможно, бесплатные Open Source-решения после некоторой реконфигурации покажут себя нисколько не хуже.

В крупных компаниях обязанности администраторов сети и сетевой безопасности могут быть распределены между разными подразделениями. Системы IDS/IPS после внедрения выполняют сугубо роль обнаружения атак без активного вмешательства в трафик. Этот этап может длиться несколько лет.

Активная защита периметра выполняется файерволом, доступы к сетевым ресурсам внутри компании реализуются либо с помощью отдельных брандмауэров, либо посредством ACL (Access Control Lists), а обнаружение аномального сетевого трафика производится сенсором, на который направляется копия трафика через «зеркалированный» (SPAN-порт) коммутатор. Если сетевые администраторы и администраторы систем безопасности не извещают друг друга о проводимых работах в сети, вполне может случиться ситуация, при которой разбирается SPAN-сессия, и сенсор перестает отрабатывать события. Также возможен сбой работы как самого сенсора, так и программ мониторинга. В компаниях с большим количеством сенсоров это можно заметить далеко не сразу, и соответственно потерять данные, возможно, необходимые для расследования инцидента.

Исходим из того, что у нас есть 10 сенсоров, дополнительных денег на ПО и железо, кроме лицензий, нет, а задачу выполнить надо. Cisco systems предлагает для мониторинга и управления сенсорами программу IPS Manager Express, которая является бесплатной для скачивания пользователям с сервисным контрактом. Ограничение – максимум 5 устройств. Логично, что можно использовать 2 ПК, в которые завести управление по 5 сенсоров.

Проблемы, с которыми сталкиваешься, но не всегда сразу замечаешь:

- При реконфигурации сети разбирается SPAN-сессия либо меняются идентификаторы VLAN.
- Происходит сбой в работе сенсора либо программы мониторинга.

Настройка

Своевременное реагирование на вышеописанные проблемы можно обеспечить с помощью ПО MRTG. Рассмотрим пример настройки MRTG под Debian Linux.

Устанавливаем MRTG:

```
#apt-get install mrtg
```

Для того чтобы было возможно осуществлять мониторинг IPS, необходимо включить на нем управление по SNMP и прописать значения read-only и read-write community. Последний параметр связан исключительно с особенностями сенсора. Тем не менее стоит учесть, что открытое на запись community дает возможность всем, кто имеет доступ по сети к сенсору, изменять его конфигурацию с помощью SNMP. В целях безопасности настоятельно рекомендуется изменить значения по умолчанию public и private на более сложные community.

Через CLI возможность управления по SNMP конфигурируется следующим набором команд:

```
sensor1#configure terminal
sensor1(config)#service notification
sensor1(config-not)#enable-set-get true
sensor1(config-not)#read-only-community DlY@_$en$ora
sensor1(config-not)#read-write-community Dly@_@dmln@_$en$ora
sensor1(config-not)#exit
Apply Changes?[yes]:
sensor1(config)#exit
```

Конфигурация интерфейсов записывается в файл /etc/mrtg.cfg с помощью команды:

```
# cfgmaker read-only-community@sensor.address > ↵
      /etc/mrtg.cfg
```

Но в этом случае затем придется существенно править конфигурационный файл руками. Хоть без этого все равно не обойтись, рекомедую для IDSM2 создавать настройки с параметрами:

```
# cfgmaker --no-down read-only-community@sensor.address > ↵
      /etc/mrtg.cfg
```

В целях безопасности рекомендуется не давать доступ к файлу всем:

```
# chmod 640 /etc/mrtg.cfg
```

У модуля IDSM2 определяется 6 интерфейсов:

- Interface 1 – loopback (lo);

- Interface 2 – GigabitEthernet0/7 (ge0_7);
- Interface 3 – GigabitEthernet0/8 (ge0_8);
- Interface 4 – sy0_1;
- Interface 5 – GigabitEthernet0/2 (ge0_2);
- Interface 6 – sy0_0.

Нас интересуют всего 2 из них:

- **GigabitEthernet0/2**, через который происходит управление и сбор событий;
- **GigabitEthernet0/7** (или 0/8 – в зависимости от настроек) – порт, на который приходит SPAN-сессия.

Если запускать cfgmaker без параметра --no-down – интерфейсы loopback, GigabitEthernet0/7 и GigabitEthernet0/8 будут в конфигурационном файле закомментированы, и придется раскомментировать тот интерфейс, который принимает SPAN.

Интерфейсы sy0_0 и sy0_1, как альтернативные TCP RST-интерфейсы, будут считаться активными.

Адаптация и кастомизация

По умолчанию загрузка интерфейса отображается в байтах/сек, шкала времени идет справа налево. Для того чтобы изменить направление шкалы, необходимо в конфигурационном файле /etc/mrtg.cfg раскомментировать строку:

```
Options[_]: growright, bits
```

и оставить те параметры, которые больше по вкусу администратору, либо приняты в компании. Параметр growright направляет шкалу времени вправо, а bits отвечает за отображение загрузки в битах/сек.

С каждого интерфейса IDSM2 в конфигурационный файл MRTG по умолчанию считываются следующие параметры, которые необходимо отредактировать:

```
MaxBytes[sensor1_5]: 1250000
Title[sensor1_5]: Traffic Analysis for 5 -- sensor1
PageTop[sensor1_5]: <h1>Traffic Analysis for 5 -- sensor1</h1>
--------------output omitted--------------------
 <td>Max Speed:</td>
 <td>1250.0 kBytes/s</td>
--------------output omitted--------------------
```

Красным шрифтом показаны несоответствия данных, полученных с помощью SNMP, реальным данным. По умолчанию интерфейсы перечисляются по номерам. Также можно заметить, что гигабитные интерфейсы сенсора MRTG определяет как 10-мегабитные. Cisco в своей документации (http://www.cisco.com/en/US/docs/security/ips/6.2/configuration/guide/ime/ime_troubleshooting.html#wp1020491) указывает, что MIB II поддерживаются сенсорами, однако корректность полученных данных не гарантируется. Соответственно в конфигурационном файле изменяем скорость в местах:

```
MaxBytes[sensor1_5]: 125000000
```

и

```
<td>Max Speed:</td>
<td>125.0 MBytes/s</td>
```

Если не редактировать скорость, то мониторинг загрузки будет работать, пока не превысится указанный порог. Если же нагрузка на интерфейс постоянно выше, то статистика собираться не начнет.

В итоге конфигурационный файл /etc/mrtg.cfg, полученный для 1-го сенсора, с учетом того, что нам нужен мониторинг только 2 интерфейсов, будет выглядеть приблизительно так:

```
# Created by
# /usr/bin/cfgmaker DlY@_$en$ora@sensor1


### Global Config Options

#  for UNIX
# WorkDir: /home/http/mrtg

#  for Debian
WorkDir: /var/www/mrtg

#  or for NT
# WorkDir: c:\mrtgdata

### Global Defaults

#  to get bits instead of bytes and graphs growing to the right
Options[_]: growright, bits

EnableIPv6: no


######################################################
# System: sensor1
# Description: Linux sensor1 2.4.30-IDS-smp-bigphys #2 SMP
# Sat Jul 12 04:12:55 UTC 2008 i686
# Contact: dugin
# Location: sensor1
######################################################


### Interface 2 >> Descr: 'ge0_7' | Name: 'ge0_7' | Ip:  | ↵
      Eth:  ###
#
Target[sensor1_2]: 2:DlY@_$en$ora@sensor1:
SetEnv[sensor1_2]: MRTG_INT_IP="" MRTG_INT_DESCR="ge0_7"
MaxBytes[sensor1_2]: 125000000
Title[sensor1_2]: Traffic Analysis for SPAN -- sensor1
PageTop[sensor1_2]: <h1>Traffic Analysis for SPAN -- sensor1</h1>
      <div id="sysdetails">
          <table>
               <tr>
                        <td>System:</td>
                        <td>sensor1 in sensor1</td>
               </tr>
               <tr>
                        <td>Maintainer:</td>
                        <td>dugin</td>
               </tr>
               <tr>
                        <td>Description:</td>
                        <td>ge0_7  </td>
               </tr>
               <tr>
                        <td>ifType:</td>
                        <td>ethernetCsmacd (6)</td>
               </tr>
               <tr>
                        <td>ifName:</td>
                        <td>ge0_7</td>
               </tr>
               <tr>
                        <td>Max Speed:</td>
                        <td>125.0 MBytes/s</td>
               </tr>
          </table>
      </div>

### Interface 5 >> Descr: 'ge0_2' | Name: 'ge0_2' | Ip:  | ↵
      Eth: '00-03-e4-72-38-0c' ###

Target[sensor1_5]: 5:DlY@_$en$ora@sensor1:
SetEnv[sensor1_5]: MRTG_INT_IP="" MRTG_INT_DESCR="ge0_2"
MaxBytes[sensor1_5]: 125000000
```

```
Title[sensor1_5]: Traffic Analysis for MGMT -- sensor1
PageTop[sensor1_5]: <h1>Traffic Analysis for MGMT -- sensor1</h1>
      <div id="sysdetails">
          <table>
               <tr>
                         <td>System:</td>
                         <td>sensor1 in sensor1</td>
               </tr>
               <tr>
                         <td>Maintainer:</td>
                         <td>dugin</td>
               </tr>
               <tr>
                         <td>Description:</td>
                         <td>ge0_2  </td>
               </tr>
               <tr>
                         <td>ifType:</td>
                         <td>ethernetCsmacd (6)</td>
               </tr>
               <tr>
                         <td>ifName:</td>
                         <td>ge0_2</td>
               </tr>
               <tr>
                         <td>Max Speed:</td>
                         <td>125.0 MBytes/s</td>
               </tr>
          </table>
      </div>
```

Добавляем новые сенсоры в конец конфигурационного файла:

```
# cfgmaker --no-down new_sensor_ro_community@ ↵
      new_sensor_address >> /etc/mrtg.cfg
```

Мониторинг

Когда в конфигурационный файл добавлены все сенсоры, из него можно делать HTML-страницу, на которой будет отображаться загрузка интерфейсов:

```
# indexmaker /etc/mrtg.cfg > /var/www/mrtg/index.html
```

Страница должна находиться в том же каталоге, который указан в конфигурации /etc/mrtg.cfg как:

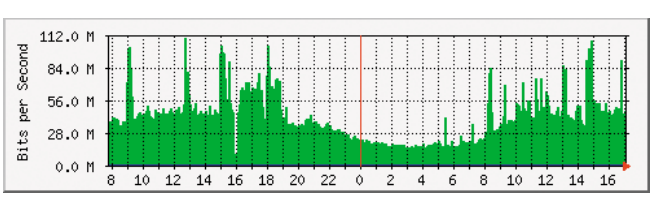


Рисунок 1. График загрузки SPAN-порта IDSM2 в норме

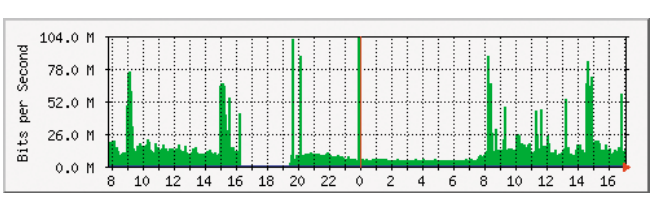


Рисунок 2. График загрузки SPAN-порта IDSM2 показывает резкий спад

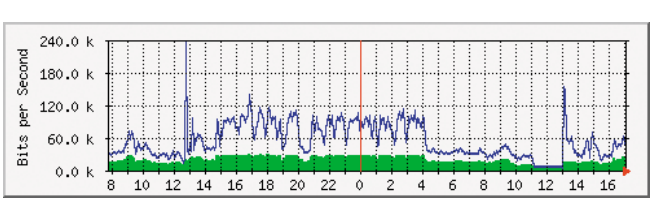


Рисунок 3. График загрузки порта управления

```
#  for Debian
WorkDir: /var/www/mrtg
```

Разумеется, также необходим веб-сервер. Особого конфигурирования не нужно, достаточно, чтобы он был запущен. Мониторинг после настройки производится через веб-браузер по адресу http://your.server.addres/mrtg.

Итак, после проведения настройки, каким образом можно узнавать о проблемах?

Приблизительно так выглядит график загрузки SPAN-порта IDSM2 в норме (см. **рис. 1**). Зеленым показан входящий в интерфейс трафик, синим – исходящий. Логично, что на слушающем порту не будет исходящего трафика.

MRTG по умолчанию снимает показатели с портов 1 раз в 5 минут, что можно заметить в cron. Это минимально возможный интервал опроса. Соответственно, когда график показывает резкий спад и длительное время находится около нуля, как показано на **рис. 2**, – значит разобрали SPAN-сессию или поменяли идентификаторы VLAN, завернутых в нее.

Но возможно, что перенесена нагрузка на другой коммутатор либо произошел сбой в работе модуля IDSM2. Необходимо зайти на интерфейс и послушать некоторое время:

```
sensor1# packet display gigabitEthernet0/7
```

чтобы понять, ходит ли вообще какой-либо трафик.

Причины того, что ни один пакет не пришел за определенное время:

- Разобрана SPAN-сессия. Однако в этом случае на порт будет приходить широковещательный и служебный трафик.
- Сетевики сменили номера VLAN, при этом забыли завернуть их в SPAN.
- Сбой в работе модуля IDSM2.

Последняя причина определяется следующим образом: при попытке зайти на веб-консоль управления IDSM2 через https java-апплет запускается, в Dashboard видно, что интерфейсы GigabitEthernet0/7 и 0/8 в состоянии down, затем вылетает ошибка, и веб-консоль закрывается. Поскольку вручную интерфейсами IDSM2 манипулировать не так просто, как с интерфейсами свитчей и роутеров, лучше рестартовать модуль:

```
sensor1# reset
```

График загрузки порта управления выглядит приблизительно так (см. **рис. 3**). В данном случае можно определить по наличию абсолютно ровной прямой, держащейся на определенном уровне, отличном от нуля, что в 11:10-11:20 произошел сбой программы управления, это привело к отсутствию сбора событий, а к 13:00 администратор рестартовал необходимые процессы.

Таким образом, приходим к выводу, что в данном случае нет крайней необходимости использовать дорогостоящие решения, и проблема со своевременным обнаружением отсутствия отработки событий или сбоя систем управления сенсорами сводится к минимуму исключительно с помощью бесплатного ПО при корректной его конфигурации.

Dr.WEB®

с 1992

Защити созданное

Больше, чем антивирус!

Антивирус — лидер в лечении активных заражений

Веб-антивирус — проверка веб-страниц в режиме реального времени и гарантированная загрузка только «чистого» контента из сети Интернет

Антируткит — надежная защита от действий вирусов, использующих rootkit-технологии

Антишпион — охрана конфиденциальной информации — лучшее в отрасли детектирование троянских программ и клавиатурных шпионов

Антиспам — высокая эффективность распознавания спама и других видов нежелательных сообщений при близком к нулю проценте ложных срабатываний

Родительский контроль — защита от кибер-преступности, направленной против детей

На базе технологий Dr.Web для Windows 5.0

Бесплатно демо на **30 дней**

www.drweb.com

Реклама

Настраиваем хранение логов в базе данных MySQL

Сергей Крутилин

Не всегда есть возможность зайти на удалённый сервер для просмотра журналов системы или приложений. Иногда возникает необходимость делегировать другому сотруднику задачи мониторинга. А может, под рукой не оказалось средств для удалённого доступа? Этих проблем можно избежать при помощи средств, настройка которых будет описана в данной статье.

Для решения поставленных целей нам понадобится следующее ПО – rsyslog (http://www.rsyslog.com) и phpLogcon (http://www.phplogcon.com). Первое будет записывать различные события журналов в базу данных MySQL, второе – предоставлять веб-интерфейс для их просмотра.

Необходимые требования:

- Сервер MySQL (http://www.mysql.com).
- Веб-сервер Apache (http://apache.org).
- PHP5 (http://php.net).
- Перед запуском rsyslogd системный демон syslogd должен быть остановлен и деактивирован в автозагрузке системы.

Примечание: все действия по установке ПО на *nix-сервере выполняем под пользователем root.

Установка rsyslog

Авторизуемся под учётной записью root на сервере с помощью консоли или используя ssh-клиент, удалённо (к примеру, putty – http://www.chiark.greenend.org.uk/~sgtatham/putty). Для работы с файлами на удалённом *nix-сервере можно использовать WinSCP (будет рассмотрена далее).

Загружаем последнюю стабильную версию (для порядка лучше создать директорию, в которой будут лежать все дистрибутивы, к примеру, это может быть /usr/Distr), после чего распаковываем полученный архив:

```
#mkdir /usr/Distr
# cd /usr/Distr/
#wget http://www.rsyslog.com/ ↵
      Downloads-req-viewsdownload-sid-1.phtml
# tar -zxf rsyslog-3.20.5
#cd rsyslog-3.20.5
```

Конфигурируем rsyslog (с поддержкой MySQL):

```
./configure CFLAGS="-I/usr/local/include/" ↵
      LDFLAGS="-L/usr/local/lib" --enable-mysql
```

После чего выполняем:

```
#make
#make install
```

Создаём базу MySQL для rsyslog, используя файл createDB.sql. В нашем случае он находится в директории /usr/Distr/rsyslog-3.20.5/plugins/ommysql/. Также нам необходим пользователь баз данных samaglog с паролем samagpassword, который имеет все права на созданную базу данных с именем Syslog:

```
# /usr/local/bin/mysql --user=root --password=password < ↵
      /usr/Distr/rsyslog-3.20.5/plugins/ommysql/createDB.sql
# /usr/local/bin/mysql --user=root --password=password
```

```
mysql>create user 'samaglog'@'localhost' identified by ↵
      'samagpassword';
mysql>GRANT ALL PRIVILEGES ON Syslog.* ↵
      TO 'samaglog'@'localhost';
mysql>quit;
```

Модифицируем rsyslog.conf. По умолчанию он находится в директории /etc. Включаем поддержку MySQL:

```
$ModLoad ommysql.so
```

Синтаксис записи событий в определённый файл схож с системным. Для базы MySQL он будет следующим:

```
*.*      >servername,dbname,user,password
```

Рассмотрим пример записи событий системы, связанных с безопасностью:

```
security.*      >127.0.0.1,syslog,samaglog,samagpassword
```

Запускаем демон rsyslogd со следующими параметрами:

```
rsyslogd -c3 -4 -f /etc/rsyslog.conf
```

где:

- c – обязательный параметр для определения совместимости со старыми версиями rsyslog,
- 4 – использование ipv4,
- f – путь к файлу конфигурации.

Дополнительную информацию о ключах запуска смотрите в документации по адресу http://wiki.rsyslog.com/index.php/Main_Page.

На этом установка rsyslog закончена, и мы переходим к phpLogcon.

Установка phpLogcon

Скачиваем последнюю стабильную версию phpLogcon и распаковываем её в новую директорию нашего веб-сервера:

```
# mkdir  /var/www/samaglogs/ && ↵
   cd /var/www/samaglogs/
# wget http://www.phplogcon.org/ ↵
   Downloads-req-getit-lid-54.phtml
# tar -zxf phplogcon-2.6.2.tar.gz
# cp -R phplogcon-2.6.2/src/* .
# rm -r phplogcon*
```

Создаём пустой файл конфигурации и устанавливаем необходимые разрешения:

```
# touch /var/www/samaglogs/ ↵
      config.php
# chmod 666 /var/www/samaglogs/ ↵
      config.php
```

Для запуска скрипта установки phpLogcon необходимо открыть в браузере следующий адрес: http://samag.local/samaglogs/install.php, где samag.local – это имя или IP-адрес вашего веб-сервера.

Следуя указаниям мастера, доходим до 7-го шага и в поле Source Type выбираем MySQL Native, как показано на **рис. 1**. Обращаю ваше внимание на то, что данные в поле Database Tablename чувствительны к регистру. Если после установки возникнет ошибка:

```
No syslog records found - Error Details:
Could not find the configured table, maybe misspelled or the
tablenames are case sensitive
```

Значит, вы неверно указали имя таблицы (вместо SystemEvents написали systemevents). В случае возникновения данной ошибки нужно исправить следующую строчку в файле /var/www/samaglogs/config.php:

```
$CFG['Sources']['Source1']['DBTableName'] = 'SystemEvents';
```

Практика

Рассмотрим пример использования нескольких экземпляров rsyslogd и phplogcon. Нам необходим мониторинг событий mail.* (почтового сервера).

Модифицируем в файле createDB.sql в /usr/Distr/rsyslog-3.20.5/plugins/ommysql две первые строчки:

```
CREATE DATABASE Maillog;
USE Maillog;
```

Остальное оставляем без изменений.

Аналогично установке rsyslog создаём базу и даём на неё все права пользователю samaglog:

```
# /usr/local/bin/mysql --user=root --password=password < ↵
      /usr/Distr/rsyslog-3.20.5/plugins/ommysql/createDB.sql
# /usr/local/bin/mysql --user=root --password=password
mysql>GRANT ALL PRIVILEGES ON Maillog.* ↵
      TO 'samaglog'@'localhost';
mysql>quit;
```

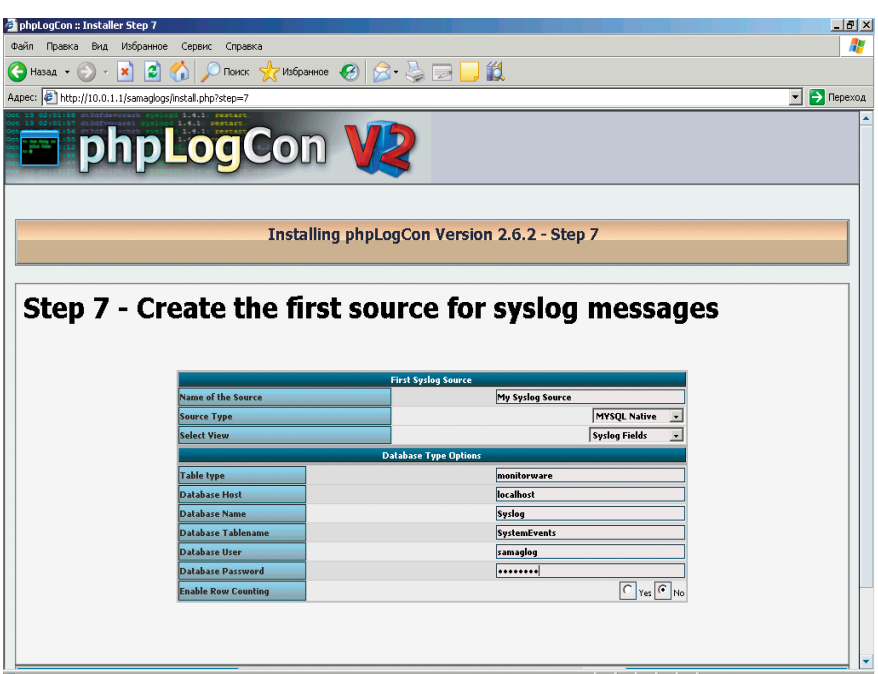


Рисунок 1. Настройка базы MySQL для phpLogcon

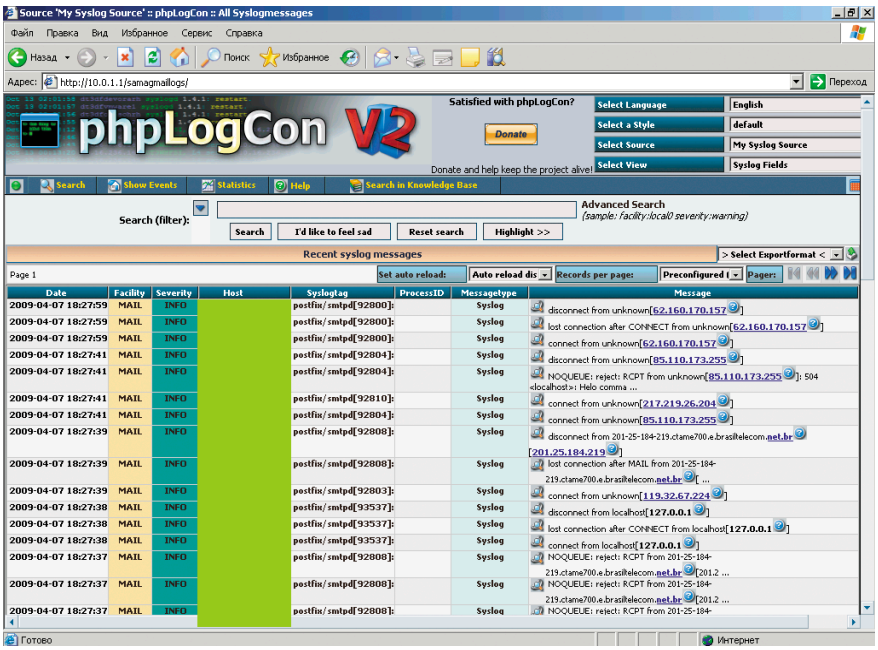


Рисунок 2. Пример работы phpLogcon

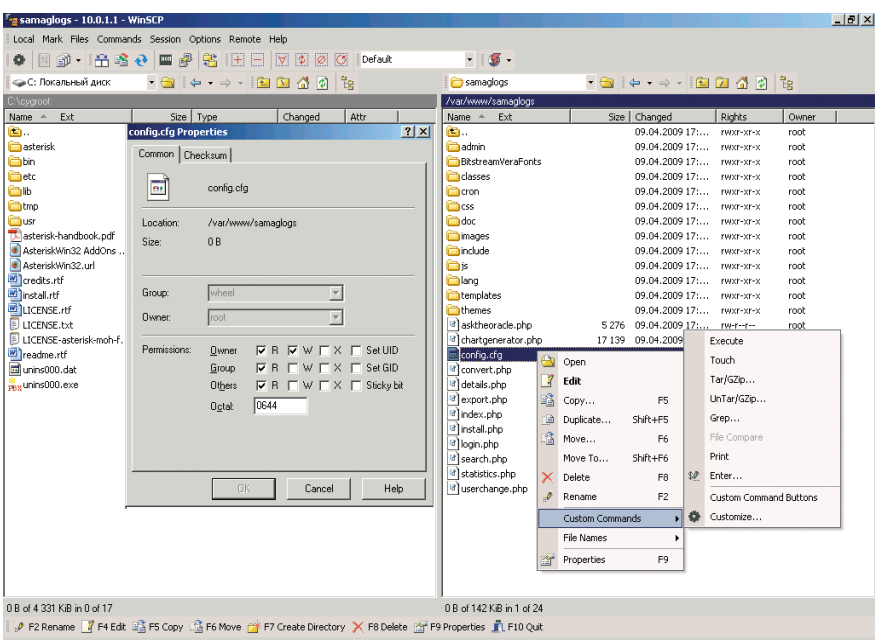


Рисунок 3. Пример работы WinSCP

Копируем файл /etc/rsyslog.conf в /etc/rsyslogmail.conf. После перечисления модулей в файле /etc/rsyslogmail.conf оставляем лишь:

```
mail.*      >127.0.0.1,maillog,samaglog,samagpassword
```

Запускаем rsyslogd со следующими ключами:

```
rsyslogd -c3 -4 -f  /etc/ rsyslogmail.conf ↵
     -i /var/run/samag.pid
```

где i – путь к pid-файлу, для второго экземпляра rsyslogd.

Копируем директорию /var/www/samaglogs/ в другую (к примеру, /var/www/samagmaillogs/).

Переходим в новую директорию и изменяем следующую строчку в конце файла config.php:

```
$CFG['Sources']['Source1'] ↵
     ['DBName'] = 'maillog';
```

Получаем отдельный мониторинг по адресу http://samag.local/samagmaillogs, как показано на **рис. 2**.

Как видно из примера, просматривать журналы намного удобнее через веб-интерфейс. Можно задавать различные фильтры, выбирать тип отображаемых данных и просматривать графики. Также rsyslog можно использовать для консолидации журналов нескольких серверов или сетевых устройств. Один интерфейс просмотра всегда удобнее, чем несколько.

WinSCP

В заключение рассмотрим упомянутый выше инструмент – WinSCP (http://winscp.net/eng/docs/lang:ru). Это файл-менеджер, который работает по протоколу SFTP (http://en.wikipedia.org/wiki/SFTP).

При помощи WinSCP вы можете работать с удалённым сервером *nix посредством демона SSH. WinSCP имеет следующие возможности:

- графический интерфейс;
- интеграция с ОС Windows (drag&drop, поддержка схем URL, ярлыки);
- все основные файловые операции.

Остальное вы найдёте на официальном сайте проекта по адресу http://winscp.net/eng/docs/lang:ru#возможности_программы.

Для работы с WinSCP необходимо настроить сервис SSH. Раскомментируйте в файле /etc/ssh/sshd_config следующую строчку:

```
Subsystem       sftp    ↵
     /usr/libexec/sftp-server
```

После чего перезапустите демон sshd, используя следующую команду:

```
kill -HUP $(cat /var/run/sshd.pid)
```

где /var/run/sshd.pid – путь к pid-файлу демона sshd.

Пример работы WinSCP показан на **рис. 3**.

Заключение

Оптимизация повседневных задач упрощает вашу работу. Единая система мониторинга позволит избежать многих проблем. Грамотное использование средств администрирования, будь то скрипты или сторонне ПО, в большинстве своём принесут только пользу.

Большой каталог свободно распространяемого ПО вы найдёте по адресу http://sf.net.

Выполнение произвольных команд в DNS Tools

Программа: DNS Tools от 2009-04-17.
Опасность: Высокая.
Наличие эксплоита: Нет.
Описание: Уязвимость существует из-за недостаточной обработки входных данных в параметрах «ns» и «host» в сценарии dig.php перед вызовом функции «system()». Удаленный пользователь может с помощью специально сформированного запроса выполнить произвольные команды на системе.

Пример:

```
http://[host]/dig.php?ns=||COMMAND HERE||&host= ↵
      mortal-team.net&query_type=NS&status=digging
```

URL производителя: gscripts.net/free-php-scripts/Other/DNS_Tools/details.html.
Решение: В настоящее время способов устранения уязвимости не существует.

Обход ограничений безопасности в Online Password Manager

Программа: Online Password Manager 4.1, возможно, другие версии.
Опасность: Средняя.
Наличие эксплоита: Нет.
Описание: Уязвимость существует из-за некорректного ограничения доступа к интерфейсу управления. Удаленный пользователь может установить параметр файла куки auth в значение действительной учетной записи и обойти механизм аутентификации.
URL производителя: www.esoftpro.com/web_scripts_online_password_manager.php.
Решение: В настоящее время способов устранения уязвимости не существует.

Множественные уязвимости в HP StorageWorks Storage Mirroring Software

Программа: HP StorageWorks Storage Mirroring Software версии до 5.1.1.1090.15.
Опасность: Средняя.
Наличие эксплоита: Нет.
Описание: 1. Уязвимость существует из-за неизвестной ошибки, которая позволяет злоумышленнику получить неавторизованный доступ к системе. Подробности уязвимости не сообщаются.

2. Уязвимость существует из-за неизвестной ошибки, которая позволяет злоумышленнику вызвать отказ в обслуживании. Подробности уязвимости не сообщаются.

3. Уязвимость существует из-за неизвестной ошибки, которая позволяет злоумышленнику выполнить произвольный код на целевой системе. Подробности уязвимости не сообщаются.
URL производителя: h18006.www1.hp.com/products/storage/software/sm.
Решение: Установите последнюю версию 5.1.1.1090.15 с сайта производителя.

Обход ограничений безопасности в Microsoft Internet Information Services

Программа: Microsoft Internet Information Services 5.1 и 6.0.
Опасность: Средняя.
Наличие эксплоита: Нет.
Описание: Уязвимость существует из-за ошибки при обработке WebDAV-запросов к директориям, требующим аутентификацию. Удаленный пользователь может с помощью специально сформированного HTTP GET-запроса, содержащего Unicode-символы и «Translate: f» HTTP-заголовок, обойти ограничения безопасности и, например, скачать файлы с защищенных каталогов. Удачная эксплуатация уязвимости также может позволить загрузку произвольных файлов в защищенные WebDAV-каталоги.
URL производителя: www.microsoft.com.
Решение: В настоящее время способов устранения уязвимости не существует.

Уязвимости в Alert Management System 2 в продуктах Symantec

Программа: Symantec AntiVirus Corporate Edition 9.0 MR6 and prior, 10.0 (все версии), 10.1 MR7 и более ранние версии и 10.2 MR1 и более ранние версии; Symantec Client Security 2.0 MR6 и более ранние версии, 3.0 (все версии) и 3.1 MR7 и более ранние версии; Symantec Endpoint Protection 11.0 MR2 и более ранние версии.
Опасность: Средняя.
Наличие эксплоита: Нет.
Описание: 1. Уязвимость существует из-за неизвестной ошибки в Intel LANDesk Common Base Agent (CBA), которая позволяет передать содержимое пакета в качестве аргумента функции CreateProcessA(). Удаленный пользователь может отправить специально сформированный TCP-пакет на порт 12174 и выполнить произвольные команды на системе с привилегиями учетной записи SYSTEM.

2. Уязвимость существует из-за ошибки проверки границ данных в службе Intel Alert Originator Service (iao.exe). Удаленный пользователь может отправить специально сформированный TCP-пакет на порт 38292, вызвать переполнение стека и выполнить произвольный код на целевой системе с привилегиями учетной записи SYSTEM.

3. Уязвимость существует из-за ошибки проверки границ данных в службе Intel Alert Originator Service (iao.exe) при обработке входных данных от процесса MsgSys.exe. Злоумышленник может вызвать переполнение стека и выполнить произвольный код на целевой системе с привилегиями учетной записи SYSTEM.

4. Уязвимость существует из-за ошибки дизайна в службе Intel File Transfer Service (XFR.EXE) при обработке путей к программам в запросах, отправленных на порт 12174/TCP. Злоумышленник, способный установить TCP-соединение с уязвимой системой, может выполнить произвольный код на системе с привилегиями учетной записи SYSTEM.
URL производителя: www.symantec.com.
Решение: Установите последнюю версию с сайта производителя.

Составил Александр Антипов

Делегируем права на перемещение учетных записей пользователей в Active Directory

Часть 3. Реализуем необходимые операции

Вадим Андросов

Продолжим изучать функции поддержки работы надстройки для Windows 2003 Server, реализующей перевод пользователя из одного подразделения в другое силами двух администраторов. В частности, будут затронуты вопросы программной манипуляции объектами Active Directory, работы с событиями с помощью WMI, модификации списков контроля доступа (ACL).

Делегирование полномочий менеджеру

Реализуем механизм автоматического делегирования прав на манипуляцию объектами пользователей. Конечно, эта операция может быть выполнена и вручную. Однако было бы гораздо удобнее назначить руководителя организационной единицы. Необходимые права должны быть предоставлены менеджеру автоматически. Соответственно при потере пользователем роли менеджера подразделения эти права нужно также автоматически отнять.

Такие вещи очень важны для предприятий со сложной структурой, когда администратор должен быть избавлен от необходимости выполнять взаимосвязанные действия вручную. Вместо этого достаточно выполнить только инициирующую операцию (назначение менеджера по персоналу отдела). Это существенно снизит уровень ошибок администратора (например, лишив пользователя роли менеджера можно забыть отключить у него соответствующие права), как следствие, повысив общий уровень безопасности системы.

Методы, связанные с делегированием, будут также реализованы в рамках единого класса надстройки UserMove.Engine.

Начнем с метода, предоставляющего менеджеру права на манипуляции с объектами пользователей в рамках заданного подразделения. В качестве параметров он получает путь к организационной единице и менеджеру, которому требуется предоставить необходимые полномочия.

```
function delegateOU(ouPath, userPath)
dim trustee, sec, acl, ace, ou, user, i
Set ou = getObject(ouPath)
Set user = getObject(userPath)
```

Для начала нужно привязаться к объекту «Список контроля доступа» текущей организационной единицы, как это делалось в методах проверки, реализованных в предыдущей части статьи [2].

```
Set sec = ou.Get("ntSecurityDescriptor")
```

```
Set acl = sec.DiscretionaryAcl
trustee = info.domainShortName & "\" & ↲
      user.samAccountName
for i = 0 to UBound(delegationClasses)
```

Затем по очереди создаются необходимые записи списка контроля доступа для каждого из классов массива delegationClasses. Они уже обсуждались при реализации проверки, поэтому подробно останавливаться на них не будем. Как будет видно из программы ниже, для этого нужно создать объект типа AccessControlEntry, проинициализировать необходимые поля и записать новый элемент в список контроля доступа с помощью метода списка AddAce.

```
  Set ace = createAcceptAce(ADS_RIGHT_DS_CREATE_CHILD Or ↲
      ADS_RIGHT_DS_DELETE_CHILD, delegationClasses(i), ↲
      ADS_FLAG_OBJECT_TYPE_PRESENT, Trustee)
```

Эта запись разрешает создавать в организационной единице объекты заданного типа.

```
  acl.AddAce ace

  Set ace = createAcceptAce(FULL_CONTROL , ↲
      delegationClasses(i), ↲
      ADS_FLAG_INHERITED_OBJECT_TYPE_PRESENT, Trustee)
```

Эта запись разрешает изменение свойств объектов, принадлежащих классу с идентификатором delegation Classes(i)

```
  acl.AddAce ace
next
```

Обновленный список привязывается к отделу. Важно не забыть вызвать метод организационной единицы SetInfo, чтобы изменения были физически сохранены.

```
sec.DiscretionaryAcl = acl
ou.Put "ntSecurityDescriptor", Array(sec)
ou.SetInfo
```

Кроме того, в первой части статьи [1] упоминалась специальная группа безопасности, содержащая всех менеджеров по персоналу. Вызов следующей подпрограммы будет добавлять текущего пользователя в такую группу. Его реализация будет рассмотрена позже.

```
makeManager user
end function
```

Рассмотрим функцию создания записи списка контроля доступа.

```
function createAcceptAce(accessMask, classGUID, flag, ↲
      trustee)
```

Сначала создается экземпляр класса AccessControlEntry, посредством которого будет предоставляться заданное право.

```
set createAcceptAce = CreateObject("AccessControlEntry")
createAcceptAce.AceType = ADS_ACETYPE_ACCESS_ALLOWED_OBJECT
createAcceptAce.accessMask = accessMask
```

Затем в зависимости от параметра flag целевой объект записывается в поле ObjectType или InheritedObjectType.

```
select case flag
  case ADS_FLAG_OBJECT_TYPE_PRESENT:
    createAcceptAce.ObjectType = classGUID
    createAcceptAce.AceFlags = ADS_ACEFLAG_INHERIT_ACE
  case ADS_FLAG_INHERITED_OBJECT_TYPE_PRESENT:
    createAcceptAce.InheritedObjectType = classGUID
    createAcceptAce.AceFlags = ADS_ACEFLAG_INHERIT_ACE + ↲
        ADS_ACEFLAG_INHERIT_ONLY_ACE
end select
createAcceptAce.Flags = flag
createAcceptAce.Trustee = trustee
end function
```

Потребуется и обратная функция для отмены делегирования. Сразу нужно оговориться, что фактически будет происходить удаление тех записей списка контроля доступа, которые добавлялись в функции делегирования выше. Если пользователь имеет те же права, например, участвуя в определенных группах, то их он не потеряет. То есть речь идет не об отмене делегирования управления организационной единицей как таковой, а, скорее, о функции, обратной delegateOU. Такое поведение было выбрано, чтобы минимизировать влияние надстройки на другие политики безопасности предприятия.

Листинг 1. Отмена делегирования управления организационной единицей

```
function undelegateOU(ouPath, userPath)
dim ou, user, i
set ou = getObject(ouPath)
set user = getObject(userPath)
for i = 0 to UBound(delegationClasses)
  undelegate ou, user, FULL_CONTROL , ↲
      delegationClasses(i), true
  undelegate ou, user, ADS_RIGHT_DS_DELETE_CHILD Or ↲
      ADS_RIGHT_DS_CREATE_CHILD, delegationClasses(i), false
next
makeNotManager user
end function
```

Отмена конкретного разрешения выполняется следующей подпрограммой. Все записи списка контроля доступа проверяются с помощью метода shouldBeDeleted и, если он вернул истину, удаляются.

Листинг 2. Удаление из ACL записей, позволяющих управлять организационной единицей

```
function undelegate(ou, user, oper, targetClass, isInherited)
Dim sec, acl, ace
Set sec = ou.Get("ntSecurityDescriptor")
Set acl = sec.DiscretionaryAcl
For Each ace In acl
 if shouldBeDeleted(user, ace, oper, ↲
      targetClass, isInherited) then
   acl.RemoveAce ace
 end if
Next
sec.DiscretionaryAcl = acl
ou.Put "ntSecurityDescriptor", Array(sec)
ou.SetInfo
end function
```

Следующая подпрограмма выясняет, нужно ли удалить определенную запись списка контроля доступа при удалении у пользователя прав менеджера по персоналу. Она проверяет, что запись относится к целевому пользователю и предоставляет права на управление организационной единицей.

Листинг 3. Требуется ли удалять запись ACL для отмены делегирования

```
function shouldBeDeleted(user, ace, oper, targetClass, ↲
```

```
      isInherited)
    shouldBeDeleted = false
    if ace.trustee <> (info.domainShortName & "\" & ↵
       user.samAccountName) then exit function
    dim classGUID
    if isInherited then
      classGUID = ace.InheritedObjectType
    else
      classGUID = ace.ObjectType
    end if
    if (classGUID = targetClass) and ↵
       isMask(ace.accessMask, oper) then
        if ace.AceType =
         ADS_ACETYPE_ACCESS_ALLOWED_OBJECT then
        shouldBeDeleted = true
        exit function
      end if
    end if
end function
```

Наконец, рассмотрим подпрограммы поддержки актуальности группы безопасности менеджеров по персоналу. Было принято решение назвать ее Staff Managers. Жестко прописанное название специальной группы не является самым удачным решением. Я остановился на нем, чтобы не отвлекать внимания от сущности надстройки мелкими деталями реализации. Вся функциональность описывается с помощью двух методов: makeManager (добавляет пользователя в группу менеджеров при назначении его руководителем организационной единицы) и makeNotManager (соответственно удаляет пользователя из группы. Для привязки к группе я использовал провайдер WinNT, чтобы не зависеть от расположения объекта группы в иерархии.

Итак, первый метод добавления пользователя в группу. В нем сначала происходит привязка к объекту группы с помощью провайдера WinNT. Для этого используется путь, состоящий только из домена и имени группы, например WinNT://MARKLAR/Staff Managers. Сама группа может быть расположена в любом контейнере. Затем составляется описатель пользователя в таком же формате (переменная userWinNTPath). Если пользователь уже является членом группы, функция завершает работу. В противном случае пользователь добавляется в группу с помощью метода add.

Листинг 4. Назначение менеджера по персоналу для подразделения

```
function makeManager(newManager)
dim managerGroup, userWinNTPath
set managerGroup = getObject("WinNT://" & ↵
      info.domainShortName & "/Staff Managers")
userWinNTPath = "WinNT://" & info.domainShortName & ↵
      "/" & newManager.samAccountName
if managerGroup.isMember(userWinNTPath) then exit function
managerGroup.add userWinNTPath
managerGroup.setInfo
end function
```

Метод удаления пользователя из группы очень похож на предыдущий. Главное отличие – если проверка показывает, что пользователь содержится в группе менеджеров по персоналу, он из нее удаляется.

Листинг 5. Отмена полномочий менеджера по персоналу для пользователя

```
function makeNotManager
dim managerGroup, userWinNTPath
set managerGroup = getObject("WinNT://" & ↵
      info.domainShortName & "/Staff Managers")
userWinNTPath = "WinNT://" & ↵
      info.domainShortName & "/" & user.samAccountName
if managerGroup.isMember(userWinNTPath) then
  managerGroup.remove userWinNTPath
  managerGroup.setInfo
end if
end function
```

Таким образом, группа Staff Managers будет всегда содержать действительный список менеджеров по персоналу организации.

Автоматизация делегирования

Функции делегирования и его отмены реализованы. Теперь остается только обеспечить их автоматическое выполнение при смене руководителя подразделения (см. **рисунок**).

Подробно реализация обработки событий на основе сценариев была рассмотрена в [3], поэтому ограничусь поверхностным описанием. В этом случае потребуется обрабатывать события изменения объекта организационной единицы (__InstanceModificationEvent).

Для фильтрации событий будет использоваться специальный язык WQL [4] (WMI Query Language). Он основан на SQL (точнее, является подмножеством структурированного языка запросов) и во многом повторяет его синтаксис. WQL содержит только оператор SELECT, модифицированный для работы с WMI (Windows Management Instrumentation). Особенности языка будут рассмотрены в статье по мере его использования.

Сначала рассмотрим сценарий установки обработчика событий. Для этого требуется создать и соответствующим образом проинициализировать объекты трех классов

- **__EventFilter.** С помощью объекта этого класса операционная система ставится в известность, какие именно события должны обрабатываться. Для этого используется запрос на языке WQL. Для нашего случая запрос будет иметь вид:

```
SELECT * FROM __InstanceModificationEvent ↵
      "WITHIN 5 WHERE TargetInstance ISA ↵
      'ds_organizationalunit'
```

  Это значит, что требуется обрабатывать события класса __InstanceModificationEvent для объектов типа ds_organizationalunit, наличие событий должно проверяться раз в 5 секунд.
- **ActiveScriptEventConsumer.** Объект этого класса инкапсулирует реакцию на событие и позволяет выполнить произвольный сценарий. Текст выполняемой программы должен быть сохранен в поле ScriptText.
- **__FilterToConsumerBinding.** Класс, объект которого используется для связи объектов предыдущих двух типов. Инициализация его полей включает механизм слежения за событиями. Удаление объекта этого класса приводит к прекращению обработки соответствующего события.

Сначала рассмотрим функцию, устанавливающую слушателя на событие. Первый ее параметр – название операции. Используется при формировании имен вспомогательных классов, чтобы они были нагляднее. Второй вариант – имя события, обработчик которого создается. Третий – имя файла с кодом обработки события.

```
Const FOR_READING = 1
Function addListener(sOperation, sEvent, sClass, sScript)
```

Сначала создается объект для работы с файловой системой. Текст сценария, выполняемого в ответ на событие, для удобства будет храниться в отдельном файле и загружаться при установке обработчика.

```
Set fso = createObject("Scripting.FileSystemObject")

  path = "\\.\root\directory\LDAP"
  Set objSWbemServices = GetObject("winmgmts:" ↵
      & "{impersonationLevel=impersonate}!" & path)
```

Затем подключаемся к классам, экземпляры которых будем создавать впоследствии. Классы __EventFilter и __FilterToConsumerBinding являются стандартными и уже присутствуют в пространстве имен root\directory\LDAP.

```
  Set eventFilterClass = ↵
    objSWbemServices.Get("__EventFilter")
  Set consumerClass = ↵
   objSWbemServices.Get("ActiveScriptEventConsumer")
  Set bindingClass = ↵
   objSWbemServices.Get("__FilterToConsumerBinding")
```

ActiveScriptEventConsumer нужно отдельно скомпилировать в этом пространстве имен с помощью команды:

```
mofcomp -N:root\directory\LDAP ↵
      %SYSTEMROOT%\system32\wbem\scrcons.mof
```

Затем с помощью метода SpawnInstance_ создаются экземпляры каждого класса и инициализируются необходимые поля. Вызов метода Put_ приводит к сохранению экземпляра в постоянном хранилище.

Инициализируем класс-фильтр. Основная настройка здесь – текст запроса на языке WQL, в котором указывается, события какого типа требуется обрабатывать. С помощью конструкции WITHIN 5 системе предписывается проверять очередь событий раз в 5 секунд. Операция перевода человека в другой отдел достаточно длительная, поэтому значение может быть и больше.

```
  set userFilter = eventFilterClass.SpawnInstance_()
  userFilter.Name = sOperation & "Filter"
  userFilter.QueryLanguage = "WQL"
  userFilter.Query = "SELECT * FROM " & sEvent & ↵
      " " & "WITHIN 5 WHERE TargetInstance ISA '" & ↵
      sClass & "'"
  userFilter.EventNamespace = "root\directory\LDAP"
  userFilter.Put_()
```

Код непосредственной обработки события загружаем из файла. В нем не должно быть символов перевода строки, поэтому предварительно код сценария преобразовывается в однострочный с помощью функции multyLine2SingleString (ее реализация будет указана ниже).

```
  Set srcFile = fso.OpenTextFile(sScript, FOR_READING)
  set userConsumer = consumerClass.SpawnInstance_()
  userConsumer.Name = "Run" & sOperation & "Script"
  userConsumer.ScriptText = ↵
      multyLine2SingleString(srcFile.readAll)
  userConsumer.ScriptingEngine = "VBScript"
  userConsumer.Put_()
  srcFile.close

  set userBinder = bindingClass.SpawnInstance_()
  userBinder.Filter = "__EventFilter.Name=" & ↵
      chr(34) & sOperation & "Filter" & chr(34)
  userBinder.Consumer = ↵
      "ActiveScriptEventConsumer.Name=" & chr(34) & ↵
      "Run" & sOperation & "Script" & chr(34)
```

После выполнения следующей строки начнется обработка событий изменения объектов организационных единиц.

```
  userBinder.Put_()
end function
```

Код непосредственной обработки события хранится в отдельных файлах. Следующая функция служит для его преобразования в одну линию. В VBScript можно получить работающий однострочный сценарий, заменив разрывы строк двоеточием.

```
Function multyLine2SingleString(multyLine)
multyLine2SingleString = replace(multyLine, vbCrLf, " : ")
end Function
```

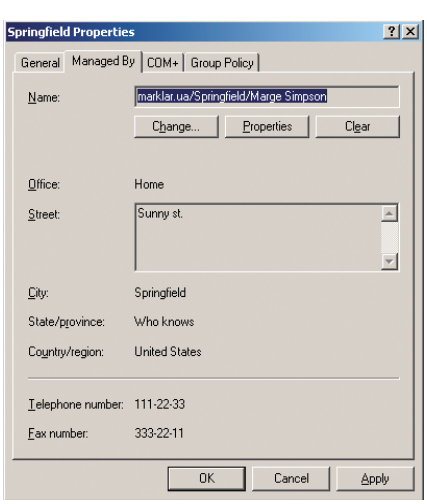
Функции установки слушателей событий нужно сохранить в отдельном файле с расширением vbs. В начале файла будут содержаться их вызовы.

```
addListener "OUModificate", __InstanceModificationEvent", ↵
      "ds_organizationalunit", "onOUModification.vbs_"
addListener "CommandSeed", "__InstanceCreationEvent", ↵
      "ads_usermovecommand", "onCommand.vbs_"
```

Функция вызывается дважды. Первый вызов устанавливает обработчик события смены руководителя подразделения (см. **рисунок**). Рассмотрим содержимое файла onOUModification.vbs_. Расширение файла может быть любым, поскольку используется он только для хранения текста сценария. Сам по себе он не запускается.

Итак, цель – добиться того, чтобы при смене руководителя подразделения ему автоматически делегировались полномочия манипулирования пользовательскими объектами. У предыдущего руководителя эти полномочия нужно соответственно отнять. Реализуем эту функциональность (далее приводится содержание файла onOUModification.vbs_, т.е. сценарий, выполняющийся при смене менеджера организационной единицы).

В сценариях обработки событий можно использовать экземпляр объекта текущего события, ссылка на которых хранится в переменной targetEvent. Создавать или инициализировать ее вручную не нужно. При обработке события изменения имеется доступ как к текущему (TargetInstance), так и к предыдущему (Previous Instance) состояниям объекта. Это очень удобно, так как таким образом можно получить информацию о новом и старом менед-



Назначение руководителя подразделения

жерах. Собственно, это и делается в первых двух строках сценария.

```
newManager = targetEvent.TargetInstance.DS_managedBy
oldManager = targetEvent.PreviousInstance.DS_managedBy
```

Затем производится проверка, а изменился ли менеджер. Дело в том, что событие этого типа возникает при изменении любого свойства организационной единицы (переименовании, например), продолжать же данный сценарий нужно, только если изменился менеджер.

```
if newManager <> oldManager then
```

Сначала создается объект основного класса надстройки, разрабатываемый в ходе этой статьи, который инкапсулирует основные операции надстройки.

```
  set engine = createObject("UserMove.Engine")
```

Затем сохраняем путь к организационной единице в переменной ouPath:

```
  ouPath = targetEvent.TargetInstance.ADSIPath
if oldManager <> "" then
```

Если у этого подразделения был другой менеджер, аннулируем его права.

```
    engine.undelegateOU ouPath, "LDAP://" & oldManager
  end if
```

Затем осуществляется делегирование прав манипуляции пользовательскими объектами новому менеджеру.

```
  if newManager <> "" then
```

Если новый менеджер назначен (возможен сброс этого поля, когда старое значение удаляется, а новое не назначается), ему предоставляются необходимые права.

```
    engine.delegateOU ouPath, "LDAP://" & newManager
  end if
end if
```

Теперь автоматическое делегирование прав работает. Достаточно назначить менеджера подразделения с помощью оснастки Active Directory Users and Computers (см. **рисунок**), чтобы ему были делегированы полномочия работы с объектами пользователей в рамках данного подразделения.

Далее проанализируем файл, который содержит обработчик событий, связанных с объектами команд onCommand.vbs_:

```
set cmd = getObject(targetEvent.TargetInstance.ADSIPath)
createObject("UserMove.Engine").dispatchCommand cmd
```

Он содержит две строчки. Потому что весь код реальной обработки инкапсулирован в методе dispatchCommand основного класса надстройки UserMove.Engine. Его реализации и будет посвящена следующая часть статьи.

Но сначала рассмотрим отключение обработчиков событий. Как уже говорилось, события обрабатываются, только когда существует соответствующим образом проинициализированная цепочка из объектов трех классов: __EventFilter, ActiveScriptEventConsumer и __FilterToConsumerBinding. Удаление любого из них приведет к остановке обработки. Тем не менее приведем более аккуратный сценарий, удаляющий все объекты.

```
Set objWIMService = _ ↵
      GetObject("winmgmts:\\.\root\directory\LDAP")
```

Сначала удаляются объекты классы __FilterToConsumerBinding. Они не имеют имен, поэтому для подключения к ним используется специальный запрос на получение всех объектов, ссылающихся на фильтр удаляемого события (__EventFilter). Результат выборки обходится, и все найденные объекты удаляются из хранилища.

```
Set objList = objWIMService.ExecQuery( ↵
      "references of {__EventFilter.Name= ↵
      'OUModificateFilter'}")
  For each objInst in objList
      objInst.Delete_
  Next
```

Операции выше достаточно для прекращения обработки событий. Ее можно применять для временного отключения надстройки. Однако для полного удаления всех следов нужно удалить и оставшиеся два объекта. У них уже есть отличительные имена, поэтому операция удаления заключается в привязке на основе имени и вызова метода obj.Delete_:

```
Set obj =  GetObject("winmgmts:\\.\root\directory\LDAP:" & ↵
      "ActiveScriptEventConsumer='RunOUModificateScript'")
obj.Delete_
Set obj = GetObject("winmgmts:\\.\root\directory\LDAP:" & ↵
      & "__EventFilter='OUModificateFilter'")
obj.Delete_
```

Обработчик команд

В этом разделе будет описан еще ряд методов основного класса надстройки UserMove.Engine. Здесь основное внимание сосредоточим на обработке объектов-команд. Для этого будет использоваться единственный открытый метод dispatchCommand и несколько закрытых вспомогательных.

Каждая команда имеет поле своего типа. Тип команды – строка. Все они определены в файле класса надстройки посредством ввода следующих констант.

Команда начала перемещения:

```
Const START_MOVE_COMMAND = "StartMove"
```

Команда отказа принять переводимого сотрудника в отдел:

```
Const DENY_COMMAND = "Deny"
```

Команда подтверждения перевода сотрудника:

```
Const ACCEPT_COMMAND = "Accept"
```

Команда отмены операции перевода:

```
Const ROLLBACK_COMMAND = "RollBack"
function dispatchCommand(cmd)
```

Здесь используется обработка ошибок, поскольку преждевременное завершение функции может привести к «потерям» объектов пользователей. В кавычках это слово потому, что физически удален объект пользователя не будет, лишь перестанет быть видимым. Кроме того, сбой в этой подпрограмме без обработки ошибок может привести к переводу надстройки в противоречивое состояние. Поэтому в самом начале функции используется директива продолжения выполнения сценария, несмотря на возникающие ошибки. В конце анализируется переменная специальная err – если она не равна нулю, ошибки были. В этом случае обрабатываемая команда отменяется с помощью специального метода resetCommand.

```
on error resume next
```

Далее команда проверяется на корректность с помощью метода checkIntegrity. Некорректная команда отменяется.

```
if not checkIntegrity(cmd) then
  resetCommand cmd
  exit function
end if
```

Если команда успешно прошла проверку, вызывается ее обработчик. Для каждого типа команд существует свой метод обработки. Далее все они будут рассмотрены.

```
select case cmd.userMoveID
  case START_MOVE_COMMAND:
    dispatchStartMoveCommand cmd
  case ACCEPT_COMMAND:
    dispatchAcceptCommand cmd
  case DENY_COMMAND:
    dispatchDenyCommand cmd
  case ROLLBACK_COMMAND:
    dispatchRollbackCommand cmd
  default:
    resetCommand cmd
end select
if err<>0 then resetCommand cmd
end function
```

Сначала рассмотрим метод проверки целостности команды. Это важная часть надстройки, которая относится к функциональности сервера. Сами команды создаются на рабочих станциях клиентов (менеджеров по персоналу). Поэтому существует вероятность фальсификации этих объектов. Выполняться же должны только корректные команды. Функция checkIntegrity возвращает значение логического типа. Возвращает истину, если команда прошла проверку, и ложь в противном случае.

```
function checkIntegrity(cmd)
```

Функция может работать с не вполне корректными объектами, поэтому возможны ошибки, которые не должны прервать ее выполнение.

```
  On Error resume next
  dim owner, executor, stOwner
```

Изначально предполагаем худшее – команда не прошла проверку.

```
checkIntegrity = false
```

Далее получаем объект владельца команды. Поле userMoveExecutor должно указывать на этого же пользователя – менеджера по персоналу, создавшего команду. То есть команда может быть создана с использованием одной учетной записи, а в поле userMoveExecutor установлен указатель на другую. Установить поле легко, поменять владельца объекта – сложнее (для этого требуются права администратора).

```
stOwner = cmd.get("ntsecuritydescriptor").owner
set owner = getObject("WinNT://" & ↵
    replace(stOwner,"\", "/"))
set executor = getObject(cmd.userMoveExecutor)
if err <> 0 then exit function
if owner.class = "Group" then
```

Если владелец объекта команды – группа, пользователь, создавший ее, должен быть членом этой группы.

```
    checkIntegrity = owner.isMember("WinNT://" & ↵
      info.domainShortName & "/" & executor.samAccountName)
  elseif owner.class = "User" then
    checkIntegrity = (executor.samAccountName = owner.name)
  end if
end function
```

Метод проверяет целостность объекта. Имеет ли право пользователь пользоваться командой, проверяется при ее выполнении.

Метод «Сброс команды» удаляет ее объект. Единственное исключение – команда начала перемещения, которая содержит в себе объект пользователя. В этом случае перед удалением объект пользователя извлекается в текущую организационную единицу. Поскольку эта ситуация потенциально опасна, профиль пользователя отключается.

Листинг 6. Сброс некорректной команды

```
function resetCommand(cmd)
  On error resume next
  dim ou
  set ou = getObject(cmd.parent)
  if cmd.class = START_MOVE_COMMAND_CLASS then
    dim user
    for each user in cmd
      user.accountDisabled = true
      user.setInfo
      ou.moveHere user.ADSPath, vbNullString
    next
   end if
   ou.delete cmd.class, cmd.name
end function
```

Начало перемещения

Перейдем к рассмотрению непосредственных обработчиков команд. Сначала команда начала перемещения. Логика ее работы подробно описана в первой части статьи [2]. Единственный параметр метода – объект команды, которую нужно выполнить. Проверку на целостность к этому моменту команда уже прошла. Здесь используется ряд вспомогательных методов, реализация которых будет рассмотрена позже.

```
function dispatchStartMoveCommand(cmd)
dim chair, room, whomObject, parentOU
```

Сначала создается объект стула ожидания в целевом подразделении.

```
set chair = createChair(cmd)
for each whomObject in cmd
```

Затем объект пользователя, инкапсулированный в команду, перемещается в объект стула ожидания.

```
  chair.moveHere whomObject.ADSPath, vbNullString
next
set parentOU = getObject(cmd.parent)
```

Далее подключаемся к комнате ожидания организационной единицы – источника перемещения. Она понадобится для добавления ссылки на перемещенный объект, чтобы облегчить его поиск в случае необходимости отката операции.

```
set room = getWaitingRoom(parentOU)
for each whomObject in chair
```

Функция createBackLink создает эту самую обратную ссылку:

```
  createBackLink room, whomObject.ADSPath
```

В конце объект выполненной команды удаляется.

```
  parentOU.delete START_MOVE_COMMAND_CLASS, ↵
      "CN=cmd_" & START_MOVE_COMMAND & "_" & ↵
      whomObject.samAccountName
next
end function
```

Рассмотрим использованные при обработке дополнительные методы. Первой использовалась функция создания стула ожидания.

```
function createChair(cmd)
dim chairNumber, room
```

Свойство userMoveTo команды содержит указатель на организационную единицу – пункт конечного назначения. Указатель на комнату ожидания этого подразделения снова получаем, используя функцию getWaitingRoom.

```
set room = getWaitingRoom(getObject(cmd.userMoveTo))
```

Объекты стульев пронумерованы, чтобы избежать совпадений имен. Они называются chair_1, chair_2 и так далее. Метод getNextNumber позволяет получить следующий свободный номер стула в заданной комнате.

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

Теперь можно создать объект стула. Практически все основные свойства перемещения (инициатор, время и др.) копируются из объекта команды.

```
set createChair = room.create(CHAIR_CLASS, ↵
      "CN=chair_" & chairNumber)
createChair.userMoveFrom = cmd.userMoveFrom
```

```
createChair.userMoveWho = cmd.userMoveWho
createChair.userMoveComment = cmd.userMoveComment
createChair.userMoveWhen = cmd.userMoveWhen
createChair.userMoveDisabled = cmd.userMoveDisabled
```

После выполнения следующей строки новый объект стула ожидания будет создан и готов к перемещению в него пользователя.

```
createChair.setInfo
end function
```

Далее рассмотрим функцию получения объекта комнаты ожидания, прикрепленного к заданной организационной единице. Если комнаты ожидания нет, метод создает ее. Единственный параметр – целевое подразделение.

```
function getWaitingRoom(ou)
dim el
```

Устанавливаем фильтр, чтобы в перебор с помощью цикла for each попали только объекты типа «Комната ожидания» (на самом деле в этой надстройке используется только одна комната ожидания для каждой организационной единицы).

```
ou.filter = Array(ROOM_CLASS)
for each el in ou
  set getWaitingRoom = el
```

Если комната ожидания найдена, функция возвращает ссылку на нее и завершает работу.

```
  exit Function
next
```

В противном случае объект комнаты ожидания сначала создается.

```
set getWaitingRoom = ou.create(ROOM_CLASS, ↵
      "CN=waiting_room")
getWaitingRoom.setInfo
end function
```

Также при создании стула использовалась функция определения первого свободного номера объекта заданного типа в конкретном контейнере. Рассмотрим ее подробнее. Функция позволяет получить следующий номер для объектов любого класса (имя типа передается вторым параметром), которые именуются в виде <имя>_<номер>.

```
function getNextNumber(room, className)
room.Filter = Array(className)
dim i, n
getNextNumber = 0
```

Реализация достаточно простая. Сначала для контейнера устанавливается фильтр, чтобы в перебор посредством for each попадали только объекты нужного типа. Затем получается номер каждого объекта (функция getUnderlinedNumber). Функция определяет максимальный встреченный номер и возвращает его, увеличив на единицу.

```
for each i in room
  n = getUnderlinedNumber(i.cn)
  if n > getNextNumber then getNextNumber = n
next
getNextNumber = getNextNumber + 1
end function
```

Этот метод использует функцию извлечения из строки имени номера, основываясь на том, что он отделен подчеркиванием. Функция находит символ подчеркивания и пытается преобразовать символы справа от него в число. Это достаточно примитивное решение, поддерживающее только имена с одним подчеркиванием. Однако для целей надстройки этого вполне достаточно.

Листинг 7. Извлечение номера объекта из его имени

```
function getUnderlinedNumber(src)
dim pos
pos = instr(1, src, "_", vbTextCompare)
if pos > 0 then
  getUnderlinedNumber = CInt(right(src, len(src) - pos))
end if
end function
```

Ну и в конце этой части статьи рассмотрим последнюю вспомогательную функцию создания ссылки на перенесенный объект. Напомню, что ссылка в данной надстройке – объект, содержащий единственное поле – путь к объекту Active Directory. Схема именования используется такая же, как и для стульев ожидания: link_<номер ссылки>. Метод получает два параметра: организационную единицу, откуда осуществляется перемещение, и собственно ссылку. Реализация довольно очевидна – с помощью getNextNumber определяется первый свободный номер, затем создается экземпляр класса ссылки, инициализируется и сохраняется.

Листинг 8. Создание обратной ссылки

```
function createBackLink(room, backLink)
dim linkNumber
linkNumber = getNextNumber(room, LINK_CLASS)
set createBackLink = room.create(LINK_CLASS, ↵
      "CN=link_" & linkNumber)
createBackLink.userMoveLink = backLink
createBackLink.setInfo
end function
```

Заключение

В этой части статьи была начата реализация механизма обработки команд. В следующей части она будет завершена. Остается сделать обработчики остальных типов команд, а также разработать подпрограммы создания новых команд. Также в следующей части будет рассмотрено использование регулярных выражений для упрощения обработки строк.

1. Андросов В. Делегирование прав на перемещение учетных записей пользователей в Active Directory. Часть 1. Постановка задачи. //Системный администратор, №3, 2009 г. – С. 16-21.
2. Андросов В. Делегирование прав на перемещение учетных записей пользователей в Active Directory. Часть 2. Реализация основных функций. //Системный администратор, №4, 2009 г. – С. 24-30.
3. Андросов В. Синхронизация ACL и структуры организации. Часть 3. //Системный администратор», №2, 2008 г. – С. 82-87.
4. msdn.microsoft.com.

Установка Windows XP с помощью System Center Configuration Manager 2007 R2

Алексей Тараненко

Для облегчения труда системного администратора компания Microsoft создавала различные средства автоматизации процесса установки ОС. Вначале это были файлы ответов и Remote Installation Services (RIS), затем Windows Deployment Services (WDS). Сегодня я расскажу вам об Operation System Deployment (OSD) в SCCM 2007 R2.

Установка операционной системы – одна из операций, которую периодически необходимо проводить системному администратору. Особенно рутинной она становится, когда нужно одновременно установить ОС на несколько компьютеров. Хорошо, если их будет три или четыре, а представьте, что вам поручили подготовиться к открытию офиса в новом городе и одновременно нужно установить 50 или 100 компьютеров. Ес-

тественно, что процесс ручной установки операционной системы на каждый компьютер займет очень много времени.

В статье будет рассмотрена установка сервера Windows Deployment Services и ролей System Center Configuration Manager 2007 в среде Windows Server 2003 в режиме работы сайта SCCM 2007 – mixed mode. Статья подразумевает, что читатель обладает начальными знаниями по работе с SCCM 2007.

Способы установки ОС в SCCM

Configuration Manager 2007 предлагает нам несколько способов установки операционных систем:

- установка с помощью образа WIM с загрузкой по сети или с использованием диска (USD\CD\DVD);
- установка из сетевой папки (подобие RIS).

Установка из сетевой папки является более предпочтительным вариантом для операционных систем Windows 2000 и Windows XP. Хотя эта установка требует больше времени, однако она позволяет полностью избавиться от проблем с несовместимостью аппаратных уровней (уровней HAL). Следует отметить, что установка из сетевой папки, это именно установка (как с CD\DVD-диска), а не развертывание эталонного WIM-образа.

Системные требования

Operation System Deployment использует технологию Windows Deployment Services для распространения образов на клиентские компьютеры. Для использования OSD в среде сайта SCCM нужно выполнить следующие условия:

- сервер WDS;
- сервер DHCP;
- сервер с ролью PXE;
- более 512 Мб оперативной памяти на клиенте для успешной установки.

Требование 512 Мб оперативной памяти обусловлено размером, занимаемым Windows PE 2.0 в памяти компьютера при развертывании.

Для хранения образа системы Configuration Manager использует файлы формата WIM.

Глоссарий

- ☑ **Windows Preinstallation Environment (Windows PE)** – прединсталляционная платформа Microsoft, которая пришла на смену MS-DOS при установке операционной системы. Помимо своей основной функции – подготовки компьютера к установке операционной системы, она может быть использована в качестве самостоятельной ОС (LiveCD) для запуска сторонних программ.
- ☑ **Windows Imaging Format (WIM)** – это файл-ориентированный формат образов, который предоставляет значительные преимущества по сравнению с более распространенными сегодня сектор-ориентированными форматами. Формат WIM позволяет также хранить несколько образов в одном WIM-файле. Формат WIM существенно уменьшает размер файловых образов, используя методы сжатия и хранения единичных копий. (WIM-файлы содержат одну физическую копию файла для каждого экземпляра этого файла в образах, содержащихся в WIM-файле, что существенно уменьшает размер WIM-файлов, содержащих несколько образов). Кроме этого, формат WIM-образов позволяет проводить неразрушающее развертывание. Это означает, что вам не нужно делать резервную копию информации, находящейся на томе, куда устанавливается образ, так как процедура установки образа не приводит к удалению существующего содержимого диска.

В формате WIM распространяются все последние ОС Microsoft: Windows Vista, Windows 7 и Windows Server 2008. Windows XP недоступна в качестве готового WIM-образа, однако мы можем самостоятельно установить Windows XP на эталонный компьютер, а затем сохранить полученный образ в формате WIM. OSD поддерживает операционные системы, начиная с версии Windows 2000 SP4.

Давайте рассмотрим следующий сценарий – установка Windows XP на новый компьютер. Хотя Windows XP существует уже более 7 лет и жизненный цикл этой системы подходит к своему финальному этапу, она все еще является самой распространенной клиентской операционной системой в мире.

Преимущества OSD SCCM над WDS

Поскольку распространение операционных систем в SCCM базируется на WDS, многие читатели могут задаться вопросом: «В чем же заключаются плюсы от использования OSD»? В OSD вы работаете с последовательностью задач (task sequence), таким образом, вы можете создавать различные сценарии установки и при этом использовать для них один образ WIM.

Например: вам необходимо установить ОС на два типа компьютеров с разным набором программ. Для первого типа необходимы: Windows Vista и Microsoft Word, для второго – Windows Vista, Microsoft Office (Word + Excel + Outlook + Powerpoint), архиватор, антивирус и ряд других программ.

В случае использования WDS у нас есть несколько вариантов решения этой задачи: мы можем внедрить все программы в один WIM-файл или использовать несколько WIM-файлов, каждый для своего типа компьютеров. Понятно, что это не очень удобно – мы тратим место на сервере под несколько WIM-файлов, устанавливается не минимальный необходимый набор программ и т.д.

Другим выходом в случае использования WDS может стать установка программ через групповые политики. Этот метод также имеет свои минусы. Если же мы используем SCCM, то благодаря возможности построения различных последовательностей задач (task sequence), мы используем один образ WIM для установки на все типы компьютеров с любым набором программ. И это касается не только установки программ, но и драйверов, и обновлений безопасности.

В OSD SCCM возможно устанавливать операционные системы на неизвестные/новые компьютеры. Причем установка на неизвестный компьютер не потребует от системного администратора дополнительных усилий.

Неизвестным компьютером в среде сайта SCCM будет компьютер, не содержащий записи в базе данных сайта. Такими компьютерами могут быть: новые, впервые подключающиеся к сети компьютеры, компьютеры без установленного агента SCCM.

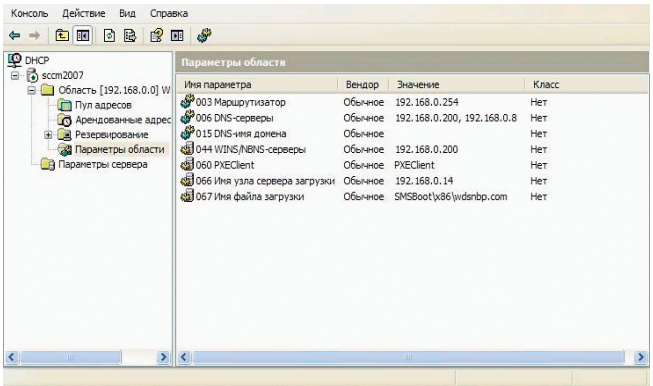


Рисунок 1. Настройка параметров DCHP

В OSD вы можете забыть о необходимости установки драйверов для компьютера. Все драйверы могут быть интегрированы в единую базу, которую удобно поддерживать и обновлять. Размер базы неограничен.

Установка WDS

Для Windows Server 2003 установка WDS доступна через пункт «Установка компонентов системы», оснастки «Установка и удаление программ». Найдите и отметьте для установки компонент «Службы развертывания Windows». Для установки этого компонента вам, возможно, понадобится диск с инсталляционными файлами Windows Server 2003.

После завершения установки компонента находим в консоли администрирования сервера («Пуск → Панель управления → Администрирование») пункт «Службы развертывания Windows» и запускаем консоль, выбираем сервер и щелкаем по нему правой кнопкой мыши, контекстное меню – «Настроить сервер».

В окне появившегося мастера указываем место нахождения папки RemoteInstall, хорошей практикой будет держать эту и другие папки SCCM на выделенном NTFS-томе.

Следующим шагом необходимо настроить взаимодействие с DCHP-сервером. Если службы DHCP и WDS установлены на одном и том же сервере, необходимо в окне мастера настройки служб развертывания Windows отметить параметры: «Не прослушивать порт 67» и «Настроить тег 60 DCHP-параметра для значения «PXEClient».

В следующем окне мастера отмечаем пункт «Не отвечать никаким клиентским компьютерам», поскольку отвечать компьютерам у нас будет SCCM.

На этом настройка WDS завершена. Закройте консоль администрирования WDS и забудьте о ней! Не добавляйте никаких образов в WDS, все это делается через консоль SCCM. Кстати, можно настроить сервер WDS и из командной строки:

```
WDSUTIL /Initialize-server /Reminst:"D:\RemoteInstall"
```

Проверяем настройки DHCP-сервера и дописываем туда еще один тег: 66 – имя сервера загрузки (см. **рис. 1**).

Теперь переходим к установке роли PXE сайта SCCM. В консоли администрирования SCCM – Configuration Manager Console переходим к Site Database → Site → Site Settings → Site Systems → Server WDS\SCCM, правой кнопкой мыши контекстное меню New roles.

Если вы установили WDS на отдельный сервер, и при этом на этот сервер не было предварительно развернуто ни одной другой роли SCCM, тогда нужно в консоли SCCM вначале добавить объект-сервер через меню New → Server.

Находим среди доступных ролей ConfigMgr PXE service point и выбираем ее для установки.

На первой странице появившегося мастера проверяем FQDN-имя сервера, указываем с помощью каких учетных данных будет установлена роль (служебный акаунт SCCM или произвольная учетная запись).

SCCM выведет сообщение о необходимых портах для своей работы. Если внутри сети применяются файерволы, проследите, чтобы они были настроены на пропуск пакетов от SCCM по следующим портам: UDP 67, 68, 69, 4011.

На следующей странице мастера можно ограничить ответы сервера SCCM каким-либо одним сетевым интерфейсом, а также задаем пароль для входа в режим установки. Пароль может быть полезен, чтобы пользователи не смогли случайно войти в режим установки при загрузке компьютера и не переустановили себе операционную систему.

Затем, генерируем сертификат и назначаем учетную запись для доступа к базе данных SCCM.

Просматриваем страницу Summary, еще раз соглашаемся с изменениями нажатием кнопки Next. Роль PXE SCCM успешно установлена.

После этого необходимо включить поддержку неизвестных компьютеров в SCCM. В консоли администрирования SCCM выбираем раздел Site manager → Site Systems, далее указываем сервер SCCM и переходим к пункту ConfigMgr PXE service point и выбираем свойства, где необходимо установить галочку Enable unknown computer support (см. **рис. 2**).

Устранение неполадок установки WDS-PXE

Если у вас возникли какие-то проблемы с работой связки WDS-PXE, решить которые штатными средствами вы не в состоянии, попробуйте переустановить WDS и PXE SCCM в следующем порядке:

- удаляем WDS, удаляем все папки с именем Remoteinstall, не забываем про сетевые ресурсы;
- удаляем PXE SCCM;
- перезагружаем сервер.

Далее:

- устанавливаем WDS;
- перезагружаем сервер;
- инициализируем WDS;

```
C:\>wdsutil /verbose /initialize-server ↵
     /server:srvname /reminst:"c:\remoteinstall"
```

- устанавливаем PXE SCCM.

Далее не забываем проверить настройки DHCP, в определенной подсети настраиваем теги 60, 66, 67:

- **60** – имя сервера с WDS, либо IP;
- **66** – имя сервера с WDS, либо IP;
- **67** – SMSBoot\x86\wdsnbp.com.

Завершение настройки WDS-PXE

Теперь осталось проверить некоторые пункты установки, и можно переходить к процессу захвата и развертыванию образа.

В консоли администрирования SCCM выбираем пункт Site database → Computer management → Operation System Deployment (см. **рис. 3**).

Далее по тексту указание на пункт OSD в консоли администрирования SCCM будет означать обращение именно к этому разделу либо его подразделам.

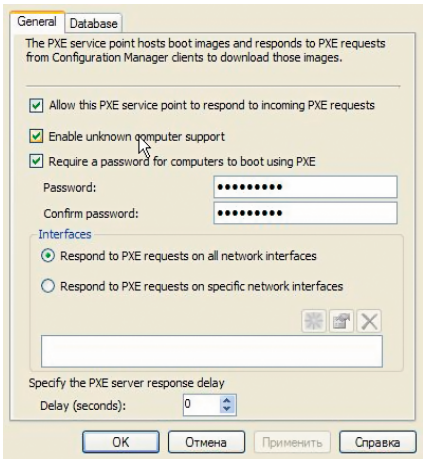


Рисунок 2. Включение поддержки неизвестных компьютеров в SCCM

Загрузочные образы

Для начала проверим, создались ли у нас образы для загрузки. Переходим к пункту Boot image. По умолчанию создается два образа загрузки для x86-систем и x64-систем соответственно. Если по какой-либо причине они не создались или вы удалили их, можно добавить эти образы через команду Add boot image. Стандартные образы хранятся в папке установки SCCM – \Microsoft Configuration Manager\OSD\boot. Стоит отметить, что в общем случае у вас для загрузки будет использоваться тот образ, который соответствует вашей архитектуре. Не стоит путать разрядность образа загрузки и разрядность устанавливаемой операционной системы.

Если не планируется устанавливать x64-версии операционных систем, то можно смело использовать для загрузки только образ x86, он будет успешно загружаться на любых процессорах. Щелкаем правой кнопкой на образе загрузки и открываем свойства.

Иногда бывает, что стандартный загрузочный образ не может начать процесс установки. Чаще всего это связано с тем, что Windows PE не может найти подходящие драйверы для сетевой карты. На вкладке Windows PE вы можете их добавить. Не стоит злоупотреблять добавлением драйверов! Помните, что все драйверы будут распакованы в память компьютера при загрузке. Добавляйте их только для тех сетевых плат и контроллеров дисков, которые отказываются работать со стандартными драйверами. Также на этой вкладке можно включить поддержку командной строки в среде Windows PE (вызывается по нажатию кнопки <F8>) и установить собственные обои для программы загрузки.

Если у нас в одном WIM-файле содержится несколько образов, а формат WIM такое позволяет, то мы можем задать используемый образ на вкладке Data Source (см. **рис. 4**).

На вкладке Distribution Settings мы можем указать использование опции multicast. Мультикаст – это новая возможность в SCCM 2007 R2, которая позволяет отдавать образ одновременно на несколько машин, таким образом снижая загруженность сети. Включите опцию, если собираетесь устанавливать одинаковую версию ОС одновременно на несколько компьютеров.

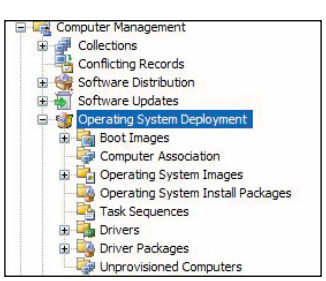


Рисунок 3. Консоль администрирования Configuration Manager – раздел OSD

Теперь необходимо опубликовать загрузочный образ на точке распространения (Distribution point). В консоли администрирования SCCM перейдите к пункту OSD → Boot Image → Distribution point, далее правой кнопкой мыши вызываем контекстное меню New Distribution Point. В появившемся мастере обязательно выберите точку распространения – \\SCCM\SMSPXEIMAGES$ и вашу стандартную точку распространения.

Важно! Точка SMSPXEIMAGES$ является служебной точкой распространения только для образов загрузки. Обычные образы установки не нужно распространять на эту точку.

Подготовка эталонного компьютера

Пришло время ненадолго отвлечься от настройки Configuration Manager и настроить эталонный компьютер.

Самой большой проблемой при установке Windows XP является несовместимость аппаратно-зависимых уровней (уровней HAL) и драйверов контроллеров дисков.

Подробнее об уровнях HAL: http://support.microsoft.com/kb/309283/ru.

Если парк компьютеров у вас стандартный, то такая проблема, скорее всего, обойдет вас стороной. Если же компьютеры у вас закупались в разное время и Core 2 Quad соседствует с Pentium IV и Celeron, то возможно вам придется создавать несколько образов. Но перед тем как делать несколько образов, попробуйте такой способ: находите компьютер, у которого HAL соответствует «Однопроцессорный компьютер с ACPI», ACPI APIC UP HAL (Halaacpi.dll) (посмотреть уровень HAL можно в диспетчере устройств раздела «Компьютер»), и делаете захват эталонного образа именно с этого компьютера.

Такой образ должен без проблем установиться и на многопроцессорные компьютеры, что в принципе покрывает большинство современных рабочих станций.

Кроме того, ошибку Stop 0x0000007b могут вызвать неправильные драйверы контроллера диска. И хотя на большинстве рабочих станций применяются стандартные контроллеры, драйверы которых присутствуют в Windows XP, вы можете столкнуться с рабочей станцией, которая требует для своей работы определенного драйвера. Нам поможет утилита Sysprep.

Программа подготовки системы (Sysprep.exe) применяется в целях подготовки установленной копии Windows для создания образа.

Драйверы контроллеров лучше интегрировать в Windows XP через программу Sysprep. Для добавления в файл sysprep.inf списка стандартных и уже установленных контроллеров измените файл sysprep.inf следующим образом:

```
[Sysprep]
  BuildMassStorageSection = Yes
[SysprepMassStorage]
```

Выполните команду «sysprep -bmsd», и в файл sysprep.inf будут добавлены известные системе драйверы контроллеров дисков.

```
*pnp0a00=c:\windows\inf\machine.inf
*pnp0a01=c:\windows\inf\machine.inf
*pnp0a04=c:\windows\inf\machine.inf
*pnp0a03=c:\windows\inf\machine.inf
pci\cc_0604=c:\windows\inf\machine.inf
pci\cc_0601=c:\windows\inf\machine.inf
pci\cc_0602=c:\windows\inf\machine.inf
pci\cc_0600=c:\windows\inf\machine.inf
pci\cc_0500=c:\windows\inf\machine.inf
```

Если нам необходимо добавить драйверы вручную, то заполняем секцию [SysprepMassStorage] файла sysprep.inf:

```
;VIA
    PCI\VEN_1106&DEV_3349&CC_0104 = c:\drive\viamraid.inf
    PCI\VEN_1106&DEV_6287&CC_0106 = c:\drive\viamraid.inf
;ITEATAPI
    PCI\VEN_1283&DEV_8212&SUBSYS_00011283 = ↵
      c:\drive\iteatapi.inf; 8212/CX
```

Код устройства PCI\VEN_1106&DEV_3349&CC_0104 можно узнать из inf-файла драйвера, c:\drive\viamraid.inf – путь к нашему драйверу.

Важно! Драйвер должен будет находиться на диске перед снятием образа. Кроме того, при снятии образа Windows XP может генерировать запросы на установку драйверов.

Стоит также обратить внимание на используемый тип дисков – IDE или SATA. У вас могут возникнуть проблемы, если эталонная ОС была установлена на более «быстрый» диск, чем диск, на который устанавливает операционная система. К примеру, попытка установки образа, снятого с SATA-диска, на IDE-диск может закончиться ошибкой BSOD.

Теперь пора перейти к наполнению эталонной станции программами. Определите для себя наиболее распространенный набор программ, которые установлены на всех ваших рабочих станциях. Естественно, для каждой компании этот набор программ будет различным. При создании образа стоит учитывать, необходима ли масштабная установка. Так, если предстоит в кратчайший срок развернуть несколько десятков или сотен копий ОС, то лучше включить все программы в образ, возможно, создав несколько разных образов для разного набора программ. Если же установка планируется в текущем режиме, то рекомендую вынести установку программ в отдельный пункт. К тому же SCCM позволяет устанавливать программы на этапе развертывания операционной системы. Что же стоит установить в эталонном образе:

- ОС Windows XP + последний пакет обновлений и последние обновления безопасности;
- .net Framework 3.5;
- программы, которые трудно устанавливать в автоматическом режиме (например, doPDF).

Зачем ставить .net Framework 3.5? На большинстве клиентских компьютеров вам рано или поздно придется установить .net Framework 2.0 или 3.0. Пакет .net Framework 3.5 содержит в себе и тот и другой, поэтому логичнее установить его сразу. Разумеется, вы можете его не устанавливать, если считаете, что платформа .net вам не нужна.

Да, в случае исключения большого количества программ из образа в раздел распространения программ SCCM у нас увеличивается время установки ОС. Но в случае установки на один-два компьютера время установки для нас становится некритичным, зато появляется гибкость в распространении программ, поскольку программы не интегрированы жестко в WIM-файл, а устанавливаются дополнительно.

Снятие образа установки

В SCCM есть два базовых способа снятия образа:

- Build and capture reference operating system image.
- Capture media.

Первый способ подразумевает установку операционной системы, автоматическую установку программ и обновлений, и затем снятие эталонного образа. Такой способ больше подходит для обновления уже существующего WIM образа Windows XP либо для использования с Windows Vista/Windows 7. Я предпочитаю второй путь – создание диска с системой захвата образа. Отдав диск захвата (Capture disk) службе технической поддержки, вы избавите себя от необходимости периодически обновлять образ системы. Эти действия будут происходить без вашего вмешательства силами специалистов техподдержки, при определенных условиях обновление образа системы не потребует от вас, как администратора SCCM, вообще никаких действий.

Создание задания Build and capture reference operating system image фактически не отличается от процесса создания обычного task sequence, который мы рассмотрим дальше. Этот пункт доступен через консоль администрирования SCCM OSD → Task Sequence, далее правой кнопкой мыши вызываем контекстное меню New → Task Sequence → Build and apture reference operating system image.

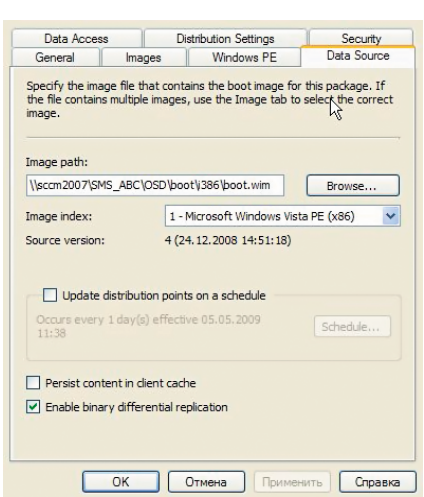


Рисунок 4. Путь к образу

Рассмотрим процесс создания диска захвата. Отмечу, что в роли диска захвата могут выступать USB/CD/DVD-диски. В консоли администрирования SCCM выбираем OSD → Task Sequence, правой кнопкой мыши вызываем контекстное меню Create task sequence media. В появившемся мастере выбираем пункт Capture media. Выбираем тип диска CD/DVD и место хранения образа. На следующей странице мастера выбираем используемый образ загрузки. В большинстве случаев подойдет образ x86. Указываем точку распространения.

Просматриваем страницу Summary, нажимаем Next и ждем несколько минут, пока создастся образ диска. Теперь записываем этот образ на диск. После записи диска возвращаемся к нашему эталонному компьютеру. Вставляем диск в CD-ROM и видим запуск программы (см. **рис. 5**).

Напомню, что папка Sysprep уже должна существовать на разделе с операционной системой. Иначе мы получим сообщение об ошибке.

Затем мы указываем место хранения образа и учетные данные для подключения к этой сетевой папке.

После того как мастер закончит снятие образа, в указанной папке на сервере появится файл образа эталонного компьютера в формате WIM. Теперь необходимо добавить образ в базу Configuration Manager. В консоли администрирования SCCM переходим к разделу Operation System Deployent → Operation System Images → Add operating system Image. В появившемся мастере указываем размещение файла образа в сети, вводим название, версию и комментарий.

Остальные пункты оставляем по умолчанию и жмем кнопку Finish – образ готов. В консоли администрирования находим образ в разделе OSD → Operation System Image, вводим имя образа, далее правой кнопкой мыши вызываем контекстное меню Properets. Переходим на вкладку Image , где можем увидеть сводку WIM-файла (см. **рис. 6**).

Теперь необходимо опубликовать образ на точке распространения. OSD → Operation System Image, вводим имя образа, далее переходим к Distribution point, далее правой кнопкой мыши вызываем контекстное меню New distribution point. В появившемся мастере отмечаем точку распространения.

Важно! Помните, что точку \SMSPXEIMAGES$ мы не отмечаем!

Создание пакета установки агента Configuration Manager

Рассмотрим создание пакета установки программы на примере агента ConfigManager. В консоли администрирования SCCM переходим к пункту Site database → Computer management → Software distribution → Packages, далее правой кнопкой мыши вызываем контекстное меню New → Package from definition и выбираем Configuration Manager Client update. Указываем, что пакет будет содержать инсталляционные файлы (Always obtain files from a source directory). Если мы работаем с консолью на сервере SCCM, то выбираем вариант Local drive on site server и указываем путь к инсталляционным файлам клиента, по умолчанию C:\Program files\Microsoft Configuration Manager\Client\. Если же мы работаем с консолью с рабочей станции администратора, то следует указать сетевой путь: \\server_sccm\SMS_SITECODE\Client. После создания пакета в консоли SCCM разворачиваем пункт с нашим пакетом и переходим к разделу Programs.

Заходим в свойства Advanced client silent upgrade. Нам важно убедиться, чтобы в параметре Command line была прописана строка CCMSETUP.EXE /noservice SMSSITECODE=AUTO. Если ее там нет, необходимо ее прописать. После этого переходим к разделу Distibution point и опубликовываем пакет на основной точке распространения.

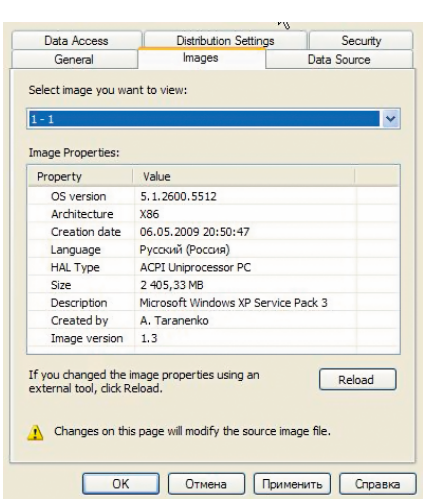


Рисунок 6. Свойства образа WIM

Рисунок 5. Экран приветствия мастера захвата образа

Создание пакета драйверов

Для начала необходимо добавить драйверы в базу сайта Config Manager. Для этого драйверы должны быть расположены в сетевой папке и сервер SCCM должен иметь разрешение на чтение данной папки. В консоли администрирования SCCM переходим к OSD → Drivers, правая кнопка мыши, контекстное меню Import. В появившемся мастере указываем UNC-путь к папке с драйверами. На странице Add driver to packages необходимо создать новый пакет драйверов (New package), указав место расположения драйвера – сетевую папку, в которой будут храниться все драйверы пакета. Эта папка может быть скрытой с помощью символа $. В этом же мастере при необходимости мы можем добавить драйвер к образам загрузки Windows PE2. Если вы решили добавить драйвер к образу загрузки, то не забудьте поставить галочку напротив параметра Update distribution point when finished. После завершения мастера импортирования драйвера не забудьте указать точку распространения для пакета драйверов. В консоли администрирования SCCM переходим к OSD → Driver packages → Distribution point, правая кнопка мыши, контекстное меню New distribution point.

Важно! Существует ограничение: Windows XP не поддерживает загрузку более 150 драйверов на клиента. Причем из личного опыта мне известно, что эта цифра еще меньше – 144. Подробнее о процессе установки драйверов и подготовке пакета драйверов вы можете узнать на сайтах:

- http://technet.microsoft.com/ru-ru/library/bb680651.aspx;
- http://itband.ru/tag/sccm;
- http://blogs.sysfaq.ru/altaranenco.

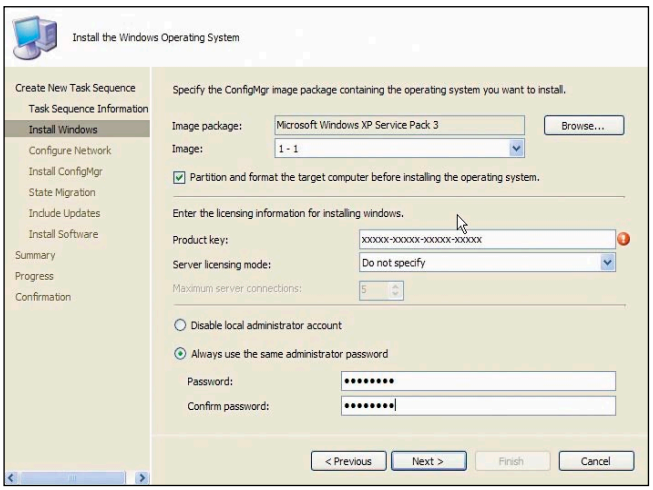


Рисунок 7. Мастер создания Task Sequence

Создание последовательности заданий установки (Task Sequence)

Теперь, когда у нас есть WIM-файл с образом Windows XP, мы можем вернуться к процессу создания последовательности установки (Task Sequence). В меню администрирования SCCM переходим к пункту OSD → Task Sequence, правой кнопкой мыши вызываем контекстное меню New → Task Sequence. В появившемся мастере выбираем вариант установки из файла образа (Install an existing image package). Затем вводим название пакета, наш комментарий, а также выбираем загрузочный образ для пакета. На следующей странице нажимаем на кнопку Browse и выбираем файл с образом WIM. Если в файле несколько образов, то нужно выбрать, какой из них мы будем устанавливать. Вводим ключ установки и действие над учетной записью локального администратора – либо устанавливаем пароль, либо отключаем (см. **рис. 7**).

На следующей странице мастера указываем, вводить ли компьютер в рабочую группу или домен. Не забываем, что для ввода в домен мы должны указать учетную запись с соответствующими правами. На странице Install ConfigMgr мастера создания Task Sequence с помощью кнопки Browse

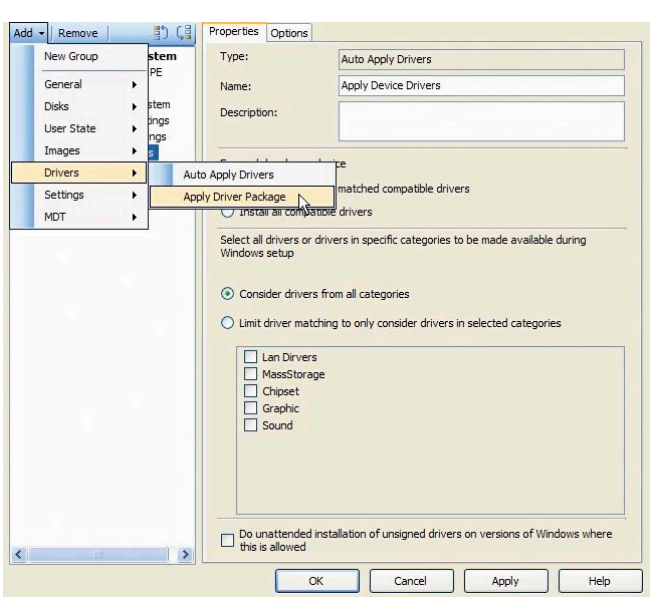


Рисунок 8. Добавление пакета драйверов

указываем пакет установки агента SCCM. Следующая страница (State migration) позволяет нам захватить настройки пользователя и системы, но поскольку развертывание мы выполняем на чистую машину, то снимаем галочки с раздела захвата настроек пользователя и компьютера. Кроме того, для использования данной возможности в будущем необходимо будет установить комплекты Microsoft Delpoyment Toolkit 2008 (MDT) и User State Migration Tool (USMT) на сервере SCCM. На последующих страницах указываем, что обновления не будут загружаться в процессе установки ОС (Don't install any software updates), и при необходимости указываем, какие программы будут установлены на компьютер в ходе развертывания ОС. Разумеется, для этого предварительно необходимо создать соответствующие пакеты программ. Завершаем процесс создания последовательности задач установки ОС просмотром страницы Summary.

Почти все готово для развертывания образа, но я предлагаю вам немного отредактировать полученный Task Sequence. В консоли администрирования выбираем OSD → Task sequence, вводим имя нашего задания, вызываем правой кнопкой мыши контекстное меню Edit. В появившемся окне можно отредактировать любые свойства задания, при необходимости удалив или добавив новые пункты (см. **рис. 8**).

Начнем с подготовки диска компьютера. По умолчанию SCCM предлагает создать на жестком диске один NTFS-раздел. Возможно, кому-то это покажется неудобным. Изменим распределение дискового пространства так, чтобы диск C занимал у нас 15 Гб, а все остальное стало диском D. Переходим к пункту Partition disk 0, в разделе Volume выбираем редактирование свойств записи Default (primary).

В появившемся окне задаем размер первого диска (см. **рис. 9**). Затем создаем новый раздел (кнопка с символом «звездочка»). Теперь жесткий диск будет разбит на два раздела.

Переходим к следующему пункту (Apply Operating Systems), указываем, какой образ операционной системы будем применять. А также указываем, на какой раздел жесткого диска будет установлена система.

В пункте (Apply Windows Settings) проверяем данные для регистрации системы: имя пользователя, компании и серийный номер ключа.

Пункт (Apply Network Settings) ответственен за сетевые настройки. При необходимости мы можем прописать IP-адрес и другие сетевые настройки вручную, но лучше все же использовать для этого DHCP.

Переходим к пункту с драйверами (Apply Device Drivers). По умолчанию Task Sequence создается так, чтобы обращаться к базе драйверов на сервере SCCM, однако для установки Windows XP через WIM необходимо устанавливать драйверы через пакет.

Поскольку установка драйверов через категорию нам не подходит, создадим пункт установки драйвера через пакет. Меню Add → Drivers → Apply driver package, вводим имя пакета с драйверами (см. **рис. 8**).

С помощью кнопки «Browse» выбираем, какой пакет будет использоваться для установки драйверов.

С помощью кнопок Move up и Move down переносим пункт Apply device driver ниже пункта Apply driver package. Посколь-

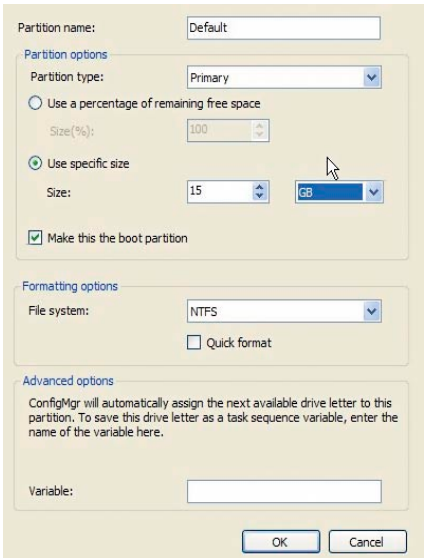


Рисунок 9. Свойства разметки диска в Task Sequence

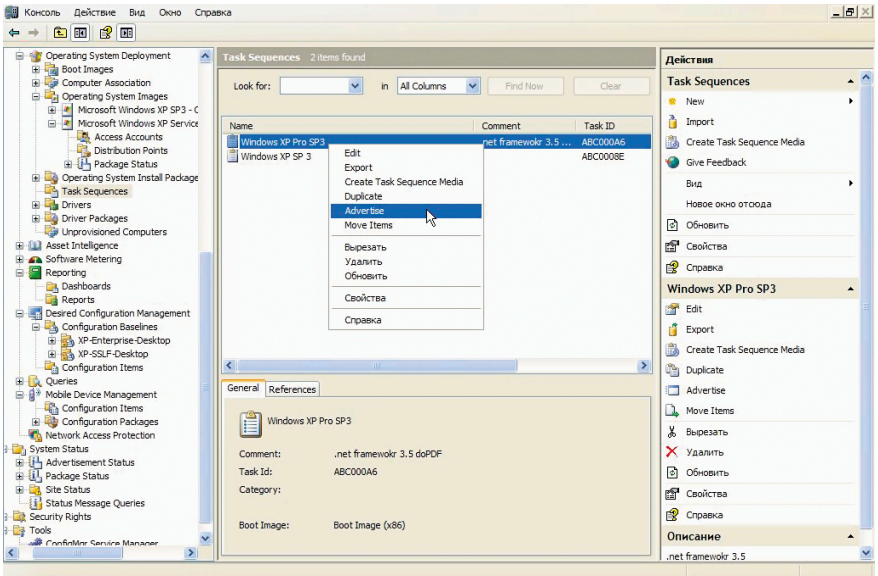


Рисунок 10. Объявление для установки ОС (Advertisment Task Sequence)

ку именно в этом пункте задаются настройки применения всех драйверов или только совместимых, а также поведение системы при установке неподписанных драйверов.

При необходимости добавляем произвольные шаги последовательности установки, например такие как установка программ или обновлений. На этом подготовку к развертыванию можно считать оконченной.

Назначение установки операционной системы на коллекцию компьютеров

Коллекция (collection) – группа объектов (пользователи, компьютеры, группы безопасности), объединенная по какому-либо признаку. Мы будем работать со стандартной коллекцией ConfigManager 2007 R2 – коллекцией для неизвестных компьютеров – All unknown computers. До версии SCCM 2007 R2 установка на неизвестные для сайта SCCM компьютеры была возможна только при использовании сторонних средств, в частности скрипта pxefilter.vbs из комплекта MDT 2007. Если хотите установить ОС на компьютер, который уже является клиентом SCCM-сайта, добавьте этот компьютер в члены соответствующей коллекции. Кроме того, для нового компьютера мы можем вручную создать запись в базе данных сайта через пункт OSD → Computer association. Для этого потребуется MAC-адрес сетевой карты компьютера. В таком случае мы сможем сразу задать имя компьютера, которое применится при установке.

Для того чтобы назначить установку операционной системы на коллекцию, необходимо в консоли SCCM выполнить OSD → Task sequence, вводим имя задания, далее правой кнопкой мыши вызываем контекстное меню Advertise (см. **рис. 10**).

В появившемся окне мастера вводим имя для задания распространения, выбираем созданный нами task sequence и коллекцию («All unknown computers»), на которую будет применяться это задание. Также обязательно нужно отметить использование PXE для этого задания (Make this task sequence avialable to boot media and PXE). На следующей странице выбираем время, с которого будет доступно задание для клиентов.

Важно! Не устанавливайте принудительную установку операционной системы (mandatory assignment) если вы не уверены в своих действиях. Неверная установка данного параметра вместе с назначением задания на ошибочную коллекцию приведет к переустановке всех компьютеров этой коллекции.

Остальные параметры можно оставить по умолчанию. После этого SCCM полностью готов к развертыванию операционной системы на клиентские компьютеры.

Теперь перейдем к целевому компьютеру. В BIOS компьютера выставьте первым вариантом загрузку по сети (PXE BOOT), а вторым – загрузку с жесткого диска. Включите компьютер, при загрузке вы увидите экран, подобный экрану на **рис. 11**. После нажатия клавиши <F12> начнутся загрузка и запуск системы Windows PE.

Заключение

Установка Windows XP через WIM-файлы в SCCM является нетривиальной задачей. Помимо отсутствия фабричного файла WIM (как Windows Vista\Windows 7) и, следовательно, необходимости создавать свой файл образа системы, нужно еще решить проблему несовместимости уровней HAL и установки драйверов. Надеюсь, что данная статья поможет вам лучше ориентироваться в возможностях продукта system Center Configuration Manager 2007.

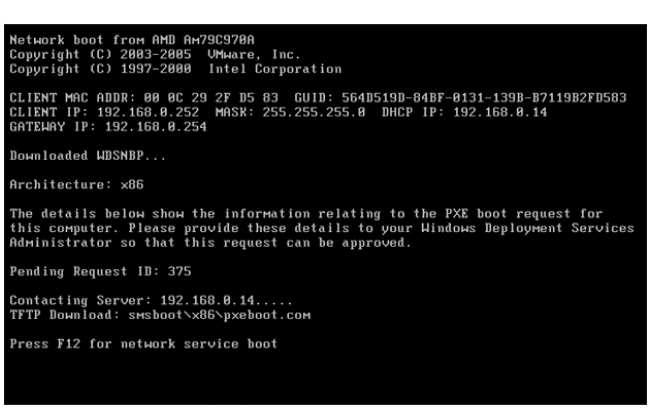


Рисунок 11. Экран загрузки агента PXE boot

PowerShell. Поиск объектов в каталоге Active Directory

Иван Коробко

Большинство операций в каталоге Active Directory сводится к поиску объектов по различным критериям. Рассмотрим подробно процедуру с помощью библиотек .NET Framework на PowerShell.

Поиск объектов в Active Directory осуществляется с помощью класса .NET FrameWork System.Directory Services.DirectorySearcher и одного из методов: FindAll() или FindOne() в зависимости от условий поиска. Сценарий поиска можно условно разделить на несколько логических частей:

- доступ к контейнеру;
- фильтр поиска;
- атрибуты поиска;
- область поиска;
- сортировка элементов;
- поиск объектов.

Доступ к контейнеру

Для поиска объекта необходимо определить точку входа – путь к контейнеру, в котором будет осуществляться поиск. Для выполнения этого условия необходимо создать объект DirectorySearcher:

```
$path = "LDAP://OU=WorkSpace,DC=Island,DC=ru"
$obj = New-Object DirectoryServices.DirectorySearcher($Path)
```

Созданный объект содержит ряд свойств и методов. Полный отображения списка свойств и методов, поддерживаемых объектом, необходимо использовать командлетом Get-Member или его псевдонимом (gm):

```
$obj | Get-Member
```

Примечание: командлет – это обычная команда, выполняющая определённое действие с указанным объектом. Любой командлет состоит из глагола и существительного, разделенных дефисом. Глагол указывает, какое действие будет производиться, а существительное указывает объект, над которым будет производиться это действие. Командлеты поддерживают сокращения. Полный список сокращений можно получить с помощью команды:

```
Get-Alias | Format-Table -Property Definition, Name -Autosize
```

Для осуществления процедуры поиска необходимо задать несколько параметров:

- **Фильтр поиска** (обязательный параметр). С помощью него формируется поисковый запрос.
- **Список атрибутов.** Задается для сокращения времени поиска.
- **Область поиска.** Определяет глубину поиска.
- **Сортировка.** Позволяет получить результат в нужном виде.

Фильтр поиска

При написании фильтра поиска используются выражения, строящиеся по определенным правилам, а именно (см. **таблицу 1**):

- каждое выражение должно быть заключено в скобках;
- в выражениях допускается использование операторов сравнения: «<», «<=», «=», «>=» и «>»;
- допускаются составные выражения, образуемые с помощью префиксных операторов «&», «|», «!».

Любой фильтр обычно состоит из двух логических частей. С помощью одной части определяют тип искомых объектов, в другой – искомое значение. Наличие фильтра необязательно.

Тип объекта определяется последним значением массива objectClass. Например, для учетной записи пользова-

Таблица 1. Операторы фильтра поиска

Оператор	Значение	Оператор	Значение
=	Эквивалентно	&	И
~=	Примерно равно	|	ИЛИ
<=	Меньше или равно	!	НЕ
>=	Больше или равно	*	ВСЕ

теля objectClass = person, для группы – group, для контейнера – organizationalUnit.

Приведу несколько характерных примеров фильтров:

- **(objectClass=*).** Все объекты имеют принадлежность к одному из классов. Данный фильтр вернёт все объекты в области поиска;
- **&((objectClass=person)(!objectClass=computer)).** Будут возвращены все объекты, принадлежащие к классу Person и не принадлежащие к классу computer. Такими объектами являются учетные записи пользователей;
- **&((description=test)(|(cn=User*)(cn=Group1))).** Будут возвращены все объекты с описанием test и именем, начинающимся со слова User, а также объект Group1.

Встречаются случаи, в которых необходимо указывать служебные символы в качестве значений, такие как звездочку, скобку и др. Чтобы реализовать эту возможность, вместо символа необходимо указать соответствующее ему кодовое значение, приведенное в **таблице 2**.

Атрибуты объекта

Для ускорения процедуры поиска используется свойство PropertiesToLoad. Используя метод Add()формируется массив полей, значения которых загружаются в память во время поиска. Например: PropertiesToLoad.Add("cn").

Область поиска

Область поиска задается с помощью свойства SearchScope:

- **SearchScope.Base или 0** – поиск осуществляется по корневому объекту, указанному в первой части запроса. Всегда возвращается либо один объект, либо пустой набор объектов. Эта область поиска чаще всего используется для проверки существования объекта, указанного в запросе.
- **SearchScope.OneLevel или 1** – поиск осуществляется в пределах указанного контейнера, указанного в первой части запроса. Поиск по вложенным объектам более низких уровней не производится. В поиск также не попадет и сам объект-контейнер.
- **SearchScope.SubTree или 2** – поиск осуществляется по всем вложенным объектам. В поиск при этом не попадает сам объект-контейнер. Эта область поиска задана по умолчанию.

Сортировка элементов

Сортировка элементов осуществляется с помощью метода Sort, поддерживающего два свойства: PropertyName и Direction. С помощью свойства PropertyName указывается название поля, по которому будет осуществляться сортировка, а с помощью Direction – направление. В случае Sort.Direction = 0 или Sort.Direction = "Ascending" осуществляется упорядочивание от «А» до «Я», при Sort.Direction = 1 или Sort.Direction = «Descending» – в обратном порядке.

Поиск объктов

В зависимости от конкретного случая для выполнения процедуры поиска после задания всех условий осуществляется вызов одного из методов поиска:

- **FindOne()** – возвращает только один/первый объект;
- **FindAll()** – возвращают коллекцию (массив) объектов, элементы которой удовлетворяют заданным критериям поиска.

Приведу по одному примеру на каждый из методов.

Таблица 2. Зарезервированные имена, используемые в фильтрах поиска

Символ	Значение
*	\2a
(	\28
)	\29
\	\5c
NUL	\00
/	\2f

Каталог Active Directory устроен так, что имя учетной записи группы или пользователя должны быть уникальны. Например, если необходимо определить список членов группы и если имя группы точно известно, то разумнее всего использовать метод FindOne(). В **листинге 1** приведен пример определения списка пользователей, являющихся членами группы Print Managers. Поскольку результат поиска единственный элемент, то управлять сортировкой выводимых значений не имеет смысла.

Замечание: комментарии в листинге на языке Power Shell начинаются с символа решетки (#).

Листинг 1. Поиск объекта с помощью метода FindOne()

```
# Получение доступа к корню домена
$Search = New-Object DirectoryServices.DirectorySearcher( ↵
      "LDAP://DC=Island,DC=ru")

# Критерий поиска – отображаемое имя группы
$Search.Filter = "(&(cn=Print Managers))"

# Поиск по всему каталогу Active Directory
$Search.SearchScope = 2

# Выполнение поиска
$result = $Search.FindOne()

# Получение доступа к группе с помощью относительного пути
$obj = $result.GetDirectoryEntry()

# Чтение элементов массива
$obj.psbase.properties.member | % {
$member = [ADSI]( "LDAP://"+$_)
Write-Host $member.Name}
```

Рассмотрим подробно алгоритм работы сценария. На первом этапе определяется контейнер, в котором будет осуществляться поиск. Затем осуществляется настройка параметров поиска: фильтр, глубина и др. Исходя из поставленной задачи можно составить несколько вариантов фильтра.

Предпочтение стоит отдать самому короткому, поскольку это, с одной стороны, упростит скорость поиска, а с другой – сделает ваш листинг более понятным. После того как все необходимые параметры заданы, осуществляется вызов метода FindOne(). Результат поиска в данном случае присваивается объекту $result.

Для получения доступа к указанному объекту используют метод GetDirectoryEntry(). Обратите внимание, что при его вызове относительный составной путь (distinguishedName) найденного объекта не указывается, поскольку он подставляется автоматически.

По своему действию строка:

```
$obj = $result.GetDirectoryEntry()
```

эквивалентна строке:

```
$obj=[ADSI]("LDAP://"+ $result.distinguishedName)
```

На завершающем этапе осуществляется чтение значений указанного атрибута. PowerShell представляет значения атрибутов в зависимости от их типа: в строку (числа, строки), в массив (массив). Получение доступа к данным осуществляется по шаблону:

```
$data = $obj.psbase.properties.СВОЙСТВО
```

где «СВОЙСТВО» – имя атрибута. Таким образом, для чтения строковых и числовых характеристик следует использовать **шаблон 1**, для массивов – **шаблон 2**.

```
Шаблон 1. Чтение строковых и числовых атрибутов

# Атрибуты name, primarygroup, description и т.д.
$data = $obj.psbase.properties.СВОЙСТВО
write-host $data


Шаблон 2. Чтение массивов

# Атрибуты member, memberOf и т.д.
$data = $obj.psbase.properties.СВОЙСТВО
ForEach ($item in $data) {
Write-Host $item}
```

Для чтения массивов используется оператор ForEach, который в отличие от других языков программирования в PowerShell имеет сокращенную форму записи (см. **шаблон 3**). Конструкция «ForEach ($element in $array){}» заменяется конструкцией «$array | % {}». В этом случае в цикле обращение к текущему элементу массива осуществляется с помощью $_.

```
Шаблон 3. Чтение массивов (сокращенная запись)

# Атрибуты member, memberOf и т.д.
$obj.psbase.properties.СВОЙСТВО | % {
Write-Host $_}
```

Метод поиска FindAll() используется в тех случаях, когда необходимо найти все объекты, удовлетворяющие указанным критериям, например, все учетные записи пользователей в указанном контейнере или выключенные учетные записи и др. Приведем пример поиска всех учетных записей пользователей (см. **листинг 2**), находящихся в указанном контейнере, имена которых начинаются с буквы «А».

```
Листинг 2. Поиск объекта с помощью метода FindAll()

# Получение доступа к корню домена
$Search = New-Object DirectoryServices.DirectorySearcher( ↵
      "LDAP://DC=Island,DC=ru")

# Критерий поиска – отображаемое имя группы
$Search.Filter = "(&(objectClass=User)(cn=A*) ↵
      (!objectClass=Computer))"

# Поиск по всему каталогу Active Directory
$Search.SearchScope = 2

# Сортировка результатов поиска
$Search.Sort.Direction = 1
$Search. Sort.PropertyName="sAMAccountName"

# Выполнение поиска
$Search.FindAll() | % {

# Получение доступа к группе с помощью относительного пути
$obj = $_.GetDirectoryEntry()

# Чтение данных
Write-Host $obj.samaccountname}
```

Исходя из поставленной задачи отметим, что фильтр поиска состоит из двух частей. В первой из них выбираются учетные записи пользователей (см. **таблицу 3**):

```
(&(objectClass=User)(!(objectClass=Computer)))
```

Вторая часть – из отобранных учетных записей выбрать начинающиеся с буквы «А». Фамилия пользователя хранится в значении атрибута sn (second name), поэтому фильтр будет выглядеть следующим образом:

```
(&(cn=A*))
```

Таблица 3. Взаимосвязь типов объектов Active Directory и значений параметра objectClass

Комментарий	Тип объекта	Значение objectClass	Фрагмент поискового запроса
Учетная запись компьютера	Computer	Top Person OrganizationalPerson User Computer	(&(objectClass=Computer))
Группа безопасности	Group	Top Group	(&(objectClass=Group))
Папка дерева каталогов Active Directory	OU	Top OrganizationalUnit	(&(objectClass=OrganizationalUnit))
Опубликованный в Active Directory сетевой принтер	Printer	Top Leaf ConnectionPoint PrintQueue	(&(objectClass=PrintQueue))
Опубликованная в Active Directory сетевая папка	Shared Folder	Top Leaf ConnectionPoint Volume	(&(objectClass=Volume))
Учетная запись пользователя, совместимая с доменами Windows NT	User	Top Person OrganizationalPerson User	(&(objectClass=User)(!(objectClass=Computer)))

Объединим два фильтра в один, получим:

```
(&(objectClass=User)(cn=A*) ↵
      (!objectClass=Computer))
```

Заключение

Уже на стадии поиска можно осуществлять сортировку значений выбранного поля в указанном направлении. Составлять запрос стало гораздо проще по сравнению с VBScript. Если раньше для составления запроса требовались хотя бы минимальные знания по SQL, то сейчас достаточно знать названия полей. С выходом Windows Server 2008 узнать поля стало еще легче: утилита ADSI Edit теперь входит в комплект операционной системы и устанавливается по умолчанию.

Переполнение буфера в TIBCO SmartSockets

Программа: TIBCO SmartSockets версии до 6.8.2; TIBCO SmartSockets Product Family (RTworks) версии до 4.0.5; TIBCO Enterprise Message Service (EMS) версии 4.0.0 до 5.1.2.
Опасность: Средняя.
Наличие эксплоита: Нет.
Описание: Уязвимость существует из-за неизвестной ошибки при обработке UDP-запросов. Удаленный пользователь может с помощью специально сформированного UDP-запроса вызвать переполнение стека и выполнить произвольный код на целевой системе.
URL производителя: www.tibco.com.
Решение: Установите последнюю версию с сайта производителя.

Множественные уязвимости в Ingate Firewall и SIParator

Программа: Ingate Firewall версии до 4.7.1; Ingate SIParator версии до 4.7.1.
Опасность: Средняя.
Наличие эксплоита: Нет.
Описание: 1. Уязвимость существует из-за ошибки, которая позволяет удаленному пользователю сконфигурировать юнит. Для успешной эксплуатации уязвимости для IPsec-туннеля должна быть разрешена настройка юнита.

2. Уязвимость существует из-за неизвестной ошибки в реализации IDS/IPS, которая позволяет SIP-пакетам обойти защиту от спуфинга и IPSec-проверки.

3. Уязвимость существует из-за ошибки при подтверждении подлинности DSA- и ECDSA-ключей. Удаленный пользователь может подменить сертификат сервера.

4. Уязвимость существует из-за ошибки при подтверждении подлинности HMAC-дайджеста, что повышает шанс успешной подмены SNMPv3-пакета.

5. Уязвимость существует из-за ошибки при применении политики reject для пакетов, приходящих из недоверенных шлюзов. Удаленный пользователь может обойти защиту от спуфинга.

6. Различные ошибки существуют при обработке SIP-пакетов. Удаленный пользователь может с помощью специально сформированных SIP-пакетов аварийно завершить работу устройства.
URL производителя: www.ingate.com.
Решение: Установите последнюю версию 4.7.1 с сайта производителя.

Обход ограничений безопасности в Citrix Licensing

Программа: Citrix Licensing 11.5, возможно, другие версии.
Опасность: Средняя.
Наличие эксплоита: Нет.
Описание: Уязвимость существует из-за неизвестной ошибки в компонентах License Management Console. Подробности уязвимости не сообщаются.
URL производителя: support.citrix.com/product/lic/v11.5.
Решение: Установите последнюю версию с сайта производителя.

Межсайтовый скриптинг в AXIGEN Mail Server

Программа: AXIGEN Mail Server 6.2.2, возможно, более ранние версии.
Опасность: Средняя.
Наличие эксплоита: Нет.
Описание: Уязвимость существует из-за недостаточной обработки входных данных в e-mail-сообщениях. Удаленный пользователь может с помощью специально сформированного e-mail-сообщения выполнить произвольный код сценария в браузере жертвы в контексте безопасности уязвимого сайта.
URL производителя: http://www.axigen.com/mail-server/products.php.
Решение: Установите последнюю версию 7.1.0 с сайта производителя.

Уязвимость в DB2 Content Manager

Программа: DB2 Content Manager версии до 8.4.1 Fix Pack 1.
Опасность: Средняя.
Наличие эксплоита: Нет.
Описание: Уязвимость существует из-за неизвестной ошибки в eClient. Подробности уязвимости не сообщаются.
URL производителя: www-306.ibm.com/software/data/cm/cmgr.
Решение: Установите последнюю версию 8.4.1 Fix Pack 1 с сайта производителя.

Отказ в обслуживании в Sun Java System Calendar Server

Программа: Sun ONE Calendar Server 6.0; Sun Java System Calendar Server 6 2005Q4 и более ранние версии.
Опасность: Средняя.
Наличие эксплоита: Да.
Описание: Уязвимость существует из-за ошибки при обработке большого количества HTTP-запросов, содержащих некорректное значение в параметре tzid. Удаленный пользователь может аварийно завершить работу веб-сервера.

Пример:

```
https://[host]:3443/?tzid=crash
```

URL производителя: www.sun.com.
Решение: Установите исправление с сайта производителя.

Повышение привилегий в HP-UX

Программа: HP-UX B.11.11, B.11.23 и B.11.31.
Опасность: Низкая.
Наличие эксплоита: Нет.
Описание: Уязвимость существует из-за ошибки в команде useradd при установке домашней директории и идентификатора группы. Злоумышленник может получить неавторизованный доступ к некоторым директориям и файлам.
URL производителя: www.hp.com
Решение: Установите исправление с сайта производителя.

Составил Александр Антипов

Доступный WiMAX

Подключение USB-модема Samsung SWC-U200 к маршрутизатору Asus WL-500gP

Павел Закляков
Георгий Пахомов

Мировое стремление развивать WiMAX-сети дошло и до России. Конечно, покрытие WiMAX-сетей по России далеко от GSM-покрытия «большой тройки», но сети развиваются, растёт интерес и к устройствам, поддерживающим WiMAX. В статье будет рассказано о том, как к многофункциональному маршрутизатору фирмы Asustek со встроенной ОС Linux подключить WiMAX-модем.

Не успели ещё внедрить стандарт 3G, как на рынке уже появился 4G – WiMAX. Его распространение не обошло стороной и Россию.

Зона покрытия пока невелика – Москва, Санкт-Петербург, а с недавнего времени Уфа.

С одной стороны, предложение протестировать сеть WiMAX бесплатно до 31 марта [3] или 31 мая [2] заманчиво, с другой, цена «входного билета» достаточно высока – не у всех найдутся лишние 4-5 тысяч рублей для покупки WiMAX-модема.

Не спешите перелистывать страницу, не найдя свой город в списке городов, охваченных WiMAX, ведь стандарт может завтра прийти и в ваш город.

Возможно, вам будет интересно узнать и про то, что внутри маршрутизатора Asus WL-500gP [1] используется Linux, а опыт подключения модема Samsung SWC-U200 удастся перенести на другие полезные вам устройства.

Есть спрос – будет предложение. Не успели оглянуться, как количество домашних устройств с сетевыми интерфейсами увеличилось, а их подключение к глобальным сетям свелось к использованию недорогих маршрутизаторов, сочетающих в себе ещё и функции коммутатора, межсетевого экрана, точки доступа, DHCP-сервера, сервера печати, файлового сервера и пр. Однако до сих пор найти недорогую точку доступа, поддерживающую подключения по WiMAX, довольно сложно из-за новизны стандарта.

Тут-то и пришла на помощь русская смекалка. Если у вас есть маршрутизатор Asus WL-500gP с USB-портами, а в руках вы держите USB WiMAX-модем Samsung SWC-U200, то что мешает соединить эти два устройства?

Оказалось, что ничто не мешает, только в штатном режиме работать вместе эти два устройства не хотят.

Дальше будет описано техническое решение по сопряжению указанных устройств.

Если же у вас есть только интерес в использовании WiMAX и нет желания заниматься настройкой оборудования, то спешим сообщить, что в продаже уже имеются готовые решения на базе Asus WMVN25E2+, а также готовые решения по сопряжению упомянутых нами устройств. Например, компания «ГНУ/Линуксцентр» предлагает не только купить адаптированные

маршрутизаторы ASUS WL-500gP или D-Link DIR-320, но и предоставляет возможность взять эти устройства на тестирование [6]. Не отстаёт по предложениям и WiMAXstore [7]. Мы же рассмотрим вопрос самостоятельной перепрошивки и настройки.

Взгляд внутрь

Получив в руки маршрутизатор и модем (см. **рис. 1**) для экспериментов, было очень сложно удержаться от того, чтобы не раскрутить их первым делом и не посмотреть, что же там находится внутри.

Для этого переворачиваем маршрутизатор и отклеиваем ножки, под которыми находятся 4 винта (см. **рис. 2**).

Разворачиваем устройство, переворачиваем и снимаем крышку (см. **рис. 3**). Довольно много места, отключаемый Wi-Fi-модуль, чипсет (см. **рис. 4**) и процессор Broadcom с памятью под экраном (см. **рис. 5**).

Если выполнить команды:

```
$ cat /proc/cpuinfo
...
system type             : Broadcom BCM4704 chip rev 9 pkg 0
cpu model               : BCM3302 V0.6
$ cat /proc/meminfo
        total:    used:    free:  shared: buffers:  cached:
Mem:  30887936 18956288 11931648        0  1871872  6782976
```

то увидим, что информация о процессоре и памяти совпала с тем, что можно увидеть в устройстве.

Выбор прошивки

Изучив обсуждения на форумах, можно прийти к выводу, что лучшим решением является использование прошивки от Олега Вдовикина. Судя по исходным кодам (изученным позже), где можно найти e-mail-адреса всех авторов, это выпускник МГУ с немалым стажем администрирования. Прошивки распространяются по лицензии GPL и доступны по адресу [9], там же можно найти ссылки на форум с предложением присоединиться к обсуждению маршрутизаторов http://wl500g.info.

Лицензия GPL не только обязывает авторов оставлять свои координаты, но и делать доступными исходные коды. Так, пытаясь найти корни, откуда взялась первоначальная прошивка, логичнее искать на сайте Asus, но что побудило Олега внести в неё правку? Ответ не ясен, так как связаться по указанному в исходных кодах адресу не получилось, но ясно одно, – Open Source-решения предоставляют энтузиастам возможности улучшения исходного кода. Из информации, предоставленной на сайте [9], можно предположить, что некая фирма hornington выложила исходные коды неофициальной прошивки 1.7.5.9 от Asustek (кстати, по лицензии GPL можно было бы их и затребовать), после чего улучшения кода не заставили себя долго ждать.

Изучая исходные коды версии 1.9.2.7-10 (март 2008 года), можно заключить, что она основана на версии ядра 2.4.20:

```
$ uname -a
```

Рисунок 1. Маршрутизатор Asus WL-500gP и USB-модем Samsung SWC-U200

Рисунок 2. Вид маршрутизатора снизу. Отклеиваем ножки для разбора

Рисунок 3. Вид маршрутизатора внутри

Рисунок 4. Чипсет маршрутизатора

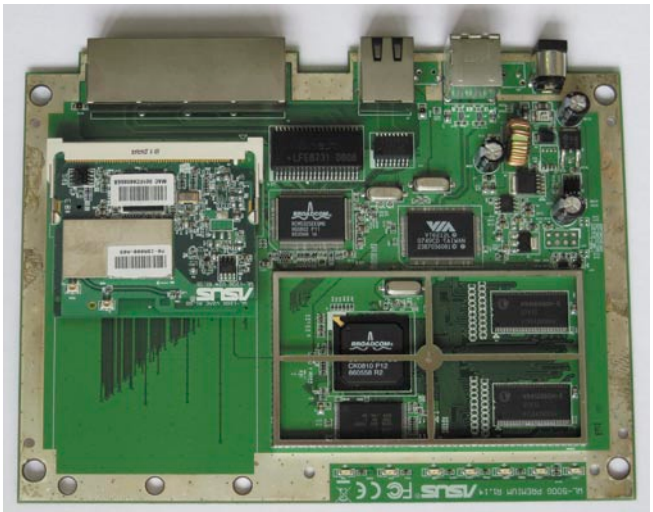


Рисунок 5. Вид платы с памятью и процессором без экрана

```
Linux WL-001FC660E3C3 2.4.20 #18 Sun Mar 30 13:13:29 MSD
2008 mips unknown
```

а поддержка обновлений прекратилась полтора-два года назад. При последней версии ядра 2.4.37.1 из серии 2.4.x на момент написания статьи следует сделать соответствующие выводы. Конечно, основные ошибки и критические уязвимости в версиях ядра и программного обеспечения на тот момент закрыты соответствующими патчами, которых на одно ядро накладывается около полусотни, но мысль о том, что жизнь не стоит на месте и новые версии могут быть чем-то лучше старых, промелькивает. Скорее всего, падение интереса к этой модели маршрутизатора связано с появлением новых.

Мы же, следуя [8], скачиваем последнюю прошивку из http://oleg.wl500g.info/1.9.2.7-9 (или http://code.google.com/p/wl500g) и устанавливаем её. Эта прошивка или другая нужны для того, чтобы ядро поддерживало модули и TUN/TAP-устройства, коим будет WiMAX-модем.

Замена прошивки

Существует два варианта прошивки модема [18]: через веб-интерфейс (см. **рис. 6**) и через утилиту восстановления. В обоих рекомендуется использовать только проводное подключение (не используя Wi-Fi и промежуточные сетевые устройства), отключить различные межсетевые экраны и обеспечить бесперебойное питание компьютера и маршрутизатора. С одной стороны, эти требования разумны, чтобы избежать лишних вопросов, но с другой стороны, они могут показаться чрезмерными и выставляющими читателей как не понимающих суть происходящих процессов. Например, логично спросить, а зачем отключать персональный межсетевой экран при прошивке через веб-интерфейс?

Ведь если я сам создавал правила пакетной фильтрации и соединение с маршрутизатором через браузер, установлено к моменту начала прошивки, то значит и во время перепрошивки соответствующие пакеты по протоколу TCP будут передаваться на 80-й порт маршрутизатора и приходят обратно без проблем. С надёжностью радиоканала и электропитания сложнее, но если у вас нет источника бесперебойного питания, то вы можете не расстраиваться и не тратить часы на его поиски.

В случае сбоя устройство всегда можно вернуть к заводским установкам, используя соответствующие кнопки, либо перепрошить с помощью утилиты восстановления. Можно предположить, что именно поэтому в веб-интерфейсе маршрутизатора нет функции сохранения старой прошивки (именно прошивки, а не настроек). Если ваш маршрутизатор будет находиться в общественном месте, то во избежание возможности восстановления заводских настроек без вашего участия следует выпаять кнопки (см. **рис. 7**).

При желании восстановить заводские настройки можно будет замкнуть контакты на плате (ведь такая необходимость возникает очень редко). Если всё же вам не доступен веб-интерфейс или произошёл сбой, то о втором способе перепрошивки с помощью утилиты восстановления коротко написано тут [15], для чего следует выполнить следующие шаги:

- Убеждаемся, что маршрутизатор, как и компьютер, через который мы будем им управлять, подключены к исправному источнику бесперебойного питания и ёмкости аккумуляторов которого хватит на время прошивки (обычно не более 10 минут).

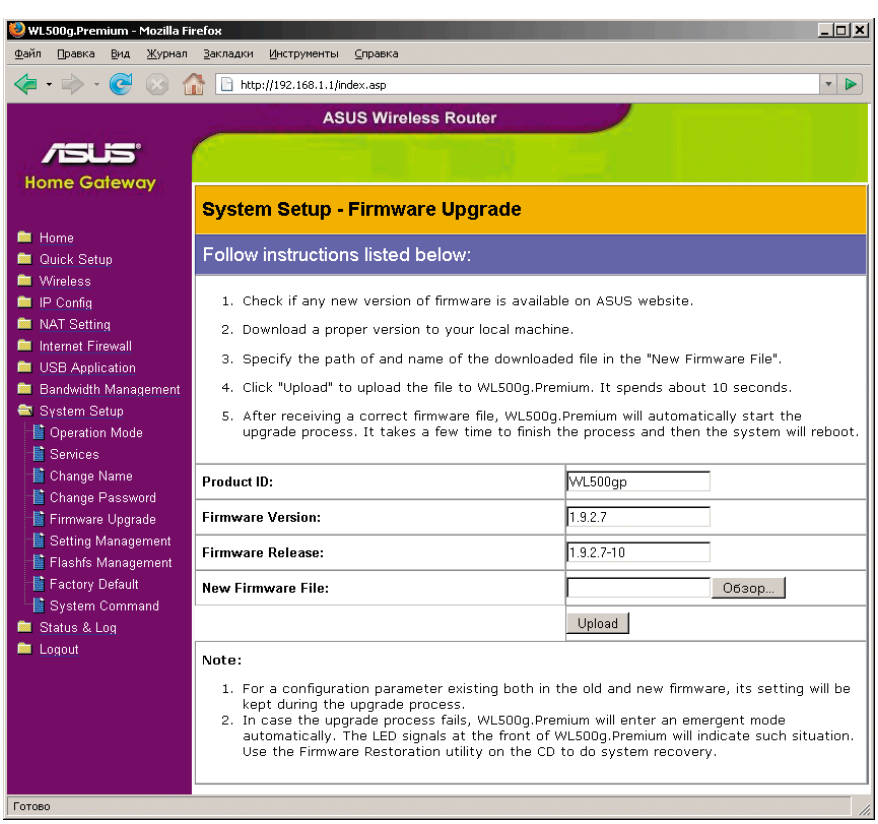


Рисунок 6. Обновление программного обеспечения через веб-интерфейс

- Убеждаемся, что маршрутизатор и компьютер соединены патч-кордом, либо промежуточные сетевые устройства между ними надёжны и обеспечены бесперебойным электропитанием.
- Нажимаем и держим кнопку перезагрузки на задней стенке маршрутизатора.
- Обесточиваем на несколько секунд маршрутизатор и снова его включаем.
- Дожидаемся мигания индикатора питания, после чего отпускаем кнопку перезагрузки.
- На компьютере пользователя запускаем ASUS Firmware Restoration Application (поставляется на диске вместе с маршрутизатором).
- В программе выбираем распакованную прошивку (файл .trx).
- Жмём Upload (загрузить).

Старая прошивка, как было отмечено выше, пропадает.

Драйверы от модема

Скачиваем уже скомпилированные модуль libusb и драйвер madwimax [11]. Если вас интересуют исходные коды, то их можно найти в [12] и на сайте проекта wimax [10].

Чтобы не отставать от жизни, рекомендуем посетить форум http://www.wl500g.info/showthread.php?p=119756&page=1, где ведётся практически ежедневная дискуссия, обсуждаются проблемы и появляются новые решения.

Также необходимые файлы можно найти и тут: http://lvk.cs.msu.su/~lasaine/madwimax/wl500g.

Загрузка файлов в маршрутизатор

Для загрузки файлов из-под ОС Linux можно воспользоваться штатной программой scp.

Но предполагая, что данная ОС может оказаться не у всех читателей, предложим и другое решение. Для этого нам понадобится утилита WinSCP [14] или одноимённый plugin к Far. Также может подойти pscp [13]. Если с утилитой для загрузки файлов вопросов быть не должно, то вопрос «куда загружать?» подразумевает два ответа.

Первый – во внутреннюю память маршрутизатора. В этом случае следует помнить, что она не резиновая и от каких-то функций, возможно, придётся отказаться. Все продаваемые решения используют этот подход.

Второй – подключить внешнюю USB-флешку, размер которой ограничен вашей фантазией, и использовать её. Конечно, занятый USB-порт и ещё одно устройство – плохо, но указанный путь наиболее прост для самостоятельной реализации, поэтому мы его и рассмотрим.

Для подключения USB-флешки лучше выбрать нижний порт маршрутизатора, так как верхний позже будет занят WiMAX-модемом.

Поддержка файловых систем FAT или NTFS в ядре маршрутизатора, скорее всего, будет отключена, поэтому флешку с большой вероятностью придётся переформатировать под файловую систему ext2 или ext3. Для тех, у кого есть ОС Linux под рукой и некоторый опыт работы с этой ОС, проблем быть не должно, остальным проще будет воспользоваться возможностями самого маршрутизатора [9], имеющего команды fdisk и mke2fs.

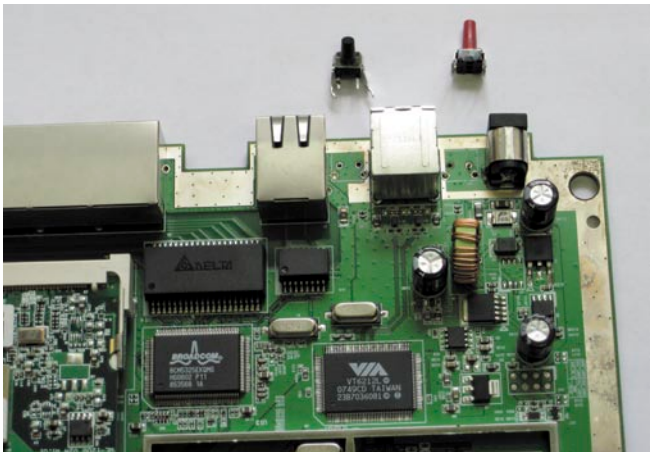


Рисунок 7. Выпаянные кнопки

Рисунок 8. USB WiMAX-модем Samsung SWC-U200

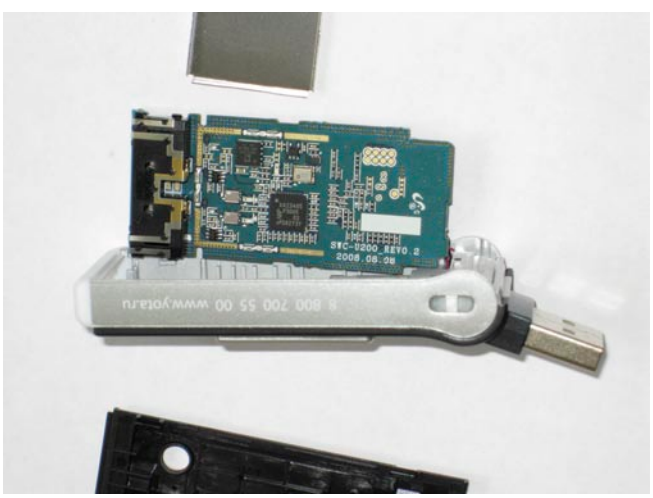


Рисунок 9. USB WiMAX-модем Samsung SWC-U200 в разборе

Отформатированную флешку монтируем в директорию /opt маршрутизатора, после чего создаём директорию /tmp/mnt/disc0_1/bin и осуществляем монтирование директории /tmp/mnt/disc0_1 в /opt. Объяснить, зачем выполняются такие операции, а не используются мягкие ссылки, сложно. Вполне возможно, что внутреннее программное обеспечение маршрутизатора может обращаться к файлам по определённому пути, но не может следовать по ссылкам (устройство может работать и как FTP/SAMBA-файловый сервер).

Так как команды, на наш взгляд, не являются потенциально опасными, мы их оставили без изменений:

```
# mount -o sync,noatime,rw ↵
     /dev/scsi/host0/bus0/target0/lun0/part1 /opt
# mkdir /tmp/mnt/disc0_1/bin
# mount -o bind /tmp/mnt/disc0_1 /opt
```

Создаём временную директорию:

```
# mkdir -p /opt/tmp/ipkg
```

Упрощаем жизнь

Для того чтобы упростить себе жизнь, установим дополнительное программное обеспечение, для этого подключаем маршрутизатор через порт WAN к Интернету (после настройки WiMAX можно использовать и этот канал) и устанавливаем программы от суперпользователя. Для того чтобы устанавливались последние версии, следует выполнить команду обновления:

```
$ ipkg.sh update
Downloading http://ipkg.nslu2-linux.org/feeds/optware/oleg/cross/
stable/Packages.gz
Inflating http://ipkg.nslu2-linux.org/feeds/optware/oleg/cross/
stable/Packages.gz
Updated list of available packages in /opt/lib/ipkg/lists/optware
Successfully terminated.
```

Если не сделать обновления списка доступных пакетов для установки, то при последующих шагах может появиться информация о том, что существует более новая версия устанавливаемого вами пакета и надо выполнить команду «ipkg update» перед установкой.

Для установки пакета screen (ссылка на него будет в конце статьи) выполнить команду:

```
$ ipkg install screen
Installing screen (4.0.3-2) to /opt/...
Downloading http://ipkg.nslu2-linux.org/feeds/optware/oleg/cross/
stable/screen_4.0.3-2_mipsel.ipk
Installing termcap (1.3.1-2) to /opt/...
Downloading http://ipkg.nslu2-linux.org/feeds/optware/oleg/cross/
stable/termcap_1.3.1-2_mipsel.ipk
Configuring screen
chown: unknown user name: root
Configuring termcap
Successfully terminated.
```

Аналогично с командами:

- ipkg install ipkg-opt
- ipkg install mc
- ipkg install gzip
- ipkg install bzip2

После того как программное обеспечение установлено либо внесены правки в конфигурационные файлы, следует сохранить изменения во внутреннюю flash-память маршрутизатора, для этого выполняем следующие три команды:

```
$ flashfs save
tar: Removing leading '/' from member names
tmp/local/
tmp/local/etc/
tmp/local/etc/dropbear/
tmp/local/etc/dropbear/dropbear_rsa_host_key
tmp/local/etc/dropbear/dropbear_dss_host_key
tmp/local/sbin/
tmp/local/sbin/pre-shutdown
tmp/local/sbin/post-mount
tmp/local/sbin/post-firewall
tmp/local/sbin/post-boot
tmp/local/root/
tmp/local/root/.mc/
tmp/local/root/.mc/Tree
tmp/local/root/.mc/filepos
tmp/local/root/.mc/ini
tmp/local/root/.mc/history
tmp/local/root/.mc/cedit/
-rw-r--r--    1 gp     root          3081 May  8 19:03 /tmp/flash.tar.gz
Check saved image and type "/sbin/flashfs commit" to commit changes
```

```
$ flashfs commit
.
Committed.
```

```
$ flashfs enable
```

Последняя команда ничего не выводит.

Для простоты эти три команды можно написать и в одну строчку в виде «flashfs save && flashfs commit && flashfs enable», что нередко можно увидеть на форумах, описаниях и в howto.

Для корректной работы в mc надо выполнить ещё две команды, устанавливающие переменные TERMINFO и TERM.

```
export TERMINFO="/opt/share/terminfo"
export TERM="xterm"
```

Поддержка WiMAX-модема

Далее, небходимо перейти к тому, с чего начался раздел, и переписать скачанные ранее файлы liveusb и madwimax, распаковав liveusb в директорию /opt, а madwimax в /opt/sbin. Как вариант это можно сделать через файловые менеджеры Far+WinSCP и mc. После необходимо проследить, чтобы файл /opt/sbin/madwimax имел установленным атрибут выполнения.

Например, командой:

```
ls -l /opt/sbin/madwimax
```

если права на запуск не выставлены, то их стоит установить командой:

```
chmod +x /opt/sbin/madwimax
```

Либо можно скачать файлы заново из консоли и там же распаковать:

```
cd /tmp
wget http://lvk.cs.msu.su/~lasaine/madwimax/wl500g/ ↵
     libusb-1.0-mipsel.tgz
wget http://lvk.cs.msu.su/~lasaine/madwimax/wl500g/ ↵
     madwimax-latest-mipsel.tgz
cd /
tar -xzf /tmp/libusb-1.0-mipsel.tgz
tar -xzf /tmp/madwimax-latest-mipsel.tgz
```

По завершению распаковки скачанные архивы можно удалить.

```
rm /tmp/libusb-1.0-mipsel.tgz ↵
     /tmp/madwimax-latest-mipsel.tgz
```

В этом случае атрибуты должны быть настроены правильно после распаковки архива.

Сами файлы теперь находятся на флешке, подключенной к маршрутизатору, но далее необходимо, чтобы кто-то после перезагрузки устройства монтировал флешку, подгружал модуль tun.o, запускал madwimax, настраивал сетевой интерфейс, перепрописывал маршрутизацию. Для того чтобы не выполнять эти все функции вручную, создадим два скрипта, которые позволят автоматизировать вышеописанную работу.

«Поднимаем» SSH

Если вы планируете использовать локальное администрирование в доверенной сети, то можно вполне обойтись программой telnet и протоколом FTP либо флешкой для переноса файлов. Но если вы планируете настраивать ваш модем через Интернет либо ваша локальная сеть не является доверенной, то лучше потратить несколько минут и настроить SSH-сервис, использование которого предпочтительнее с точки зрения безопасности.

Подключаемся по протоколу telnet к адресу маршрутизатора. По умолчанию это 192.168.1.1. Логин и пароль по умолчанию – admin/admin.

Замечание: предполагая, что статью могут читать не только администраторы и продвинутые пользователи, предложим таким читателям несколько советов.

- ☑ **Совет 1.** Если вы используете Windows Vista, то telnet-клиент по умолчанию отсутствует в системе. Включить его можно через «Панель управления → Программы и компоненты → Включение и отключение компонентов Windows → Клиент Telnet».
- ☑ **Совет 2.** Используйте лучше утилиту PuTTY [13].
- ☑ **Совет 3.** Запуск сервиса ssh и его использование позволяют защититься от угрозы конфиденциальности, но не приводит к отключению сервиса telnet. Поэтому, если вы хотите избежать других атак на маршрутизатор через telnet, то следует дополнительно позаботиться об этом.

Начиная с версии 1.7.5.9-4 в комплект поставки программного обеспечения маршрутизатора уже входит ssh-демон dropbear поддерживающий как RSA- так и DSS-ключи. Наша задача – сгенерировать пару ключей и запустить демон. Для этого после подключения создадим директорию, где будут храниться ключи.

```
# mkdir -p /usr/local/etc/dropbear
```

Сгенерируем DSS- и RSA-ключи:

```
# dropbearkey -t dss -f /usr/local/ ↵
      etc/dropbear/dropbear_dss_host_key
# dropbearkey -t rsa -f /usr/local/ ↵
      etc/dropbear/dropbear_rsa_host_key
```

После того как ключи созданы, вы можете запустить ssh-демон, просто набрав dropbear, но в случае перезагрузки маршрутизатора запуск придётся повторить. Чтобы осуществлять запуск сервиса каждый раз вручную, пропишем его в авторазгрузку (файл post-boot) и сохраним настройки во флеш-память (flashfs). Для этого вначале проверим наличие файла post-boot командой:

```
# ls /usr/local/sbin/post-boot
```

В случае ошибки «No such file or directory» (файла нет) его надо создать. Для этого создадим, при необходимости, вышестоящие директории, запишем имя командного интерпретатора первой строчкой и изменим атрибуты файла командами:

```
# mkdir -p /usr/local/sbin/
# echo "#!/bin/sh" >> ↵
      /usr/local/sbin/post-boot
# chmod +x /usr/local/sbin/post-boot
```

После, когда файл уже создан (или существовал ранее), допишем в конец строчку запуска ssh-демона dropbear:

```
#  echo "dropbear" >> ↵
      /usr/local/sbin/post-boot
```

После сохраним изменения во флеш-память и активируем работу с сохранёнными настройками:

```
#  flashfs save && flashfs commit && ↵
      flashfs enable
```

Выйти из telnet-сессии можно командой «exit».

Автоматизация загрузки

Из консоли запускаем mc и дописываем в файл /usr/local/sbin/post-boot две строчки:

```
export TERMINFO="/opt/share/terminfo"
export TERM="xterm"
```

Также редактируем /usr/local/sbin/post-mount и записываем в него:

```
#!/bin/sh

mount -o sync,noatime,rw ↵
      /dev/scsi/host0/bus0/target0/lun0/part1 /opt
mount -o bind /tmp/mnt/disc0_1 /opt
insmod tun.o
/opt/sbin/madwimax --device 04e9:6761
sleep 45
/opt/etc/madwimax/event.sh if-up tap0
```

Значение 04e9:6761 идентифицирует вставленный в маршрутизатор WiMAX-модем. Если у вас имеется дополнительный компьютер с ОС Linux и свободным USB-портом, то вставьте в него модем и посмотрите файл /var/log/messages, где вы сможете увидеть примерно следующее:

```
May  8 21:46:57 notebook kernel: usb 1-7: new high speed USB
device using ehci_hcd and address 2
May  8 21:46:57 notebook kernel: usb 1-7: configuration #1 chosen
from 1 choice
May  8 21:46:57 notebook kernel: usb 1-7: New USB device found,
idVendor=04e9, idProduct=6761
May  8 21:46:57 notebook kernel: usb 1-7: New USB device strings:
Mfr=1, Product=2, SerialNumber=0
May  8 21:46:57 notebook kernel: usb 1-7: Product: Samsung USB
mWiMAX Modem..
May  8 21:46:57 notebook kernel: usb 1-7: Manufacturer: SAMSUNG
ELECTRONICS Co.Ltd.
May  8 21:46:57 notebook kernel: Initializing USB Mass Storage
driver...
May  8 21:46:57 notebook kernel: scsi6 : SCSI emulation for USB
Mass Storage devices
May  8 21:46:57 notebook kernel: usbcore: registered new interface
driver usb-storage
May  8 21:46:57 notebook kernel: USB Mass Storage support
registered.
May  8 21:47:02 notebook kernel: scsi 6:0:0:0: CD-ROM
Samsung  Install Disk     0.10 PQ: 0 ANSI: 0 CCS
May  8 21:47:02 notebook kernel: sr1: scsi3-mmc drive: 48x/48x
xa/form2 cdda tray
May  8 21:47:02 notebook kernel: sr 6:0:0:0: Attached scsi
generic sg2 type 5
May  8 21:47:02 notebook kernel: sr1: Hmm, seems the drive
doesn't support multisession CD's
```

Как легко заметить, указанные значения – это idVendor и idProduct. Интересно отметить, что модем на самом деле является и вторым устройством, а именно моделирует работу USB CD-ROM со вставленным компакт-диском с драйверами модема. Поэтому для ОС Windows драйверы на компакт-диске, как это бывает обычно, не поставляются.

Также ID устройства можно узнать и из команды lsusb:

```
Bus 001 Device 002: ID 04e9:6761 PC-Tel, Inc.
```

К сожалению, в маршрутизаторе используется урезанный комплект программного обеспечения, и поэтому команды lsusb там нет. Если следовать [8], значение бывает

или 04e9:6761, или 04e8:6761 и определяется перебором. С неправильным значением модем просто не заработает. В новых прошивках маршрутизатора предусмотрена возможность посмотреть ID подключенных к USB-порту устройств через веб-интерфейс: Status & Log, Diagnostic Info, USB Devices, в прошивке, используемой авторами, такой возможности нет.

Строчки sleep 45 и /opt/etc/madwimax/event.sh if-up tap0 прописаны авторами для поднятия сетевого интерфейса модема (tap0) после загрузки маршрутизатора. Значение задержки установлено опытным путём и может варьироваться. Обычно 45 секунд хватает для того, чтобы модем успел установить связь с сетью WiMAX. Предполагается, что расположение модема выбрано оптимально. Подробнее как это сделать будет рассказано в конце статьи.

Ещё один вариант загрузки модуля поддержки WiMAX-модема предложен в [15], где вместо строчек:

```
insmod tun.o
/opt/sbin/madwimax --device 04e9:6761
```

используются:

```
insmod /lib/modules/tun.o
(while true; do /opt/sbin/madwimax -qof; sleep 10; done) &
```

Так как авторам вариант с бесконечным циклом не понравился, мы от него отказались.

Замечание: если файл /usr/local/sbin/post-mount отсутствовал у вас изначально, то создать его можно командой:

```
touch /usr/local/sbin/post-mount
```

или нажатием <CTRL> + <F4> в mc. После завершения редактирования необходимо файлу присвоить атрибут исполняемости командой:

```
chmod +x /usr/local/sbin/post-mount
```

При создании (редактировании) файла /usr/local/sbin/post-mount мы указали команды для монтирования флешки, загрузки модуля поддержки TUN/TAP-устройств, инициализации модема и в конце предусмотрительно обратились к программе event.sh для поднятия сетевого интерфейса и присваивания ему сетевых настроек.

Чтобы не делать одну операцию два раза, сделанные изменения мы не сохраняем во flash-памяти маршрутизатора, так как ниже пойдёт речь о программах event.sh и udhcpc.script, которые надо создать и после сохранить.

Получение сетевых настроек

Создадим файл event.sh, который будет отвечать за получение IP-адреса и других сетевых параметров по протоколу DHCP от Yota. Файл udhcpc.script сохранит полученные параметры в систему и изменит таблицу маршрутизации так, чтобы внешним интерфейсом считался не WAN Enternet-модем, а WiMAX USB-модем.

Создаём файлы с установленным разрешением на запуск:

```
touch /opt/etc/madwimax/event.sh
touch /opt/etc/madwimax/udhcpc.script
chmod +x /opt/etc/madwimax/event.sh
chmod +x /opt/etc/madwimax/udhcpc.script
```

И наполняем следующим содержимым.
Файл event.sh:

```
#!/bin/sh
# Usage: event.sh

case "$1" in
start)
      ;;
end)
      ;;
if-up)
      /sbin/udhcpc -i "$2" -p /var/run/udhcpc1.pid -s ↲
               /opt/etc/madwimax/udhcpc.script -b
      iptables -A INPUT -i "$2" -m state --state NEW ↲
               -j SECURITY
      iptables -A FORWARD -i "$2" -m state --state NEW ↲
               -j SECURITY
iptables -t nat -A POSTROUTING -o "$2" ! -s ↲
      `ifconfig "$2" | grep 'inet addr' | tr ':' ' ' | ↲
      awk '{print $3}'` -j MASQUERADE
      iptables -t mangle -A FORWARD -p tcp ↲
               --tcp-flags SYN,RST SYN ↲
               -j TCPMSS --clamp-mss-to-pmtu
      ;;
if-down)
      cat /var/run/udhcpc1.pid | xargs -i kill -TERM {}
      ;;
*)
      echo "Usage: $0 {start|end|if-up|if-down}" >&2
      exit 3
      ;;
esac
```

Файл udhcpc.script:

```
#!/bin/sh

RESOLV_CONF=/tmp/resolv.conf

case "$1" in
        bound|renew)
        ifconfig $interface up
        ifconfig $interface $ip netmask $subnet
        route add default gw $router
                for ii in $dns; do
                echo nameserver $ii >> $RESOLV_CONF
                done
# trigger dnsmasq restart
        kill -s SIGHUP `pidof dnsmasq`
        ;;
        deconfig)
        ifconfig $interface 0.0.0.0
        echo deleting $RESOLV_CONF
        echo -n > $RESOLV_CONF
        kill -s SIGHUP `pidof dnsmasq`
        ;;
esac
```

При желании готовый файл udhcpc.script можно взять тут: http://lvk.cs.msu.su/~lasaine/madwimax/wl500g/udhcpc-script.tgz и по аналогии с командами выше для liveusb и madwimax скачать и распаковать.

Файл event.sh является основным и запускается первым. После, если необходимо, он вызывает вспомогательный скрипт udhcpc.script.

Сохраним изменения во flash-памяти маршрутизатора:

```
#  flashfs save && flashfs commit && flashfs enable
```

Можно попробовать выполнить команды, указанные в /usr/local/sbin/post-boot, вручную, после чего, в случае обнаружения сети WiMAX, у модема изменится цвет индика-

тора на синий и оба устройства будут работать, как мы этого ожидаем. Если это для вас сложно или подключение таким способом не получилось, перезагрузите маршрутизатор командой:

```
# reboot
```

После перезагрузки маршрутизатор автоматически подмонтирует USB-флешку, загрузит с неё модуль TUN/TAP-устройств, драйвер модема, после чего, если модем обнаружит сеть, будут получены сетевые настройки и перепрописана маршрутизация внутри устройства.

На этом моменте настройку маршрутизатора можно считать законченной и переходить к использованию. Однако есть ряд вещей, о которых лучше знать читателям.

Диагностика сети WiMAX

Рекомендуем запустить в консоли команду madwimax с ключом -help и узучить назначение ключей.

Например, madwimax с ключом -f может выводить различную диагностическую информацию в консоль, либо при запуске как «madwimax -fvvd» записывать всю информацию в syslog, что не очень удобно на устройстве с ограниченным размером диска, либо через команду:

```
madwimax -fvvd -l /tmp/mnt/disc0_1/madwimax.log
```

переопределить вывод на флешку. Постоянно работать в таком режиме не рекомендуется, так как лог-файл быстро пополняется.

Проблема отключения

Когда вы долго не передаёте данные в сети, провайдер вас отключает из-за бездействия, после чего необходимо переподключение. Эту проблему, по аналогии с GPRS и EVDO от операторов сотовой связи, можно решить периодической посылкой пакетов. Самое простое решение, предложенное на форуме, – «пинговать» DNS-сервер провайдера. Для этого предлагается установить утилиту screen (выше по тексту указано, как её установить) и после дописать в файл /opt/etc/madwimax/event.sh в конце секции if-up) строчку /opt/bin/screen -dm ping ip_адрес_dns_провайдера, к указанному решению можно ещё дописать ключ -s 0, минимизирующего размер поля данных отправляемых пакетов, например:

```
/opt/bin/screen -dm ping  -s 0 94.25.208.74
```

После запуска команды можно увидеть её в списке процессов:

```
$ ps | grep ping
571 gp       764 S   /opt/bin/SCREEN -dm ping -s 0 94.25.208.74
572 gp       404 S   ping -s 0 94.25.208.74
```

а также с помощью tcpdump зарегистрировать исходящие и входящие пакеты:

```
$ tcpdump -i tap0 icmp
```

```
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on tap0, link-type EN10MB (Ethernet), capture size 68 bytes
20:05:30.915018 IP 10.129.27.141 > yota.ru: icmp 28: echo request seq 54
20:05:31.019343 IP yota.ru > 10.129.27.141: icmp 28: echo reply seq 54
20:05:31.915008 IP 10.129.27.141 > yota.ru: icmp 28: echo request seq 55
20:05:32.109125 IP yota.ru > 10.129.27.141: icmp 28: echo reply seq 55
```

Многие заметят, что хорошо бы использовать ключ -i для задания интервала посылки ICMP-пакетов в секундах, чтобы уменьшить нагрузку на сеть, но, увы, так сделать не получится, так как в программе busybox, установленной в модеме, используется урезанная функциональность утилиты ping. Решить проблему можно установкой полнофункциональной версии ping либо hping [19]. Последняя утилита обладает большими возможностями и рекомендуется авторами.

Несколько слов о сети Yota

Для того чтобы работать в WiMAX-сети провайдера Yota, следует не только зарегистрироваться, но и найти оптимальную точку приёма сигнала. Далее в статье рассказываются технические вопросы подключения модема Samsung SWC-U200 к маршрутизатору со встроенной ОС Linux, подразумевая, что читатель уже подключён к этой сети. Желая расширить аудиторию читателей, статью можно трактовать и как отдалённое пособие по настройке WiMAX в Linux, а также добавить немного полезной информации, интересной не только системным администраторам, но и будущим пользователям WiMAX.

Полезная информация о сети и о модеме

Подключить модем в ОС Windows несложно. Как было описано выше, на тот момент, когда драйверы не установлены, модем определяется как обычный USB CD-ROM, к которому в операционной системе должны быть штатные драйверы. В случае если у вас не запрещён запуск из Autorun.inf, установка начнётся автоматически. Несмотря на то что модем был куплен в начале мая, в его «USB CD-ROM»-памяти были драйвера версии 1.9.6, когда на сайте yota.ru доступна для скачивания версия 1.2.0 [20].

Лучше отключить автозапуск и установить драйверы вручную. После установки программы Yota Access и подключения модема запустилось обновление (см. **рис. 10**). Другой вариант обновления и более «тонкой настройки» модема описан в [26].

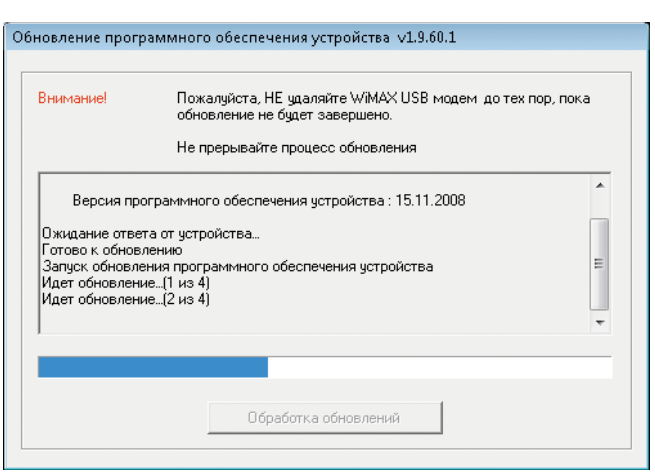


Рисунок 10. Обновление программного обеспечения модема

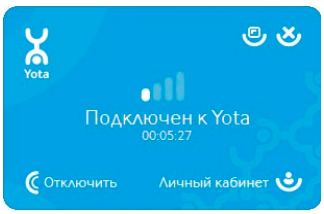


Рисунок 11. Окно Yota Access после подключения

После завершения обновления в результате перемещения модема в пространстве удалось обнаружить сеть, хотя, судя по карте покрытия, в месте расположения модема сигнала быть не должно. Вывод: для нахождения сети подключите модем с использованием USB-удлинителя, что даст возможность гибко перемещать модем в пространстве. Поворот работающего модема на 90 градусов, как и смещение на 5-10 см могут привести к потери модемом сигнала и отключению от сети, как и наоборот.

Поиск сигнала

Для поиска сигнала или точки наилучшего приёма лучше всего воспользоваться утилитой DebugScreen. В директории с установленной программой Yota Access можно найти одноимённый exe-файл, но запуск утилиты производится более хитрым образом. На форумах можно найти информацию о том, как её запустить, но на практике это не получилось. Не долго думая, мы позвонили по телефону, указанному на модеме. На удивление техническая поддержка компетентно ответила на все наши вопросы и даже подсказала, как запустить DebugScreen, что стало приятной неожиданностью. Для этого надо щёлкнуть на индикатор приёма в окне Yota Access (см. **рис. 11**).

И нажать <Ctrl> + <Alt> + <Shift> + <F1>, после чего появится окно для ввода пароля, где ввести «1234». В появившемся окне Debug Screen нажать меню File → Start. После этого появится окно диагностики (см. **рис. 12**).

Наиболее интересный параметр это RSSI – уровень сигнала. Ещё можно обратить внимание на параметр BSID, чем-то напоминающий по форме записи MAC-адрес, – это ID базовой станции, с которой вы работаете.

Замечание: по адресу[21] содержатся не только наблюдения за данными, выводимыми утилитой Debug Screen, но и ещё один способ её запуска. Для этого необходимо создать ярлык для DebugScreen.exe на рабочем столе, после на нём правой кнопкой мыши выбрать «Свойства» и в поле «Обьект» после последней кавычки через пробел дописать параметр 0x12345678. После сохранения изменений ярлык для запуска утилиты готов. Пароль тот же, что и при запуске через программу Yota Access, – 1234.

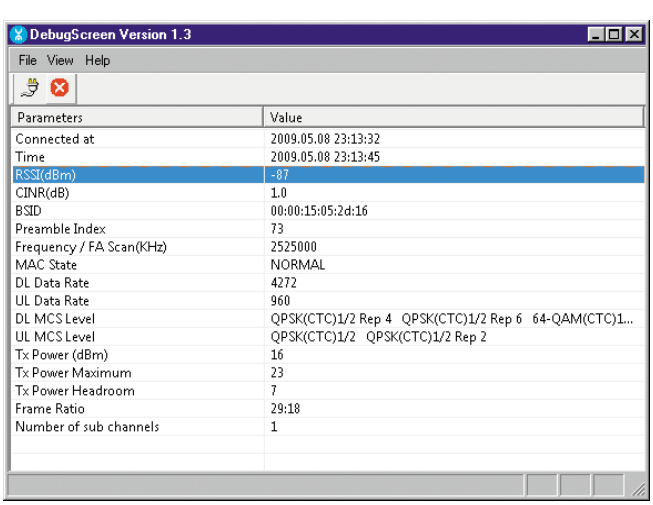


Рисунок 12. Утилита Debug Screen

Сложно сказать, где ещё можно использовать информацию, полученную из программы отладки, но два применения можно найти сразу: первое – это позиционирование модема относительно базовых станций, например, когда сигнал Глонасс или GPS не принимается, (в тоннелях, зданиях и пр.), как альтернатива сотовому и Wi-Fi позиционированию. А второе применение – создание любительских общественных карт покрытия сети, например [22].

Ошибки регистрации

После подключения к сети можно зайти только на сайт yota.ru. Для того чтобы получить доступ дальше сайта провайдера (даже на момент тестирования), следует зарегистрироваться. Регистрация может производиться с любого компьютера. Но после, чтобы привязать WiMAX-модем к вашему личному кабинету, всё равно придётся зайти в кабинет через сеть Yota. «Логин или номер лицевого счёта» и «пароль», указанные на пластиковой карточке, приложенной к модему, не подходят для входа в личный кабинет. Данная информация понадобится лишь на последнем шаге регистрации. То есть логин и пароль у вас будут собственные, не привязанные к карте и счёту. После регистрации модема в личном кабинете следует переподключиться к сети, причём сделать это надо с физическим отключением модема от компьютера.

Улучшение приёма

Если вы посмотрите внимательно на **рис. 8,** то увидите, что модем имеет два разъёма для подключения внешней антенны. У вас эти разъёмы будут заклеены белой наклейкой, которая на фотографии переклеена правее. Есть разъём – будет переходник для внешней антенны (см. **рис. 13**). В комплекте переходник не поставляется, но его можно спаять самостоятельно либо купить, например на сайтах [23-25].

Используя направленные антенны, вполне возможно добиться приёма сигнала там, где для работы через встроенную антенну не достаёт мощности сигнала.

А можно без флешки?

В нашем примере мы устанавливали midnight commander и другие программы – удобные, но не нужные для непосредственной работы модема и маршрутизатора. Логично предположить, что если мы не будем поднимать FTP-сервер и использовать другие программы, то можно всё лишнее стереть и обойтись минимумом файлов. Возникает вопрос: если файлы уместятся по объёму, то можно ли записать их во внутреннюю flash-память маршрутизатора и обойтись без USB-флешки? Ответ – можно! Как раз вышла статья о том, как это сделать [27].

А можно подключить два WiMAX-модема?

Логично предположить, что если у устройства два USB-порта, то даже без использования USB-разветвителей можно подключить второй WiMAX-модем. А можно ли настроить два модема на одновременную работу? Учитывая, что внутри маршрутизатора имеется пакет iproute2, можно не только

подключить одновременно два WiMAX-модема, но и обеспечить балансировку нагрузки штатными средствами маршрутизатора. Правда для этого потребуется некоторое знание ОС Linux и утилиты ip из вышеуказанного пакета. Читатели могут заметить, что два модема, подключенные к одной базовой станции одного провайдера, повысят скорость, но не повысят надёжность. Но не забывайте, что сеть активно развивается, и у жителей столицы уже сейчас есть возможность выбора между сетями «Комстар-ОТС» и Yota.

Нужен com-порт?

На плате маршрутизатора имеется нераспаянный разъём, который можно распаять и использовать (см. **рис. 14**).

Заключение

Сеть WiMAX развивается, растёт число устройств – это приятный факт. Даже есть официальный драйвер для MacOS. Обидно лишь одно, что драйверы под Linux идут не изначально с устройствами, как было бы правильнее, а получены с помощью исследования двоичных файлов и восстановления исходного алгоритма [10].

Рисунок 13. Переходник для антенны

1. Страница маршрутизатора Asus WL-500gP – http://www.asuscom.ru/products.aspx?l1=12&l2=43&l3=0&l4=0&model=1712&modelmenu=1.
2. WiMAX-провайдер Yota – http://www.yota.ru/ru.
3. WiMAX-провайдер «Комстар» – http://wimax.comstar.ru.
4. Yota Egg – автономный WiMax-роутер – http://wimax.livebusiness.ru/tags/WIMAX_router.
5. Готовое WiMAX-решение на базе Asus WL 500gP – http://www.linuxcenter.ru/shop/wimax/devices/asus_wl500gpv2.
6. В Москве появились WiMax-роутеры – http://wimax.livebusiness.ru/news/5806.
7. WiMAX-оборудование – http://wimaxstore.ru/shop/wimax/devices/asus_wl500gpv2.
8. Инструкция: как раздавать Интернет от Yota через WiMAX-модем Samsung SWC-U200 и роутера ASuS WL-500gP – http://www.wimaxinfo.ru/?q=node/201.
9. Страница альтернативных прошивок для Asus WL-500g от Олега Вдовикина – http://oleg.wl500g.info.
10. madwimax A reverse-engineered Linux driver for mobile WiMAX devices based on Samsung CMC-730 chip – http://code.google.com/p/madwimax.
11. Драйверы для модема WiMAX – http://files.linux.ru/index.php?dir=wimax/asus-500gP.
12. Библиотека libusb – http://libusb.wiki.sourceforge.net/Libusb1.0.
13. PuTTY: A Free Telnet/SSH Client – http://www.chiark.greenend.org.uk/~sgtatham/putty.
14. WinSCP Plugin to FAR File Manager – http://winscp.net/eng/docs/far.
15. Yota-роутер или wimax2wifi за 15 минут – http://www.rusdoc.ru/articles/yota-router_ili_wimax2wifi_za_15_minut/18369/print.
16. Информация о ASUS WL-500g Premium – http://oldwiki.openwrt.org/OpenWrtDocs(2f)Hardware(2f)Asus(2f)WL500GP.html.
17. Сравнительная таблица маршрутизаторов Asus WL-500 и других – http://notepad.timyou.com/page/Router+Hacks?t=anon.
18. Firmware upgrading HOWTO WL-500g/WL-500gx Tutorials – http://www.wl500g.info/showthread.php?t=1329.
19. Hping – Active Network Security Tool – http://www.hping.org.
20. Последняя версии программы Yota Access, май 2009 – http://www.yota.ru/downloads/YotaAccess_v.120_BL22.exe.
21. Ветка форума «Как правильно тестить Йоту + софт для этого» – http://forum.yotatester.ru/showthread.php?t=51.
22. Карта покрытия WiMAX – http://www.wimaxmonitor.ru.
23. Переходник для внешней антенны для модема WiMAX YOTA – http://www.radioport.ru/index.cgi/shop?id=2207&dir=13.
24. Антенный переходник – http://www.yota-shop.ru/index.php?go=goods&cat=10&gid=119.
25. Антенный переходник – http://forwimax.ru/show_good.php?idtov=90025.
26. Обновление прошивки и «тонкая настройка» модема Samsung SWC-U200 – http://yota-wimax.ru/category/yota-firmware.
27. Делаем WiMAX-роутер (WI500gP+SWC-U200) без флешки – http://yota-wimax.ru/wimax-device/delaem-wimax-router-wl500gpswc-u200-bez-fleshki.

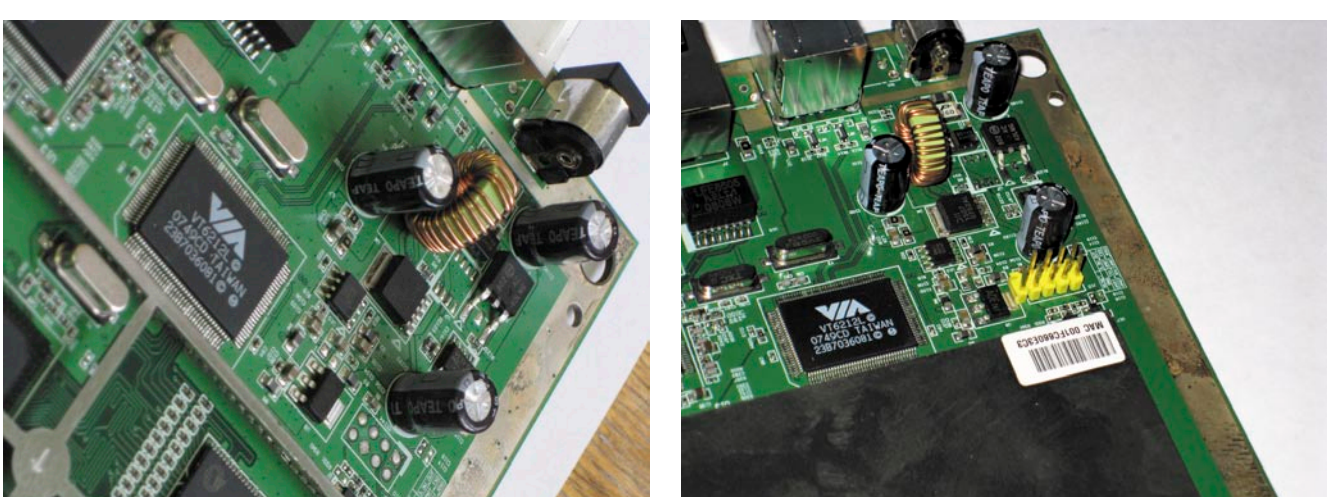


Рисунок 14. Подключение COM-порта: слева – нераспаянная площадка для подключения контактов; справа – контакты для подключения разъёма COM-порта

Обзор операционной системы gNewSense GNU/Linux 2.2 Deltah

Среди большого количества доступных дистрибутивов GNU/Linux есть такие, которые полностью соответствуют четырем принципам свободного программного обеспечения, сформулированным проектом GNU. Встречайте gNewSense GNU/Linux Deltah 2.2 – полностью свободную операционную систему.

Игорь Штомпель

Особенности gNewSense

15 апреля 2009 года разработчики представили новый выпуск операционной системы, получившей название – gNewSense GNU/Linux Deltah 2.2 и основанной на базе Debian GNU/Linux и Ubuntu [1]. Система выпускается для архитектуры x86 (i386), с рабочим столом GNOME 2.22.1 по умолчанию (KDE и Xfce доступны после установки). Это полностью свободный дистрибутив, отвечающий духу и букве проекта GNU. Последний, кстати, рекомендует ее к использованию [2], а Free Software Foundation включил в список приоритетных проектов [3]. Кроме того, Free Software Foundation ввел загрузочные членские карточки (карточка с номером 0 принадлежит Ричарду Столлману – см. **рис. 1**) со встроенным флеш (содержит видео о свободном программном обеспечении и выступления основателя Free Software Foundation) и дистрибутивом gNewSense, имеющие USB-порт [4]. Карточка содержит информацию: имя владельца, членский номер. На обратной стороне дано определение свободного программного обеспечения.

Итак, что делает рассматриваемый нами проект 100% свободным? Удалены несвободные прошивки из ядра, несвободные linux-ubuntu-modules, репозитории restricted и multiverse [5]. Репозиторий restricted – официально поддерживаемый, но включающий несвободные пакеты, а репозиторий multiverse – официально не поддерживаемый, существующий за счет усилий сторонних разработчиков, также включающий несвободные пакеты. Таким образом, ядро и модули ядра очищены от несвободных компонентов, а репозитории оставлены только те, что содержат свободные пакеты – main и universe. В целом репозитории gNewSense содержат более 24 тысяч пакетов программного обеспечения. Таким образом, дистрибутив можно рекомендовать использовать тем, кто хочет быть уверен, что использует исключительно свободное программное обеспечение. Например, последний релиз Debian GNU/Linux 5.0, как известно, содержит несвободные прошивки (firmware), лицензии на которые разработчики дистрибутива подробно стали изучать только после выхода «Lenny» [6], а Ubuntu устанавливает несвободные программы по умолчанию. Пользователь gNewSense избавлен от данных проблем, так как программное обеспечение не попадет в его репозитории, пока оно не выпущено под свободной лицензией (исключением является включение в репозиторий несвободной программы по ошибке).

Установка gNewSense

Получить дистрибутив можно на официальном сайте по ссылке http://www.gnewsense.org/index.php?n=Main.Download. Размер образа в формате .iso – 621 Мб. Последний представляет собой LiveCD с возможностью установки на жесткий диск.

Для установки gNewSense необходимо загрузиться с LiveCD (процесс проходит в графическом режиме). После чего запустить программу установки, щелкнув на значке с названием «Install», как показано на **рис. 2** (данный процесс осуществляется за семь шагов). Далее будет предложено выбрать город и часовой пояс, раскладку клавиатуры. На следующем шаге потребуется выполнить разметку диска (доступны два режима: авто – использовать весь диск и второй вариант – вручную). После разметки диска, как показано на **рис. 3**, программа предложит вам представиться, ввести входное имя пользователя, а также пароль и имя компьютера.

Затем появится окно с сообщением о том, что все готово к установке,

Рисунок 1. Новая членская карточка FSF

и отображением сводной информации о настройках, с которыми будет произведена последняя. Выбрав «Установить» для продолжения процесса установки, мы увидим окно «Установка системы», которое показано на **рис. 4**. После выполнения всех операций можно выбрать – работать далее, используя LiveCD или перезагрузиться. Выбираем второе. Перезагружаемся и видим рабочий стол, который показан на **рис. 5**. Все, дистрибутив установлен.

Стоит отметить, что в дальнейшем для управления пакетами в формате .deb можно использовать либо утилиту APT (в консоли), либо Synaptic (в графическом режиме).

gNewSense на сервере

Системный администратор, пожелавший установить сервер с дистрибутива gNewsense, имеет богатый выбор программных продуктов. Так, серверные службы представлены Apache 2.2.8,

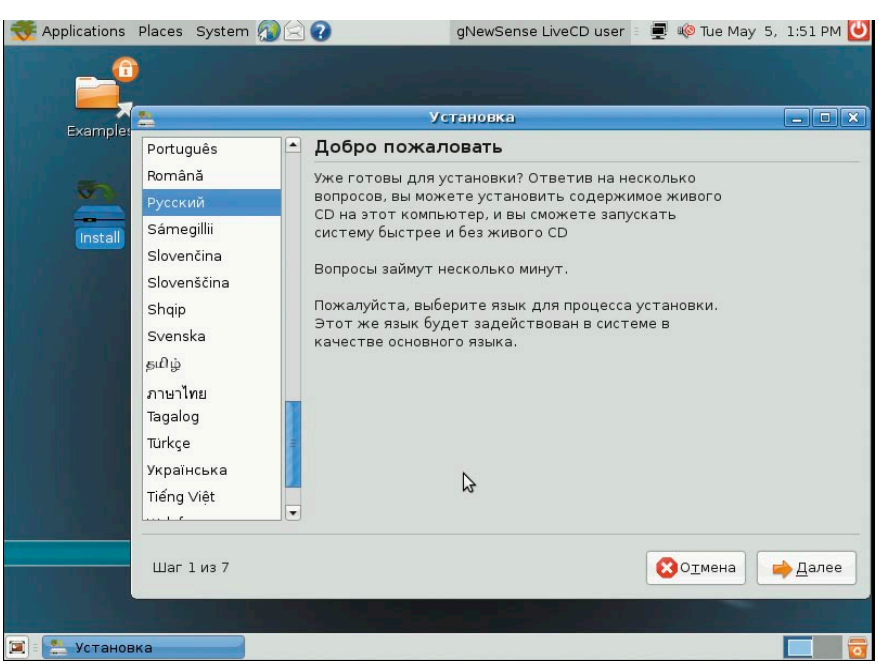


Рисунок 2. Запуск программы установки

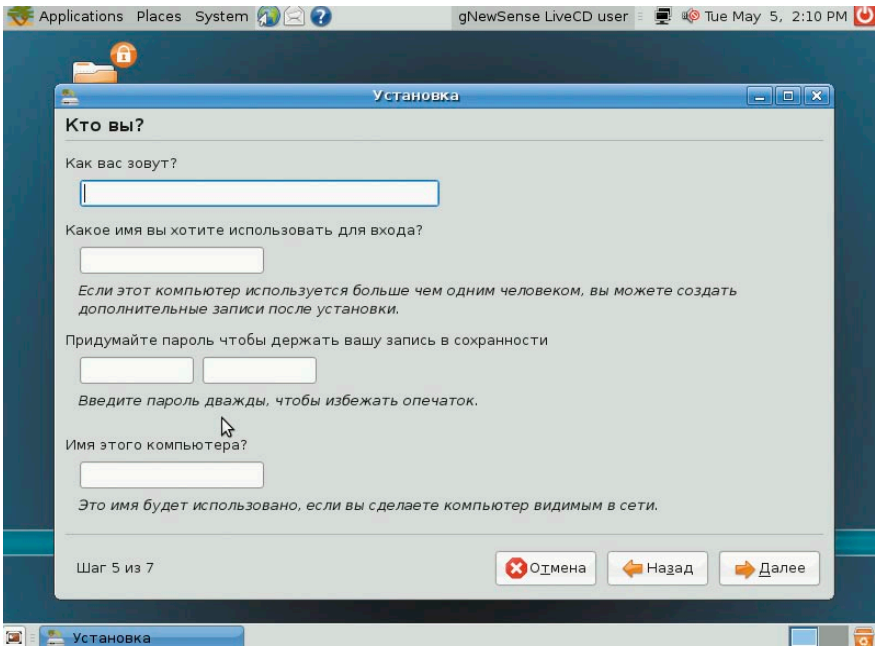


Рисунок 3. Окно входного имени, пароля и имени компьютера

Ftpd 0.17 с поддержкой SSL-шифрования (пакет ftpd-ssl), Proftpd 1.3.1, Vsftpd 2.0.6, Sendmail 8.14.2, Postfix 2.5.1, Cyrus 2.2.13, Dovecot 1.0.10, Slapd 2.4.9 (сервер OpenLDAP), Dhcp3-server 3.0.6, OpenSSH 4.7p1, Freeradius 1.1.7, Squid 3.0 STABLE1, MySQL 5.051a, PostgreSQL 8.2 и 8.3, Samba 3.0.28a, Cups 1.3.7. Но это далеко не полный перечень.

Среди средств шифрования можно выделить GnuPG 1.4.6, GnuPG2 2.0.7 и Onak 0.3.3 – сервер ключей OpenPGP, Singin-party – набор инструментов для работы с PGP/GnuPG (pgp-clean, pgp-fixkey, gpg-mailkeys и другие). Кроме того, имеются PGP-плагин для Claws Mail (inline и MIME) и Enigmail 0.95.0 для Mozilla Thunderbird, Mew – почтовый клиент с поддержкой PGP, S/MIME, SSH и SSL для Emacs.

Что касается средств разработки, то они представлены не менее широко. Это и Perl 5.8.8, и Python 2.4.5, и Php 5.2.4 – скриптовые языки. Для создания программм на C/C++ доступны – cpp и gcc 4.2.3 (3.3, 3.4, 4.1), g++ 3.4.6, anjuta 2.4.1, eclipse-cdt 3.1.2, MonoDevelop 1.0. Программировать на Java можно с использованием Eclipse 3.2.2, free-java-sdk 1.0, gcj 4.2.3, javacc 4.0, OpenJDK 6b11.

gNewSense на рабочей станции

Операционная система может быть использована и на рабочей станции. Репозитории программного обеспечения содержат все необходимые пакеты. Так, для решения офисных задач доступны OpenOffice.org 2.4.1, почтовый клиент и календарь Evolution 2.22.2, xsane 0.995. Работу в Интернете сделают удобной Mozilla Firefox 2.0.0.21 – веб-браузер; Mozilla Thunderbird 2.0.0.21 – почтовый клиент; Pidgin 2.4.1 – клиент обмена сообщениями, позволяющий работать с использованием протоколов AIM/ICQ, Yahoo!, MSN, IRC, Jabber, Napster, Zephyr, Gadu-Gadu, Bonjour, Groupwise, Sametime, SILC; Psi 0.11 – Jabber-клиент; Transmission 1.06 – BitTorrent-клиент; Ekiga – VoIP-клиент для работы с протоколами H.323 и SIP.

Что касается использования аудио, видео и работы с графикой, то также, как и для решения офисных задач имеется все необходимое программное обеспечение. Totem 2.22.1 (использует Gstreamer 0.10 по умолчанию) – мультимедиа плеер (имеются также и другие, например, gxine 0.5.901, Kaffeine 0.8.6, Dragonplayer 2.0.1, KMPlayer 0.10.0c, а VLC и Mplayer не включены в дистрибутив с целью соблюдения лицензионной чистоты); Ogle 0.9.2 – DVD-плеер с поддержкой DVD-меню; Rhytmbox 0.11.5 и XMMS2 0.2 – музыкальные проигрыватели; Kino – нелинейный редактор цифрового видео, позволяющий работать с цифровыми камерами через порт IEEE1394; OggConvert 0.3.1 – конвертер видеофайлов в свободный формат .ogg; sound-juicer 2.22.0 (звуковыжималка) – программа копирования AudioCD. Для работы с графикой можно использовать GIMP 2.4.5; Inkscape 0.46; ImageMagick6.3.7.9. Для работы с цифровыми фотоаппаратами доступны – Digikam 0.9.3; F-Spot 0.4.2.

Для воспроизведения mp3-файлов используются свободные кодеки (например, gstreamer0.10-fluendo-mp3) и проигрыватели (например, audacios 1.5.0 и уже упоминавшиеся медиаплееры Totem, gxine, и другие). Позиция Фонда свободного програм-

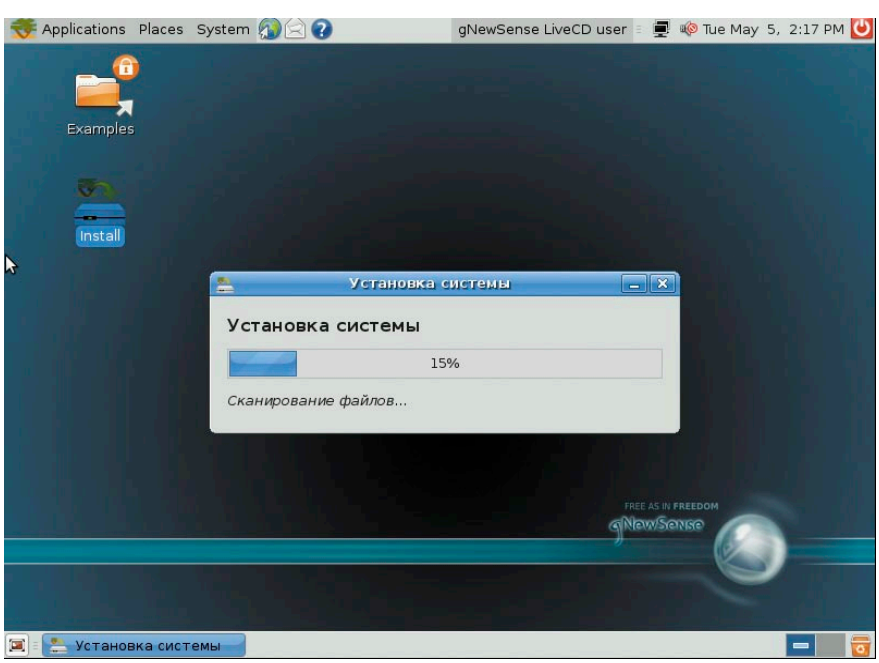


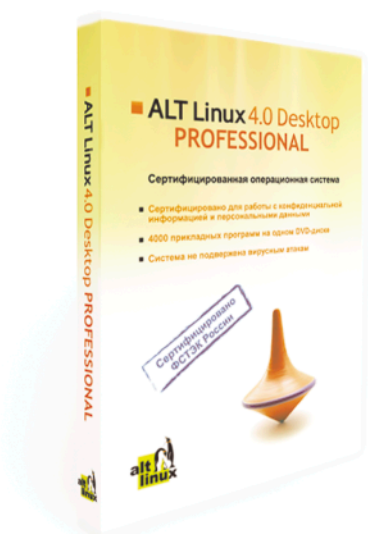
Рисунок 4. Окно «Установка системы»

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

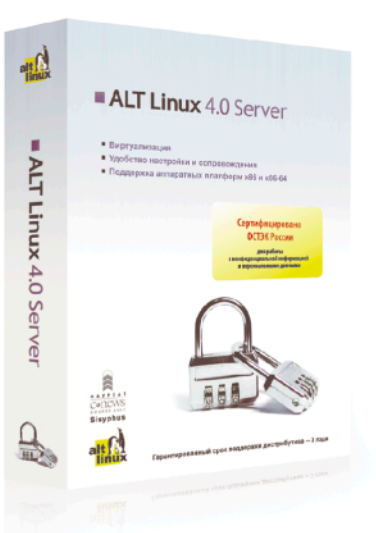


ALT Linux 4.0 Desktop Professional сертифицирован Федеральной службой по техническому и экспортному контролю (ФСТЭК России).
Сертификат соответствия **№1649 от 23 июля 2008**:
- Классификация по уровню контроля отсутствия недекларированных возможностей (НДВ) — **4 уровень**.
- Показатели защищённости от несанкционированного доступа к информации (СВТ) — по **5 классу защищённости**.

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 недекларированных возможностей — **4 уровень**.
- Показатели защищённости от несанкционированного доступа к информации — по **5 классу защищённости**.

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

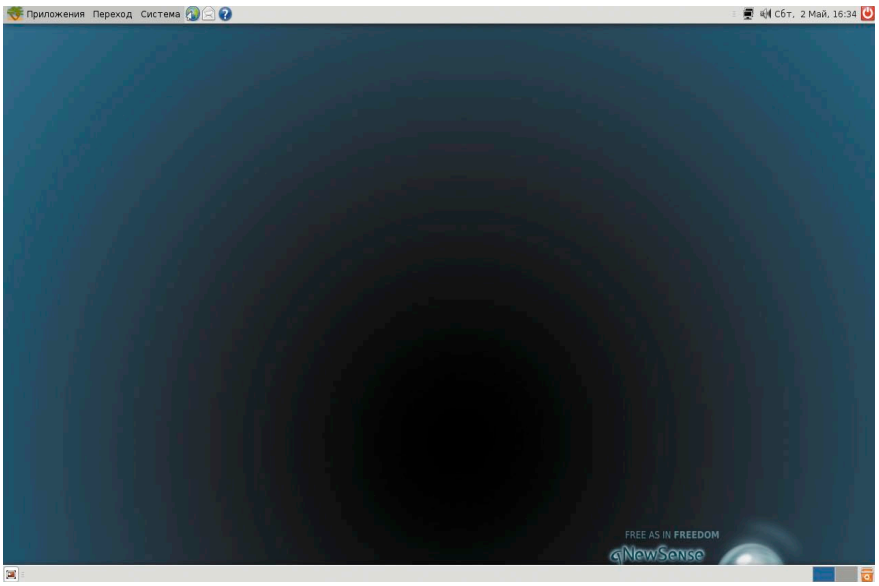


Рисунок 5. gNewSense установлен

много обеспечения допускает создание свободных аналогов кодирования/декодирования, а также плееров с поддержкой патентованного формата mp3 [7].

Если пользователю потребуется записать диски или образ диска, то для этих задач вы можете ему предложить использовать K3b 1.04 или Brasero 0.7.1.

Что нового в версии 2.2?

Давно ожидаемым новшеством в новой версии gNewSense стало включение поддержки GLX (расширение для X Window, позволяющее использовать OpenGL), который был удален из gNewSense 2.1 как несвободный [8]. Это стало возможным благодаря совместной работе SGI и Фонда свободного программного обеспечения по перелицензированию кода 3D-библиотек [9]. На официальном сайте дистрибутива даже есть раздел, посвященный «поврежденным» 3D-приложениям [10]. Теперь поддержка аппаратного ускорения включена по умолчанию. Таким образом, Compiz и 3D-игры будут работать. Кроме того, разработчики произвели исправление ошибок, не позволявших создавать разделы с файловыми системами XFS и JFS на этапе установки операционной системы. Пример ошибки, возникающей при создании раздела с JFS, показан на **рис. 6**. Также произвели замену ядра linux-image-386 на ядро версии linux-image-generic. A GNU Icecat (GNU-версия Mozilla Firefox[11]) был добавлен в репозиторий исходного кода – Source code.

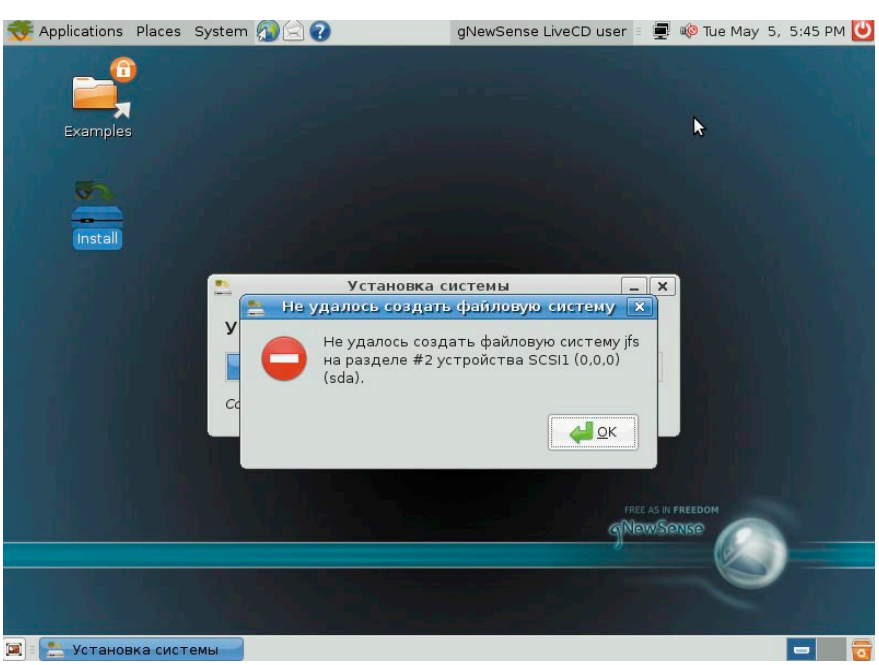


Рисунок 6. Ошибка при создании JFS-раздела на этапе установки в gNewSense 2.1

Что касается Mozilla Firefox, то его выпуски 1.0, 1.5, 2.0 были несвободными, так как включали Talkback – несвободный плагин от компании Support Soft. Это, а также то, что Mozilla распространяла (распространяет по сей день), несвободные плагины, привело к запуску проекта по созданию свободного браузера на базе Mozilla Firefox, который получил название GNU Icecat. Программа имеет свой набор свободных расширений и тем [12], а также дополнительные функции для обеспечения безопасности.

Итоги

Таким образом, gNewSense представляет собой полностью свободную операционную систему с поддержкой 3D, пригодную для использования как на сервере, так и на рабочей станции.

Если у вас возникнут определенные проблемы или вопросы при работе с системой, то обсудить их можно в официальном списке рассылки, зарегистрировавшись по адресу: http://lists.nongnu.org/mailman/listinfo/gnewsense-users-ru.

1. http://lists.gnu.org/archive/html/gnewsense-users/2009-04/msg00028.html.
2. http://www.gnu.org/distros/free-distros.html#translations.
3. http://www.fsf.org/campaigns/priority.html#gnewsense.
4. http://www.fsf.org/blogs/membership/bootablemembership.
5. http://www.gnewsense.org/Main/Features.
6. http://www.debian.org/vote/2008/vote_003.en.html#outcome.
7. http://fedoraproject.org/wiki/FreeSoftwareAnalysis/FSF.
8. http://lists.gnu.org/archive/html/gnewsense-users/2009-01/msg00041.html.
9. http://www.fsf.org/news/thank-you-sgi.
10. http://wiki.gnewsense.org/Main/Broken3dApps.
11. http://www.gnu.org/software/gnuzilla.
12. http://www.gnu.org/software/gnuzilla/addons.html.

Раскрытие данных в Sun Java System Directory Server

Программа: Sun Java System Directory Server версии 5 и 5.2.
Опасность: Низкая.
Наличие эксплоита: Нет.
Описание: Уязвимость существует из-за неизвестной ошибки, которая позволяет удаленному пользователю определить наличие файла на системе и просмотреть одну строку содержимого файла.
URL производителя: wwws.sun.com/software/products/directory_srvr/home_directory.html.
Решение: Установите последнюю версию 6.0 с сайта производителя.

Уязвимость при обработке ссылок в Reporting Server в продуктах Symantec

Программа: Symantec AntiVirus Corporate Edition 10.1 MR7 и более ранние версии; Symantec AntiVirus Corporate Edition 10.2 MR1 и более ранние версии; Symantec Client Security 3.1 MR7 и более ранние версии; Symantec Endpoint Protection 11.0 MR1 и более ранние версии.
Опасность: Низкая.
Наличие эксплоита: Нет.
Описание: Уязвимость существует из-за ошибки при обработке ссылок в интерфейсе входа в Reporting Server. Злоумышленник может отобразить произвольное сообщение в интерфейсе входа в Reporting Server.
URL производителя: www.symantec.com.
Решение: Установите последнюю версию с сайта производителя.

Отказ в обслуживании в Sun Solaris

Программа: Sun Solaris 10.
Опасность: Низкая.
Наличие эксплоита: Нет.
Описание: Уязвимость существует из-за неизвестной ошибки в DTrace ioctl-обработчиках. Локальный пользователь может вызвать панику ядра системы. Для успешной эксплуатации уязвимости требуется наличие на системе пакета SUNWdtrp.
URL производителя: www.sun.com.
Решение: Для устранения уязвимости следуйте инструкциям производителя.

Межсайтовый скриптинг в Citrix Web Interface

Программа: Citrix Web Interface версии 4.6, 5.0 и 5.0.1.
Опасность: Низкая.
Наличие эксплоита: Нет.
Описание: Уязвимость существует из-за недостаточной обработки входных данных. Удаленный пользователь может с помощью специально сформированного запроса выполнить произвольный код сценария в браузере жертвы в контексте безопасности уязвимого сайта.
URL производителя: support.citrix.com/product/wi.
Решение: Установите последнюю версию 5.1.0 с сайта производителя.

Межсайтовый скриптинг в Sun Java System Calendar Server

Программа: Sun ONE Calendar Server 6.0; Sun Java System Calendar Server 6 2005Q4 и более ранние версии.
Опасность: Низкая.
Наличие эксплоита: Да.
Описание: 1. Уязвимость существует из-за недостаточной обработки входных данных в параметре fmt-out в сценарии login.wcap. Удаленный пользователь может с помощью специально сформированного запроса выполнить произвольный код сценария в браузере жертвы в контексте безопасности уязвимого сайта.

Пример:

```
https://<server>:3443/login.wcap?calid=&calname=&date= ↵
      &fmt-out=<script>alert(document.cookie) ↵
      </script>&view=&locale=&tzid=&test= ↵
      1229606492214&user=test&password=test
```

2. Уязвимость существует из-за недостаточной обработки входных данных в параметре date в сценарии command.shtml. Удаленный пользователь может с помощью специально сформированного запроса выполнить произвольный код сценария в браузере жертвы в контексте безопасности уязвимого сайта.

Пример:

```
https://<server>:3443//command.shtml?view= ↵
      overview&id=HK8CjQOkmbY&date=20081217T200734%27; ↵
      alert('xss');//Z&caliad=someid@test.com&security=1
```

URL производителя: www.sun.com.
Решение: Установите исправление с сайта производителя.

Раскрытие важных данных в Apache mod_proxy_aj

Программа: Apache 2.2.11.
Опасность: Средняя.
Наличие эксплоита: Нет.
Описание: Уязвимость существует из-за ошибки в mod_proxy_ajp при обработке некорректно сформированных HTTP POST-запросов. Удаленный пользователь может с помощью специально сформированных HTTP-запросов просмотреть данные, возвращаемые в качестве ответов другим пользователям.
URL производителя: www.apache.org.
Решение: Производитель рекомендует установить временное исправление.

Раскрытие данных в продуктах VMware

Программа: VMware VirtualCenter версии до 2.5 Update 4; VMware ESX 3.5; VMware ESXi 3.5.
Опасность: Низкая.
Наличие эксплоита: Нет.
Описание: Уязвимость существует из-за того, что приложение некорректно сохраняет пароли в памяти. Злоумышленник может прочитать память клиентского процесса и получить пароль к VirtualCenter Server.
URL производителя: www.vmware.com.
Решение: Установите исправление с сайта производителя.

Составил Александр Антипов

В чем секрет популярности Linux User Group из Пекина?

Залогом успешного развития какого-либо проекта зачастую является удачное стечение обстоятельств и присутствие определенного типа людей, которые заряжены на создание позитивной атмосферы вокруг себя. Одним из таких интересных проектов является пекинская группа Linux-пользователей – BeiJing Linux User Group. С ярким представителем BLUG – Фредериком Мюллером (Frederic Muller) мы и побеседовали сегодня.

Фредерик, расскажите, пожалуйста, о себе. Я знаю, что за вашими плечами скрывается достаточно богатый опыт, да и вообще интересно, как вы начинали и почему связали свою судьбу с Linux.

О, спасибо за комплимент. Мое погружение в Linux началось в 1995 году, когда мы открывали один из первых интернет-провайдеров в Камбодже. Наши системы наполовину находились в Камбодже и наполовину в Сингапуре. И на серверах мы использовали Linux. Затем в начале 1997 года я продал бизнес и решил попробовать установить Linux на свой новенький ноутбук. Наверное, мой выбор не отличался от выбора большинства людей в то время, поэтому я положил глаз на Red Hat. В настоящий момент я вице-президент в BLUG, заведую также связями с общественностью и правительственными/государственными учреждениями. Также еще я являюсь вице-президентом в Software Freedom International – организации, которая устраивает Software Freedom Day. Работаю в качестве генерального конструктора в китайском филиале Dexxon и вместе с Патриком Зинцем (Patrick Sinz, ex-Mandriva) принимаю участие в проекте OLPH – это программа разработчиков, опекаемая Dexxon. Если остается время, то на добровольных началах занимаюсь еще и рептилиями в пекинском зоопарке.

Давайте вернемся к началу, к созданию BLUG. Кто был основателем и какие цели преследовались?

Первый сбор группы состоялся в ноябре 2002 года, и я был на нем. Майкл Ианнини (Michael Iannini) был вдохновлен на создание группы своим другом, который, предполагалось, будет президентом. Однако его друг так и не появился, поэтому Майклу самому пришлось выступать в роли главного на протяжении почти что 5 лет, пока он не переехал в Индию и не передал бразды правления мне. Все это время он был заводилой, который организовывал регулярные ежемесячные мероприятия и встречи – «chuanr nights» («Шашлычные ночи»). Нашей целью тогда было желание пообщаться на Linux-тему и быть мостом между двумя мирами – китайским и мировым Linux/OSS-сообществом. В действительности же мы пытались выяснить, что происходит в китайской Linux-субкультуре в то время. На сегодняшний момент у нас есть устойчивое представление, что проис-

ходит в Китае, и наша группа – часть этой культуры.

Группа организует встречи дважды в месяц. Из вашего личного опыта, это оптимально или, наоборот, слишком часто?

Ситуация выглядит следующим образом. У нас ежемесячно происходит сбор, для которого готовятся 2 презентации. Затем у нас бывает в среднем два социальных события в месяц – «Шашлычные ночи». Еще раз в месяц получается организовать событие «Гость в городе» («Guest in town») – презентация, которую преподносит специальный гость, будучи в Пекине (например, кто-либо из большой компании, такой как Sun Microsystems). Потом у нас бывают еженедельные встречи по поводу развития OSS-проекта quadcopter и раз в месяц проводятся мероприятия «coding for fun» – аналог hackathon'a. В последнее время «coding for fun» удается проводить каждую неделю, что не может не радовать. Так что каждый может найти занятие себе по вкусу. Понятно, что каждый участник не ходит сразу на все названные мероприятия – все-таки кто-то больше кодер, а кто-то интересуется больше техническими штучками. А некоторые приходят на все сразу – им больше нравится находиться среди единомышленников и просто общаться на разные темы.

Если кто-либо, прочитав вышенаписанное, решит организовать свою собственную Linux User Group, то я бы очень рекомендовал к прочтению LUG Howto – и начинать с ежемесячного сбора. В один и тот же день, в одно и то же время. Секрет успеха здесь – регулярность. Тогда люди будут приходить и обмениваться мнениями и в конце концов решатся на что-то большее. Первоначально у нас были грандиозные планы, даже хотели иметь группы поддержки и распределять для каждого его роль. Но это не сработало. LUG очень напоминает любой Open Source-проект, в том плане, что нужны пользователи и некоторое количество разработчиков, которое периодически увеличивается. Но пользователи – члены проекта не обязательно должны быть разработчиками – так что не предъявляйте заранее завышенные требования (как мы первоначально имели неосторожность).

Я смотрю на список событий, которые у вас произошли в прошлом году, и вижу много интересных приглашенных персон, которые посетили ваши мероприятия. Как вам удается их заполучить?

Нам очень повезло, что многие сотрудники из крупных Open Source-компаний также являются членами нашей группы. Кроме того, в Пекине находится много исследовательских центров. Когда кто-либо прибывает в Пекин, то мы уже знаем об этом, да и означенные компании сами присылают гостей к нам. Иногда они находят нас через онлайн и сообщают, что ходят организовать мероприятие по определенной тематике. Иногда мы сами организовываем крупные конференции и приглашаем приехать гостей в Китай. В организации конференций нам помогают как China OSS Promotion Union – китайская правительственная организация по продвижению Open Source, так и Linux Foundation. Все происходит в дружественной обстановке сотрудничества, и очень приятно видеть и встречаться с таким количеством мотивированных людей.

Каково, на ваш взгляд, текущее положение дел с развитием Linux в Китае? Можно ли охарактеризовать его как взрывной эффект, достаточно плавное развитие или как-то еще?

Взрывной эффект, вне всякого сомнения! Все основные разработчики Linux-дистрибутивов имеют офисы в Китае, и эти офисы расширяются. Местные разработчики дистрибутивов также развиваются отлично. Я являюсь свидетелем того, как заключаются сделки по предустановке Linux на оборудование. Все больше студентов интересуются Linux и Open Source. Очень много embedded-устройств разрабатываются и производятся в Китае – и они работают под Linux. Так что это именно то место, где вы должны быть, если вы Linux-разработчик.

Некоторые компании подарили свои продукты BLUG-сообществу, например, Nokia с своим N810. Были также разговоры об аппаратуре от Lemote и т. д. Это что, какая-то личная инициатива этих компаний или же что-то притягательное есть в BLUG?

Такая тенденция наметилась, когда Openmoko подарила нам Freerunner в 2007 году на мероприятии Software Freedom Day. Затем нам удалось выиграть в еще одном мероприятии и получить XO-ноутбук. Обе эти игрушки выдали мне, и некоторое время они пылились у меня на полке. Потом я решил, что лучше раздать их группе. Некоторое время спустя меня пригласили на одну встречу – Foo Camp BeiJing. Где я получил несколько бесплатных книжек от O'Reilly. Один человек из нашей группы решил написать Open Source-приложение, основанное на примерах из подаренных книг и для аппаратного обеспечения, которое у нас уже было, чтобы в дальнейшем пустить во внутренний кругооборот как книги, так и устройства. После этого мы уже сами стали спрашивать в компаниях, а могут ли они нам дать на изучение свои продукты.

Сейчас же, я думаю, компании уже знают, кто мы такие, и по собственной инициативе предлагают нам «попробовать» те или иные аппаратные продукты. Мы возимся с ними, показываем всей группе, что это такое и что можно на них сделать. И потом организовываем коллективную покупку со скидкой. Так что я думаю, что это получается выгодно всем.

Не могли бы вы рассказать, что из себя представляет Software Freedom Day и каково его влияние на сообщество?

Software Freedom Day – это мероприятие, посвященное пропаганде свободного и Open Source программного обеспечения. Наша цель в нем – научить и рассказать людям по всему миру о преимуществах высококачественного FOSS-обеспечения в образовании, для использования в государственных структурах, дома, в бизнесе – везде. Мы видели, как создавались те или иные команды в структуре этого движения, которые росли на 50% каждый год. Я не уверен, что в этом году будут схожие показатели, но тенденция, конечно же, сохранится. На местном уровне приходится общаться с людьми, которые вообще могли не слышать об FOSS либо же имеют о нем лишь отдаленное представление – так что довольно интересно видеть, как люди воспринимают идеи свободного обеспечения и его цели. Также это очеред-

ная возможность встретиться с другими участниками Open Source-движения да и тонус своей собственной группы поднимается. Здесь, в Пекине, нам удалось привлечь большое внимание публики новыми докладчиками, новыми идеями и новыми членами нашей группы. Так что со своей стороны я бы рекомендовал любой LUG-группе проводить Software Freedom Day.

Сколько проектов ведется членами BLUG и какова их практическая ценность, на ваш взгляд?

Как правило, проекты начинаются с какой-либо идеи, которую высказывают сами участники группы, либо с какой-либо технической новинки. В случае если нам нужна помощь инжиниринговой компании, мы им звоним и просим оказать нам помощь. Так как за нами уже сложилась хорошая слава и люди понимают, что в Open Source не следует ждать немедленной отдачи, мы получаем обещанную помощь – люди приходят, показывают и рассказывают, и это здорово. Практический результат – мы вовлекаем сообщество в организацию событий и встреч, которые так полюбились нашей команде. Также мы пишем код, который подпадает под определение Open Source. Помимо этого мы также исправляем ошибки в ПО, поддерживаем компании, которые помогают нам. То есть если говорить глобально, то мы развиваем экосистему, которая называется Open Source. Группа играет свою роль, хотя бы тем, что мы можем влиять на изменения спецификаций того или иного продукта. Не правда ли, это очень вдохновляет – знать, что за этим стоит какая-то команда, которая только тем и занимается, что лопает шашлыки с пивом?

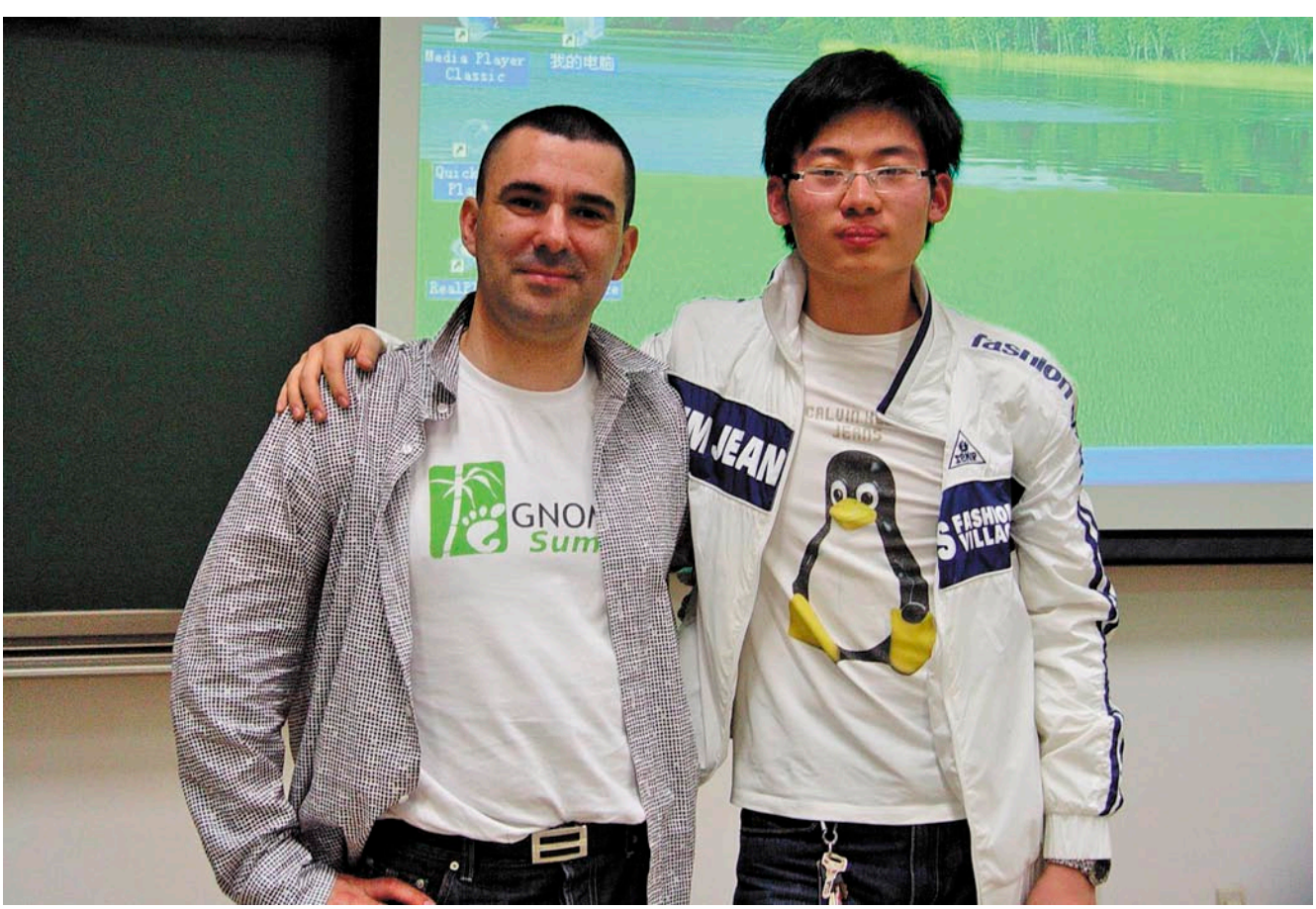
Сейчас глобальная экономика находится в интересном состоянии. Отразилось ли это на Китае, особенно в сфере Linux-разработки?

Возможно. Пекин – это особое место, так как Open Source-компании все еще проводят набор, причем очень и очень много. Я полагаю, что большая часть позиций попадает в Пекин по outsource-схеме, из-за желания сократить издержки Но если судить по нашей группе, то я не вижу, чтобы ситуация в экономике повлияла бы на нас. Если смотреть на другие секторы экономики Китая, то да, не все так замечательно.

И в завершение – изменились ли те фундаментальные основы, которые были заложены при организации группы?

Вы знаете, организационные решения, которые приходилось принимать тогда и сейчас, в целом не изменились. Конечно, в последнее время приходится больше ездить и находиться за пределами Пекина – это и организация встреч, анализ, нужны ли спонсоры для какой-либо встречи или нет, популяризация FOSS-движения и т. п. Должен с гордостью отметить, что группа функционирует на добровольных началах и тот свод правил, о которых мы уже ранее говорили, остался неизменным – это ориентация на сообщество и группу в целом, на здоровый образ жизни и на то, чтобы все это вместе взятое приносило удовольствие.

Текст: Антон Борисов, фотографии предоставлены Линусом Вангом



Фредерик Мюллер (руководитель подразделения Dexxon в КНР) и Линус Ванг (репортер из издания Full Circle Magazine)

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

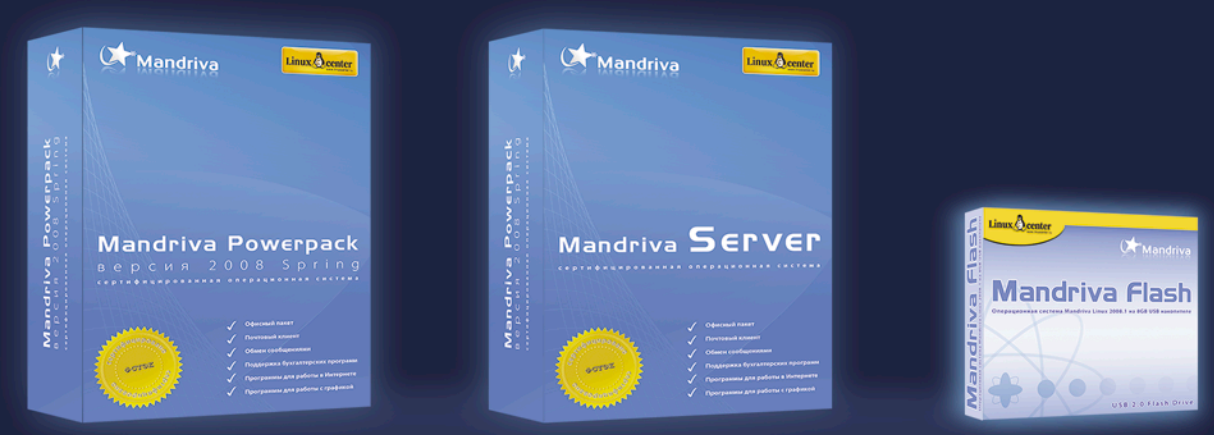
Mandriva Powerpack 2008 Spring — надежное решение для рабочей станции. Включает в себя офисный пакет OpenOffice.org: текстовый редактор, электронные таблицы, редактор презентаций, конструктор баз данных, почтовый клиент, браузер, другие интернет-приложения, графические редакторы, приложения для работы 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 | Телефон в Москве: (499)271-49-55 | Телефон в Санкт-Петербурге: 8(812) 309-06-86

Реклама

Работаем с FTP-сервером из «1С»

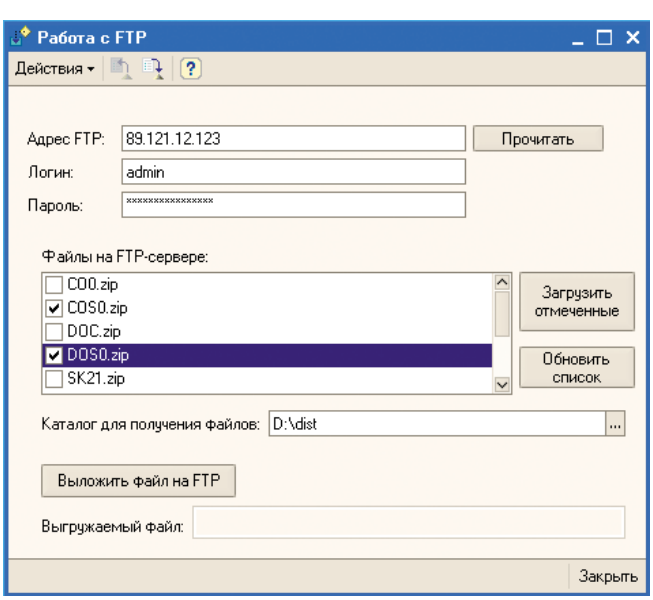
Андрей Луконькин

Столкнувшись с острой необходимостью получить довольно большой файл из удаленного офиса, я начал поиск программы для комфортной работы с FTP. Интерфейс FAR напомнил мне полузабытый DOS, Google предлагает в основном платные клиенты, из командной строки работать тоже не совсем удобно. Поэтому я задумался о создании собственного инструмента в той среде, в которой я работаю каждый день, т.е. в «1С».

Что нам нужно от обработки? Чтобы была возможность по указанному адресу, с заданным логином и паролем подключаться к FTP-серверу, смотреть список находящихся там файлов, получать необходимые файлы с сервера, и наоборот, закачивать туда что-то.

Создадим внешнюю обработку, а в ней реквизиты:

- «АдресFTP», «Логин», «Пароль», «КаталогДляПолученияФайлов», «ВыгружаемыйФайл» – тип «Строка» неограниченной длины;
- на форме разместим «ПолеСписка» с признаком «ОтображатьПометку»;
- кнопки «Прочитать», «ЗагрузитьОтмеченные», «ОбновитьСписок» и «ВыложитьФайл».



После подключения видим файлы на сервере

Теперь перейдем непосредственно к программному коду.

Определим переменную «НашеСоединение», которая будет использоваться в нескольких процедурах.

```
Перем НашеСоединение;
```

При открытии формы убираем доступность всех кнопок до тех пор, пока не будет установлено соединение, и зададим каталог для получения файлов по умолчанию.

```
Процедура ПриОткрытии()
    ЭлементыФормы.ЗагрузитьОтмеченные.Доступность = Ложь;
    ЭлементыФормы.ВыложитьФайл.Доступность = Ложь;
    ЭлементыФормы.ОбновитьСписок.Доступность = Ложь;
    КаталогДляПолученияФайлов = "C:\";
КонецПроцедуры
```

После указания адреса, логина и пароля нужно нажать кнопку «Прочитать» для установки соединения. Список файлов заполнится при обращении к процедуре «ОбновитьСписок()».

```
Процедура ПрочитатьНажатие(Элемент)
    ПроксиСервер = Новый ИнтернетПрокси(Истина);
    Попытка
      НашеСоединение = Новый FTPСоединение(АдресFTP, 21, ↵
                Логин, Пароль , , );
    Исключение
```

```
        Сообщить("Ошибка создания соединения: " ↵
                 +ОписаниеОшибки());
        Возврат;
    КонецПопытки;
    ЭлементыФормы.ЗагрузитьОтмеченные.Доступность = Истина;
    ЭлементыФормы.ВыложитьФайл.Доступность = Истина;
    ЭлементыФормы.ОбновитьСписок.Доступность = Истина;
    ОбновитьСписок();
КонецПроцедуры

Процедура ОбновитьСписок()
    ПолеСписка.Очистить();
    СписокФайлов = НашеСоединение.НайтиФайлы("/","*.*");
    Для Каждого Файл Из СписокФайлов Цикл
      Если Файл.ЭтоФайл() Тогда
          ПолеСписка.Добавить(Файл, Файл.Имя);
      КонецЕсли;
    КонецЦикла;
КонецПроцедуры
```

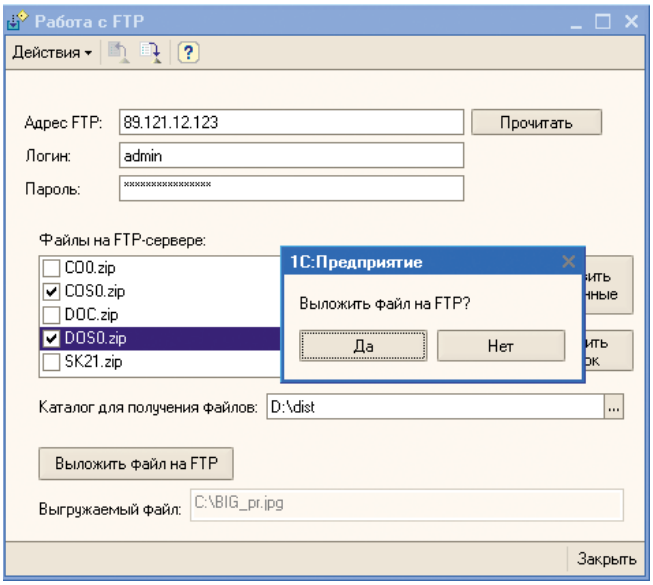
Отметив галочками нужные файлы, их можно сохранить локально в предварительно выбранный каталог.

```
Процедура КаталогДляПолученияФайловНачалоВыбора( ↵
      Элемент, СтандартнаяОбработка)
    СтандартнаяОбработка = Ложь;
    РежимДиалога = РежимДиалогаВыбораФайла.ВыборКаталога;
    ДиалогВыбораКаталога = Новый ДиалогВыбораФайла( ↵
      РежимДиалога);
    ДиалогВыбораКаталога.МножественныйВыбор = Ложь;
    ДиалогВыбораКаталога.Заголовок = "Выберите путь ↵
      для сохранения файлов";
    Если ДиалогВыбораКаталога.Выбрать() Тогда
      КаталогДляПолученияФайлов = ↵
            ДиалогВыбораКаталога.Каталог;
    КонецЕсли;
КонецПроцедуры

Процедура ЗагрузитьОтмеченныеНажатие(Элемент)
    Для каждого Файл из ПолеСписка Цикл
      Если Файл.Пометка Тогда
НашеСоединение.Получить(Файл.Значение.ПолноеИмя, ↵
      КаталогДляПолученияФайлов+Файл.Значение.ПолноеИмя);
      КонецЕсли;
    КонецЦикла;
КонецПроцедуры
```

Для размещения файла на сервере нужно нажать кнопку «Выложить файл на FTP» и выбрать необходимый файл. Ответив «Да» в дополнительном подтверждении о размещении, мы инициализируем запуск процедуры «ВыложитьФайлНажатие()».

```
Процедура ВыложитьФайлНажатие(Элемент)
    РежимДиалога = РежимДиалогаВыбораФайла.Открытие;
    ДиалогВыбораФайла = Новый ДиалогВыбораФайла( ↵
      РежимДиалога);
    ДиалогВыбораФайла.МножественныйВыбор = Ложь;
    ДиалогВыбораФайла.Заголовок = "Выберите файл ↵
```



Перед отправкой файла на сервер запросим подтверждение

```
      для загрузки";
    ДиалогВыбораФайла.ПолноеИмяФайла = ВыгружаемыйФайл;
    Если ДиалогВыбораФайла.Выбрать() Тогда
      ВыгружаемыйФайл = ДиалогВыбораФайла.ПолноеИмяФайла;
      ВыгружаемыйФайлОбъект = Прав(ВыгружаемыйФайл, ↵
            СтрДлина(ВыгружаемыйФайл)-СтрДлина(↵
            ДиалогВыбораФайла.Каталог));
      Ответ = Вопрос("Выложить файл на FTP?", ↵
            РежимДиалогаВопрос.ДаНет);
      Если Ответ = КодВозвратаДиалога.Да Тогда
          НашеСоединение.Записать(ВыгружаемыйФайл, ↵
            ВыгружаемыйФайлОбъект);
          ОбновитьСписок();
      КонецЕсли;
      ВыгружаемыйФайл="";
    Иначе
      ВыгружаемыйФайл="";
    КонецЕсли;
КонецПроцедуры

Процедура ОбновитьСписокНажатие(Элемент)
    ОбновитьСписок();
КонецПроцедуры
```

Что мы имеем? Нехитрая, в несколько десятков строчек, обработка позволяет принимать файлы и отправлять их на FTP-сервер.

Цель нами достигнута, остается только совершенствовать программу, наращивая её дополнительным функционалом.

Наше «1С». Собрание авторских материалов

В апреле 2009 года открылся новый проект «Наше 1С» по адресу http://www.nashe1c.ru. Здесь собираются авторские материалы, относящиеся к программному продукту «1С». Каждый желающий может опубликовать свою разработку, поделиться с коллегами методиками, получив при этом оценку своего творчества или «know how».

Чем примечателен этот портал и в чем его принципиальное отличие от множества существующих сайтов на данный момент? Во-первых, этот проект создан и курируется самой фирмой «1С», что говорит об уровне и масштабе мероприятия. Во-вторых, работы оценивают не только пользователи, но и представители фирмы «1С» оставляют оценки и комментарии. В-третьих, материалы предварительно отбираются и фильтруются таким образом, что посетители избавляются от некачественных «изобретений».

Ресурс полезен как разработчикам, так и администраторам. Желающие опубликовать свои материалы получают официальные оценки, а также возможность использовать прямую ссылку на свой профиль в резюме.

В открытом доступе любой посетитель может найти что-то полезное из следующих рубрик:

- ☑ «Работа с программами»;
- ☑ «Установка, администрирование»;
- ☑ «Разработка и программирование»;
- ☑ «Внедрение»;
- ☑ «Библиотека дипломных проектов»;
- ☑ «Программы «1С:Предприятие 7.7».

Сейчас на сайте уже десятки опубликованных работ, с каждым днем их количество увеличивается, а это значит, что уникальная коллекция высококачественного материала собирается в одном месте и будет доступна любому желающему.

Управление базами данных «1С» 7.7 при помощи групповых политик

Владимир Борисов

«1С: Бухгалтерия» предыдущаей версии 7.7 не имеет механизмов управления подключенными базами данных. Если баз одна-две и пользователей немного, то настроить руками не составляет проблем. Но бывают ситуации посложнее.

Ситуация

Существует локальная сеть организации, очень многие пользователи работают с «1С» 7.7, количество баз «1С» переваливает за полсотни, многие пользователи работают с несколькими базами одновременно, часто происходят «переходы» (т.е. пользователю необходимо, например, всю следующую неделю работать с определенным набором баз, или пользователя переводят в другой отдел, или пересаживают на другое рабочее место). Заявки на доступ к той или иной базе данных составляют значимую долю в общем потоке заявок.

Исходные данные

Локальная сеть централизованно управляется Active Directory, дисковая система существующего сервера стала сбоить, приобретен сервер с более быстрой и надежной дисковой системой под эту задачу. На существующем сервере папки с базами «1С» не имели единообразного названия, были раскиданы по иерархии папок бессистемно.

Задача

Требуется перенести все базы на новый сервер, единообразно назвать папки с базами данных, всем пользователям обновить список баз данных, ввести централизованное управление списком доступных пользователю баз данных.

Решение

«1С» 7.7 считывает список доступных баз данных из ветки реестра HKEY_CURRENT_USER\Software\1C\1Cv7\7.7\Titles, а раз так, то этим списком возможно различными путями управлять. Было решено написать шаблон групповой политики для управления этой веткой реестра. Воспользовавшись статьей Ивана Коробко «Автоматизация процессов в сети» из журнала «Системный администратор» №8 за 2004 год, был написан следующий шаблон групповой политики:

```
Листинг 1. Шаблон групповой политики для управления
базами данных «1С» 7.7

CLASS USER
    CATEGORY !!cat_name
      KEYNAME "Software\1C\1Cv7\7.7\Titles"
          POLICY !!pol_name
               PART !!part_name LISTBOX EXPLICITVALUE ↵
                    ADDITIVE
               END PART
          END POLICY
    END CATEGORY

[strings]
cat_name="Управление 1С"
pol_name="Подключенные базы данных"
part_name="Список подключенных баз данных"
```

На новом сервере создается папка общего доступа, в ней создаются папки для баз данных «1С» со следующим шаблоном имени «название_тип_версия», например, dormash_buh_7, из названия понятно, что это база организации «ДорМаш», тип базы – «1С: Бухгалтерия», версия 7.

В Active Directory создаются группы доступа с названием, точно соответствующим имени папки с базой, в комментарии группы более развернуто описываем, что это за группа (например, «Группа доступа к базе «1С ДорМаш: Бухгалтерия»). У руководства соответствующих подразделений выясняем, кто в какой базе работает, распределяем пользователей по соответствующим группам. Включаем в списки доступа соответствующих папок с базами соответствующие им группы доступа.

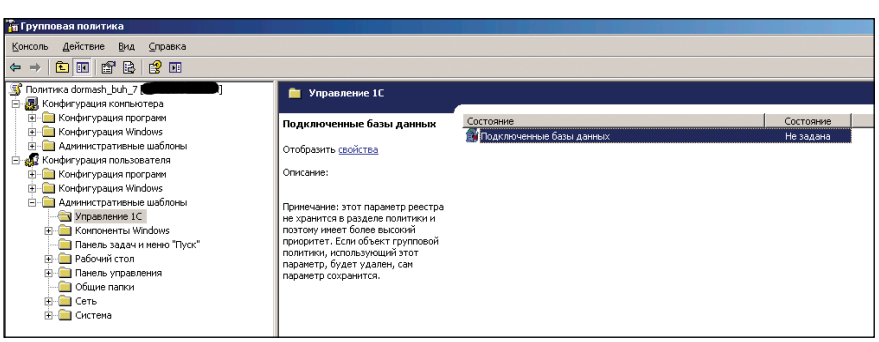


Рисунок 1. Управление базами данных 1С в редакторе групповой политики

Подключаем папку с базами к существующему доменному корню DFS (распределенная файловая система в нашем случае применяется для консолидации папок общего доступа в единый корень). Заготовка для переноса баз сделана.

Создаем в дереве Active Directory подразделение с названием наподобие 1C_group_policy_templates и объект групповой политики с именем, точно соответствующим имени папки с базой

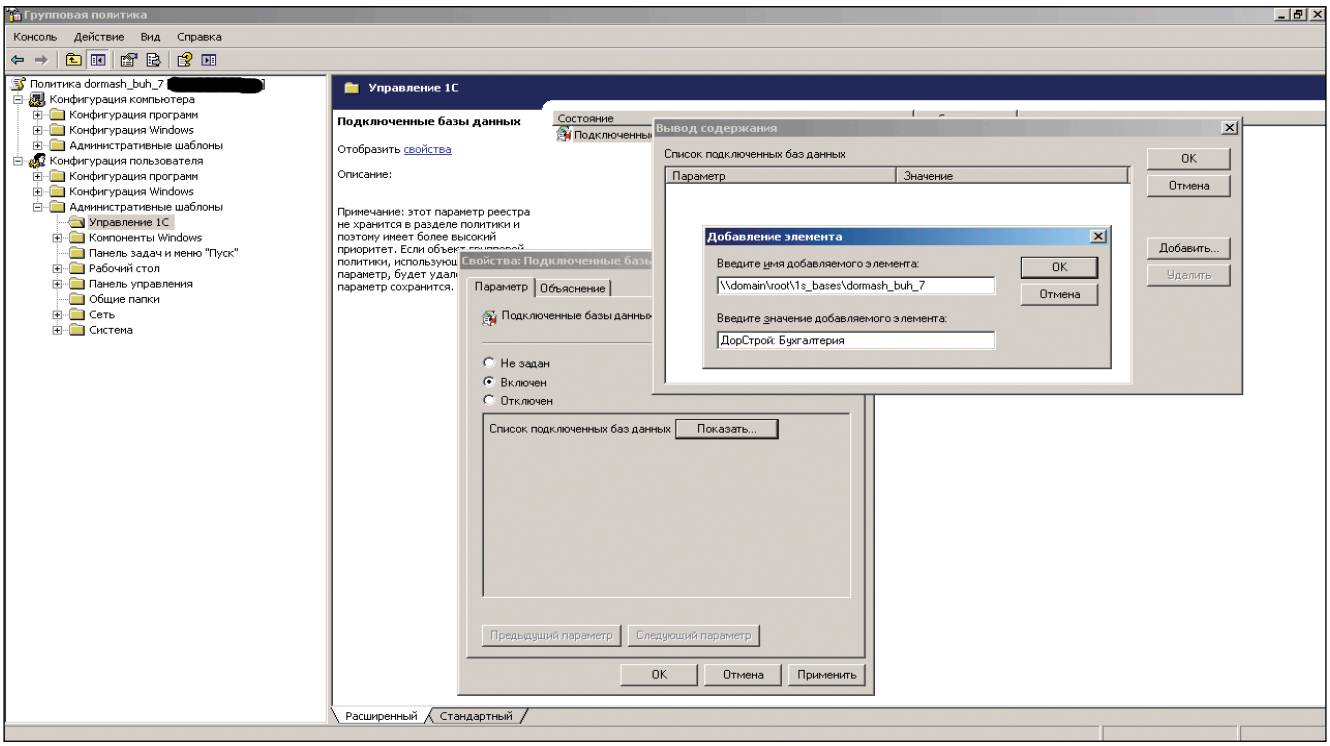


Рисунок 2. Добавление БД в список доступных баз

и соответствующей группы доступа. Открываем объект групповой политики в редакторе и подключаем созданный ранее административный шаблон. У нас в списке административных шаблонов появляется ветка «Управление 1С». Но ветка пустая, для того чтобы нужная нам настройка отображалась, необходимо открыть контекстное меню ветки, выбрать «Вид → Фильтрация», снять галочку с пункта «Показывать только управляемые политики». После этих действий в ветке «Управление 1С» появляется параметр «Подключенные базы данных» (см. **рис. 1**).

Теперь мы можем отредактировать список баз, в моем случае ситуация такова, что на каждую БД пришлось создавать отдельный объект групповой политики. Добавление базы происходит следующим образом: в поле «Введите имя добавляемого элемента» вводится путь к папке с базой данных, а в поле «Введите значение добавляемого элемента» вводится название базы, которое будет отображаться у пользователя (см. **рис. 2**). Проводим аналогичные пассы для каждой базы данных.

Теперь необходимо сделать так, чтобы данная политика распространялась только на тех пользователей, которым необходим доступ к этой БД. Для этого воспользуемся существующими и уже заполненными группами доступа. В свойствах объекта групповой политики в закладке «Безопасность» надо удалить группу «Прошедшие проверку», добавить группу, соответствующую названию базы, и дать права на применение групповой политики (см. **рис. 3**).

Далее остаётся только связать созданные объекты ГП с подразделением, в котором находятся пользователи.

Итог

- все БД «1С» имеют единообразное название;
- все БД «1С» находятся в одном месте;
- управлять доступом к БД можно путем изменения членства в группах доступа;
- добавление в список доступных БД «1С» происходит автоматически, если у пользователя есть доступ к соответствующей папке;
- при переносе папки с БД в другое место достаточно изменить запись в ГП, и у пользователя в списке поменяется соответствующий путь.

Единственный минус – запись из списка доступных БД не убирается вместе с исключением пользователя из соответствующей группы доступа, но это терпимо.

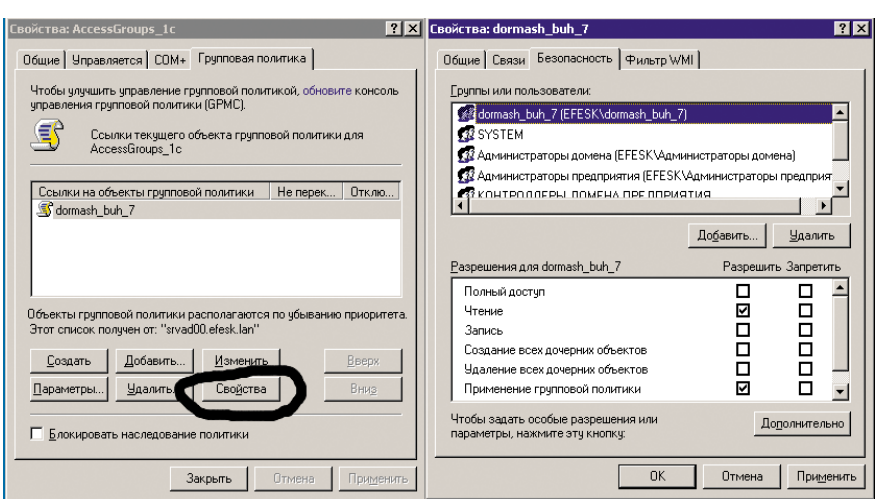


Рисунок 3. Права на применение групповой политики

Приключения продолжаются...

Для Алексея Гончарова жизнь – веселое путешествие с приключениями и чудесами.

Если вы думаете, что все любители приключений – хулиганы, бандиты, авантюристы, джеки воробьи, то вы ошибаетесь… Можно быть вполне респектабельным бизнесменом, мирным семьянином и вместе с тем горячим поклонником неожиданных событий, который не боится жить в эпоху перемен. Наоборот, по-другому себе не представляет. Ведь если бы не смена эпох в нашем славном государстве, многие детские мечты Алексея Гончарова, директора компании «Русоникс», никогда бы не сбылись…

Здравствуй, НЛО! Hello, Сингапур!

Жил-был мальчик, который любил экспериментировать с техникой. Причем самостоятельно, без помощи взрослых и всяких там кружков для юных талантов. Было ему года четыре, когда тайком от родителей Алеша провел в свою комнату провод от телевизора, присоединил к нему наушники и по вечерам, когда мама с папой смотрели взрослые фильмы, их сынок эти фильмы слушал… Техническое открытие, конечно, осталось тайной, вряд ли папа – врач по профессии – одобрил бы такое нарушение режима… В первом классе Алексей решился на более смелый эксперимент – разобрал и снова собрал телевизор. Уверяет, что это было совсем несложно. Думается, однако, что сердечко ёкало – а будет ли работать? Такой адреналин – чем вам не приключение? Впрочем, всякую электронику Алеша разбирал в детстве часто – интересно было, как что устроено. Более значимым событием стала встреча с неопознанным летающим объектом.

– Просто увидел летающую тарелку за окном.

– В Москве?

– В Москве. Пролетела мимо. Понял – «они» есть.

Кто «они», не очень осознал, фантастику Алексей Гончаров начал читать позже. Но главное – появилась мечта попасть на другую планету. Не «правильное» желание стать космонавтом, как у многих детей, но стремление очутиться в другом мире, где не курят, не пьют, где все счастливы.

Для советского мальчика другой планетой было зарубежье, где не только язык, но и культура, быт, привычки – все другое. Но Алексей об этом тогда не думал. Он был пионером, комсомольцем, даже комиссаром районного комсомольского штаба – водил школьников на овощную базу отрабатывать трудовую вахту. Верил во всю идеологическую составляющую, естественно, как почти все тогда верили. Разрушение идеалов произошло так же естественно с падением советского строя… И в один прекрасный (потому что солнечный) день жители «другой планеты» сказали «Добро пожаловать» молодому Алексею Гончарову и его семье – жене и двухлетнему сынишке. Друзья предложили работу в Сингапуре. На 13 лет Гончаровы попали в рай земной, где Алексей постоянно чувствовал себя счастливым ребенком, у которого каждый день – именины. Несмотря на все сложности и трудности, с которыми сталкивается человек, приехавший без средств и знакомств, без знания языка в чужую страну. Помогли, считает мой герой, «вечно хорошая погода, любовь к бурно развивающейся компьютерной индустрии Сингапура и курсы английского языка в British Council». Если бы не семейные обстоятельства, Алексей и сегодня жил бы там. Несмотря на то что вернулся два года назад, воспоминания ярки и свежи: «Там все не так, как везде. Люди ходят, улыбаются. Сингапур – небольшое государство, всего 4,5 миллиона человек живут. Наверное, из-за того, что страна небольшая, ее сумели превратить в рай земной. Сингапур весь цветущий, зеленый, красивый. Там государство думает о людях постоянно, это чувствуется во всем. Если власти что-то делают, они всегда объясняют, для чего это сделано… У людей хорошие пенсионные накопления. Там заботятся о детях. Очень много делают для безработных, активно занимаются переподготовкой кадров. Любопытно – вот ты приходишь в какую-нибудь государственную организацию, и сразу видно, как государство к тебе относится. Они стараются обслужить тебя поскорее, а если приходится ждать – то в комфортных условиях: удобно сидеть, можно попить воды, почитать журналы, посмотреть телевизор, воздух чистый… Они обо всем этом думают!»

Итак, приключение – это когда попадаешь на другую планету и счастливо там живешь.

НАИВ, рифма, портрет

Когда Алексей уезжал в страну своей мечты, у него родились такие строки:

Нам сложный Быт мешает «стать собою»,
А им Уют мешает «стать собой».
По сути Быт мы сделали виною
Тому, что жизнь нам кажется чужой.
Вся наша жизнь, как Подпрограмма
В большой Программе Суеты
Зациклена вокруг дивана –
Там, где мы «спим и видим сны»...
Сменить наш Быт не так уж «невозможно»,
Сменить страну, друзей, подруг,
Отдать диван соседу тоже можно,
Сменить бардак на «их» уют.
Уехать далеко, укрыться...
Забыть о страхе в тишине
И посвятить остаток жизни
Своим детишкам и жене.

Творчество всегда было составной частью жизни Алексея, так же, как чудеса, как исследование техники и создание своих собственных технических новшеств. Вы только представьте, Алексей Гончаров окончил сначала музыкальную школу по классу фортепиано, а три года спустя – физико-математическую, поступил в МВТУ им. Баумана, сдав экзамены на «отлично». Просто-таки гармоничный человек Леонардо да Винчи. Музыку и стихи пишет до сих пор. Но настоящий всплеск вдохновения случился, как это ни странно, в армии. Друзья – Саша Иванов и Макс Кочетков – организовали группу «НАИВ» («Новые Арлекины и Волтижеры») и взяли солдатика призыва 1987 года играть на клавишных. «Я бы сравнил это с глотком безудержной радости и свободы», – говорит Алексей. Да и для многих в начале перестройки эти песни стали откровением, меняя, уверен Гончаров, «не только нас, но и весь мир вокруг нас».

Творчеству сегодня ничуть не мешает занятость, строгий распорядок рабочего дня, наличие семьи – между прочим, у Гончаровых трое детей! Наоборот, какая-нибудь детская фраза порой становится импульсом, из которого рождается строка, рифма, куплет… Или мелодия для души, для себя, для близких. Дети вдохновляют Алексея и как фотохудожника. Из всех жанров фотографии ему ближе всего портрет, и лучше всего получаются портре-

ты сына и двух дочек. А еще пейзажи с цветами. А еще лучше, когда на фото они вместе – цветы и радостные ребятишки. Получается очень естественно и искренне.

Старший ребенок, впрочем, выходит из благодатного возраста детства – ему уже 16 лет. Ему скоро предстоит задуматься о будущей профессии, а это всегда нелегко. Тем более в наши непростые времена. Тем более, когда большую часть жизни провел за рубежом, и, значит, выбор жизненных путей-дорог больше, и голову поломать есть над чем. Кстати, дочери Алексея Гончарова там, в Сингапуре, родились и пока еще здесь, на Родине, говорят по-русски несколько хуже, чем их ровесники. Но Алексея волнует как раз не это (психологи считают, что в этом возрасте и язык быстро «нарабатывается», и вообще ребенок шустрее взрослого адаптируется к новой обстановке), а как бы девочки английский не потеряли. Ходят «сингапурские москвички» в школу с углубленным изучением языка, и с удовольствием смотрят диснеевские мультики без перевода. Продолжат ли дети отцовскую «техническую» линию (и материнскую – супруга Алексея тоже окончила МВТУ им. Баумана), пока непонятно. Старшая дочь хочет быть врачом…

Вот вам еще одна разновидность приключения – когда «строку диктует чувство – оно на сцену шлет раба» (Пастернак).

Обиженный клиент – двигатель прогресса

Он может часами наблюдать за цветком, чтобы сфотографировать его в нужном ракурсе, при нужном освещении и с нужной капелькой росы на лепесточке. Молча и терпеливо. В критическую минуту, когда жизнь разрушит планы, отберет надежды, оставит без гроша в кармане, он будет радоваться… что хуже не вышло, руки есть, голова на месте – проживем! Не нужно ничему удивляться… «Я Рак, я гибкий», – улыбается Алексей. Представители этого знака Зодиака редко теряют голову, ведь у них даже в случае краха обязательно есть пара-тройка планов отхода, подготовлены «базы» для отступления. Дом – их крепость, а работа – святое место, где они счастливы. Безмятежный образ созерцателя теряет плавность черт, когда Алексей говорит о своем Деле. Вот так, с большой буквы. Да и как не любить профессию, в которой выстроил все своими руками, кирпичик за кирпичиком. Сначала, в конце 80-х, программист в Космоаэрогеологической экспедиции №1 писал программы обработки космических фотографий. Потом пошел программистом в кооператив – занимался установкой сетей на базе ПО Novell и внедрением CAD-систем компьютерного дизайна. О, девственные времена, когда компьютеры и плоттеры возили просто в купейных вагонах… И когда для легализации деятельности покупали юр. лицо – кооператив по вязке варежек – и продолжали собирать компьютеры… Насмешливо-восторженное воспоминание: «Наняли одноклассницу бухгалтером. Хотя денег было мало, мысль о том, что у тебя есть сотрудник, который эти деньги считает, да еще на компьютере… ну просто окрыляла». Для полноты картины остается добавить, что на первый тогда суперсовременный 386-й Алексей заработал вместе с другом, разгружая вагоны с картошкой, свеклой, луком, арбузами, помидорами…

Потом была защита диплома – уже в МЭИ, куда Алексей перешел, когда пришлось задуматься о хлебе насущном. Компьютерный магазин в солнечном Сим Лиме – в Сингапуре тоже нужна была новейшая техника. А потом рынок «железа» потерпел крах. И опять невозмутимый Рак не растерялся. «Зато бизнес в области разработки ПО пошел в гору! Пришлось переучиваться. Закончил курсы по базам данных BTrieve, Pervasive.SQL, Microsoft SQL. Прошел стажировку в Техасе».

Найти место под солнцем всегда легче, когда обладаешь недюжинными организаторскими способностями. Еще в армии, где Алексей служил оператором ЭВМ, он не только наловчился оперативно снимать клавиши с терминала ЕС 1065, мыть их с мылом в горячей воде, сушить в портянке и на память вставлять каждую клавишу на место, но и еще кое-что придумал. «Используя спутниковую связь и ком-

пьютерную сеть, я предложил разным операторам сверять данные для улучшения достоверности и, используя эти общие данные, спать по очереди». Нечто подобное повторилось, когда нужно было организовать по разумной цене круглосуточную поддержку ПО (она только входила «в моду»). «Я предложил руководству Pervasive перенести американские ночные смены в Сингапур. За счет разницы во времени дневная смена в Сингапуре обслуживала ночное время суток в США. Это стоило в несколько раз дешевле, чем организация ночных смен в Техасе. Да и вменяемость людей в дневное время существенно лучше! Сам подготовил и провел тренинги. Организовал работу службы технической поддержки».

А потом наступил XXI век. И компания SWsoft, где Алексей Гончаров служил на тот момент заместителем директора по развитию бизнеса, предложила Intel систему виртуализации Virtuozzo, которая позволила разделить «монстр» – восьмипроцессорный сервер Dell 8450 на большое количество виртуальных выделенных серверов. SWsoft получила сервер и деньги на телевизионную рекламу. Мир ИТ получил термин VPS-сервер. А Алексей Гончаров – Дело и страсть на многие годы. Называется эта «любовь» – виртуализация вычислительных ресурсов. Вот как образно рассказывает о VPS-сервере герой этого очерка: «Это как отдельный офис в небольшом особняке. Хотя в «доме» находится несколько «офисов» – от 5 до 50, но каждый очень хорошо изолирован от остальных и по шуму, и по безопасности. Каждый «офис» имеет отдельный вход, свои «удобства» и средства коммуникации. Естественно, такой «офис» стоит своих денег (от 999 руб. в месяц) и рассчитан на бизнесы, которым на имидже экономить нельзя. Как потом туда приглашать солидных клиентов?» А еще есть виртуальный хостинг – это те же «офисы», но расположенные в общежитии, где те же услуги, однако много общих «удобств», поэтому сервис дешевле.

Директор «Русоникса» (www.rusonyx.ru) очень гордится, что его компания – лидер в области предоставления VPS-серверов на российском рынке. «Мы в прошлом году заработали первый миллион долларов по обороту. Сейчас у нас свыше 20 тысяч доменов».

А главное – на самом деле это самая главная точка интереса – тут опять пахнет приключением!.. «Фантастика – серверы, к которым мы привыкли, эти металлические ящики, становятся виртуальными!»

– Есть чувство, что вы занимаетесь полезным делом?

– Безусловно. Удовлетворение есть. Мне хочется, чтобы клиенты были довольны.

– Но наверное, всегда найдутся недовольные?..

– Это же хорошо. У всех людей разные точки зрения. Ожидания разные. Надо просто выслушать человека и сделать какие-то выводы. Если он прав, надо что-то изменить в организации работы или в услугах. Такие обиженные клиенты – двигатель прогресса.

То есть выходит, недовольный клиент – не повод для того, чтобы рвать на себе волосы и менять профессию, а очередная причина для оптимизма... Шанс для очередного приключения и чудесного спасения из пут обыденности и серых будней!

Текст: Оксана Родионова, фото: Евгения Тарабрина

Портал в стиле Web 2.0

В настоящее время в корпоративной среде все большую популярность набирают решения, ориентированные на Web как на среду размещения различных приложений, предназначенных для повседневного использования в пределах офиса, – так называемый портал офиса в стиле Web 2.0.

Александр Башкиров

История возникновения

Исторически порталы начинали свое развитие от «корпоративных сайтов», представляющих собой новости компании и список сотрудников. При этом основное наполнение такого сайта лежало на плечах специального сотрудника, который периодически обновлял сайт, актуализируя размещенную на нем информацию.

Следующим шагом в развитии порталов стала интерактивность – то есть пользователи получили персонализированный доступ к порталу, появилась возможность комментировать избранные материалы и получать обновления информации по электронной почте.

Следующий виток в развитии заключался в качественном пересмотре идеологии места портала в организации и его функций: в эпоху Web 2.0 в понятие «портал» стали вкладывать несколько иной смыл, чем раньше: наполнение содержимым такого ресурса частично происходит силами его пользователей – в рамках выделенных прав (это вообще один из основополагающих признаков, указывающих на «вебдванольность»), широкое использование JavaScript и AJAX в пользовательском интерфейсе, и интеграцию приложений – на уровне его архитектуры.

Рассмотрим небольшой пример. Внутренний портал (корпоративный сайт, размещенный в интрасети) содержит блок новостей с разделением по «каналам» («новости компании», «новости отделов», «новости пользователей»), с возможностью комментировать любую новость каждым зарегистрированным пользователем (сотрудником организации), размещение сотрудниками новостей в определенном канале («новости пользователей»), справочник сотрудников, содержащий как информацию, которую вносит отдел кадров, так и информацию, которую дополнительно может внести сам сотрудник – например, ссылку на личный веб-сайт, описание хобби и т.д., с возможностью позвонить на один из опубликованных для каждого сотрудника телефонов прямо из его карточки, «личный кабинет» сотрудника с возможностью просмотра сотрудником своей статистики – естественно, без возможности правки (по заработной плате и бонусам, по телефонным переговорам, по трафику Интернета и т.д.), список назначенных на него заданий и перечень различных документов, сгруппированных по различным признакам, с возможностью их редактирования непосредственно в браузере в зависимости от прав пользователя и занимаемой им должности.

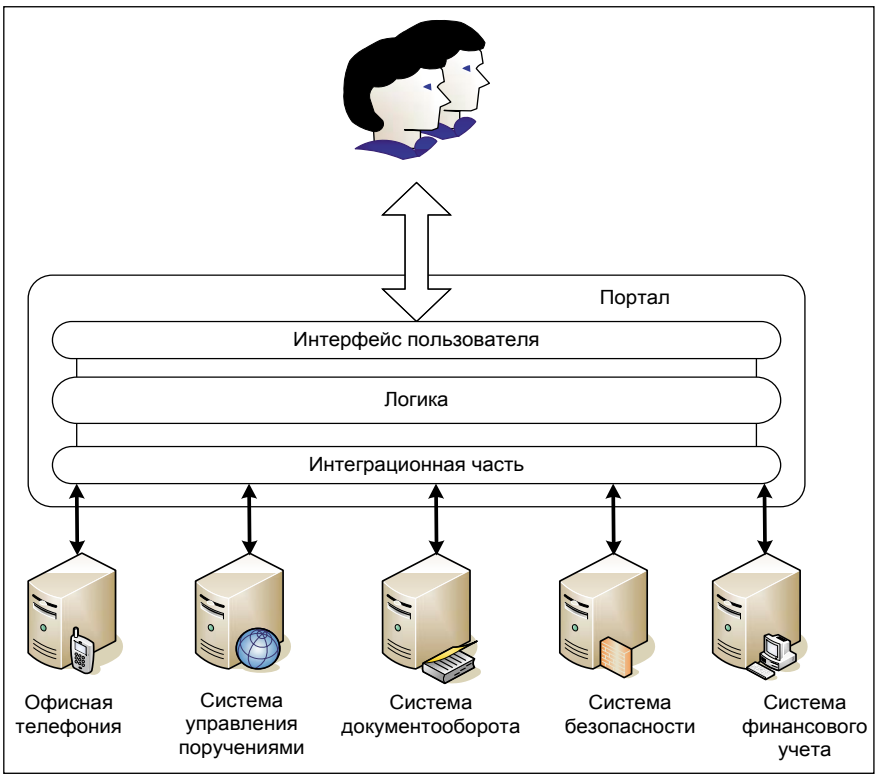


Схема архитектуры решения

В приведенном примере имеется контейнер, построенный на базе веб-технологий, реализующий функции базового интерфейса, а также части функций и набор приложений, интегрированных с ним, в частности:

- систему офисной телефонии;
- систему управления поручениями;
- систему документооборота;
- систему финансового учета;
- систему безопасности (система контроля интернет-трафика).

При этом сам портал (движок) реализует функции размещения новостей и справочника сотрудников с редактированием элементов посредством Windows-подобного веб-интерфейса, и для конечного пользователя решение выглядит монолитным: единый интерфейс пользователя скрывает подробности архитектуры решения. Схема архитектуры решения из примера приведена на **рисунке**.

Плюсы и минусы

Таким образом, корпоративный портал может стать единым центром, «входом» во все приложения, которые доступны пользователю в соответствии с его уровнем доступа. Преимуществом такого рода решений будут являться:

- **Простота развертывания новых рабочих мест** – для развертывания нового рабочего места достаточно занести пользователя в корпоративный каталог пользователей и назначить ему права на приложения, после чего выдать ссылку на вход в портал.
- **Низкие требования к аппаратной части** – для работы портала на клиентском рабочем месте достаточно браузера: почти все действия выполняются на стороне сервера, исключение составляет лишь JavaScript, flash и Java-апплеты, выполнение которых происходит на стороне пользователя.
- **Скорость освоения пользователем корпоративного рабочего места** – единый стиль интерфейса для всех приложений портала позволяет пользователям сконцентрироваться на функциональном наполнении, а не на запоминании тонкостей работы с тем или иным приложением.

- **Информационная безопасность** – большинство действий пользователя, все манипуляции с документами происходят на стороне сервера, следовательно, снижаются требования к обеспечению информационной безопасности рабочего места сотрудника, то есть акценты безопасности смещаются в сторону сетей – то есть того сегмента, который традиционно является наиболее хорошо защищенным.

Минусами такого решения будут являться:

- Необходимость построения уникального интегрированного решения.
- Возможные сложности в процессе сопровождения такого решения.

Основные преимущества

Тем не менее, несмотря на минусы, подобные внутриофисные портальные ресурсы приобретают все большую популярность. Этому в немалой степени способствует то, что посредством Web 2.0 порталов реализуются функции, которые сложно реализуемы или нереализуемы при помощи традиционных технологий, в частности:

- On-line office application;
- средства совместной работы;
- средства удаленной работы;
- концепция «Онлайн-офис» и «офис удаленных сотрудников».

Рассмотрим эти функциональные аспекты более подробно.

On-line office application

Под этим понимаются приложения, предназначенные для выполнения традиционных «офисных» операций: набор и редактирование текстов, создание электронных таблиц и презентаций. Самый известный пример такого рода приложений – Google Mail&Docs (Google, кстати, сдает в аренду свои приложения для корпоративного использования – с использованием собственного домена заказчика).

Средства совместной работы

Под этим подразумевается в первую очередь возможность совместного одновременного редактирования одного и того же документа или файла. По сути, средства совместной работы над документом представляют собой функциональную особенность on-line application, а средства совместной работы над файлом – некий аналог систем, предназначенных для работы с репозиториями кода (CVS, SVN и т.д.).

В том же Google Docs такая возможность присутствует: достаточно «расшарить» созданный документ с возможностью редактирования на еще одного пользователя («ключиком» к бесплатной, некоммерческой версии Google Docs является аккаунт Google), и одновременно приступить к его редактированию, чтобы увидеть в онлайн-режиме изменения, вносимые каждым пользователем, а при необходимости – просмотреть историю изменений документа.

Средства удаленной работы

Это, с одной стороны, удаленный доступ к порталу извне (через Интернет), а с другой стороны – политики и система безопасности, позволяющие обеспечивать удобную работу сотрудников из мест, не находящихся в локальной сети организации, и обеспечивающие безопасность этой самой работы. Как правило, в подавляющем большинстве случаев для доступа используют или SSL, или VPN.

Концепция «Онлайн-офис»

Это, по сути, особый стиль обеспечения рабочим местом отдельных сотрудников: такие сотрудники в силу характера выполняемой работы (например, работа, связанная с командировками, или сотрудники из других регионов, либо просто удаленные сотрудники – например, корпирайтеры, редакторы сайтов и т.д.) могут вообще не иметь рабочего места в офисе и работать из любого места, где присутствует широкополосный Интернет. При этом вся работа с корпоративной информацией осуществляется в веб-портале: от создания документов до звонков и внутреннего чата. Следует отметить, что при подобной постановке вопроса необязательно даже иметь корпоративный ноутбук: в крайнем случае (с небольшими ограничениями), работать можно хоть через интернет-кафе.

Концепция «онлайн-офис» может быть применима и к традиционным (и не совсем) офисам: в частности, при реализации этой концепции в традиционном офисе сотрудники могут работать с ПК с минимальными аппаратными требованиями или с терминальными станциями.

В «не совсем традиционных» офисах концепция «онлайн-офиса» успешно применятся при организации офиса по принципу Open Space (открытого пространства) – то есть ситуации, при которой у сотрудника нет явно выделенного рабочего места, а при приходе на работу он занимает любое свободное рабочее место.

Вариантом «не совсем традиционного офиса» является концепция «виртуальной компании», то есть компании, в которой собственный офис отсутствует, а все без исключения сотрудники которой работают с офисными приложениями через Интернет. Примером такой компании может служить, например, небольшой интернет-магазин, не имеющий собственного офиса и осуществляющий общение сотрудников посредством портальной части решения (веб-сайта компании).

Средства реализации

Средства реализации такого рода порталов делятся на два типа: арендуемые и платформенные.

Первые – это готовые веб-приложения с готовым набором компонентов приложений и функций, сдаваемые в аренду «как есть», без возможности «тонкой» (а порой и вообще какой-либо) настройки. Как правило, эти приложения не имеют отдельно выделенных блоков новостей, справочников и т.д. – их приходится реализовывать на какой-либо CMS, обеспечивая прозрачную работу и сквозную авторизацию с компонентами веб-приложений. К такого рода системам относятся продукты Google Docs (http://docs.google.com) и, например, Zoho (http://zoho.com).

Вторые – «платформенные» порталы – представляют собой инсталлируемые решения, открытые (в определенных рамках) для самостоятельных доработок. Пожалуй, самыми известными примерами таких решений является Micosoft Share Point Portal (http://www.microsoft.com/rus/sharepoint/default.mspx) или (в более усеченном варианте) Micosoft Share Point Services (http://technet.microsoft.

com/en-us/windowsserver/sharepoint/default.aspx) и IBM WebSphere Portal (http://www-01.ibm.com/software/ru/websphere), хотя портал в минимальной функциональности можно построить даже на Open Source-движке, предназначенном для построения обычных сайтов (с соответствующими доработками).

Выбор конкретного решения сильно зависит от бюджета, который имеется на внедрение, и задач, которые ставятся перед порталом.

В случае «виртуальных» компаний или небольших компаний, у которых большинство сотрудников находятся вне офиса, логичнее использовать арендуемые приложения с единой точкой входа на базе Open Source-движка.

В случае больших компаний логика несколько иная: лучше использовать портальную платформу, обеспечив ее интеграцию с необходимыми приложениями.

Что же касается средних компаний, то в жизни встречается множество вариаций портальных решений: от справочника сотрудников с хранилищем файлов без возможности онлайн-редактирования и ленты новостей до вполне «взрослых» решений, которые включают в себя интеграцию с функциональными приложениями, IP-телефонию и прочие атрибуты пресловутой «вебдванольности».

В любом случае все сильно зависит от тех задач, которые призван решать портал. Рассмотрим некоторые примеры.

Пример 1

Небольшая компания, для которой портал – это средство оповестить сотрудников об изменениях, новостях и предоставить возможность каждому из них иметь под рукой корпоративный справочник (внутренний номер телефона, сотовый номер, e-mail, личная информация) с возможностью комментирования новостей компании (которые заносятся на портал централизованно, через редактора), отображения статуса пользователя: online/offline (то есть находится в данный момент сотрудник на портале или нет), возможностью отправить ему письмо прямо из справочника и чата с ним.

В этом случае для реализации подойдет любая Open Source-платформа (например, Wordpress – http://www.wordpress.com) или, если в компании есть Microsoft Windows 2003 Server, входящий в его состав Microsoft Share Point Services.

Реализация потребует поиска или создания специализированных компонентов (справочник сотрудников в виде дерева карточек отсутствует как в Microsoft Share Point Services, так и в Open Source-движках – в том же Wordpress придется писать отдельный плагин). В этом случае затраты на создание и внедрение будут сведены к минимуму.

Следует отметить, что в последнее время в Интернете появилось довольно много компаний, предлагающих типовой портал на базе Microsoft Share Point Services за относительно небольшие деньги. Основная цель такого портала – создание модного ныне «единого информационного пространства» или, говоря проще, максимально оперативно информировать сотрудников обо всем, что может быть использовано в повседневной работе

или повлиять на нее, а также возможность общения.

Пример 2

Небольшая виртуальная компания, которая занимается разработкой программного обеспечения. В этом случае портал также может представлять собой доработанную CMS (те же Wordpress или Joomla, как альтернатива – Microsoft Share Point Services), на базе которой выполнена интеграция с системами контроля версий (типа CVS, SVN, Microsoft SourceSafe), размещен справочник сотрудников, с возможностью обмена e-mail, чата и звонков друг другу с портала посредством одного из популярных сервисов звонков через Интернет (Skype, Google), или через собственное решение для IP-телефонии (например, Open Source-решение Asterisk). Основная цель такого портала – возможность работы и общения в рамках выполняемой работы.

Пример 3

Средняя организация, имеющая несколько офисов и сотрудников, которые должны работать из любого места, где есть Интернет (например, торговые представители). В этом случае портал будет представлять собой более серьезное решение, построение которого на базе Open Source-продуктов может оказаться нецелесообразным – слишком велик получается объем доработок, и, как следствие, стоимость создания решения. В этом случае портал целесообразно строить на основе портальных продуктов, таких как Microsoft Share Point Services, Microsoft Share Point Server, IBM WebSphere.

Такой портал будет обладать всеми функциями, которые рассмотрены выше (новости, коммуникации сотрудников через Интернет), но в дополнение к этому будет иметь функции для работы с документами – причем не просто размещения заранее подготовленных файлов, но и онлайн-создания и редактирования документов прямо в Интернете, в Windows-подобном интерфейсе.

Второй вариант решения задачи состоит в аренде готовых веб-приложений у провайдеров такого рода услуг (те же упомянутые выше Google и Zoho) и интеграции их с Open Source-решениями на базе CMS. В частности, связка доработанной Joomla с GoogleDocs вполне способна обеспечить требуемые функции.

Пример 4

Большая организация, которая кроме новостей и справочника сотрудников хочет иметь единую точку входа в корпоративные приложения, документооборот на портале, корпоративную систему Service Desk и т.д., интегрированную с доменной авторизацией и системой безопасности. Очевидно, что большая часть усилий по внедрению такого рода решения будет лежать в интеграции приложений в портал.

В этом случае решение будет лежать, как это ни парадоксально, либо в поиске команды независимых разработчиков (внутри компании или по найму на проект), либо в привлечении сторонней организации. Дело в том, что бюджет такого рода проектов, как правило, велик, а ключевым фактором успеха является компетенция конкретных исполнителей по отношению к конкретному продукту. При этом стоимость лицензий проприетарного ПО может составлять незначительную сумму по сравнению со стоимостью интеграционных работ.

Критерии выбора

Оценивая то, насколько подходит или не подходит то или иное решение для реализации портала, следует иметь в виду не только начальную стоимость приобретения, но и такие немаловажные вещи, как поддержка и сроки внедрения. Если эти сроки не критичны, то можно использовать и Open Source: рано или поздно все получится, просто для достижения результата придется проанализировать большой объем чужого кода. Если сроки критичны и позволяет выделенный на реализацию бюджет, то можно и нужно использовать коммерческое решение, зафиксировав в договоре с поставщиком дату, к которой должна быть выполнена реализация, объем, срок и параметры качества технической поддержки внедренного портала.

Итого

В настоящее время с появлением все более широких каналов появилась тенденция выноса «традиционных» приложений в Web. Это касается не только многочисленных онлайновых клонов Microsoft Word (такого рода функциональностью уже мало кого удивишь) или специализированных систем (например, систем управления предприятием, изначально разрабатываемых с веб-интерфейсом и широкими возможностями интеграции), но и таких совсем «не веб»-вещей, как, например, редакторы изображений (например, http://pixlr.com/app или http://www.splashup.com/splashup), клиентов электронной почты (Outlook Web Access, Gmail) и множество других полезных утилит (мессенджеры – www.icq.com; планировщики – http://organaizer.ru, http://napominatel.ru; антивирусы – http://online.us.drweb.com, http://www.kaspersky.ru/scanforvirus; упрвление проектами – http://www.comindwork.ru и т.д.).

В этом свете порталы имеют огромный потенциал развития: по мере того, как будет расти мощность вычислительных ресурсов и полоса пропускания каналов, порталы будут обрастать новыми полезными функциями, фактически выводя в веб традиционные «десктопные» приложения (например, тот же MS Project или Visio), окончательно реализуя, таким образом, идею on-line рабочего места без привязки к конкретному местоположению сотрудника.

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

Реклама

Python: сложные аспекты

Дмитрий Васильев

Рассматриваем метаклассы, дескрипторы атрибутов и менеджеры контекста.

В этой статье мы рассмотрим некоторые достаточно сложные аспекты языка Python, а именно:

- **метаклассы**, позволяющие создавать классы с необычным поведением;
- **дескрипторы атрибутов**, предоставляющие наиболее гибкий контроль доступа к атрибутам объектов и классов;
- **менеджеры контекста**, объекты, позволяющие управлять поведением ключевого слова with.

Метаклассы

В общем случае, как и следует из названия, метаклассы – это классы классов. Таким образом, классы являются экземплярами метаклассов. Начиная с Python 2.2 стандартным метаклассом является type, который служит метаклассом для всех встроенных типов. Это можно увидеть на следующем примере:

```
>>> ().__class__
<type 'tuple'>
>>> ().__class__.__class__
<type 'type'>
```

Здесь классом для создания кортежа является tuple и соответственно классом для создания tuple является type. В этой статье мы рассматриваем только так называемые новые классы, то есть классы, которые наследуются от встроенного класса object. На данный момент «старые» (или «классические») классы должны представлять только исторический интерес, хотя они еще используются в некоторых проектах.

В Python при выполнении выражения, описывающего класс, интерпретатор сначала определяет соответствующий классу метакласс M и затем вызывает M(name, bases, dict) для создания класса. Это происходит после того как было обработано тело класса, где определены его методы и атрибу-

ты. Аргументами при вызове метакласса являются:

- **name** – имя класса, строка, получаемая из выражения, описывающего класс;
- **bases** – кортеж базовых классов, получаемый в начале обработки выражения класса, или () если класс не определил базовых классов;
- **dict** – словарь с методами и атрибутами класса, которые были определены в теле класса;

Затем результат вызова M присваивается переменной с именем класса. Описание вызова метакласса для создания класса можно проиллюстрировать следующим примером:

```
>>> T = type("test", (object,), {"name": "Test"})
>>> T
<class '__main__.test'>
>>> T.name
'Test'
>>> t = T()
>>> t
<__main__.test object at 0x2863550>
>>> t.name
'Test'
```

После того как мы рассмотрели, как метакласс создает класс, остается понять, как выбирается метакласс. Для выбора метакласса используются следующие шаги:

- Если определен dict['__metaclass__'] (то есть в теле класса был определен атрибут __metaclass__), то он используется.
- Иначе, если определен хотя бы один базовый класс, используется метакласс базового класса.
- Иначе будет использоваться глобальная переменная __metaclass__, если она определена.
- В противном случае будет использоваться метакласс для «классических» классов types.ClassType и соответственно будет создан «классический» класс.

Начиная с Python 3.0 метакласс можно указывать только как именованный параметр при определении класса, следующим образом:

```
>>> class Test(metaclass=type):
...     pass
...
```

Основные ограничения, связанные с метаклассами языка Python:

- Нельзя наследоваться одновременно от «классического» и «нового» классов. В этом случае возможности «новых» классов, описанные в этой статье, работать не будут.
- Метакласс класса должен соответствовать метаклассу базового класса или быть его потомком.

«Новые» классы

Новая система типов и классов (так называемые новые классы) была добавлена в Python 2.2 для унификации классов и типов. Основная причина их появления – это предоставление унифицированной объектной модели с полноценной моделью метаклассов. «Новые» классы также предоставляют следующие возможности:

- ☑ Наследование от встроенных типов, например списков (list) и даже целых (int), которые должны работать везде, где требуется оригинальный тип.
- ☑ Создание статических методов и методов класса.
- ☑ Вызов методов при доступе к атрибутам. Эта функциональность реализуется с помощью дескрипторов атрибутов.

В Python 2 простейший способ создать «новый» класс – это наследовать его от object:

```
class Test(object):
    pass
```

Начиная с Python 3.0 «старые» классы были удалены и по умолчанию используются «новые» классы (которые уже нет необходимости называть «новыми»).

Примеры метаклассов

После описания работы метаклассов обратимся к примерам собственных реализаций. Как уже было рассмотрено ранее, класс создается при вызове метакласса следующим образом: M(name, bases, dict). Более детально при создании классов (можно провести аналогию с созданием объектов класса) вызываются методы метакласса __new__() и затем __init__(), как в следующей последовательности строк:

```
cls = M.__new__(M, name, bases, dict)
assert cls.__class__ is M
M.__init__(cls, name, bases, dict)
```

Напишем наш первый метакласс, чтобы рассмотреть последовательность вызова методов при создании класса и объекта:

```
class MetaTest(type):

    def __new__(cls, name, bases, dict):
        klass = super(MetaTest, cls).__new__(cls, name, ↵
                bases, dict)
        print "__new__(%r, %r, %r) -> %r" % (name, bases, ↵
                dict, klass)
        return klass

    def __init__(cls, name, bases, dict):
        super(MetaTest, cls).__init__(name, bases, dict)
        print "__init__(%r, %r, %r)" % (name, bases, dict)

    def __call__(cls, *args, **kwargs):
        obj = super(MetaTest, cls).__call__(*args, **kwargs)
        print "__call__(%r, %r) -> %r" % (args, kwargs, obj)
        return obj
```

Здесь мы просто выводим информацию о вызове методов __new__(), __init__() и __call__(). Вот как это работает:

```
>>> from meta import MetaTest
>>> class Test(object):
...     __metaclass__ = MetaTest
...
__new__('Test', (<type 'object'>,), {'__module__': '__main__',
'__metaclass__': <class 'meta.MetaTest'>}) -> <class '__main__.Test'>
__init__('Test', (<type 'object'>,), {'__module__': '__main__',
'__metaclass__': <class 'meta.MetaTest'>})
>>> test = Test()
```

```
__call__((), {}) -> <__main__.Test object at 0x7f62e95ca650>
```

Обратите внимание на атрибут __metaclass__ в теле класса, как уже было описано выше, это один из способов присвоения метакласса классу.

Таким образом, мы видим последовательность вызова методов метакласса:

- **__new__()** – вызывается для создания класса;
- **__init__()** – для инициализации класса;
- **__call__()** – вызывается при создании объектов класса.

Нужно также отметить, что атрибуты и методы, определенные в метаклассе, являются статическими, то есть доступны только на уровне класса, но не на уровне объектов класса:

```
>>> class MetaTest(type):
...     def test(cls):
...         print "test()"
...
>>> class Test(object):
...     __metaclass__ = MetaTest
...
>>> Test.test()
test()

>>> Test().test()
Traceback (most recent call last):
  File "<stdin>", line 1, in <module>
AttributeError: 'Test' object has no attribute 'test'
```

Рассмотрим примеры более полезных метаклассов. Метакласс AutoSuper добавляет приватный атрибут __super для доступа к атрибутам и методам базовых классов:

```
class AutoSuper(type):

    def __init__(cls, name, bases, dict):
        super(AutoSuper, cls).__init__(name, bases, dict)
        setattr(cls, "_%s__super" % name, super(cls))
```

Теперь он может быть использован так:

```
>>> from super import AutoSuper
>>> class A(object):
...     __metaclass__ = AutoSuper
...     def method(self):
...         return "A"
...
>>> class B(A):
...     def method(self):
...         return "B" + self.__super.method()
...
>>> B().method()
'BA'
```

Таким образом, при работе с классом и его подклассами можно везде заменить вызов встроенной функции super на обращение к приватному атрибуту __super. Это позволяет контролировать доступ к базовым классам на уровне класса или даже объекта. Плюс к этому уменьшается вероятность ошибок, связанных с опечатками, и в случае изменения имени класса нет необходимости изменять имя в нескольких местах.

Следующий пример представляет собой метакласс, устанавливающий атрибуты для объектов, создаваемых классом без необходимости определения конструктора класса:

```
class AttrInit(type):

    def __call__(cls, **kwargs):
        obj = super(AttrInit, cls).__call__()
        for name, value in kwargs.items():
            setattr(obj, name, value)
        return obj
```

Этот метакласс может быть использован так:

```
>>> from attr import AttrInit
>>> class Message(object):
...     __metaclass__ = AttrInit
...
>>> class ResultRow(object):
...     __metaclass__ = AttrInit
...
>>> msg = Message(type='text', text='text body')
>>> msg.type
'text'

>>> msg.text
'text body'

>>> row = ResultRow(id=1, name='John')
>>> row.id
1

>>> row.name
'John'
```

Такой метакласс может быть полезен для создания классов, объекты которых служат в основном как хранилище атрибутов. Например, классов, описывающих передаваемые по сети пакеты данных, или строки результата запроса к базе данных, к полям которых удобнее обращаться как к атрибутам.

Таким образом, метаклассы позволяют создавать классы с достаточно необычным поведением, но в то же время вряд ли стоит их использовать в каждой программе.

Дескрипторы атрибутов

Дескрипторы атрибутов (далее просто дескрипторы) описывают протокол доступа к атрибутам объекта или класса. В общем случае дескрипторы – это объекты, в которых определен один из методов: __get__(), __set__() или __delete__(). Среди уже определенных в Python дескрипторов можно назвать следующие: property, classmethod и staticmethod. Рассмотрим интерфейс дескрипторов на примере:

```
class TestDescriptor(object):

    def __get__(self, obj, type=None):
        print "__get__(%r, %r)" % (obj, type)
        return "value"

    def __set__(self, obj, value):
        print "__set__(%r, %r)" % (obj, value)

    def __delete__(self, obj):
        print "__delete__(%r)" % obj
```

При доступе к атрибуту методы этого дескриптора вызываются следующим образом:

```
>>> from desc import TestDescriptor
>>> class Test(object):
...     attribute = TestDescriptor()
...
>>> Test.attribute
__get__(None, <class '__main__.Test'>)
'value'
>>> t = Test()
>>> t.attribute
__get__(<__main__.Test object at 0x7f757d88d510>,
<class '__main__.Test'>)
'value'
>>> t.attribute = "new value"
__set__(<__main__.Test object at 0x7f757d88d510>, 'new value')
>>> del t.attribute
__delete__(<__main__.Test object at 0x7f757d88d510>)
```

Здесь мы видим, что при доступе к атрибуту attribute, являющемуся дескриптором, на самом деле вызываются методы дескриптора. Надо также заметить, что дескрипторы вызываются из метода __getattribute__() (который в свою очередь имеет смысл только для «новых» классов), определенного в классе object, и его переопределение может отменить автоматическое обращение к дескрипторам при доступе к атрибутам. Также следует знать, что если дескриптор определяет только метод __get__(), то атрибут, за которым стоит такой дескриптор, может быть переопределен присваиванием другого значения атрибута объекту. Если же дополнительно определен метод __set__(), то атрибут объекта не может быть переопределен таким образом.

Примеры дескрипторов

Для примера реализуем аналоги встроенных дескрипторов property, classmethod и staticmethod в Python.

Дескриптор, имеющий поведение property, может быть представлен следующим классом:

```
class Property(object):

    def __init__(self, fget=None, fset=None, fdel=None, ↵
      doc=None):
        self.fget = fget
        self.fset = fset
        self.fdel = fdel
        self.__doc__ = doc

    def __get__(self, obj, type=None):
        if obj is None:
            return self
        if self.fget is None:
            raise AttributeError("unreadable attribute")
        return self.fget(obj)

    def __set__(self, obj, value):
        if self.fset is None:
            raise AttributeError("can't set attribute")
        self.fset(obj, value)

    def __delete__(self, obj):
        if self.fdel is None:
            raise AttributeError("can't delete attribute")
        self.fdel(obj)
```

Здесь операции запроса значения атрибута, установки атрибута и его удаления делегируются функциям, переданным в конструктор.

Поведение classmethod можно эмулировать следующим образом:

```
class ClassMethod(object):

    def __init__(self, f):
        self.f = f

    def __get__(self, obj, klass=None):
        if klass is None:
            klass = type(obj)
        def newfunc(*args, **kwargs):
            return self.f(klass, *args, **kwargs)
        return newfunc
```

Здесь первый атрибут при вызове метода заменяется классом объекта.

И наконец staticmethod может быть представлен так:

```
class StaticMethod(object):

    def __init__(self, f):
        self.f = f

    def __get__(self, obj, type=None):
        return self.f
```

Менеджеры контекста

Менеджеры контекста – это механизм, стоящий за ключевым словом with. Ключевое слово with появилось еще в Python 2.5, но к нему можно было получить доступ только через __future__ импорт: from __future__ import with_statement. Начиная с Python 2.6 ключевое слово with может быть полностью доступно без импортирования из __future__.

Ключевое слово with определяет блоки кода, которые прежде использовали try/finally. Для уверенности в выполнении кода его заключали в блок finally. With имеет следующую форму:

```
with выражение [as переменная]:
    блок with
```

Здесь «выражение» должно вернуть объект, предоставляющий протокол менеджера контекста. Для некоторых встроенных объектов уже определены менеджеры контекста. Например, такой менеджер определен для файлов, чтобы быть уверенным, что файл будет закрыт при выходе из блока:

```
with open('file.txt', 'rb') as f:
    for line in f:
        print line
```

В простейшем случае такая конструкция эквивалентна следующей:

```
f = open('file.txt', 'rb')
try:
    for line in f:
        print line
finally:
    f.close()
```

Протокол менеджера контекста содержит всего два метода: __enter__() и __exit__(). В начале выполнения блока кода вызывается метод __enter__(), который должен вернуть объект, присваиваемый переменной, после чего выполняется блок кода. Если блок кода выкидывает исключение, то вы-

зывается метод __enter__() с информацией об исключении. Если выполнение блока завершилось успешно, вся информация об исключении равна None. Пример работы:

```
class TestContext(object):

    def __init__(self, ignore_error=False):
        self.ignore_error = ignore_error

    def __enter__(self):
        print "__enter__()"
        return self

    def execute(self, error=False):
        print "execute()"
        if error:
            raise Exception("error")

    def __exit__(self, exc_type, exc_val, exc_tb):
        print "__exit__(%r, %r, %r)" % ↵
              (exc_type, exc_val, exc_tb)
        return self.ignore_error
```

Кроме методов, предоставляющих протокол менеджера контекста, здесь также определен вспомогательный метод execute(), который будет представлять код внутри блока:

```
>>> from context import TestContext
>>> with TestContext() as context:
...     context.execute()
...
__enter__()
execute()
__exit__(None, None, None)
```

```
>>> with TestContext() as context:
...     context.execute(error=True)
...
__enter__()
execute()
__exit__(<type 'exceptions.Exception'>, Exception('error',),
<traceback object at 0x7f6da88bffc8>)
Traceback (most recent call last):
  File "<stdin>", line 2, in <module>
  File "context.py", line 10, in execute
    raise Exception("error")
Exception: error
```

В случае, если метод __exit__() возвращает «ложь», исключение будет выкинуто за пределы блока. При этом метод __exit__() никогда не должен сам выкидывать полученное исключение, а управлять этим только через возвращаемое значение:

```
>>> with TestContext(ignore_error=True) as context:
...     context.execute(error=True)
...
__enter__()
execute()
__exit__(<type 'exceptions.Exception'>, Exception('error',),
<traceback object at 0x7fa35497a200>)
```

Модуль contextlib

Новый модуль contextlib (появившийся в Python 2.5) предоставляет функции и декораторы, упрощающие создание и работу с менеджерами контекста. На данный момент модуль предоставляет три функции:

Contextmanager(функция) – декоратор, упрощающий создание менеджеров контекста. Вместо создания класса, предоставляющего интерфейс менеджера контекста, можно использовать декоратор с функцией-генератором, например:

```
from contextlib import contextmanager

@contextmanager
def test():
    print "__enter__()"
    try:
        yield "execute()"
    finally:
        print "__exit__()"
```

Теперь мы можем использовать test() как менеджер контекста. Результат yield будет присвоен переменной:

```
>>> from context import test
>>> with test() as body:
...     print body
...
__enter__()
execute()
__exit__()
```

Nested(менеджер1[, менеджер2[,...]]) – функция, комбинирующая несколько менеджеров контекста в один. Следующий код:

```
from contextlib import nested

with nested(A(), B(), C()) as (X, Y, Z):
    body()
```

будет эквивалентен коду:

```
m1, m2, m3 = A(), B(), C()
with m1 as X:
    with m2 as Y:
        with m3 as Z:
            body()
```

Closing(объект) – функция, возвращающая менеджер контекста, который закрывает объект по завершении блока. Например:

```
from contextlib import closing
from urllib import urlopen

with closing(urlopen('http://www.python.org')) as page:
    for line in page:
        print line
```

В этом примере в конце блока будет вызван метод page.close().

Заключение

В этой статье были рассмотрены достаточно сложные аспекты использования Python, которые вы скорее всего не будете использовать в каждой программе. Но в то же время описанный инструментарий может значительно упростить и сделать более гибким сложный код, что позволит взглянуть по-новому на все разрабатываемое приложение в целом. Плюс знание этих инструментов и описанные особенности внутренней работы интерпретатора, должны поднять на новую ступень ваш уровень как разработчика ПО.

Подробнее про особенности «новых» классов можно прочитать по ссылке: http://www.python.org/doc/newstyle.

Переполнение буфера в muxatmd в IBM AIX

Программа: IBM AIX версии 5.2, 5.3 и 6.1.
Опасность: Низкая.
Наличие эксплоита: Нет.
Описание: Уязвимость существует из-за ошибки проверки границ данных в setuid-приложении /usr/sbin/muxatmd. Локальный пользователь может вызвать программу muxatmd со специально сформированными параметрами, вызвать переполнение стека и выполнить произвольный код на системе с повышенными привилегиями.
URL производителя: www.ibm.com.
Решение: Установите исправление с сайта производителя.

Отказ в обслуживании в Openswan

Программа: Openswan версии до 2.4.14 и 2.6.21.
Опасность: Средняя.
Наличие эксплоита: Нет.
Описание: Уязвимость существует из-за ошибки разыменования нулевого указателя при обработке Dead Peer Detection-пакетов. Удаленный пользователь может с помощью специально сформированного R_U_THERE или R_U_THERE_ACK Dead Peer Detection пакета аварийно завершить работу или перезапустить «pluto» IKE-демон.
URL производителя: www.openswan.org.
Решение: Установите последнюю версию 2.4.14 или 2.6.21 с сайта производителя.

Множественные уязвимости в ядре Linux

Программа: Linux kernel версии до 2.6.30-rc3.
Опасность: Низкая.
Наличие эксплоита: Нет.
Описание: 1. Уязвимость существует из-за ошибки проверки границ данных в функции CIFSTCon() в файле fs/cifs/connect.c. Удаленный пользователь может с помощью специально сформированного Tree Connect-ответа клиенту вызвать переполнение буфера и выполнить произвольный код на целевой системе.

2. Уязвимость существует из-за ошибки проверки границ данных в функции decode_unicode_ssetup() в файле fs/cifs/sess.c. Злоумышленник может обманом заставить пользователя подключиться к специально сформированному серверу и вызвать переполнение буфера.

3. Уязвимость существует из-за того, что CAP_FS_MASK_B0 не содержит CAP_MKNOD, и CAP_FS_SET не содержит CAP_LINUX_IMMUTABLE. Злоумышленник может создать новые узлы устройств.

4. Уязвимость существует из-за ошибки в функции agp_generic_alloc_page() в файле drivers/char/agp/generic.c. Локальный пользователь может получить доступ к потенциально важным данным в памяти ядра.
URL производителя: www.kernel.org.
Решение: Установите последнюю версию 2.6.30-rc3 с сайта производителя.

Раскрытие данных в nss-ldapd

Программа: nss-ldapd версии до 0.6.8.
Опасность: Низкая.
Наличие эксплоита: Нет.
Описание: Уязвимость существует из-за наличия небезопасных привилегий на доступ к файлу /etc/nss-ldapd.conf. Локальный пользователь может получить доступ к паролю, используемому для подключения к LDAP-серверу.
URL производителя: ch.tudelft.nl/~arthur/nss-ldapd.
Решение: Установите последнюю версию 0.6.8 с сайта производителя.

Повышение привилегий в dircmp в Sun Solaris

Программа: Sun Solaris 8, 9, 10.
Опасность: Низкая.
Наличие эксплоита: Нет.
Описание: Уязвимость существует из-за ошибки состояния операции в сценарии dircmp. Локальный пользователь может перезаписать произвольные файлы на системе с привилегиями пользователя, запустившего dircmp.
URL производителя: www.sun.com.
Решение: Установите исправление с сайта производителя.

Множественные уязвимости в Symantec Brightmail Gateway Control Center

Программа: Symantec Brightmail Gateway версии до 8.0.1.
Опасность: Низкая.
Наличие эксплоита: Нет.
Описание: 1. Уязвимость существует из-за недостаточной обработки входных данных Control Center. Удаленный пользователь может с помощью специально сформированного запроса выполнить произвольный код сценария в браузере жертвы в контексте безопасности уязвимого сайта.

2. Уязвимость существует из-за неизвестной ошибки при обработке определенных консольных функций в Control Center. Удаленный пользователь может получить административные привилегии.
URL производителя: www.symantec.com/business/brightmail-gateway.
Решение: Установите последнюю версию 8.0.1 с сайта производителя.

Обход ограничений безопасности в Device Mapper

Программа: multipath-tools 0.4.8, возможно, другие версии.
Опасность: Низкая.
Наличие эксплоита: Нет.
Описание: Уязвимость существует из-за того, что multipathd-демон создает доступные на запись всем сокеты. Локальный пользователь может отправить произвольные команды приложению.
URL производителя: christophe.varoqui.free.fr.
Решение: В настоящее время способов устранения уязвимости не существует.

Составил Александр Антипов

Последние минуты

За окном шелестел совсем не по-весеннему занудный дождик, а в комнате было тепло и уютно. Погода не располагала к «высокому» настроению, да и делать ничего не хотелось. А потому Стас сидел и занимался пустым веб-серфингом. Переходя со страницы на страницу, он попал на livejournal и, бесцельно перескакивая от одного ЖЖ к другому, думал о том, что ведь за каждой страничкой скрывается чья-то жизнь. Радость и тоска, любовь и ненависть, удачи и промахи – маленькие эпизоды жизней, выставленные на всеобщее обозрение. Стас тоже когда-то вел онлайн-дневник, но потом ему надоело, графоманством он не страдал и постепенно забросил это занятие. Он вспомнил тот брошенный блог и подумал, что даже если он вдруг умрет, то еще долго в Сети будет лежать этот маленький отпечаток его жизни. Стас закрыл ЖЖ и переключился в другую вкладку браузера.

Хоть и говорят, что все ссылки рано или поздно приводят на порносайты, Стас был не первый год в Интернете и умело избегал всяческих баннеров-«заманух». От самых назойливых его ограждал фильтр в браузере, а оставшиеся Стас по привычке даже не замечал. Однако этот баннер привлек его внимание, так как надпись на нем оказалась созвучна его мыслям. «Последние минуты». Низкобюджетный баннер – подумал Стас и щелкнул по нему. Даже интернетчики со стажем иногда щелкают по баннерам. Почему они это делают, никто не знает, даже, наверное, они сами. Так сейчас сделал и Стас. И попал на очень простенький сайтик, под стать баннеру – буквально из одной страницы. Оформление было симпатичным, но сайт практически без контента по нынешним временам воспринимался как-то несолидно. Основной текст гласил следующее:

«Вы хотите ощутить конец своей жизни? Узнать, что вы будете чувствовать в свои последние минуты? Заранее пережить эти мгновения? С нами это возможно. Компания «Последние минуты».

Далее следовал телефон, адрес и мелким шрифтом номер лицензии.

Стас улыбнулся. Опять какие-то шарлатаны пытаются сделать деньги на оригинальной идее. Сама по себе такая возможность казалась ему привлекательной, вот только ее реализация немного не укладывалась в голове. Адрес оказался в знакомом районе города, где он изредка бывал, поэтому, поразмышляв над тем, каким образом можно было бы достичь того, о чем говорилось на сайте, Стас в шутку подумал: не заглянуть ли к этим «деятелям» и не удовлетворить ли свое любопытство вживую? Затем он закрыл страницу и снова окунулся в Сеть, выкинув из головы только что прочтенное.

Спустя пару дней Стас шел по улице и настроение его также оставляло желать лучшего. Как говорится, жизнь состоит из черных и белых полос, а в конце – хвост. Сейчас в жизни у него была явно не белая полоска. Но понимание еще не обеспечивает принятие, поэтому Стас был раздражен и немного зол на весь окружающий мир. Ближайшее будущее тоже не давало намека на улучшение положения – на выходные родители вообще хотели забрать Стаса поработать на дачу, а такая перспектива его отнюдь не радовала. Пришлось сказать, что у него срочная работа, которую придется делать в выходные, а Стас очень не любил врать, тем более близким людям. Но сельскохозяйственные работы на даче он не любил еще больше. Зазвонил мобильник – входящий вызов от одной знакомой девушки. Настроения болтать у Стаса не было, однако он все же ответил:

– Привет, Вика.

– Привет, Стас, как дела, как жизнь?

– Так себе…

– Ну это ты зря, не куксись, все будет хорошо! Слушай, Стас, у меня тут компьютер что-то глючит, ты не мог бы приехать и посмотреть как-нибудь на днях?

«Ну вот, – зло подумал Стас, – всем плевать на то, что я чувствую, нужна, видите ли, моя профессиональная помощь! Знакомые всегда вспоминают о компьютерщике, только когда что-то случается с компьютером!»

– Знаешь, Вика, в ближайшую неделю можешь считать, что меня не существует, что я уехал, умер, потому что у меня совершенно не будет времени, чтобы приехать ни к тебе, ни к твоему компьютеру!

– Ну ладно, извини, что побеспокоила, счастливо… – раздался в трубке ошарашенный голос Вики, но Стас нажал кнопку разрыва связи.

«Да, зря я так грубо, тем более с девушкой», – подумал Стас, но потом оправдал себя тем, что в конце концов у них такое бывает с периодичностью раз в месяц, а он тоже человек и имеет право на плохое настроение.

Злясь на себя, на свое настроение, на родителей, дачу и Вику, а также на все вокруг, Стас изучил витрину ближайшей торговой точки. Несмотря на отвратительное настроение, время для пива еще не пришло, поэтому он разжился банкой широко разрекламированного безалкогольного напитка и решил немного прогуляться по улице пешком. Пешие прогулки хоть и по не очень свежему городскому воздуху обычно помогали собрать все мысли в порядок. Неторопливо идя по улице, попивая химическое содержимое из жестяной банки и рас-

сеянно бросая взгляды по сторонам, Стас вдруг увидел знакомое название и остановился. Обычное не очень новое офисное здание, с небольшим палисадником вдоль парадной части дома, обычный вход и только неприметная среди других себе подобных табличка с надписью «компания «Последние минуты» освежила воспоминания о рекламном баннере из Интернета. «Это судьба, – подумал Стас, – вот сейчас я как раз и выясню, в чем у них там подвох!». Он допил остатки жидкости и поискал глазами ближайшую урну, которая оказалась на расстоянии около сотни метров. Это показалось далеко, поэтому пустая банка отправилась прямиком на газон. Такая характерная для жителей больших городов черта – когда знаешь, что твой мусор за тебя уберет кто-то другой, легко привыкаешь к плохим манерам. Поднявшись на третий этаж, Стас оказался перед массивной дверью с такой же неброской, как и у входа, табличкой и, постучавшись, вошел.

Первое, что бросалось в глаза, – это просторная светлая комната и огромное количество аппаратуры. О ее назначении можно было только догадываться. В центре стояло нечто среднее между кушеткой и стоматологическим креслом, а в уютном уголке располагался письменный стол с компьютером, за которым сидел мужчина лет 45 на вид, больше напоминающий ученого, чем офисного сотрудника. При входе Стаса он сразу оторвался от компьютера («Явно не в «линейку» игрался», – подумал Стас) и, поднявшись, пошел на встречу.

– Добрый день, меня зовут Анатолий Петрович, – представился он, протягивая руку.

– Здравствуйте, я Стас, – в свою очередь представился Стас слегка сбитый с толку подобным приемом.

После нескольких формальных фраз и предложения присесть завязалась беседа, в результате которой Стас выяснил, что компания «Последние минуты» использует в своей деятельности разработки российских ученых, работавших на ВПК. Эффект «последних минут» был обнаружен в одном из исследовательских бюро как побочное явление в одном из засекреченных до сих пор экспериментов, в отличие от которых «последним минутам» никакого стратегического значения не придавалось. Интересных открытий накопилось достаточно много за годы деятельности, но ранее они нигде не использовались. Но вот руководство сменилось, настали другие времена, и было принято решение продать несколько таких изобретений, а другие внедрить самостоятельно. Одним из таких внедрений и стали «последние минуты».

– Суть состоит в следующем, – пояснял Анатолий Петрович, – путем раздражения особым образом определенных участков головного мозга создается иллюзия наступления смерти. Она настолько реальна, что не поверить в нее можно только усилием воли. Поэтому главное – сначала расслабиться. Психике кажется, что смерть близка, и вот тогда-то и происходят очень любопытные вещи, названные «последними минутами». Люди думают, что в такие моменты проживаешь заново всю свою жизнь, только в тысячи раз более сжатые сроки. На самом деле у всех это происходит по-разному. Всю визуальную информацию

есть возможность зарегистрировать и в конце мы вам выдадим DVD с записью того, что вы видели. К сожалению, ваши чувства и эмоции мы записать не можем, они останутся только в вашей памяти. Итак, если вы хотите узнать, что вы будете чувствовать в свои последние минуты, то мы можем начать прямо сейчас.

– Анатолий Петрович, а насколько это безопасно?

– Стопроцентную гарантию вам не могут дать, даже когда вырезают аппендицит, но мы провели сотни опытов, и уже более тысячи человек воспользовались нашими услугами и никто из них не умер и не остался покалеченным. Как видите, у нас даже не предусмотрен медицинский персонал на случай осложнений, потому что это совершенно излишне.

– Хм, спасибо вам за разъяснения, звучит правдоподобно. Остается проверить на практике – ну что, давайте попробуем?

Спустя десять-пятнадцать минут, уладив все финансовые вопросы, Стас уже располагался на той самой кушетке, весь опутанный проводами, как рождественская елка, с той только разницей, что лампочки находились не на нем, а на мерно гудевших машинах. Наконец Анатолий Петрович объявил, что все готово, прикрыл жалюзи на окнах и щелкнул несколькими рубильниками. Поначалу Стас непроизвольно напрягся, но потом, вспомнив о разговоре, постарался расслабиться. В течение нескольких минут ничего не происходило, только ощущалось легкое покалывание в тех местах, где контакты были прикреплены к коже. Постепенно начала болеть левая часть головы. Господи! Как же он мог забыть! В прошлом году врачи поставили ему диагноз: подозрение на аневризму головного мозга. Нужно было ложиться в больницу и проводить ряд серьезных анализов, чтобы подтвердить или опровергнуть это. Тогда Стас сдавал сессию, а после головная боль уже перестала его мучить, и он все откладывал и откладывал свое посещение больницы. И вот теперь, когда боль из легкой и пульсирующей превратилась в постоянную и острую, Стас понял, что совершил ошибку, не сказав об этом Анатолию Петровичу. Он попытался что-то сказать, но вместо этого услышал лишь сдавленный хрип. Тело его совершенно не слушалось. Стас испугался и попытался крикнуть, но стоило ему только напрячься, как жгучая боль взорвалась у него в голове, свет померк перед глазами и он провалился в темноту...

...Стас в очередной раз ехал на междугороднем автобусе, возвращаясь после выходных, проведенных дома, в университет. Сразу за дорожной развилкой стоял щит с социальной рекламой, на котором большими буквами написано всего лишь два слова: «Живите долго». Он много раз, проезжая мимо, видел этот щит, но почему-то именно сейчас что-то было не так. Это пожелание звучало как издевательство! Но почему? Наконец Стас понял: потому что он умирает! Однажды сформировавшись в мозгу, эта мысль уже не покидала его: он умирает, умирает в результате глупого эксперимента и собственного любопытства.

Автобус и дорога исчезли, Стас стоял лицом к стене на расстоянии нескольких десятков шагов от нее. Вокруг была мрачная пустынная местность, а по небу быстро двигались низкие свинцовые тучи. Стена казалась бесконечной – влево и вправо, насколько хватало глаз, она простиралась до самого горизонта. Странная стена из LCD-панелей, причем панели были трех видов – одни светились ярко белым светом, другие напротив, были черны как сажа, а третьи были невзрачные и серые. Стас сделал несколько шагов вперед, и стена ожила. Присмотревшись, Стас на каждом экране начал различать какое-то движение. Он подошел еще ближе и оторопел – стена оказалась выложенной из фрагментов его жизни! Некоторые Стас угадывал, другие смутно припоминал, а третьи не помнил совсем. Стена не была сплошной – тут и там зияли пустоты, причем пустот было достаточно много. Это смущало – наверняка он чего-то еще не сделал в своей жизни. Не пришел к цели, не выполнил предначертанной ему миссии, и эти пустоты свидетельствуют об этом. И еще была одна закономерность – светлые панели содержали в себе его добрые дела, в то время как на черных всплывали не самые приятные и правильные моменты его жизни. Стас сначала медленно шел вдоль стены, потом шаг его стал все быстрее и быстрее пока уже не перешел в бег. И тут он обнаружил, что бежит по кругу, что стена окружила его и он оказался в колодце собственной жизни. Даже не в колодце, а в трубе, потому что Стас уже не стоял, а висел в пространстве. Небо над его головой просветлело и засияло чистым белым светом. Стенки трубы зашевелились и начали вспархивать легкими бабочками. Серые бабочки куда-то исчезали, а черные и белые стремились к Стасу. Белые садились ему на руки, на плечи, на голову – от этого он чувствовал невообразимую легкость и стремился вверх, к сияющему свету. Но черные бабочки нагоняли его и облепляли ноги, отчего он тяжелел, и движение вверх замедлялось. Наконец оно прекратилось вообще, а затем, замерев на миг, Стас стал соскальзывать вниз. Белые бабочки уже не могли противостоять грузу, и враз взметнувшись с тела Стаса, унеслись вверх, в то время как Стас стремительно понесся в непроглядную черноту, не сомневаясь, что там его ждет ад. Этого не должно было быть – ведь это был только эксперимент, он не хотел умирать вот так, он еще многого не сделал в своей жизни, это неправильно! От отчаяния Стас закричал и, сделав последний рывок вверх, к тускнеющему уже свету, не свалился с кресла только благодаря тому, что его вовремя поддержал Анатолий Петрович.

– С возвращением, – сказал тот и широко улыбнулся. Затем он снял со Стаса провода и датчики и помог встать.

– Вот обещанный DVD. Здесь все, что вы видели за эти 7 последних минут.

Анатолий Петрович помогал переживать последние минуты сотням людей. У всех это происходило по-разному, но яркий свет присутствовал везде, и никто его не достиг. Возможно, действительно у каждого человека есть миссия в жизни, не выполнив которой ему не попасть к этому свету? Вопрос, на который не дают точного ответа даже последние минуты, но его получит каждый, когда расстаться с жизнью придется по-настоящему. Вот только рассказать про это хоть кому-то будет уже невозможно.

Стас вышел из здания, рассеянно вертя диск в руках. Посмотрел на голубое весеннее небо с белыми облаками и улыбнулся. Потом достал мобильник.

– Алло, Вика, привет еще раз. Знаешь, ты извини меня, что так с тобой говорил в прошлый раз, и если тебе еще нужна помощь, я с радостью приеду повозиться с твоим компом и повидать тебя, ведь мы с тобой не встречались уже несколько месяцев!

– Ой, Стас, как здорово, что ты передумал! Ты так быстро в прошлый раз бросил трубку, что я не успела тебе сказать, что собираюсь открыть сезон катания на велосипеде и хотела тебе предложить составить мне компанию. В прошлом году мы иногда катались вместе, а уже весна!

– О, хорошая идея, спасибо, я тоже буду рад начать велосезон с совместной покатушки с приятным человеком, – ввернул небольшой комплимент Стас.

– Ну тогда договорились, до связи!

– До связи, Вика!

На душе у Стаса немного потеплело. Все-таки о компьютерщиках вспоминают не только тогда, когда ломаются компьютеры, но и иногда для того, чтобы вместе провести время. Следующий звонок Стас сделал родителям и сказал, что сумел справиться со срочной работой, а значит, в выходные сможет поехать на дачу. Мама, с которой Стас разговаривал, очень обрадовалась, и от этого ему стало еще теплее. А может быть, это весеннее солнышко, выглянувшее из-за облаков? Не важно. Главное, что жизнь все-таки весьма приятная штука! Стас спустился по ступенькам и направился к остановке, потом вернулся, подобрал с газона выброшенную им ранее банку и побежал к подходящему автобусу. На автобус он успел. Даже успел выбросить в урну банку и заодно и DVD-диск с записью его последних минут. Он был уверен, что и без диска будет помнить эти семь минут всю свою оставшуюся жизнь!

Стас в очередной раз ехал на междугороднем автобусе, возвращаясь после выходных, проведенных дома, в университет. Сразу за дорожной развилкой стоял щит с социальной рекламой, на котором большими буквами написано всего лишь два слова: «Живите долго». Вокруг было мрачно, а по небу быстро двигались низкие свинцовые тучи. Вдруг пейзаж резко покрылся туманом – это стекло запотело от дыхания Стаса, когда он непроизвольно приблизил голову к окну. Прошло уже полгода с момента его «последних минут», но всегда, проезжая этот рекламный щит, Стас старался не пропустить его. Многое изменилось в его жизни за это время, и ему бы очень хотелось верить, что он стал хоть чуточку, но лучше. И самое главное – Стас обнаружил, что это не только не сложно, а даже приятно – делать что-то хорошее этом мире. И еще он чувствовал, что вместе с ним в лучшую сторону меняется и окружающий мир. Стас улыбнулся… «Живите долго» – ну что ж, поживем долго! Вот чего он теперь не боялся в жизни – так это его будущих последних минут.

Станислав Шпак

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**.

ИЗВЕЩЕНИЕ

ООО "С 13" Форма № ПД-4
ИНН 7708654814 / КПП 770801001
Р. сч. 40702810300080001868 К. сч. 30101810100000000787
ОАО «УРАЛСИБ» г. Москва БИК 044525787
Коды: по ОКПО 84027582, по ОКОПФ 65

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	X	X	X	X	X	X

Дата _____ Сумма платежа: 2400 руб. 00 коп.

Информация о плательщике:

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

_____

_____

Кассир

Подпись _____

КВИТАНЦИЯ

ООО "С 13" Форма № ПД-4
ИНН 7708654814 / КПП 770801001
Р. сч. 40702810300080001868 К. сч. 30101810100000000787
ОАО «УРАЛСИБ» г. Москва БИК 044525787
Коды: по ОКПО 84027582, по ОКОПФ 65

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	X	X	X	X	X	X

Дата _____ Сумма платежа: 2400 руб. 00 коп.

Информация о плательщике:

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

_____

_____

Подпись _____

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-Прессервис**»
  Агентство «**ООО Урал-Пресс**» (343) 375-62-74
  ЛинуксЦентр 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 Давида, 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**» (MD-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 _____ (индекс издания)

Системный администратор

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	литер

на журнал _____ (индекс издания)

Системный администратор

Стоимость: по каталогу _____ руб. _____ коп.; за доставку _____ руб. _____ коп.

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)

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

СИСТЕМНЫЙ АДМИНИСТРАТОР
№5(78), Май, 2009 год

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
Вадим Поданс
Андрей Бирюков
Олег Щербаков
Андрей Луконькин
Андрей Уваров

РЕКЛАМНАЯ СЛУЖБА
тел./факс: (495) 628-8253 (доб. 120)
Дарья Зуморина
reclama@samag.ru
Евгения Тарабрина
expo@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

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.).

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 которым 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 погоне 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 ощутить всю прелесть аутсорсинга... но без всей словесной мишуры, типа, «утром стулья, вечером деньги...»!

Приобретайте игру «АУТСОРСЕР» в редакции.