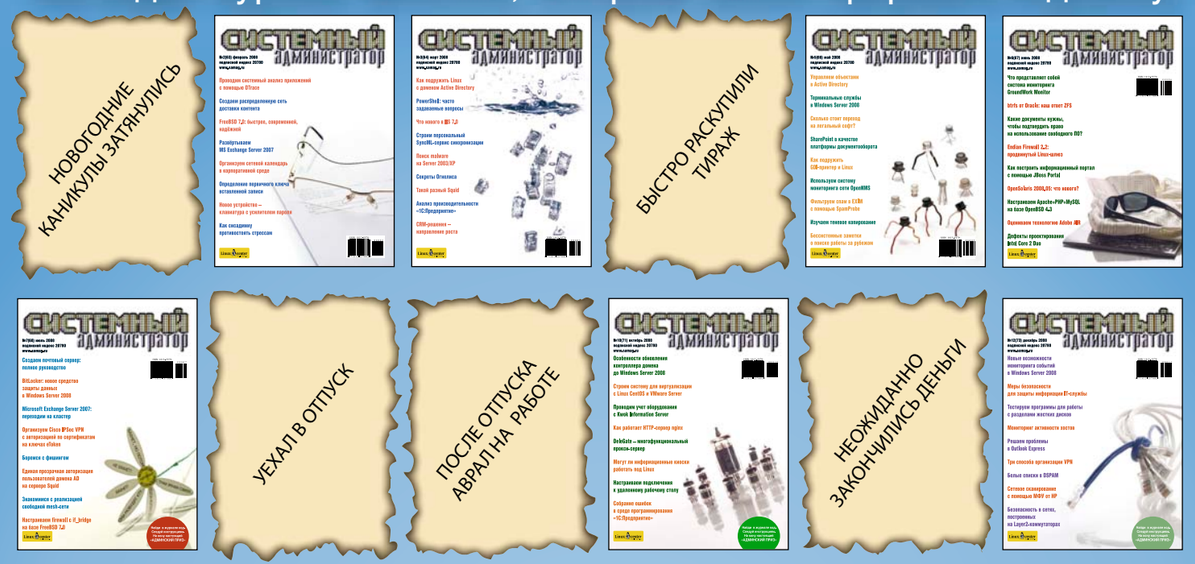
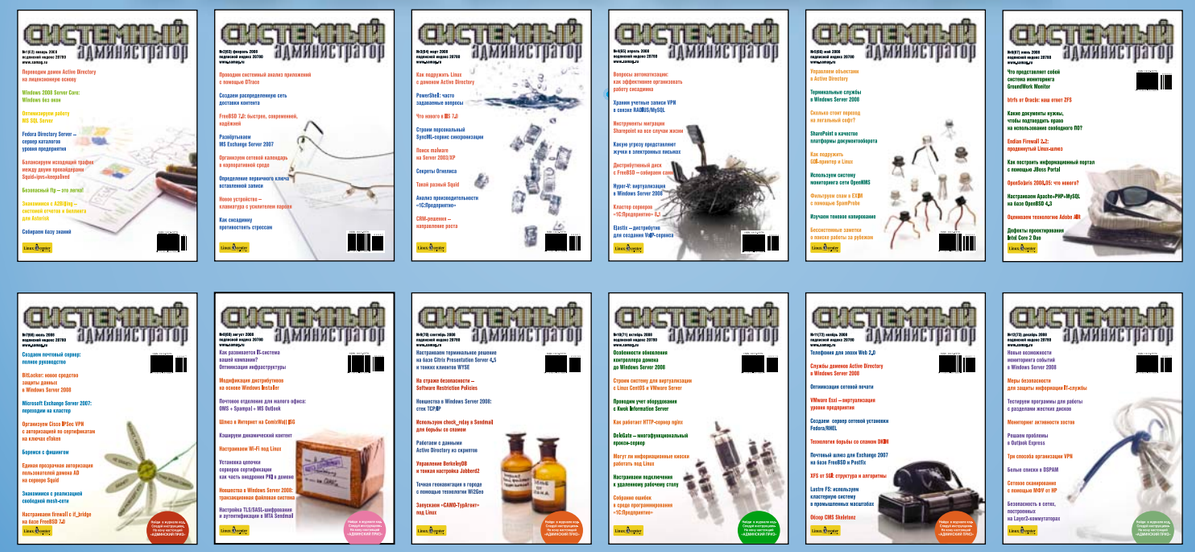
Так видит журнал читатель, который забыл оформить подписку:



Так видит журнал читатель, оформивший подписку:



ПОДПИШИТЕСЬ И ЧИТАЙТЕ!

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

Dr.WEB®
CureNet!

Пополнение библиотеки Dr.WEB

Dr.Web CureNet! — специальный выпуск

Удаленное централизованное лечение рабочих станций и серверов Windows, с установленным антивирусом другого производителя, в локальных сетях любого масштаба

http://www.products.drweb.com/curenet/

№8(81) август 2009 Системный администратор

Системный администратор

ежемесячный журнал www.samag.ru

№8(81) август 2009

Сисадмин должен быть ленив. DHCP и динамический DNS

Cisco IDS/IPS: безопасная настройка

Управление корзиной — новый сервис в Active Directory

Расчет на салфетке: как продать ИТ-проект с помощью математики

CrossBow: сетевые технологии OpenSolaris

Свои среди чужих, чужие среди своих

Строим сеть с помощью Calculate Directory Server

Стив Джобс — гений креатива!

ISSN 1813-5579

Linux Center www.linuxcenter.ru

Гений или злодей?

Дискуссию о хакерах, которую вы прочтете в этом номере, каждый будет трактовать по-своему. Кому-то захочется узнать, какие должны быть приняты законы, чтобы защититься от взлома компьютеров? Какие способы или технические новинки обезопасят тебя или твою компанию от воровства или просто «чужого глаза»? Ведь мало кому нравится, когда подсматривают за ним через замочную скважину. В конце концов, хотелось бы понять, сколько должна стоить работа специалиста – антихакера, который зачастую спасает не только миллионную прибыль компании, но и ее репутацию.

Должна разочаровать всех, кто ищет ответы на эти вопросы – в нашей дискуссии их пока нет. Мы просим вас найти их и написать в редакцию. Будьте уверены: для дельных предложений и ценных мыслей всегда найдется место на страницах журнала.

Нынешняя дискуссия скорее о другом – о Добре и Зле. Признаться, меня удивило количество сисадминов, оправдывающих хакерство. Да, нужно отдать должное героям (или антигероям?) «Острого угла». Они умны, талантливы, любознательны и амбициозны. Но каково применение их бесспорных достоинств? Каждый день приносит нам новости о хакерских преступлениях. Я назову лишь одну из последних.

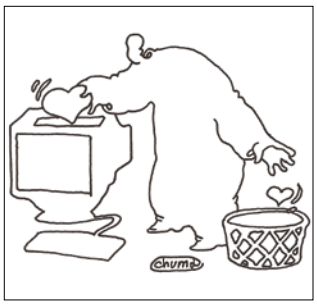
По сообщению китайских властей, экономический ущерб от действий хакеров в этой стране в прошлом году составил более миллиарда долларов! В онлайн-школах и на курсах за небольшую плату желающих учат взламывать компьютеры, воровать персональные данные и деньги с чужих электронных счетов. Общий доход организаторов такого обучения в прошлом году достиг 34,8 млн долларов. Китайские юристы считают, что хакерские школы нужно закрыть, а их руководителей предать суду. Зная жесткость китайских законов, можно не сомневаться, что горе-организаторы будут рады остаться хотя бы в живых.

Примеров, прославляющих хакерские деяния, гораздо меньше. Почему? Косвенный ответ для себя я нахожу в судьбах двух знаменитых пиратов виртуального мира, которые выступили на страницах нашего журнала – Криса Касперского и Кевина Митника. Прошли годы и они стали антихакерами! Полагаю, не потому что постарели – просто поумнели. И теперь свой талант, знания и опыт обратили на благо общества.

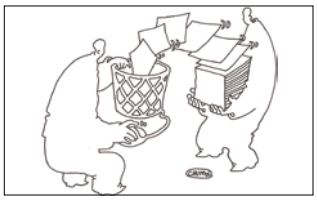
«Гений и злодейство – две вещи несовместные». Эту великую фразу Александр Пушкин когда-то сказал совсем по другому поводу. Он вложил ее в уста Моцарта, простодушно доверившегося своему заклятому другу Сальери. «Ты думаешь?» – ответил ему Сальери. А далее следует авторская ремарка: «И бросил яд в стакан Моцарта». Во всемирной истории Сальери, кстати, неплохой композитор, остался лишь как потенциальный отравитель гения. А прекрасную музыку Моцарта мы можем слушать каждый день.

Галина Положевец,
главный редактор

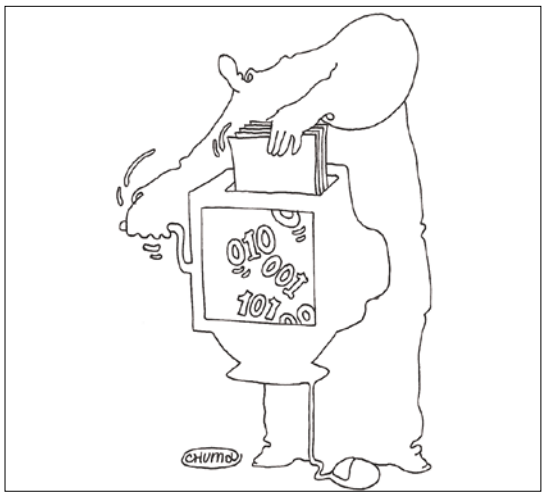
26



32



46



56

Визитка

ДМИТРИЙ ШУРУПОВ,
ведущий рубрики

Закончено тестирование версии Release Candidate Windows 7

17 июля в офисе Microsoft в Москве на Крылатских Холмах прошел пресс-семинар Windows Club, посвященный окончанию тестирования версии Release Candidate Windows 7. Президент Microsoft в России Николай Прянишников поделился планами компании касательно Windows 7. Они оказались довольно оптимистичными, до конца 2010 года Microsoft планирует продать 177 миллионов копий Windows 7. Представители Microsoft открыли список компаний, участвующих в тестовом внедрении Windows 7. Ими оказались оператор связи «Синтерра», лизинговая компания «Европлан», «Московская объединенная энергетическая компания» и другие.

Поскольку еще до выхода Windows 7 успела обрасти изрядным количеством слухов, целый ряд вопросов присутствовавших был направлен на их подтверждение или опровержение. Сейчас можно точно сказать, что продажи ОС Windows 7 на USB-носителях не будет, данная возможность была полностью отвергнута. Также был дан отрицательный ответ о включении SP1 в RTM-версию продукта. По планам выход пакета обновлений возможен не ранее чем через год после поступления продукта в продажу. Будущая операционная система должна стать самой «русской» за всю историю Microsoft, работа по локализации действительно впечатляет. Даже такой необязательный компонент, как название версии ОС, был переведен. Поскольку версия Windows 7 «Начальная» (в англ. Starter) планируется как основная для предустановки на бюджетные субноутбуки, ограничение на запуск трех приложений было убрано.

Для компаний, не имеющих Software assurance, Windows 7 будет доступна с 1 сентября по каналам корпоративного лицензирования. В скором времени станет понятно, сможет ли Windows 7, несмотря на мировой экономический спад, продолжить победное шествие и возглавить список коммерчески успешных продуктов Microsoft. EOF

Илья Рудь

Управляемые услуги – дело ближайшего будущего

На сегодняшний день ИТ – это одна из существенных статей расходов для крупных компаний. В условиях кризиса от ИТ-отделов, с одной стороны, требуют поддержку существующей инфраструктуры, автоматизации бизнеса, удобства и безопасности, но при этом сокращают бюджет и сотрудников. В качестве решения проблем ИТ для крупных компаний Cisco Systems предлагает новую услугу – Managed Services. Её смысл заключается в том, что заказчик получает все услуги по обслуживанию своей ИТ-инфраструктуры (сервисы VPN, IP-телефония, Wi-Fi, WAN и т.д.) «из одних рук». Например, если компания имеет несколько представительств в различных регионах, причем в каждом используется оборудование от разных производителей и услуги связи предоставляются местными провайдерами. Раньше для обслуживания такой ИТ-инфраструктуры заказчику требовалось содержать целый штат специалистов, отвечающих за работу ИТ в каждом из представительств. Теперь же компании-заказчику достаточно будет воспользоваться услугой Managed Service, и вся «головная боль», связанная с обслуживанием распределенной ИТ-инфраструктуры, ляжет на плечи компании, предоставляющей данную услугу. Тем самым компания-заказчик сможет сэкономить до 30% ИТ-бюджета на обслуживание ИТ-инфраструктуры. EOF

Андрей Бирюков

Canonical объявила об услугах поддержки Ubuntu на десктопах

31 июля компания Canonical, являющаяся «коммерческим крылом» Linux-дистрибутива Ubuntu, анонсировала свои услуги по обеспечению платной технической поддержки по Ubuntu Desktop Edition. Задача Desktop Support Services заключается в том, чтобы за небольшие деньги помочь пользователям в небольших инсталляциях Ubuntu на настольных компьютерах. Услуги по технической поддержке разделены на три уровня: базовый (Starter), продвинутый (Advanced) и профессиональный (Professional). Первый подразумевает помощь по установке, настройке и обучению базовым навыкам, а его стоимость составляет 54,99 $ в год. Во втором обеспечивается помощь и по таким возможностям, как перенос файлов и настроек из другой операционной системы, ведение личной бухгалтерии, а стоимость составляет 114,9 $ в год. Самый высокий уровень поддержки, который обойдется в 218,4 $ в год, подразумевает обслуживание бизнес-пользователя, работающего с Ubuntu Linux как своей основной средой. В нем предполагается помощь по подключению к корпоративной сети, интеграции десктопа с ИТ-инфраструктурой, настройке виртуализации. EOF

Microsoft опубликовала GPL-код для включения в Linux-ядро

Корпорация Microsoft во время мероприятия O'Reilly Open Source Convention, проходившего 20 июля в Сан-Хосе (США), объявила о публикации 20 тысяч строк кода под лицензией GNU GPLv2 для их включения в состав Linux-ядра. Написанный в Microsoft код предназначен для того, чтобы улучшить в Linux-ядре производительность при использовании Linux-систем в среде виртуализации серверов, работающих под управлением Windows Server 2008 Hyper-V (или 2008 R2 Hyper-V). Впрочем, через несколько дней стало известно, что код Microsoft не был принят в состав Linux-ядра, поскольку в нем нарушена лицензия GPL. Как сообщил Стивен Хеммингер (Stephen Hemminger), инженер из Vyatta и один из разработчиков Linux-ядра, некоторые компоненты статически слинкованы с закрытыми бинарными файлами, что недопустимо при использовании GPL. EOF

Участвуй сам и расскажи друзьям! Как получить Админский приз?

Редакция «СА» продолжает разыгрывать Админский приз, и приглашает к участию новых игроков. Вам необходимо зарегистрироваться на сайте www.samag.ru и активировать код, который можно получить, купив номера журнала (№№7-12, 2009). Чем больше у вас заветных кодов, тем выше шансы стать победителем розыгрыша. Дополнительные коды смогут получить самые активные участники форума на сайте www.samag.ru.

Успехов и удачи!

Админский Приз

Розыгрыш будет проходить в три этапа:

I – участвуют коды из журналов №7, 8, 9, полученные с июля по август 2009 г.

II – участвуют коды из журналов №10, 11, 12, полученные с октября по декабрь 2009 г.

III – участвуют коды из всех шести номеров журнала за 2-е полугодие 2009 г.

Админский Приз

Админский Приз

Призы:

I этап:
1 место — приз-сюрприз
2 место — учебные курсы
3 место — пакет программного обеспечения
4 место — почтовый сервер на 50 пользователей
5 место — виртуальные выделенные серверы

II этап:
1 место — приз-сюрприз
2 место — учебные курсы
3 место — пакет программного обеспечения
4 место — почтовый сервер на 50 пользователей
5 место — виртуальные выделенные серверы

III этап:
1 место — приз-сюрприз
2 место — учебные курсы
3 место — пакет программного обеспечения
4 место — почтовый сервер на 50 пользователей
5 место — виртуальные выделенные серверы

Специальный утешительный приз — электронная книга

Ваш код для участия
в розыгрыше призов:

Системный администратор

A-SYS.RU

RUSONYX
Скорость. Надежность. Поддержка.

ideco

allsoft.ru®
группа компаний Softline

KERIO

Админский Приз

Слет сисадминов
И вновь продолжается бой!

Вот под такие слова из старой комсомольской песни просыпались по утрам участники IV Всероссийского слета системных администраторов. А что, разве вся наша жизнь – не борьба, а дело сисадминов – не постоянный бой со всеми, кто покушается на Сеть? Палаточный городок, традиционно разбитый на Поляне Слетов на берегу реки Вырка, около деревни Колюпаново, что под Калугой, едва вместил в этот раз четыре тысячи человек, приехавших на самое лучшее ИТ-мероприятие лета-2009.

Встреча, которую ждали целый год, не обманула ожиданий. День сисадмина встретили достойно. Чемпионаты по футболу и волейболу, разнообразные конкурсы – метание компьютерных мышей на точность, на лучшее чучело ламера, посвящение в рыцари-Софтлайнеры, алкогольная рыбалка, антиспам с метлами – всего не перечислишь и не перескажешь. А еще встречи с читателями «СА» и особенно с прекрасными читательницами. Здорово, что девушек среди сисадминов становится все больше.

Стоит ли говорить, что три дня, с 31 июля по 2 августа, пролетели как один миг, как прекрасный сон, который хочется запомнить, чтобы он вдохновлял и согревал до следующего года – до нового слета!

Владимир Лукин, Владимир Положевец,
спецкорры «СА», Калуга-Москва

Борьба за ресурсы. Дрова привезли!

Лагерь сисадминов растет год от года

Мария, г. Москва. Сисадминами могут быть не только мужчины

Оксана, г. Шатура. Сисадмин, будь готов!

Юлия, г. Москва. Лучший друг девушек – «Системный администратор»

Катерина, г. Москва. Походный набор сисадмина – пиво, документация и, конечно, журнал «СА»

Ольга, г. Рязань. Непослушные юзеры, берегитесь!

Мария, г. Калуга. Будущий системный администратор

Админские игрища в Нижнем Новгороде

В этом году нижегородские айтишники решили отметить свой профессиональный праздник, с выездом на природу и культурной программой.

Подготовка началась задолго до дня «X», был создан информационный сайт http://dsann.ru с форумом для общения и обсуждения. После мозгового штурма инициативная группа разработала трехдневную программу праздника. Решили проводить мероприятие на природе, на берегу реки в поселке Рекшино в 14 км от Нижнего Новгорода.

В пятницу, 31 июля, начался заезд участников. Оборудовали место стоянки, поставили палатки, заготовили дрова, а вечером – вкуснейший шашлык!

В субботу гости стали прибывать с самого утра, кто на машинах, кто на электричке, а кто-то и на велосипедах, благо от города совсем близко. Оказалось, что далеко не все работают системными администраторами. Начальники, программисты, и просто люди, близкие по духу, общались непринужденно и весело.

Кроме солнца, реки, леса, костра и разговоров, были также и тематические конкурсы, повторять которые в рабочей обстановке крайне не рекомендуется.

В воскресенье админские игрища продолжились, у кого-то нашлась гитара, поэтому песни стали петь под аккомпанемент. И неизвестно, сколько бы еще продолжался этот праздник жизни, если бы не чувство долга – в понедельник снова работа.

Прошло всего несколько лет, и ДСА из баров и кафе выбрался на зеленые лесные поляны, способные вместить столько народу, сколько изъявит желание поехать. Свободных мест под палатки еще много, поэтому с интересом будем ждать следующего года.

Андрей Луконькин

Админские байки на природе

Визитка

АЛЕКСЕЙ РЕМИЗОВ, кандидат физ.-мат. наук, доцент, член-корреспондент РАЕН. Преподавал в Высшей школе КГБ. Занимал руководящие позиции в ОАО «Радиофизика», НТЦ «КАМИ». С 1997 года – председатель совета директоров компании «Ай-Теко». Входит в число 25 лучших управляющих российских ИТ-компаний

Сисадмины и хакеры:
свои среди чужих, чужие среди своих *

Не все и не всегда хотят ходить строем и в ногу. А в чем, собственно, проблема? Можно ведь и для достижения общих целей идти не в ногу, но рядом, в одном направлении

От сисадмина до хакера – дистанция огромного размера

Как я отношусь к хакерам? Ответ очень простой и краткий: я к ним не отношусь. Поэтому полноценная полемика на эту тему вряд ли получится, не поднявшись до уровня абстрактной высоты, по словам сатирика Михаила Жванецкого, который в свое время призывал спорить о вкусе устриц и кокосовых орехов с теми, кто их ел…

Да, меня позабавила интернет-комедия «Хоттабыч» о хакере Гене. Но фильм понравился в большей степени из-за игры исполнителя роли Хоттабыча Владимира Толоконникова, который был столь же органичен в образе джинна-хакера, как за 20 лет до этого блистателен в роли Шарикова в «Собачьем сердце». Признаюсь, я с превеликим удовольствием погружался в глубину Диптауна вместе с дайвером Леонидом. К слову, виртуальная трилогия С. Лукьяненко «Лабиринт отражений» – одна из любимейших моих вещей: этот роман, а также «Фальшивые зеркала» и «Призрачные витражи» я перечитал не один раз.

Между тем я не склонен слишком романтизировать, идеализировать и поэтизировать образ хакеров и не стал бы делать их героями нашего времени. Ведь в конце 1990-х, когда Крис Касперски (кстати, является одним из авторов «СА») выпустил свою первую книжку «Техника и философия хакерских атак» – этакий путеводитель-самоучитель для начинающих кракеров, мой ученик Женя Касперский, которым у меня есть все основания гордиться, уже активно отбивал эти атаки. (При этом с хакерством Е. Касперский сталкивался не только в жизни, но и на экране: если помните, в 2007-м был снят сериал о российских хакерах «Сеть», где Евгений дебютировал в качестве актера.) Развивая антивирусный проект AVP – сегодня известный как «Антивирус Касперского» – сначала в НТЦ «КАМИ», а потом и в собственной «Лаборатории Касперского», Евгений стал одним из ведущих мировых специалистов в области защиты от вирусов, да и от всей совокупности угроз информационной безопасности, настоящим человеком-легендой – знаменитым Kaspersky Anti-Hacker, Anti-Virus, Anti-Spam. А компьютерный самоучка Крис за эти два десятилетия превратился в злого гения хакинга. И кто из этих двух Касперов стал в итоге лауреатом Государственной премии? Кто из однофамильцев получил большую известность и заслуженное признание на высшем уровне? За кем будущее?

Я принципиально на стороне тех сисадминов, которые не поддаются соблазнам и сознательно – ни из природного любопытства, озорства или азарта, ни для профессионального самоутверждения и самовыражения продвинутого пользователя, ни в знак субкультурного протеста, ни в качестве партизанской виртуальной вылазки – не делают ни одного шага по пути превращения в хакеры. Для которых понятия «Хакинг, крэкинг и фрикинг» (именно так называлась книга А.Петровского, позиционируемая как первая российская энциклопедия по искусству взломов) хоть и понятны по сути, но применимы в реальной жизни не больше и не чаще, чем волшебные слова «Крэкс, фэкс, пэкс!». Если помните, именно их практиковали при выращивании денежных деревьев из золотых монет на Поле чудес в Стране дураков…

В моем понимании, от сисадмина до хакера должен быть не один шаг, а дистанция огромного размера, а еще лучше – непреодолимая пропасть. Я очень уважаю представителей этой нужной профессии, крайне востребованной и интересной специальности, и желаю сисадминам по возможности оставаться своими среди чужих и чужими среди своих, если речь заходит о принадлежности к хакерской братии.

Не все сисадмины одинаково полезны…

Как и руководители любой компании, мы, естественно, заинтересованы

* **В №7 «СА» в статье Андрея Погодина «Цари природы, энергобатарейки или биокомпьютеры?» было положено начало дискуссии на тему «От сисадмина до хакера – один шаг». Мы публикуем первые отклики и приглашаем читателей присоединиться к обсуждению темы.**

в том, чтобы система информационной безопасности предприятия была непробиваема, в идеале – неуязвима для киберугроз, максимально защищена от влияния инцидентов и атак на системы ИБ.

Наши эксперты по информационной безопасности при создании и внедрении таких систем противодействия киберугрозам классифицируют их по типам, для каждого из которых предусматриваются свои методы противодействия. Примечательно, что в числе основных категорий угроз фигурируют не только террористы, природные и техногенные катастрофы, вредоносное программное обеспечение, но и хакеры, и даже… системные администраторы. Как это возможно? Хакеры в этом случае рассматриваются как аутсайдеры, которые могут быть заинтересованы в исследовании возможности получения доступа и контроля над системой, в мониторинге трафика и реализации атак на отказ в обслуживании. А администраторы и инженеры, обслуживающие систему и хорошо знающие ее изнутри, могут либо, будучи инсайдерами (недовольными внутренними пользователями), умышленно повредить оборудование или программное обеспечение, либо нанести вред функционированию системы непреднамеренно, допустив ошибку в ее настройках или нарушив определенные правила безопасности.

Вообще именно персонал считается самым слабым звеном в деле обеспечения информационной безопасности, и более 90% ущерба от инцидентов ИБ возникает из-за неумышленных критичных ошибок сотрудников, ответственных за работу информационных систем. Поэтому среди первостепенных задач менеджмента нам видится не только создание на предприятии мощной системы экономической и информационной безопасности и рациональной организации деятельности по ее обеспечению, включая тщательный отбор ИТ-специалистов, периодическое наблюдение и контроль, но и создание продуманной схемы мотивации и стимулирования сотрудников, выработка эффективной и адекватной системы развития и оценки персонала.

Ведь первоклассные ИТ-специалисты не настолько зависят от работы именно в этой организации (айтишники изначально отличаются не самой высокой приверженностью и привязанностью к конкретному работодателю), насколько результат работы и успех всей компании зависит от них. И не случайно сентенция «People make a difference» (по смыслу: всё дело в людях) прописана в миссии на корпоративном сайте практически каждой второй фирмы. Большинство руководителей достаточно высокого мнения о собственных сотрудниках, понимают исключительную ценность интеллектуального капитала, коллективного опыта и знаний предприятия и заботятся о развитии потенциала подчиненных, по крайней мере, на словах. Поэтому речь должна идти о создании таких условий труда для ИТ-специалистов для их удержания и повышения лояльности работодателю (в том числе через перманентное повышение квалификации, инвестиции в обучение, поощрение самообразования), которые бы не только сводили к минимуму действие пресловутого человеческого фактора, но и лишали высококлассных профи – сисадминов в том числе – искушения и надобности смотреть на сторону обиженными глазами инсайдера…

Чтобы программисты чувствовали себя в компании уверенно, комфортно и спокойно, как у Христа за пазухой, но при этом камень за пазухой до лучших (вернее, худших) времен не держали. И чтобы в итоге не сделали тот самый роковой шаг по направлению к виртуальному стану хакеров.

…Но все хакеры одинаково вредны

Я, наверное, смогу при желании и необходимости понять психологию хакеров, но мне не близка их философия. Конечно, не все и не всегда хотят ходить строем и в ногу. «Кто там шагает правой?» Ну, допустим, я, он, она… А в чем, собственно, проблема? Можно ведь и для достижения общих целей (когда и сотрудникам хорошо, и социуму польза, и компании выгода) идти не в ногу, но рядом, вместе, в одном направлении.

И если попробовать нарисовать словесные портреты правильного сисадмина (качественно образованного, грамотного программиста, серьезного специалиста, не бегущего от рутины дел) и типичного хакера (безусловно,

способного и креативного, но крайне недоверчивого и подозрительного, не признающего авторитетов и монотонной работы), то образ первого – в моем восприятии, по крайней мере, получится более привлекательным, интересным и цельным. А вред от деяний хакеров лишает их в глазах любого здравомыслящего человека последних симпатий, ореола таинственности, оригинальности и избранности.

Для иллюстрации достаточно привести несколько подобранных экспертами по ИБ компании «Ай-Теко» характерных примеров инцидентов с серьезными последствиями для государства, организаций и граждан.

В США ежегодно регистрируется более 200 успешных кибератак на промышленные системы, электростанции, системы управления гражданскими авиаперевозками, ядерные объекты, очистные сооружения и т.д. В результате атаки целевая автоматизированная система попадает в полное или частичное управление злоумышленниками, утрачивая функциональность или управляемость персоналом.

За период с октября 2008 по март 2009 года Пентагон потратил более 100 млн долларов на устранение последствий различных кибератак на свои сети и усиление их безопасности.

В апреле 2009 года стало известно о хищении нескольких терабайт данных о разрабатываемом в США многоцелевом истребителе-бомбардировщике пятого поколения F-35 Lightning II (стоимость проекта оценивается в 300 млрд долларов). Предполагается, что данные были похищены с серверов компаний-подрядчиков.

Согласно статистике командования обороной и безопасностью Южной Кореи военные ежедневно сталкиваются в среднем с 10,5 тыс. попыток взлома и 81,7 тыс. компьютерных инфекций. По сравнению с 2008 годом число этих атак выросло на 20%. Представитель командования сообщил, что большая часть атак проводится обычными людьми, однако в каждом десятом случае атаки серьезны и ставят своей целью взлом военных серверов и сбор разведданных.

От вредоносных атак страдают не только государства и организации, но и обычные граждане. В каждом из многочисленных инцидентов, связанных с похищением частных данных, данных финансовых счетов, удалением и искажением персональной информации, число пострадавших исчисляется десятками тысяч. При этом в большинстве случаев умышленных атак или хакерской активности организаторов найти не удается из-за низких возможностей контроля государства и правоохранительных органов за деятельностью граждан и организаций в Интернете.

Без объявления войны

Ведущие государства мира признают важность информационного пространства для различных видов своей деятельности и принимают меры для сокращения возможных инцидентов безопасности или несанкционированной политической и военно-подрывной деятельности. Так, США и НАТО с 1970-х годов владеют разведывательной сетью «Эшелон», которая представляет собой транснациональную сеть электронных подслушивающих станций для перехвата – до 90% передаваемых во всем мире – переговоров по спутниковым телефонам, телексов, электронной почты, факсов, интернет- и радиосообщений.

В мае 2008 года в Таллинне состоялось официальное открытие Центра киберзащиты Cooperative Cyber Defense Center of Excellence (CCDCOE), который призван помочь НАТО в решении технических, юридических и политических вопросов, связанных с ведением электронных войн.

В августе 2008 года в Санкт-Петербурге продолжилась реализация совместной программы РосНИИРОС и Координационного центра домена RU по развертыванию сети узлов DNS-серверов домена RU, основная причина создания которых – повышение надежности, доступности и отказоустойчивости DNS-серверов в российских регионах и за рубежом.

В июне 2009 года министр обороны США Роберт Гейтс подписал указ о создании в Пентагоне Кибернетического командования (Cyber Command) для защиты военных компьютерных систем и операций США в киберпространстве. В открытых источниках утверждается, что задачами нового командования будут все аспекты кибервойны: как отражение ударов по национальным объектам, так и нанесение кибердударов противнику.

***

Так что необъявленная кибервойна уже довольно активно ведется. И хочется верить, что победит все-таки здравый смысл. Вернемся к метафоре с ящиком Пандоры, о котором упоминал в своей статье «Цари природы, энергобатарейки или биокомпьютеры?» уважаемый Андрей Погодин. И вспомним концовку легенды: когда неисчислимые беды и несчастья вырвались из ящика и распространились по земле, а Пандоре удалось наконец захлопнуть крышку ящика, на его дне осталась… надежда! Да пребудут с нами эта надежда на лучшее и вера в безграничные возможности и высоконравственные устремления по-настоящему своих среди наших талантливых людей – российских программистов и сисадминов. EOF

Между прочим

Если трактовать термин «хакер» по RFC 1392, то там предлагается различать термины «hacker» и «cracker», чего в последнее время, особенно в массовом сознании, не происходит. Ещё один аспект, который надо принимать во внимание, – это авторские права, которые в России пока не очень соблюдаются. Не секрет, что почти все программы можно выкачать вместе с «кряками», «кейгенами» и прочими «лекарствами», а ведь это тоже можно расценивать как работу хакеров и причинение ущерба компаниям; сюда же можно отнести и огромное количество фильмов, музыки, игр и т.п. в пиринговых сетях. Значит, каждый, кто хотя бы раз выкачивал фильм из сети, может почувствовать себя немного хакером.

Для того чтобы справиться с типичными угрозами вполне хватает настроенной политики безопасности и распространённых средств зашиты, а от мощной целенаправленной атаки, боюсь, мало что поможет.

Николай Зюков,
технический директор, г.Москва

Вы хакеров уважаете?

На вопрос «Системного администратора» отвечают ИТ-специалисты.

Андрей Луконькин, инженер-программист, г. Нижний Новгород

Некоторые хакеры очень даже ничего ребята. Уважаю их труд, который приносит благо народу. Уважаю их знания, умения, нестандартное мышление. А вот умельцев, ломающих аськи, аккаунты e-mail, банковские счета (т.е. совершающих взлом в личных целях, для наживы) – ни капельки не уважаю.

Алексей Немытов, системный администратор, г. Нарьян-Мар

Смотря что понимать под словом «хакер»: культивированное СМИ обобщенное определение различного рода крекеров, кардеров, фрикеров, фишеров, пиратов и других злоумышленников или «хакер» (hacker) в первоначальном истинном значении этого слова (см. RFC 1392). О первых: их бы энергию да на мирные цели… глядишь, и из линуксов бы уже что-нибудь нормальное сделали. С одной стороны я, как законопослушный гражданин, осуждаю такую деятельность, но с другой стороны, именно эти нехорошие люди создают нам, админам, некую часть работы и даже рабочие места. О вторых: это просто увлеченные люди. Такие же, как сумасшедшие автомеханики, создающие из своих машин шедевры.

Билла Гейтса можно тоже хакером назвать, ибо только глубокое понимание процессов, творящихся в компьютере, позволило ему практически в одиночку выиграть в свое время конкурс IBM и вырваться на вершину мира.

Макс Иргизнов, системный администратор, г. Ульяновск

Уважаю хакеров в первоначальном смысле слова: как особых компьютерных специалистов, обладающих познаниями (с творческим и нестандартным мышлением) в своих областях.

Александр Башкиров, менеджер проектов, г. Санкт-Петербург

Уважаю. Для меня хакер – человек, который интересуется не только тем, как использовать ПК, но и тем, как он «устроен изнутри», с уклоном в улучшение и развитие. То есть исследователь и создатель. А расхожий миф о миллионах «злобных хакеров», которые «ломают банки и сети», мне кажется выдумкой далеких от индустрии людей.

Александр Емельянов, инженер, г. Владимир

Я не злой, но юных вирусописателей самолично порой хочется повесить за их эго куда-нибудь повыше. Многие из этой категории откровенно вызывают восторг, многие ненависть, кто-то фразы вроде «ну да, круто… а зачем все это?», киношные хакеры вызывают улыбку.

Юлия Шумова, специалист по ИТ компании APC by Schneider Electric

Деятельность хакеров в основном противозаконна, что не может вызвать положительного отношения к ним. Однако это своего рода стимулирующий фактор, подстегивающий разработчиков совершенствовать программные продукты, делая их менее уязвимыми, что делает работу с информацией более безопасной.

Алексей Барабанов, системный администратор, г. Москва

Хакеры – это те, что неустанно долбятся в мои sshd? Нет. Не уважаю. А может, хакеры – это те, что рипают и озвучивают для меня фильмы и ваяют таблетки на софт? Вот эти полезные ребята! Я временами им перевожу небольшую спонсорскую помощь.

Антон Ананич, начальник отдела Java-разработки, г. Минск

Я уважаю хакеров. Это люди, для которых не существует технических проблем – профессионалов с многолетним опытом программирования. Они всегда находятся на острие атаки при разработке программ. Только хакер знает, как помочь разуму одержать победу над бездушным железом. Но часто под хакерами подразумевают также вандалов, орудующих в информационном пространстве. Такие действия уважения не заслуживают и хакерами их называют скорее в насмешку, чем всерьез.

Вадим Андросов, преподаватель, г. Луганск

Хакеров уважаю. В мире программного обеспечения они играют роль хищников, которые уничтожают слабых и заставляют приспосабливаться и развиваться сильных. Без этих людей наблюдаемого нами прогресса в развитии информационных технологий не было бы.

Визитка

МИХАИЛ КАЛИНИЧЕНКО,
генеральный директор компании StarForce Technologies

Они – не Робин Гуды

Их можно уважать за ум, но не за поступки

Безусловно, звание хакера несет в себе некий налет романтики. Сразу вспоминается Робин Гуд, который грабил богатых, чтобы отдавать деньги бедным. Но сегодня хакерство в основном – это криминальное действие. Ведь хакеры портят результаты иногда многолетней работы других людей, из спортивного интереса ломают программное обеспечение или получают доступ к секретным данным.

Например, после взлома программного обеспечения разработчик или издатель получает намного меньший доход, который мог бы пойти на внедрение новых фич или создание и продвижение современных продуктов. Особенно пагубно хакерство отражается на индустрии компьютерных игр: многие талантливые разработчики популярных игр разорились, потому что их создание сегодня недешево. Хотя то же можно сказать и про другое программное обеспечение. Например, в конце 2008 года на портале Cnews.ru появилось сообщение о взломе одного из самых популярных в России картографических приложений. Это привело к падению продаж на 15%.

Конечно, хакеров можно уважать за их ум и способность решать сложные технологические загадки, но не за то, что они делают и какой вред приносят. В то же время нужно разделять хакерство как профессиональный вид деятельности и как стиль жизни и способ получения доходов. Уровень пиратства зависит и от административных мер наказания, и от менталитета населения. В благополучных европейских странах процент пиратства меньше, в азиатских странах больше. Однако не секрет, что в разных странах спецслужбы создают специальные подразделения по борьбе с кибертерроризмом. По сути, сотрудники таких подразделений нередко являются профессиональными хакерами. Поэтому говорить, что хакер – это однозначно плохо, неправильно, ведь многие из них состоят на службе государства.

Наша компания косвенно сталкивается с хакерами каждый день. Потому что ее основная цель – защита наших клиентов, а точнее, их программного обеспечения от взлома.

Защищать информационную сеть компании следует сразу комплексом мер. Конфиденциальные документы нужно защищать от нелегального открытия, распространения и копирования. Для этого есть специальные инструменты защиты, которые не позволяют открывать защищенный электронный документ в обычно используемых программах. Чтобы открыть защищенный документ, необходимо иметь специальный вьювер, серийный номер и собственно документ. Человек, защитивший документ, сможет увидеть отчет по активации документа. Для безопасной же работы сети нужно использовать обязательно и антивирусное программное обеспечение, и проактивную защиту, и защищенные корпоративные приложения.

Сегодня проблема борьбы с хакерством заключается не столько в несовершенстве законодательства РФ, сколько в средствах и институтах контроля над выполнением законов. Например, в Уголовном кодексе прописано, что взлом защищенного приложения с последующей продажей программы является уголовно наказуемым преступлением. Однако на деле этот закон выполняется нечасто. EOF

ТОП10 крупнейших хакерских атак (2008-2009 гг.)

Apple iPhone. Механизм защиты Apple, который «привязывал» каждый смартфон к отдельному оператору мобильной связи, оказался несостоятельным. Во многих странах мира продавались «Айфоны» без защиты, а Интернет полон хакерских прошивок.

Goldman Sachs. Проживающий в США эмигрант Сергей Алейников совершил кражу программного обеспечения банка Goldman Sachs. Это код системы, которая считалась одной из самых совершенных способов торговли на фондовых биржах в режиме онлайн. Ущерб составил порядка миллиона долларов.

Гарвардский университет. Взломав серверы университета, хакеры получили доступ к персональным данным десятков тысяч студентов. Помимо прочего, там хранились номера полисов социального страхования, с помощью которых можно оформить кредит или даже сделать новую кредитную карточку.

Город Вэйфан. Из-за хакерских атак сервера фирм-провайдеров китайского города Вэйфан были недоступны в течение двух суток. Все это время 400 тысяч пользователей не имели доступа к Интернету. Это самый масштабный сбой работы провайдеров в истории.

Bank of Scotland. Хакеры взломали компьютерную систему банка и получили сведения о полутора миллионах клиентов. Создали клоны карт и наняли людей, которые с фальшивыми копиями могли забирать деньги из банкоматов. Ущерб банка составил 9 млн долларов, организаторы не найдены.

Визитка

АНДРЕЙ СОКОЛОВ,
консультант по информационной безопасности ЗАО «ДиалогНаука»,
автор нескольких статей об угрозах взлома, занимается проведением тестов на проникновение

Взломщик подобен художнику

По уровню защиты мы заметно отстаем от Запада

На мой взгляд, термин «хакер», исторически описанный в RFC 1392, в своем первоначальном смысле уже устарел. Ведь изначально хакерами называли людей, получавших удовольствие от досконального понимания и изучения внутренних действий систем, компьютеров и компьютерных сетей.

В 90-х годах под «хакерами» все чаще стали понимать немотивированных взломщиков, компьютерных вандалов, интернет-хулиганов, которые стремятся нанести максимальный вред без какой-либо особой цели. Безусловно, такие маргинальные субъекты уважения не заслуживают.

Однако я предпочитаю более конкретный термин – «взломщик», используемый без какой-то эмоциональной окраски. Взломщика можно уважать или не уважать в зависимости от его мотивации и уровня квалификации.

Не вызывают симпатии криминальные взломщики. Их основная мотивация – эффективное извлечение прибыли пускай и криминальным путем, но при условии сохранения собственной безопасности. Творческая же мотивация другой группы высококвалифицированных взломщиков достойна уважения. Такие талантливые люди находят себя подобно художникам, музыкантам и режиссерам, получая удовлетворение от профессионального роста и принося пользу обществу.

Как человек, занимающийся тестированием на проникновение, я с грустью смотрю на сложившуюся в России ситуацию. На Западе действительно боятся промышленного шпионажа, поэтому проблемам безопасности и методам защиты уделяют большое внимание. Там уровень защиты от хакеров высок и услуги по защите от взлома востребованы.

А в нашей же стране руководители таких компаний не боятся взлома и потери данных. Они больше боятся чиновников и силовиков. Они рассматривают в спектре рисков информационной безопасности только тех маргиналов, о которых я говорил выше. В результате в России уровень защиты от хакерских атак на десяток лет отстает от западного. Но не надо драматизировать, постепенно ситуация меняется в лучшую сторону.

В современном мире средства защиты от атак хакеров адекватно эволюционируют соответственно уровню и качеству самих атак, которые в свою очередь становятся все более изощренными. Самое слабое место в защите от взломов, как мне кажется, – отсутствие внятной корпоративной политики безопасности, внедренных стандартов, правил, частных политик и регламентов информационной безопасности.

Первый шаг в создании эффективной системы защиты от хакеров – это проведение тестирования на проникновение, процедура внешнего аудита безопасности компании. В процессе тестирования на проникновение осуществляется имитация действий «взломщика». Результаты теста позволяют оценить текущий уровень защищенности компании и запланировать дальнейшие шаги по совершенствованию системы безопасности.

Не менее важно повышать уровень осведомленности сотрудников компании. Для этого необходимо проводить тренинги для персонала, т.к. сотрудники должны четко понимать всю важность и серьезность хакерских угроз и их возможные последствия. EOF

Сайт журнала Wired. Wired – один из самых известных и авторитетных в мире журналов об информационных технологиях. На главной странице сайта журнала хакеры разместили новость о том, что Стив Джобс умер от остановки сердца. Учитывая статус издания и проблемы Стива со здоровьем, неудачная хакерская шутка до публикации опровержения воспринималась всерьез.

Gmail.com. В результате DDoS-атаки одна из крупнейших почтовых служб в Интернете была недоступна для пользователей по всему миру в течение трех часов. На следующий день после случившегося представители Google заявили, что причиной сбоя была не хакерская атака, а стечение обстоятельств и проведение технических работ.

Ботнет Storm. Эпидемия червя Storm предоставила в распоряжение хакеров огромное количество инфицированных компьютеров по всему миру. В пик эпидемии червя называлась цифра в пятьдесят миллионов зараженных ПК.

NowTorrents. NowTorrents.com входит в десятку самых посещаемых файлообменников. Хакеры не просто взяли под контроль ресурс, но даже переоформили на чужое имя домен.

T-mobile. Взломщики украли информацию с серверов одного из операторов сотовой связи в США. В руках киберпреступников оказались абонентские листы, а также финансовые и другие документы.

Илья Александров, по материалам сайтов securitylab.ru, securityfocus.com, compulenta.ru

Визитка

АЛЕКСЕЙ АНДРИЯШИН,
консультант по безопасности компании Check Point, до прихода в компанию работал в компании «Юнимилк», «Внешторгбанке», Главном управлении Центробанка по Краснодарскому краю

Киберпреступность – это бизнес

Масштабы бедствий превышают миллионы долларов

В «Манифесте хакера» Ллойда Блэнкеншипа автор называет основные ценности культуры хакера, такие как: безразличие к цвету кожи, национальности и религии, превосходство знаний и нестандартного образа мыслей, безграничная свобода информации, информации для исследования, изучение из любопытства, познание. Однако между поиском, доступом и использованием информации из любопытства и уголовным преступлением существует тонкая грань, которую легко переступить. Благодаря кинематографу и художественной литературе хакеры представляются поколением компьютерных «нигилистов» или «робин гудов», способных за несколько минут взломать систему безопасности любой компьютерной сети, идущих против системы, общественного мнения, порою не лишенных романтизма. В реальной жизни существует более подходящий термин – киберпреступник.

Киберпреступность – это очень большой бизнес. Сейчас доходы от него выше, чем от наркоторговли. А риск при этом гораздо ниже. Современные киберпреступники – профессиональны, скрытны, циничны, финансово мотивированы. Большинство компьютерных преступлений совершается с единственной целью – извлечение прибыли. При этом используются методы, применяемые при совершении других уголовных преступлений, – шантаж и вымогательство.

Статья 272 Уголовного кодекса РФ предусматривает срок лишения свободы до семи лет за преступления, совершенные в сфере компьютерной информации. Вызывает ли у вас уважение уголовный преступник?

К сожалению, большинство организаций, столкнувшихся с компьютерными атаками, скрывают этот факт, боясь огласки. Их легко понять – ничего не стоит так дорого, как репутация. Поэтому компьютерных преступлений совершено гораздо больше, чем о них известно. С компьютерными преступниками приходится сталкиваться не только коммерческим организациям. Киберпреступность представляет собой угрозу безопасности на межгосударственном уровне.

Возможность предотвращения преступлений и поиска организаторов превращается в сложно разрешимую задачу. Нужно четко понимать, что любая компания, любое устройство, любое приложение, любой сотрудник, хоть как-то соприкоснувшийся с Интернетом, нуждаются в защите.

При построении системы безопасности одинаковое внимание нужно уделять как защите периметра и рабочих станций, ноутбуков, мобильных устройств, так и управлению. Системы безопасности должны строиться по принципу проактивной защиты, способной отразить атаки до того, как появятся проблемы. Системы информационной безопасности должны развиваться вместе с компанией. Невозможно единожды потратить миллионы долларов на информационную безопасность и спать спокойно – это просто выброшенные деньги. EOF

Хакер & антихакер

Своим мнением с «Системным администратором» поделились известные специалисты по информационной безопасности (в прошлом хакеры).

Крис Касперски: «Мне интересно заглянуть «под капот» программы»

– Хакерство – своего рода искусство. Чем отличается искусство от ремесла? Допустим, два ремесленника сделали два одинаковых горшка. И это просто горшки, ни больше ни меньше. А искусство – это умение выразить себя, свою точку зрения на мир. Поэтому хакер ломает программы каждый раз немножко по-разному. Еще больший простор для самовыражения дает разработка защитных механизмов. И еще – если занимаешься делом, которое тебе по душе, видишь в нем то, что другой никогда не увидит.

Кевин Митник: «Люди не глупы – они беспечны»

– Компании по-разному разрабатывают свою политику безопасности. Одни создают ее с помощью своих сотрудников, другие нанимают кого-то со стороны. Во втором случае есть опасность, что у людей не будет мотивации следовать правилам. Если же сотрудники компании будут сами разрабатывать правила безопасности, то они начнут более тщательно их выполнять. Они будут думать: «Раз я участвовал в этом деле, то должен это как-то применять в своей работе». Таким образом, вы сможете изменить вашу корпоративную культуру и мотивировать ваш персонал.

Беседовала Оксана Родионова

Визитка

КИРИЛЛ КЕРЦЕНБАУМ,
руководитель группы технических специалистов Symantec в России и СНГ,
работает девять лет в ИТ-отрасли, из них более четырех – в области информационной безопасности

Скупой платит дважды

Защитив всего 99,9% своих ресурсов, компания рискует быть атакованной

Хакеры – это, в первую очередь, высококлассные специалисты в своей области. И, конечно же, они достойны уважения. Но, к сожалению, в последнее время под хакерами мы стали понимать только тех, кто использует свои экспертные знания для совершения преступных действий. Безусловно, такие люди не заслуживают уважения, как и любые субъекты, совершающие противоправные действия, способные нанести вред другим.

С проявлениями их деятельности корпорации Symantec приходится сталкиваться ежедневно, я бы даже сказал, ежеминутно. Постоянно появляются десятки тысяч новых вариантов вредоносного ПО. Его разработкой занимается целая индустрия, а непосредственными исполнителями заказов являются именно хакеры. Несомненно, они представляют угрозу компаниям. Фактически весь подход к обеспечению информационной безопасности в любой организации состоит в борьбе с атаками извне – прямыми проявлениями деятельности организованных групп хакеров.

В последнее время к этим угрозам добавились и внутренние риски. Если оценить ущерб от пропажи данных о клиентах и сотрудниках, информации о секретных проектах, то примерный объем потенциальных потерь можно отчетливо представить. А если учесть еще и риски возможных судебных исков или штрафов в случае утери, например, персональной информации, то цифра становится еще больше.

Законодательная база по информационной безопасности в России пока находится в зачаточной стадии, но некоторые подвижки уже есть. Например, широко обсуждаемый Закон о защите персональных данных ужесточает требования к организациям в части систем защиты личных данных, к которым относятся данные о сотрудниках и клиентах. Правильное внедрение подобных систем усложнит жизнь хакерам, однако отсутствие законов, которые позволили бы проще привлекать подобных людей к ответственности, также играет свою роль в бурном росте хакерского сообщества в России.

Я уверен, что ни в коем случае не следует экономить на средствах защиты, не стоит выбирать подобные продукты исходя из их дешевизны или потребительской привлекательности.

В первую очередь, нужно учитывать функциональность, репутацию компании и технологий на рынке, отзывы других пользователей. Нужно понимать, что защитив 99,9% своих ресурсов самыми современными технологиями и оставив всего лишь один сервер или один ПК незащищенным, компания рискует быть атакованной, несмотря на все финансовые и временные затраты на внедрение подобных систем.

Подобные решения, например, предлагает компания Symantec для бизнеса. Для домашних пользователей – продукты под маркой Norton.

Наиболее защищенными в плане ИТ-безопасности считаются США. Здесь несколько десятков тысяч сотрудников специального подразделения ФБР ежедневно занимаются огромной аналитической работой по борьбе и предотвращению хакерских атак, причем направленных не только на государственные, но и на частные структуры.

В России пока основная нагрузка по защите от хакеров лежит непосредственно на самих компаниях. EOF

Между прочим

Хакеры – это реальность, которая существует независимо от нас. Любим мы их или нет – не важно. И, наверно, даже не так интересно быть хакером. Зато очень полезно уметь извлекать пользу от хакеров. Кто лучше сможет выполнить проверку безопасности вашей информационной системы – абстрактная компания, имеющая модные сертификаты и разрешения на аудит безопасности от государственных структур, или хакер, зарабатывающий этим себе на жизнь? К сожалению, многие компании начинают заниматься безопасностью только после инцидента, приведшего к денежным потерям. А ведь мы живем не в идеальном мире. И все догадываются, что лучше не создавать соблазн взять доступную ценную информацию. У Гарри Гаррисона есть серия книг про «Стальную Крысу». Любопытна мысль главного персонажа о том, что он своими незаконными действиями позволял обосновать бюджет подразделений полиции нескольких планет.

Вячеслав Гилев,
эксперт по информационным технологиям, г. Москва

Визитка

СЕРГЕЙ ЯРЕМЧУК, инженер автоматизации. Автор более 800 статей и 4 книг. В «Системном администраторе» публикуется с первого номера. Интересы: сетевые технологии, защита информации, свободные ОС

Строим сеть
на Calculate Directory Server

Принято считать, что управлять большим количеством Linux-систем очень сложно, разработчики Calculate Linux доказали, что это не так

> Here all my tuxian friends are scared when it comes to gentoo or anything related to it. they say, "hands will be on fire, if you touch it" so much customizable. now everyone is talking of Calculate Linux. its a real blessing, i must say.
>
> Все мои друзья пугаются, когда речь идет о Gentoo. Они говорят: «Руки будут гореть, если прикоснуться к нему», – столько настроек. Сейчас они говорят о Calculate Linux. Я должен сказать, это реальное благословление.
>
> **Из сообщения в IRC проекта Calculate Linux**

Зачем еще одно «поделие»?

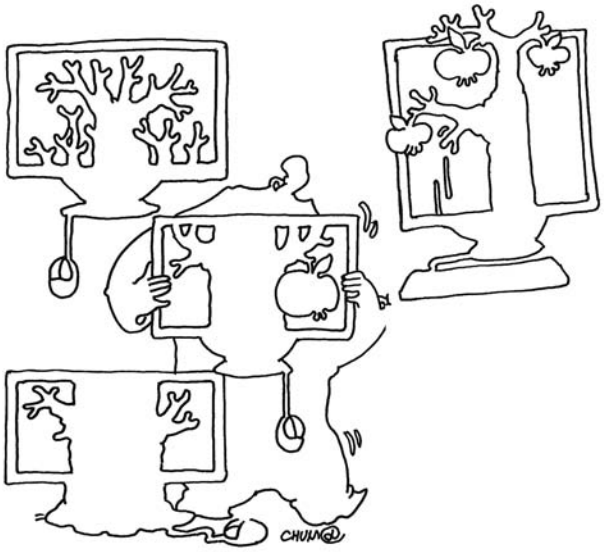
Учитывая, что подобный вопрос неизменно появляется в качестве комментариев после анонса любого нового дистрибутива, следует уделить несколько строк проекту Calculate Linux [1].

Linux-системы ассоциируются с несколькими понятиями – бесплатность, доступность, стабильность, безопасность, управляемость, доступ к коду и возможность его изменения. Но именно бесплатность ставят на первое место, когда рассматривается вопрос о внедрении. Делая ставку на то, что системы на базе этой ОС можно свободно скачать и использовать без отчислений и постепенно довести ИТ-инфраструктуру до необходимого уровня. Учитывая затяжное внедрение и необходимость в наличии подготовленных кадров, основной упор при переходе на Linux переносится с цены приобретения на стоимость сопровождения. Именно такой аргумент приводят сторонники Microsoft, указывая, что совокупное владение Linux, несмотря на нулевую стоимость, все-таки выше именно за счет обучения и оплаты системного администратора, службы поддержки и обслуживания. Вероятно, в условиях кризиса в этом даже больше выгоды, так как финансирование внедрения Linux не будет требовать больших первоначальных вложений, а развитие ИТ-инфраструктуры может идти и финансироваться постепенно, по мере необходимости. Но как раз без должного финансирования переход на свободные ОС может длиться лишь усилиями энтузиастов и длиться не один месяц.

Именно поэтому многие используют Linux дома или на отдельных системах, в частности, сервера на предприятии. На массовое повсеместное внедрение решаются не все, не говоря уже о полном переходе. Ведь необходимо не только развернуть систему на десятках/сотнях компьютеров, но и обеспечить автоматическое обновление, произвести первоначальные настройки, в том числе настроить единую систему аутентификации пользователя, переобучить персонал. Немаловажен тот факт, что многие специфические программы не имеют свободных аналогов или такие аналоги слабо документированы, некоторое оборудование не имеет драйверов под эту ОС.

Причем здесь Calculate Linux? Ответ дан в кратком описании на сайте «Calculate Linux – это открытый проект по внедрению Linux повсеместно. Проект представляет свободный и легкий доступ ко всем возможностям Gentoo». Прошу заметить, первым в списке задач стоит именно внедрение, дистрибутив лишь инструмент, обеспечивающий простоту внедрения. Собственно, и проект возник в результате перевода систем ЗАО «Калкулэйт Пак» на Linux, что примечательно – ЗАО не имеет никакого прямого отношения к ИТ. Идейным вдохновителем и руководителем является Александр Трацевский, основная группа разработчиков включает еще двух человек.

Постепенно накапливался опыт, выбирались оптимальные процедуры обновления систем и программ, входящих в состав дистрибутива, оконный менеджер и его формление, появились утилиты собственной разработки. Использование единой учетной записи позволяет не только удобно управлять доступом к ресурсам в пределах организации, но и пользователь теперь не привязан к рабочему месту. После регистрации получает с сервера свое рабочее окружение со всеми файлами и настройками. Все это работает «из коробки», настраивается очень просто и не требует от администратора глубоких знаний Linux-систем (хотя они в любом случае приветствуются). Конечно, все это дела-



лось под нужды определенной структуры, так как это удобно самим разработчикам, вводилось постепенно, не за один день. Но как показывает тестирование, довести до ума сеть на Calculate Linux можно на порядок быстрее, чем на Gentoo, который и является основой Calculate. При этом совместимость с Gentoo сохранена на 100%, все дополнительные пакеты собираются из ebuild-файлов Calculate Overlay. Релизы системы выходят стабильно раз в месяц (как правило, в первых числах), система нумерации подобна Ubuntu (год.месяц). Актуальной на момент написания статьи является версия 9.7, но уже полным ходом идет работа над 9.8, в которой нам обещают еще одну новинку – Calculate Linux Scratch (CLS), который позволит быстро собрать свой вариант дистрибутива.

Вполне естественно, что настало время поделиться своим опытом с другими и, возможно, привлечь к проекту разработчиков. Постепенно был открыт сайт, форум и IRC-канал #calculate на irc.freenode.net. Учитывая более простую систему установки и обновления, ежемесячный цикл выхода релизов, не требующих самостоятельно пересобирать систему и тестировать приложения на совместимость, многие пользователи выбрали Calculate вместо Gentoo в качестве настольной системы.

В настоящее время проект предлагает три варианта системы. Серверная версия – Calculate Directory Server (CDS), основой которого является LDAP-сервер, используемый для авторизации пользователей, централизованного хранения профилей, прав доступа, настроек сеансов пользователей и настроек приложений в едином сетевом хранилище. Поддерживается репликация почтовых и Samba-серверов, централизованное обновление серверов и рабочих станций, резервирование и восстановление данных.

Его альтернативой можно считать Mandriva Directory Server [3] стоимостью 5550 руб или Red Hat Directory Server (RHDS) [4]. Основной компонент для RHDS – 389 (ранее Fedora Directory Server Project) [5] доступен свободно, правда, с установкой в дистрибутиве, отличном от Red Hat, придется немного повозиться. Но главное – по возможностям оба этих решения уступают бесплатному CDS.

И две настольные – Calculate Linux Desktop (CLD) с рабочей средой KDE 4.x и Calculate Linux Desktop XFCE (CLDX) с рабочим столом XFce. Последняя имеет меньшие системные требования и ориентирована на применение на маломощных машинах. CLDX – это первая проба, основной настольной системой считается именно CLD, который максимально адаптирован для совместной работы с CDS. При подключении к домену с сервера забираются профили пользователей, автоматически подключаются сетевые папки, каталог FTP, соответствующий ярлык появляется на рабочем столе. Кроме этого пользователь автоматически получает доступ к почтовому, Jabber и прокси-серверу (если он ему разрешен). И главное, все это просто настраивается.

Следует отметить документацию проекта, написанную без излишних технических подробностей «под себя», но с массой практических примеров для всех вариантов использования системы. Жаль только, что она иногда запаздывает, и из всего многообразия пошаговое руководство для новичка, позволяющее настроить полноценную сеть, сложить трудно, потребуется все-таки некоторый опыт в администрировании систем. Хотя заметно оживление, возможно, в будущем проблема документации будет решена. Собственно, и сама статья является попыткой свести все к одному логическому знаменателю. Система работает на Intel-совместимых процессорах, не ниже Pentium Pro (i686, x86_64), поддерживает установку на PATA-, SATA- и SCSI-контроллеры, имеет поддержку сетевого беспроводного оборудования Wi-Fi. Интересно, что совсем молодой Calculate Linux по рейтингу Distrowatch.com занимает первое среди дистрибутивов, сделанных в России (общее 72 место).

Теперь рассмотрим, как настроить связку CDS и CLD/CLDX.

Установка Calculate Linux

Перед загрузкой рекомендую на всякий случай ознакомиться с документом «Структура FTP зеркала», это снимет ряд вопросов, что и где скачивать. Дистрибутив CDS и CLDX поставляется в виде LiveCD, а CLD – LiveDVD ISO-образов.

Образы находятся в одноименных каталогах, внутри – отдельные подкаталоги со сборками для i686- и x64-систем. Здесь же доступны tar.7z-архивы, которые предназначены для обновления дистрибутива и по составу приложений не отличаются от ISO-вариантов. Последние версии Calculate поддерживают обновление и из установочных ISO-образов, поэтому дополнительно tar.7z-файл скачивать уже не обязательно.

Аппаратные требования системы для работы невысоки: процессор класса i686, 256 Мб ОЗУ (512 Мб для CLD) и 3 Гб (6 Гб CLD) на жестком диске. После перехода в версии 9.6 на использование алгоритма LZMA во время установки требуется не менее 1 Гб ОЗУ, иначе копирование файлов завершается с ошибкой. Решить проблему можно, подключив swap-раздел командой swapon. Разработчики знают о проблеме, и уже в CLD 9.7 установочный скрипт самостоятельно монтирует swap-раздел перед началом копирования файлов (в CDS 9.7 для этого необходимо обновить установщик).

Установка дистрибутива на жесткий диск, обновление, а также сборка загрузочного ISO-образа системы производится при помощи Perl-утилиты calculate собственной разработки, работающей в консоли. Несмотря на отсутствие каких-либо графических инструментов, процесс инсталляции очень прост. Следует загрузиться в Live-режиме (при наличии 2 Гб памяти можно выгрузить образ в ОЗУ), обновить скрипт calculate.

В версии 9.6 для этого следовало выполнять:

```
# calculate --update
```

В релизе 9.7 появилась новая версия calculate 1.1.0, которая не поддерживает параметра --update, поэтому обновлять следует через emerge:

```
# layman -S && emerge calculate
```

Далее два варианта установки. Первый – самый простой и почему-то до сих пор недокументированный на сайте проекта. При наличии жесткого диска размером больше 45 Гб (при установке на флешку достаточно 512 Мб) утилита calculate умеет автоматически разбивать пространство и создавать разделы (все разделы будут уничтожены). В этом случае в качестве параметра необходимо указать только диск:

```
# calculate --disk=/dev/sda
```

В результате будет установлена система, жесткий диск будет разбит на такие разделы:

- /dev/sda1 swap
- /dev/sda2 (/) 10 Гб (десктоп) или 20 Гб (сервер)
- /dev/sda3 (/)10 Гб (десктоп) или 20 Гб (сервер)
- /dev/sda4 Extended
- /dev/sda5 Linux (/var/calculate – для CDS/CLD/CLDX)

Именно такая схема рекомендуется разработчиками, и, чтобы получить все преимущества Calculate, ее желательно придерживаться (почему – объясню чуть позже). Под корневой раздел можно отвести меньшее место (в документации указано 10-20 Гб, но нижний предел можно сделать еще меньше, установка занимает меньше 3 Гб).

Если в результате работы скрипта получаем сообщение:

```
The size of the disk is not sufficient to perform automatic
partitioning!
```

то жесткий диск необходимо разметить вручную, при помощи fdisk/cfdisk. И указать затем на корневой в параметре запуска:

```
# calculate --disk=/dev/sda2
```

При большом количестве однотипных систем (типичные размеры жестких дисков 20, 30, 40, 80 Гб …), проще подправить скрипт calculate, указав свои настройки.

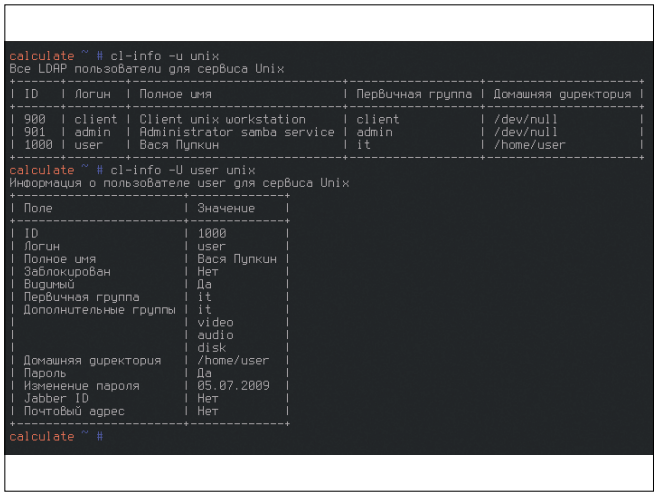
Например, за проверку объема диска отвечает такая строка:

```
if($size < 45){  printmes(gettext('The size of the disk ↵
        is not sufficient to perform automatic ↵
        partitioning')."!\n");
```

Указываем свой минимальный размер вместо 45. Параметры для разметки диска берутся из одного из файлов fdisk.*, соответствующего версии системы, который находится в /usr/calculate/install/config. Внутри файла – набор команд для fdisk, просто указываем другие размеры.

Рисунок 1. Утилиты Calculate 2 – основа Calculate Directory Server

Рисунок 2. Информация о пользователе UNIX



Разделы Calculate

Теперь следует разобраться, зачем используется такая довольно нестандартная схема разделов. Обновить Calculate можно стандартным для Gentoo способом, как описано в документации проекта Gentoo [4]:

```
# emerge --sync && emerge -uD world
# env-update
```

Но в Gentoo изначально отсутствует понятие релиза как такового, любая сборка считается стабильной, поэтому главная идеология проекта гласит – хочешь иметь стабильную систему – обновляй все. Версии пакетов привязаны к профилю, руководство рекомендует обязательно обновлять профиль, если он объявляется нежелательным. В итоге после нескольких часов пересборки системы приходится еще заниматься адаптацией существующих настроек программ к их новым версиям. Если на домашнем (персональном) компьютере это может быть приемлемо, то простой даже одного сервера или рабочей системы пользователей на предприятии невозможен. А что делать, если их несколько сотен? Именно поэтому многие администраторы, использующие Gentoo, обновляют систему на сервере максимум один раз, на вторую попытку уже мало кто решается.

Разработчики Calculate сумели выйти из этого положения, вероятно, кому-то покажется, что не так элегантно, но зато весьма практично и безопасно. После того как новый релиз будет протестирован и выпущен, ISO-образ или tar.7z-архив, достаточно скопировать в каталог /usr/calculate/share и ввести команду calculate. Инсталлятор определит текущий корневой раздел и распакует дистрибутив во второй (свободный) корневой раздел, перенесет пользовательские настройки и перенастроит загрузчик GRUB. Если обновление произошло неудачно, то у пользователя всегда будет возможность вернуться в старую рабочую систему. В результате переустановка или обновление системы на порядок упрощается и происходит приблизительно за 5-7 минут. Такое обновление очень легко автоматизировать. Достаточно на сервере открыть доступ по NFS, который и примонтировать на клиентских системах в раздел /usr/calculate/share и добавить команду calculate в скрипты, выполняющиеся при выключении системы. Пользователь утром будет работать в новой версии.

В /usr/calculate/share помимо обновлений системы (каталог linux) хранятся другие полезные ресурсы, такие как пакеты программ (distfiles), внешние профили установки (profile), патчи в виде выполняемых скриптов для внесения изменений в системы (patch), бинарные пакеты для быстрого обновления (packages). Именно чтобы упростить перенос данных, каталог /var/calculate, в котором находятся настройки для подключения к серверу (/var/calculate/calculate.env) и пользовательские данные, рекомендуется сохранить в отдельном разделе. После ввода клиентской системы в домен CDS каталог /home будет располагаться в /var/calculate/client-home (монтируется через bind).

Утилиты Calculate

Управление LDAP, Samba и другими сервисами при помощи штатных утилит требует понимания процесса, то есть некоторой подготовки, что обычно отпугивает новичков. Чтобы упростить администрирование CDS, разработчики создали набор утилит (скриптов на Python) под общим названием Calculate 2, при помощи которых и производятся настройки единого интерфейса, основных сервисов – учетных записей LDAP, а также настройки Squid, FTP, UNIX, Samba и почтовых серверов.

Распространяется Calculate 2 под свободной лицензией Apache2 и может быть использована на любом Gentoo-совместимом дистрибутиве. Учитывая, что вся идея дистрибутива заложена в Calculate 2, чтобы понять его суть, следует вначале хотя бы вкратце познакомиться с этими утилитами. Утилиты и библиотеки Calculate 2 в зависимости от назначения распределены в трех пакетах: calculate-server, calculate-client и calculate-lib. Чтобы узнать назначение конкретной утилиты, следует ее запустить с параметром --help или --help-название_сервиса (--help-samba).

В пакете calculate-server находится несколько утилит, в скобках приведены примеры использования:

cl-usermod/cl-groupmod – модификация пользовательского профиля/группы в LDAP (cl-usermod -a test guest unix);

Рисунок 3. Получаем информацию о пользователе домена

```
calculate ~ # cl-info -u samba
Все LDAP пользователи для сервиса Samba
+--------+-----------------------------+--------------+--------+
| Логин  | Полное имя                  | Заблокирован | Пароль |
+--------+-----------------------------+--------------+--------+
| client | Client unix workstation     | Нет          | Да     |
| admin  | Administrator samba service | Нет          | Да     |
| user   | Вася Пупкин                 | Нет          | Да     |
+--------+-----------------------------+--------------+--------+
calculate ~ # cl-info -U user samba
Информация о пользователе user для сервиса Samba
+---------------------+-----------------------------------------------------+
| Поле                | Значение                                            |
+---------------------+-----------------------------------------------------+
| Логин               | user                                                |
| Полное имя          | Вася Пупкин                                         |
| Заблокирован        | Нет                                                 |
| Пароль              | Да                                                  |
| Изменение пароля    | 05.07.2009                                          |
| Домашняя директория | /var/calculate/server-data/samba/home/user          |
| Общая директория    | /var/calculate/server-data/samba/share              |
| Linux профиль       | /var/calculate/server-data/samba/profiles/unix/user |
| Windows профиль     | /var/calculate/server-data/samba/profiles/win/user  |
| Windows logon       | /var/calculate/server-data/samba/netlogon/user      |
+---------------------+-----------------------------------------------------+
calculate ~ # _
```

Рисунок 4. На рабочем столе пользователя, зарегистрированного в домене, будут выведены ярлыки для доступа к Samba- и FTP-ресурсам

cl-userdel/cl-groupdel – удаление учетной записи/группы из LDAP, без параметра -r создается резервная копия удаляемой записи (cl-userdel guest samba);
cl-useradd/cl-groupadd – создание учетной записи пользователя/группы в LDAP (cl-useradd guest samba);
cl-update – обновление конфигурационных файлов определенного сервиса (cl-update samba);
cl-setup – управление сервисом (cl-setup samba);
cl-replication – настройка репликации между LDAP-сервисами (cl-replication –r server mail);
cl-rebuild – перестройка конфигурационных файлов и LDAP-базы для всех сервисов возможна с использованием резервной копии, находящейся /var/calculate/server-backup/ldap или с другого сервера (cl-rebuild);
cl-passwd – установка/изменение пароля для пользователя unix, samba, mail, Jabber, ftp и proxy (cl-passwd test samba);
cl-info – получение информации о сервисе (например, обо всех UNIX-пользователях – cl-info -u --full unix);
cl-backup – создание резервной копии и восстановление всех установленных (при помощи cl-setup) сервисов (cl-backup --backup/cl-backup --restore).

Кроме этого, в состав пакета входят и утилиты для служебных целей – replcron, repldap, proxy, вызываемые по мере необходимости из скриптов cl-*.

В клиентском пакете calculate-client всего три утилиты:
cl-sync – если пользователь зарегистрирован в домене, утилита синхронизирует настройки сеанса пользователя с сервером при входе в систему и при завершении сеанса и монтирует домашний каталог пользователя (/home/$USER/Home) и сетевые ресурсы (/home/$USER/Disk). Для передачи используется rsync, то есть передаются только изменения, что минимизирует трафик.
cl-createhome – во время входа в систему производится настройка сеанса по профилям, расположенным на клиентской системе в /usr/lib/calculate/calculate-client/profile и на сервере /var/calculate/remote/client-profile.
cl-client – при вводе ПК в домен монтируется сетевой диск в /var/calculate/remote, место для размещения профилей учетных записей пользователей.

При этом названия и параметры утилит по работе с учетными записями пользователей схожи с аналогичными UNIX-командами (useradd, groupmod, passwd и проч.), что упрощает работу с Calculate.

Профили – это еще одна из особенностей дистрибутива. Вместо прямого редактирования конфигурационных файлов Calculate хранит отличия от оригинала в файлах профиля, что упрощает перенос и модификацию данных, настройку сервисов, программ и окружения пользователя. Профили делятся на 3 типа – системный, сервиса и пользователя. И по расположению – базовый, внешний и локальный. Профили находятся в скрытых файлах .calculate_directory и могут накладываются как во время первого входа в систему, когда /home/$USER нет либо он пустой, так и при каждом входе в систему.

Таким образом можно пресечь попытки изменить стандартные настройки некоторых приложений всеми либо определенными группами пользователей.

Подробнее о профилях можно посмотреть в документе «Работа_с_профилями» [7].

После установки сервера обновите оверлей и утилиты:

```
# layman -S && emerge calculate-server calculate-lib
```

На клиентской машине соответственно:

```
# layman -S && emerge calculate-client calculate-lib
```

Устанавливаем контроллер домена

После перезагрузки регистрируемся с правами root. При наличии DHCP-сервера сеть будет определена автоматически, иначе ее следует настроить при помощи команды «net-setup eth0», которая поможет настроить ее при помощи псевдографического меню. Команда netstat показывает, что после установки CDS открыты порты SSH, NTP и Bootpc. Кроме этого, в списке обнаруживается полный набор сервисов – Apache 2.2.11, BIND 9.4.3, Squid 3.0.15, Sarg 2.2.5-r5, HAVP 0.89, Postfix 2.5.5, Dovecot 1.1.7-r1, PPTPD 1.3.4, ejabberd 2.0.5-r1, PostgreSQL 8.3.7, ProFTPD 1.3.2-r2, OpenLDAP 2.4.16, Clamd 0.95.1, Clamsmtpd 1.9.

Для настройки контролера домена нам понадобится LDAP и Samba, запускаем при помощи cl-setup. Команда проста:

```
# cl-setup ldap
```

Программа выполнит настройку LDAP, администратор получит предупреждение о том, что база данных будет перезаписана (архив сохраняется в /var/calculate/server-backup/ldap). Также сервис будет добавлен в автозагрузку. Теперь аналогично настроим сервисы UNIX и Samba.

```
# cl-setup unix
```

Этой командой мы подключаем возможность аутентификации учетных записей с системными ID, хранящихся в LDAP. И наконец:

```
# cl-setup samba
```

Будет запущен сервис Samba и созданы служебные пользователи client и admin, необходимые для ввода соответственно Linux- и Windows-компьютеров в домен. Последовательность запуска важна. Так как, например, введя перед запуском LDAP команду «cl-setup unix», получим предупреждение:

```
* LDAP service not setuped
* Setup LDAP service
* cl-setup ldap
```

Список настроенных сервисов можно узнать, просмотрев файл /etc/calculate/calculate.env:

```
# cat /etc/calculate/calculate.env

[server]
sr_ldap_set = on
sr_unix_set = on
sr_samba_set = on
```

Пароли доступа всех сервисов к LDAP хранятся в /etc/calculate/calculate.ldap (при запуске сервиса они генерируются случайным образом и уникальны для каждой системы).

```
# cat /etc/calculate/calculate.ldap

[admin]
DN = cn=ldapadmin,dc=calculate
```

```
PASS = fGdRTtajX
[unix]
DN = ou=Unix,ou=Services,dc=calculate
PASS = Fcy9dsW0y
[samba]
DN = ou=Samba,ou=Services,dc=calculate
PASS = iPyEgQTXx
```

Установим пароль для учетных записей client и admin, которые используются для ввода в домен соответственно Linux- и Windows-машин:

```
# cl-passwd --smb client samba
```

```
New password:
Retype new password:
 * Samba password of user admin is changed
```

```
# cl-passwd --smb admin samba
```

Подключение Linux-клиента к домену

Регистрируемся на клиентской Linux-системе как root, и вводим ее в домен, указав в качестве параметра cl-client имя сервера CDS или его IP-адрес. По ходу будет запрошен пароль учетной записи client:

```
# cl-client 192.168.17.147
```

```
Пароль для ввода рабочей станции в домен:
 * Подключен Samba-ресурс [remote] ...
 * Подключен /var/calculate/client-home  ...
 * Компьютер введен в домен 192.168.17.147 ...        [ ok ]
```

Команду рекомендуется вводить в локальной или удаленной (через SSH) консоли, а не под X. И вот почему. При успешном входе в домен будет выполнено ряд действий. Изменятся настройки файлов /etc/pam.d/system-auth, /etc/nsswitch.conf, в которых будут подключены пользователи Samba-сервера. В /var/calculate/remote будет смонтирован сетевой ресурс.

```
# mount | grep remote
```

```
//192.168.17.147/remote on /var/calculate/remote type cifs
(rw,mand)
```

Пока в указанном каталоге находится файл /var/calculate/remote/calculate.env настройками LDAP:

```
[client]
ur_organization =
ur_signature =
ld_samba_dn = ou=Samba,ou=Services,dc=calculate
ld_unix_dn = ou=Unix,ou=Services,dc=calculate
sr_samba_host = calculate.local
ld_services_dn = ou=Services,dc=calculate
ld_bind_dn = cn=proxyuser,dc=calculate
ld_bind_pw = calculate
ld_base_dn = dc=calculate
```

Можно его скорректировать, вписав в поле ur_organization название организации, а в ur_signature – подпись в почтовом сообщении. Чтобы исключить конфликты с локальными пользователями, поверх /home будет смонтирован локальный каталог /var/calculate/client-home. Именно поэтому на подключаемой системе лучше пока не работать.

```
# mount | grep home
```

```
/var/calculate/client-home on /home type none (rw,bind)
```

Сами разработчики не рекомендуют заводить локальные учетные записи (кроме стандартных root и guest, которые после ввода в домен будут недоступны), чтобы их ID не совпадали с ID пользователя в LDAP.

Чтобы вывести компьютер из домена, достаточно дать команду, зарегистрировавшись через SSH как локальный root:

```
# cl-client -r
```

```
 * Компьютер выведен из домена 192.168.17.147 ...   [ ok ]
```

Введенный пароль для подключения к домену на клиентской системе кэшируется в файле calculate.env.

```
# cat /var/calculate/calculate.env

[client]
cl_remote_host = 192.168.17.147
cl_remote_pw = password
```

Как подключить Windows-систему, хорошо расписано в документе «Переход на использование Linux», но Calculate/Gentoo Linux является предпочтительным при работе с CDS. Чтобы предоставить доступ пользователей к определенным ресурсам компьютера, системные UNIX-группы из /etc/group необходимо продублировать в LDAP-сервере при помощи команды cl-groupadd. Например:

```
# cat /etc/group | grep scanner
```

```
scanner:x:441
```

Дублируем в LDAP:

```
# cl-groupadd -f -g 441 scanner samba
```

```
* Added group 'scanner ' in Samba service
```

Кроме этого, учетная запись должна быть включена хотя бы в одну пользовательскую группу. Группы являются средством разграничения прав, поэтому в организации их может быть несколько. Например, создадим группу it.

```
# cl-groupadd it samba
```

```
* Added group 'it' in Samba service
```

Полностью команда для создания учетной записи выглядит так.

```
cl-useradd -p -c "Полное имя" -g пользовательская_группа ↵
        -G системная_группа -p логин samba
```

Например:

```
# cl-useradd -p -c "Сергей Яремчук" -g it -G ↵
        audio,lp,plugdev,scanner,video -p grinder samba
```

Вводим два раза пароль и получаем:

```
 * Added user grinder in Unix service
 * Added user grinder in Samba service
```

После входа пользователя на клиентской системе будет скопирован профиль, а на рабочем столе выведены ярлыки для доступа к его домашнему каталогу, ресурсам Samba и FTP (если настроен). Если перейти на другой компьютер, даже находящийся в другой подсети домена, то все настройки перекочуют за пользователем.

Все группы, в которые должен быть включен пользователь, уже должны быть созданы, иначе получаем ошибку:

```
* Group it is not found
* Can not add user grinder in Unix service
```

Удаляется учетная запись при помощи cl-userdel, но его домашние каталоги на сервере не удаляются (это нужно делать вручную). Поэтому при повторном использовании логина получаем сообщение:

```
* Path /var/calculate/server-data/samba/home/grinder exists
* Can not add user grinder
```

Для получения информации об учетных записях Samba используется cl-info. Например, выведем данные обо всех пользователях:

```
# cl-info -u samba
```

```
All users in LDAP for service Samba
+---------+----------------------------+------+----------+
| Login   | Name                       | Lock | Password |
+---------+----------------------------+------+----------+
| client  | Client unix workstation    | No   | Yes      |
| admin   | Administrator samba service | No   | Yes      |
| grinder | Сергей Яремчук             | No   | Yes      |
+---------+----------------------------+------+----------+
```

Теперь по конкретной учетной записи:

```
# cl-info -U grinder samba
```

Чтобы запустить после настройки сервисы, не поддерживаемые утилитами Calculate 2 (вроде Apache 2), введите:

```
# rc-update add apache default
# /etc/init.d/apache2 start
```

Настройка почтового (Postfix/Dovecot) и Jabber-сервисов хорошо расписана на сайте проекта, команды для добавления сервиса и учетной записи аналогичны. В документации можно найти скрипт, при помощи которого пользователь подключается ко всем сервисам. Поэтому подробно останавливаться на этом не буду.

***

Признаться, после стольких лет администрирования Linux возможности, предоставляемые дистрибутивом Calculate Directory Server, более чем впечатлили. Процесс построения домена и поддержания его в работоспособном состоянии весьма продуман и логичен и не займет много вашего времени. EOF

1. Сайт проекта – http://www.calculate-linux.ru.
2. Примеры внедрений Microsoft – http://www.microsoft.com/Rus/CaseStudies/Default.mspx.
3. Страница проекта Mandriva Directory Server – http://mandriva.ru/resheniya/produkty/mandriva_directory_server.
4. Страница проекта Red Hat Directory Server – http://www.redhat.com/directory_server.
5. Сайт 389 Directory Server – http://port389.org, http://directory.fedoraproject.org.
6. Документация Gentoo – http://www.gentoo.org/doc/ru.
7. Работа с профилями – http://www.calculate-linux.ru/Calculate2:Работа_с_профилями.

Множественные уязвимости в Cisco Wireless LAN контроллерах

Программа: Cisco Catalyst 6500 Series Wireless Service Module (WiSM); Cisco 2000 Series Wireless LAN Controller; Cisco 2100 Series Wireless LAN Controller; Cisco 4400 Series Wireless LAN Controller; Cisco Catalyst 3750 Series Integrated Wireless LAN Controllers; Cisco Wireless LAN Controller Module.
Опасность: Высокая.
Наличие эксплоита: Нет.
Описание: 1. Уязвимость существует из-за ошибки при обработке запросов HTTP Basic-аутентификации. Удаленный пользователь может отправить специально сформированный запрос, содержащий слишком длинные аутентификационные данные, на административный веб-интерфейс и вызвать перезагрузку устройства.

2. Уязвимость существует из-за утечки памяти при обработке SSH-подключений. Удаленный пользователь может вызвать перезагрузку устройства. Для успешной эксплуатации уязвимости не требуется троекратное рукопожатие.

3. Уязвимость существует из-за неизвестной ошибки при обработке запросов, отправленных административному веб-интерфейсу. Удаленный пользователь может с помощью специально сформированного запроса вызвать перезагрузку устройства.

4. Уязвимость существует из-за ошибки при обработке HTTP- и HTTPS-запросов. Удаленный пользователь может с помощью специально сформированного запроса, отправленного на IP-адрес, привязанный к административному интерфейсу или VLAN, изменить конфигурацию и получить полный контроль над устройством.
URL производителя: www.cisco.com
Решение: Установите исправление с сайта производителя.

Отказ в обслуживании в Cisco IOS Border Gateway Protoco

Программа: Cisco IOS 12.x, R12.x; Cisco IOS XE 2.3.x, 2.4.x.
Опасность: Средняя.
Наличие эксплоита: Нет.
Описание: 1. Уязвимость существует из-за неизвестной ошибки при обработке BGP-обновлений. Удаленный пользователь может с помощью BGP-обновления, содержащего специально сформированные данные о пути AS (например, который состоит из 1000 автономных систем), вызвать перезагрузку устройства.

2. Уязвимость существует из-за неизвестной ошибки при обработке BGP-обновлений. Удаленный пользователь может с помощью специально сформированного BGP-сообщения вызвать перезагрузку устройства.
URL производителя: www.cisco.com.
Решение: Установите исправление с сайта производителя.

Отказ в обслуживании в ISC BIND

Программа: ISC BIND версии до 9.4.3-P3, 9.5.1-P3 и 9.6.1-P1.
Опасность: Средняя.
Наличие эксплоита: Да.
Описание: Уязвимость существует из-за ошибки при обработке сообщений динамических обновлений. Удаленный пользователь может с помощью специально сформированных сообщений аварийно завершить работу сервера. Для успешной эксплуатации уязвимости DNS-сервер должен быть хозяином хотя бы одной зоны.
URL производителя: www.isc.org/products/BIND.
Решение: Установите последнюю версию 9.4.3-P3, 9.5.1-P3 или 9.6.1-P1 с сайта производителя.

Множественные уязвимости в Squid

Программа: Squid 3.0.STABLE16 и более ранние версии; Squid 3.1.0.11 и более ранние версии.
Опасность: Средняя.
Наличие эксплоита: Нет.
Описание: 1. Уязвимость существует из-за различных ошибок при обработке HTTP-заголовков. Удаленный пользователь может с помощью специально сформированного запроса или ответа аварийно завершить работу приложения.

2. Уязвимость существует из-за ошибки при обработке HTTP-ответов. Удаленный пользователь может с помощью специально сформированного HTTP-ответа аварийно завершить работу приложения.
URL производителя: www.squid-cache.org.
Решение: Установите последнюю версию 3.0.STABLE17 или 3.1.0.12 с сайта производителя.

Уязвимость при обработке CAB-архивов в продуктах Sophos

Программа: Sophos Anti-Virus for Windows 2000+ 7.6.7 и более ранние версии; Sophos Anti-Virus for Windows NT/95/98 4.7.22 и более ранние версии; Sophos Anti-Virus for OS X 4.9.22/7.01 и более ранние версии; Sophos Anti-Virus for UNIX 7.0.9 и более ранние версии; Sophos Anti-Virus for Linux 6.6.2 и более ранние версии; Sophos Anti-Virus for Netware 4.41.9 и более ранние версии; Sophos Email Appliance 3.1.3.1 и более ранние версии; Sophos Web Appliance 2.1.18 и более ранние версии; PureMessage for UNIX 5.5.4 и более ранние версии.
Опасность: Низкая.
Наличие эксплоита: Нет.
Описание: Уязвимость существует из-за ошибки при обработке CAB-файлов. Удаленный пользователь может с помощью специально сформированного CAB-файла обойти проверку архива антивирусом.
URL производителя: www.sophos.com.
Решение: Установите последнюю версию с сайта производителя.

Составил Александр Антипов

Визитка

ИГОРЬ КАЛИНИН, директор по маркетингу компании «КОЛАН» – дистрибьютора компании ATEN в России (http://www.colan.ru, http://www.aten.ru, тел. (495) 363-0131)

Удаленный аппаратный доступ к серверам

Системный администратор может поднять «упавший» сервер, даже если находится в другом городе. Эту задачу помогают решить IP KVM-удлинители

Любое, даже самое небольшое предприятие устанавливает ИТ-оборудование в специально отведенном помещении – серверной. В нем поддерживается специальный климатический режим, доступ в него ограничен. Пока все функционирует нормально, системный администратор здесь просто не нужен. Как всегда, проблемы возникают в самое непредсказуемое время, когда администратор находится дома или в другом филиале – словом, далеко от сервера.

Решать задачи администрирования, находясь в другом здании или даже городе, позволяют такие устройства, как IP KVM-удлинители. Их примером могут служить IP KVM-удлинители CN-6000, CN8000 (иногда их называют IP KVM-шлюз), выпущенные компанией ATEN (см. рис. 2). Такие устройства позволяют администратору по сети подключиться к KVM-интерфейсу компьютера (сервера) через Интернет или локальную сеть и работать на нем так, как будто он стоит на его рабочем столе, даже если сервер находится в другой части света.

KVM-удлинитель занимает мало места в стойке и не требует дополнительного ПО. Подключив его к серверу или через многопортовый KVM-переключатель к нескольким серверам, системный администратор получает возможность в любое время и из любого места управлять множеством устройств и даже решать проблемы на уровне BIOS.

Для удаленного доступа к серверу надо набрать IP-адрес KVM-удлинителя в браузере, получив приглашение, ввести логин и пароль.

После успешной регистрации на экране появляется стартовая веб-страничка IP KVM-удлинителя, содержащая графическое меню, с помощью которого можно настроить систему и получить доступ к KVM-интерфейсам серверов.

Запустив софт доступа к устройству (он «прошит» в IP KVM-удлинителе), вы увидите на экране вашего компьютера рабочий стол удаленного компьютера, а ваша клавиатура и мышь практически становятся устройствами управления для него.

Рисунок 1. Диаграмма подключения IP KVM-удлинителя

Рисунок 2. IP KVM-удлинители CN8000 (сверху) и CN-6000

Пользовательский интерфейс

IP KVM-удлинители имеют интуитивно понятный пользовательский интерфейс.

Стартовая веб-страничка IP KVM-удлинителя содержит административное и пользовательское меню управления и две кнопки для инициализации загрузки клиентского ПО на рабочую станцию: с операционной системы Windows и системонезависимого клиентского ПО Java.

Административное меню позволяет:

- Произвести стандартные сетевые настройки (адресацию), изменить номера портов сервисов устройства, установить адрес DNS-сервера.
- Настроить встроенный файервол для ограничения доступа к устройству по IP- и MAC-адресам. В интерфейсе предусмотрены дополнительные настройки безопасности, которые позволяют организовать прерывание сессии по тайм-ауту при бездействии и ограничение количества попыток ввода логина с ошибочным паролем, запрет/разрешения ответа устройства по ICMP (Ping), включение многопользовательского доступа.
- Произвести регистрацию пользователей, задать маски прав доступа к приложениям.
- Запустить обновление встроенного ПО.

Пользовательское меню позволяет:

- Инициировать процедуры загрузки и исполнения ПО устройства управления питанием ATEN PN0108, присоединенного к IP KVM-удлинителю.
- Просмотреть журнал системных событий.
- Принудительно разорвать сеанс управления устройством.

При загрузке одного из клиентских приложений на мониторе пользователя появляется экран удаленного компьютера (см. рис. 3). Здесь отображается OSD-меню, с помощью которого можно провести настройку горячих клавиш, скорректировать настройки видеоизображения, изменить цветовую гамму и ограничить потоки информации, передаваемой между устройством и рабочей станцией.

При помощи меню можно вызывать встроенную программу типа «ЧАТ-а» для общения между пользователями в многопользовательском режиме. Также в меню предусмотрены специальные кнопки, заменители клавиш NumLock, CapsLock и ScrLock на клавиатуре, комбинации клавиш <CTRL>+<ALT>+<DEL> и кнопка принудительного разрыва удаленного KVM-соединения.

В IP KVM CN8000 предусмотрена кнопка подключения виртуального диска.

При таком управлении мышка потребует синхронизации удаленного и локального курсоров, которая осуществляется в CN-6000 нажатием последовательной комбинации клавиш и щелканьем локальным курсором по удаленному, а в CN8000 – наведением курсора на OSD-меню. В остальном ваши экран, клавиатура и мышь полностью соответствуют KVM-консоли удаленного компьютера.

Особенности

Все модели IP KVM-удлинителей имеют порты подключения локальной консоли.

Для обеспечения безопасности и защиты от несанкционированного доступа KVM-удлинители защищены паролем, а передача данных – шифрованием с применением технологии 128-битового SSL-шифрования.

В дополнение к собственной системе безопасности CN8000 и CN-6000 позволяют настраивать политику аутентификации и авторизации, в том числе и с помощью внешних сервисов, таких как RADIUS, LDAP/LDAPS и MS Active Directory.

Модель CN8000 имеет более широкую функциональность, чем CN-6000, однако CN-6000 имеет более низкую стоимость.

IP KVM-удлинитель ATEN CN8000 обладает функцией virtual media, позволяющей удаленно, через USB-порт, загружать файлы, устанавливать программы, проводить диагностическое тестирование, загружать или обновлять операционную систему.

CN8000 имеет интерфейсы PS/2 и USB и порт для модема с поддержкой соединения по внешнему каналу (Out Of Band Configuration, OOBC) для альтернативного подключения при сбое сетевого соединения.

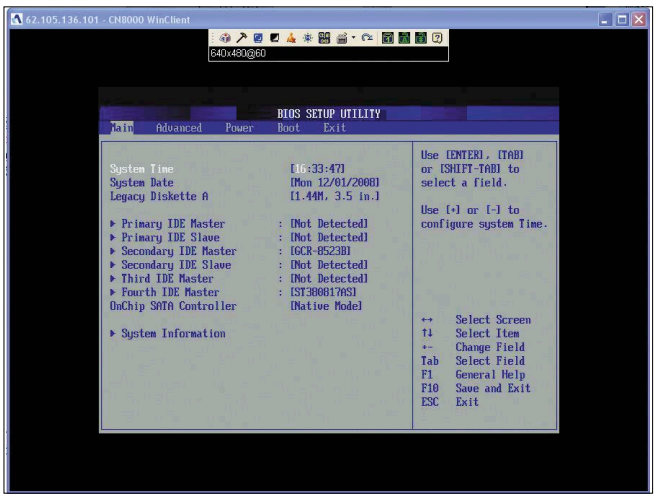
IP KVM-удлинители ATEN предусматривают возможность подключения к ним устройства управления подачей электропитания ALTUSEN PN0108. Оно позволяет включать/выключать электропитание розеток через IP KVM-удлинитель, подавать команду shutdown компьютерам, перезагружать сервер, программировать недельную последовательность включения/выключения питания. При длительном отключении электропитания последующее включение оборудования можно задать с задержками времени по каждой розетке для предотвращения пикового скачка нагрузки и последовательного «подъема» серверов.

Таким образом, при использовании IP KVM-удлинителей ATEN системный администратор получает 100% удаленное управление серверным хозяйством, включая возможность управления подачей электропитания и доступа к компьютеру до уровня BIOS (что, кстати, не позволяют делать программы удаленного доступа).

Все проблемы решаются быстрее, а расходы компаний на командировки квалифицированного персонала сокращаются. EOF

* На правах рекламы

Рисунок 3. Экран удаленного компьютера



Визитка

СЕРГЕЙ СУПРУНОВ, инженер электросвязи «широкого ИТ-профиля». В свободное время изучает FreeBSD и Python и пытается осмыслить свою нелюбовь к KDE

Сисадмин должен быть ленив

DHCP и динамический DNS

Настраивать каждый компьютер локальной сети в отдельности не обязательно. Эту работу можно доверить серверу

В наши дни невозможно представить себе предприятие, пусть даже небольшое, компьютеры которого не объединены в локальную сеть и не используют общие ресурсы, не обмениваются между собой файлами и т.п. Безусловно, всё это «хозяйство» можно настраивать и вручную, но по мере роста парка машин это становится всё более обременительным занятием. Да и вероятность ошибок возрастает пропорционально числу компьютеров. Поэтому и были придуманы протоколы, позволяющие выполнять настройку подключённых к сети машин автоматически.

Динамическое конфигурирование сети позволяет решить ряд проблем. Во-первых, администратор освобождается от необходимости следить за настройками каждой отдельно взятой машины, вести учёт уже выданных адресов, дабы исключить конфликты. Во-вторых, изменение адреса DNS-сервера, шлюза доступа в Интернет или переход на другую подсеть IP-адресов уже не потребуют обхода всех компьютеров и ручной перенастройки. В-третьих, упрощается процедура расширения сети или подключение-отключение мобильных устройств.

Часто упоминают также экономию адресного пространства (когда 30 человек, работающих посменно, смогут довольствоваться 12-ю адресами), но поскольку сети на реальных IP-адресах сейчас строят крайне редко, а в «серых» недостатка не бывает, более актуальной выглядит проблема простоя компьютеров, а не экономии адресов.

Конечно же, на смену этим проблемам приходят другие, специфичные для динамической настройки, но о них мы поговорим по ходу статьи.

В больших Windows-сетях нет нужды «изобретать велосипед» – Active Directory и прочие достижения компьютерной мысли позволяют получить высокоавтоматизированную и глубоко интегрированную сетевую инфраструктуру если и не прямо «из коробки», то при минимуме усилий. Конечно, свои особенности и хитрости есть и там, но этим вопросам были (и, уверен, ещё будут) посвящены другие статьи.

Если же у вас сравнительно небольшая бездоменная сеть, в составе которой к тому же есть машины с различными ОС, и вы хотите организовать динамическую конфигурацию сетевых параметров, то достаточно неплохим решением видится настройка DHCP-сервера на одной из UNIX-машин. В статье мы будем использовать FreeBSD.

Основы протокола DHCP

Начнём с рассмотрения общих принципов протокола динамической конфигурации хостов – DHCP. Этот протокол описан в RFC 2131 (некоторым расширениям посвящён RFC 2132 и другие документы) и решает задачу снабжения компьютеров необходимыми для работы в сети параметрами, такими как IP-адрес, маска подсети, шлюз по умолчанию, адреса DNS-серверов.

DHCP является клиент-серверным протоколом. Один или несколько серверов, размещённых в сети, отвечают за выдачу клиентам IP-адресов и всех сопутствующих параметров. Адрес может выдаваться клиенту либо динамически на некоторое время (назначается любой свободный адрес из некоторого пула IP-адресов) – данная процедура называется «арендой», либо статически (если администратор сервера явно указал в настройках, какой адрес следует отдавать данному клиенту; распознавание клиента обычно выполняется по его MAC-адресу). Выделяют также «автоматическое» назначение IP-адресов, когда клиент получает от DHCP-сервера любой свободный адрес из пула (как при динамическом назначении), но не на время, а «навсегда». Технически этот способ редко отличается от динамического назначения, в некоторых реализациях его вообще не выделяют отдельно.

В случае «аренды», что является основным режимом работы DHCP, IP-адрес выдаётся клиенту временно. Обычно в настройках сервера задаются два параметра – время аренды по умолчанию и максимальное время аренды. Первое используется, когда клиент, запрашивая адрес, не высказывает никаких пожеланий на этот счёт. Второе необходимо для ограничения аппетитов клиентов, не позволяя им владеть адресом слишком долго. Вообще вопрос времени аренды адресов обычно не играет принципиального значения, и указанные параметры иногда выбираются «с потолка». Но необходимо помнить, что именно от выбора вре-

мени аренды зависят такие вопросы, как устойчивость сети к непродолжительным сбоям, нагрузка на DHCP-сервер и скорость распространения изменений. Очевидно, что чем реже клиенты будут обращаться к серверу за адресами, тем меньше будет нагрузка на него и тем ниже вероятность, что какому-нибудь компьютеру потребуется обновить адрес именно в тот момент, когда сервер будет перегружаться. Однако при этом при любой корректировке параметров (скажем, изменении DNS-сервера или вообще переключении на другую подсеть) «переходный период» может заметно затянуться.

Стандартные рекомендации в этих случаях – для «динамичных» (например, тестовых или лабораторных) сетей задавать по возможности небольшое время аренды (один час или даже десять-пятнадцать минут); для стабильно работающих офисных сетей адреса можно выдавать и на неделю или даже месяц (за месяц перед предстоящей сменой параметров сети можно будет уменьшить максимальное время аренды до одного дня, а после изменений – вернуть обратно увеличенное время аренды). В любом случае имеет смысл пересмотреть значения по умолчанию (например, сервер ISC изначально использует 10-минутную аренду при максимальном времени владения IP-адресом 2 часа; для большинства сетей эти значения трудно назвать оптимальными).

Впрочем, невысокое время аренды не означает, что по его истечении клиент будет «отлучён от сети». Протокол DHCP предусматривает процедуру «продления аренды» клиентом, когда срок аренды истекает, но клиент ещё продолжает работать.

Рассмотрим в общих чертах, как происходит процесс получения сетевых параметров (см. рис. 1):

- После загрузки система клиента отправляет широковещательный (по адресу 255.255.255.255) запрос DHCPDISCOVER, цель которого – поиск доступных в данной сети DHCP-серверов. В качестве транспорта используется протокол UDP; серверы ожидают запросы на порту 67, клиенты используют 68-й порт.

Рисунок 1. Обмен пакетами между клиентом и сервером

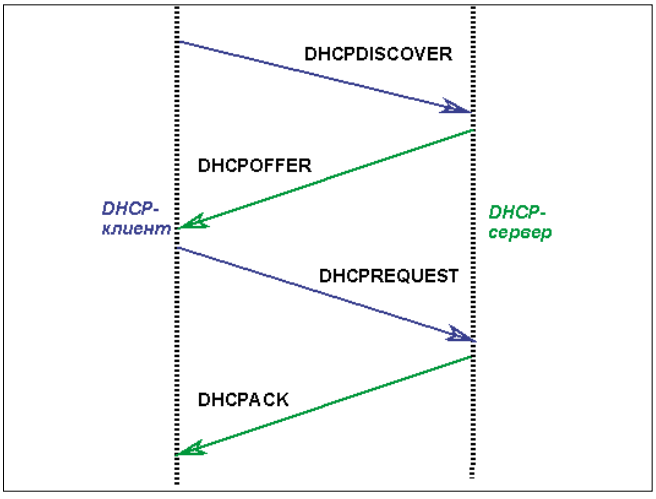
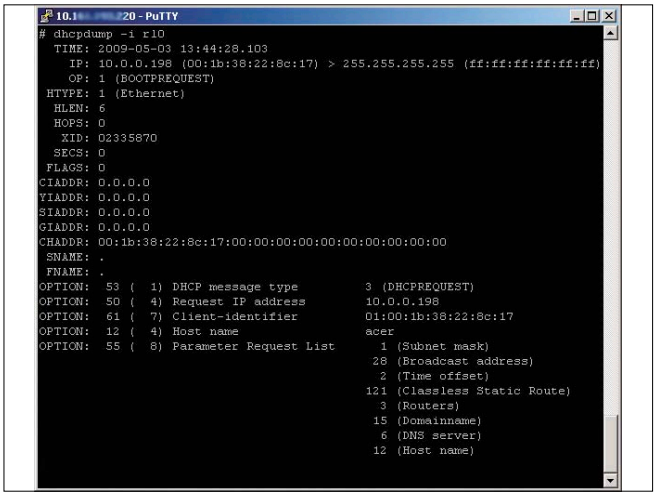


Рисунок 2. Один из пакетов, обработанных dhcpdump



Диагностические утилиты

В процессе обслуживания сети иногда возникает необходимость проверить работоспособность того или иного DHCP-сервера. Конечно, всегда можно запустить dhclient и посмотреть на результат. Но, во-первых, при этом ваша рабочая машина может временно «потерять сеть», пока будет получать новый адрес. Во-вторых, если в сети есть несколько DHCP-серверов, то протестировать таким образом менее «шустрый» будет затруднительно, поскольку с высокой вероятностью адрес будет приходить от более быстрого сервера. Ну и, в-третьих, такую проверку сложно автоматизировать.

Поэтому рекомендую установить маленькую (всего 75 Кб), но полезную утилиту – dhcping (есть в Портах). Принцип её действия заключается в следующем: утилита отправляет указанному серверу (обычным, не широковещательным, запросом) пакет DHCPREQUEST с просьбой выдать адрес 0.0.0.0. Любой разумный сервер (при условии, что он объявлен как авторитативный) ответит на это пакетом DHCPNAK. По этому ответу dhcping определяет, что сервер работоспособен, и завершает сеанс пакетом DHCPRELEASE.

Вы же получите на экране результат:

```
# dhcping -s 10.0.0.220
```

```
Got answer from: 10.0.0.220
```

В случае отсутствия ответа утилита так и сообщит: «no answer». Только имейте в виду, что такая проверка годится лишь для «авторитативных» серверов – все остальные просто проигнорируют неправильный DHCPREQUEST. Настройку серверов мы рассмотрим во второй части статьи.

Ещё одна полезная утилита – dhcpdump. Указав в качестве параметра имя интересующего вас интерфейса, вы получите расшифровку всех зафиксированных на нём DHCP-пакетов (см. рис. 2).

Как видите, информация исчерпывающая и может оказаться полезной как для решения проблем, так и для изучения работы того или иного клиента или сервера. Наименования полей соответствуют протоколу (дополнительную информацию можно получить на странице http://ru.wikipedia.org/wiki/DHCP).

В частности, на рисунке показан запрос DHCPREQUEST, сделанный клиентом acer (10.0.0.198) в надежде продлить аренду своего адреса.

- Все DHCP-серверы, получившие этот запрос (как правило, распространение широковещательных запросов ограничивается одним сегментом локальной сети, поэтому речь идёт о серверах, размещённых в том же сегменте, хотя возможно и «проксирование» запросов в другие сегменты, о чём мы поговорим отдельно), отправляют (опять-таки, широковещательным пакетом, так как клиент ещё не имеет адреса) свои «предложения» DHCPOFFER, в которых указывают предлагаемый клиенту IP-адрес.
- Клиент выбирает одно из поступивших предложений (как правило, предпочтение отдаётся первому полученному ответу) и направляет запрос DHCPREQUEST, указывая, какой из предложенных адресов он хотел бы получить, а также сообщая свои «пожелания» по дополнительным параметрам.
- Сервер, направивший предложение, устроившее клиентскую систему, отвечает либо пакетом DHCPACK, подтверждающим, что клиенту выдан данный IP-адрес, либо пакетом DHCPNAK, в случае, если выделение данного адреса уже невозможно по тем или иным причинам. В последнем случае клиент будет вынужден начинать процесс получения адреса заново.

Если компьютер-клиент уже работал ранее в сети и когда-то получал IP-адрес, то в этом случае, как правило, он сразу начинает процесс получения сетевых параметров с запроса DHCPREQUEST, указывая свой «старый» адрес в надежде на то, что он свободен и сразу будет выдан снова тем же DHCP-сервером, с которым шла работа раньше. Если адрес действительно свободен и сервер готов предложить его этому же клиенту, клиент сразу получит DHCPACK и сможет приступать к работе.

В противном случае (IP-адрес занят другим клиентом либо DHCP-сервер, обслуживающий его, недоступен) клиенту придётся проходить всю процедуру, начиная с DHCPDISCOVER.

Ещё один момент – продление аренды. В процессе работы клиент не ждёт, когда аренда выданного ему адреса истечёт, и пытается продлить время его использования заранее, для чего отправляется всё тот же пакет DHCPREQUEST спустя некоторый интервал времени (renewal-time), часто называемый T1 (обычно составляет 50% от времени аренды). Если сервер, отвечающий за данный адрес, доступен и не имеет причин отказать в продлении аренды, то клиент получает DHCPACK и начинает «отсчитывать» срок аренды заново.

Если же ответ сервера отсутствует, то клиент продолжает использование адреса до истечения срока первоначальной аренды, но время от времени предпринимает попытки её продлить. Если к некоторому моменту времени (rebinding-time, или T2, обычно около 90% от времени аренды) попытки продления не увенчались успехом, клиент отправляет запрос DHCPDISCOVER, чтобы получить хоть какой-нибудь адрес до того, как он лишится возможности работать в сети.

Таким образом, относительно времени аренды можно сказать следующее:

- интенсивность запросов к DHCP-серверу будет обратно пропорциональна интервалу T1: чем он меньше, тем чаще клиенты будут обращаться за продлением аренды;
- продолжительность допустимого перерыва в работе сервера можно определить как разницу между временем аренды и значением T1: если клиент получает адрес на 48 часов, а запрашивать продление аренды начинает через 24 часа, то у администратора сети остаётся ещё 24 часа в запасе на решение проблем с сервером;
- «переходный период», в течение которого все клиенты гарантированно получат обновлённые параметры, равен времени аренды IP-адреса.

Помимо вышеупомянутых пакетов DHCPDISCOVER, DHCPOFFER, DHCPREQUEST, DHCPACK и DHCPNAK, протоколом предусмотрены ещё три:

DHCPRELEASE – им клиент может освободить выданный ему адрес до истечения срока аренды;

DHCPDECLINE – так клиент сообщает серверу, что предложенный им адрес кем-то уже занят, проверка занятости адреса осуществляется ARP-запросом;

DHCPINFORM – этот пакет используется, если клиент уже получил IP-адрес из других источников, а у DHCP-

сервера запрашивает лишь дополнительные параметры, такие как адреса шлюзов, DNS-серверов и т.п.

DHCP-клиенты

Начнём с рассмотрения DHCP-клиентов. Эти программы, той или иной реализации, входят в состав практически всех операционных систем, так что проблем с получением сетевых параметров от DHCP-сервера ни в одной современной системе возникнуть не должно.

Рассмотрим более подробно утилиту dhclient, входящую в состав FreeBSD. В простейшем случае её использование сводится к команде:

```
dhclient <имя_интерфейса>
```

Работа может сопровождаться диагностическими сообщениями, например:

```
# dhclient nfe0
```

```
DHCPDISCOVER on nfe0 to 255.255.255.255 port 67 interval 6
DHCPOFFER from 10.0.0.220
DHCPREQUEST on nfe0 to 255.255.255.255 port 67
DHCPACK from 10.0.0.220
bound to 10.0.0.198 -- renewal in 129600 seconds.
```

В случае если адрес будет получен, запустятся два демона dhclient (один с правами root, второй от имени пользователя _dhcp, что обеспечивает необходимое разграничение прав доступа), «привязанные» к соответствующему интерфейсу, которые возьмут на себя заботу о своевременном продлении аренды. При отключении интерфейса (команда ifconfig nfe0 down) демоны dhclient также будут остановлены.

Помимо настройки соответствующего интерфейса, DHCP-клиент может вносить изменения и в конфигурацию других сетевых служб: изменять /etc/resolv.conf согласно полученным от сервера адресам DNS-серверов, добавлять статические маршруты в таблицу маршрутизации и т.п.

Все полученные от DHCP-сервера параметры сохраняются в некотором файле для использования в будущем. В частности, из этого файла система узнаёт при последующей загрузке, получала ли она адрес ранее и можно ли сразу «попытать счастье», отправив DHCPREQUEST вместо DHCPDISCOVER. Например, во FreeBSD эти данные сохраняются в файлах /var/db/dhclient.leases.<имя_интерфейса>:

```
# cat /var/db/dhclient.leases.nfe0

lease {
  interface "nfe0";
  fixed-address 10.0.0.198;
  option subnet-mask 255.255.255.0;
  option routers 10.0.0.220;
  option domain-name-servers ↵
        10.0.0.220;
  option dhcp-lease-time 259200;
  option dhcp-message-type 5;
  option dhcp-server-identifier ↵
        10.0.0.220;
  option dhcp-renewal-time 129600;
  option dhcp-rebinding-time 226800;
  renew 2 2009/2/17 03:11:11;
  rebind 3 2009/2/18 06:11:11;
  expire 3 2009/2/18 15:11:11;
}
```

«Встроенные» DHCP-серверы

Если ваша сеть совсем небольшая, а от DHCP-сервера требуется лишь раздача основных параметров (IP-адреса, маски, шлюза и адресов DNS-серверов), то в наши дни вам необязательно возиться с поиском пригодной для выполнения данной задачи машины, инсталляцией каких-то пакетов, их настройкой и последующим поддержанием работоспособности. Существует большое число устройств, способных взять на себя настройку сети при вашем минимальном участии.

Прежде всего следует упомянуть ADSL-модемы. Сейчас это наиболее распространённый способ подключения к Интернету, обеспечивающий приемлемую скорость при минимальных затратах. Выбирая модем с функцией маршрутизатора, вы в качестве бонуса получаете и DHCP-сервер. Из настроек вам нужно будет лишь указать диапазон адресов, которые должны будут раздаваться динамически (и проследить, чтобы адреса компьютеров, настраиваемых вручную, в этот диапазон не попадали). Некоторые модели модемов также позволят вам указать время аренды. Учитывая, что в большинстве ADSL-модемов сервер DHCP по умолчанию включён, автоматической настройкой сети можно начинать пользоваться в буквальном смысле прямо из коробки. И не забывайте об этом, если в вашей сети работает отдельный DHCP-сервер – не позаботившись об отключении «модемного», можно внести в процесс получения клиентами адресов некоторую путаницу.

Аппаратные маршрутизаторы также практически все имеют функцию DHCP-сервера, независимо от класса и стоимости устройства. Правда, нужно иметь в виду, что маршрутизаторы «низшего ценового диапазона», так же как и большинство DSL-модемов, жёстко передают в качестве шлюза по умолчанию свой адрес, не позволяя это изменить. То есть использовать такие устройства в качестве выделенного DHCP-сервера, когда за маршрутизацию отвечает другая «железка», будет весьма затруднительно.

Также DHCP-сервер можно найти в некоторых коммутаторах уровня Layer3. Только не путайте эту функцию с DHCP-Relay (способностью транслировать DHCP-запросы в другие подсети) – последняя встречается довольно часто, в то время как коммутатор с полноценным DHCP-сервером нужно ещё поискать.

Построить небольшую динамически конфигурируемую сеть на базе подобных устройств довольно просто. Ну а настройке полноценного DHCP-сервера будет посвящена следующая часть статьи.

Несмотря на сравнительную простоту dhclient, существует ряд параметров, позволяющих влиять на её поведение, а также можно использовать конфигурационный файл для задания постоянно используемых параметров (по умолчанию – /etc/dhclient.conf).

В большинстве случаев dhclient.conf пуст, и вам вряд ли потребуется изменять параметры по умолчанию. Но если всё же придётся, имейте в виду, что в этом файле можно изменить:

- временные параметры работы (тайм-аут ожидания ответа, интервал отправки повторных запросов и ряд других);
- перечень обязательных опций, которые сервер должен будет предоставить клиенту, а также желательных опций, которые клиент хотел бы получить от сервера;
- значения опций по умолчанию (которые будут использоваться, если ни один из серверов не определит иное значение), а также значения тех опций, которые будут перекрывать или дополнять полученные от сервера;
- адреса «плохих» DHCP-серверов, предложения которых будут отклоняться.

Пример файла можно посмотреть в справке (man dhclient.conf(5). Пожалуй, чуть подробнее следует остановиться на дополнительных опциях (полное описание вы найдёте на страницах справки dhcp-options(5). Наиболее полезные среди них: routers (шлюзы по умолчанию), domain-name-servers (DNS-серверы), static-routes (статические маршруты). Также можно указать имена smtp-, pop-, www-серверов, задавать TTL, MTU и другие параметры функционирования сети. Все эти опции можно либо задать вручную в настройках клиента, либо запросить у сервера.

Таким образом, набор доступных опций и возможность в определённой степени управлять их значениями позволяют вам занимать любую промежуточную позицию между двумя крайностями – «всё настраивать вручную» и «всё слепо получать от сервера».

Клиенты в Linux и Windows

В системах GNU/Linux в подавляющем большинстве случаев в качестве DHCP-клиента используется либо рассмотренная выше dhclient разработки ISC, либо программа dhcpcd (при желании её можно установить и во FreeBSD). Рассмотрим чуть подробнее вторую.

Запуск осуществляется командой:

```
dhcpcd <интерфейс>
```

где <интерфейс> – имя интерфейса, который будет обслуживаться клиентом dhcpcd. Дополнительно в командной строке можно задать ряд опций, таких как имя хоста, время аренды, запретить запрос шлюзов по умолчанию, адресов DNS-серверов и т.п. (см. man dhcpcd(8). Полученные от сервера данные сохраняются в файле dhcpcd-<интерфейс>.lease или dhcpcd-<интерфейс>.info, точное месторасположение которого зависит от системы (обычно /var/lib/dhcpcd).

Команда:

```
dhcpcd -k <интерфейс>
```

позволяет досрочно освободить полученный IP-адрес.

В системах MS Windows DHCP-клиент, как водится, спрятан глубоко в недра системы (в библиотеку dhcpcsvc.dll). Для динамического получения IP-адреса в свойствах протокола TCP/IP соответствующей сетевой карты выбирается опция «Получить IP-адрес автоматически». Вручную обновление IP-адреса можно выполнить с помощью утилиты ipconfig: ipconfig /release высвободит используемый в данный момент адрес, ipconfig /renew запросит адрес повторно.

Хранятся настройки DHCP-клиента и данные, полученные от сервера (текущий IP-адрес, маска подсети, адреса шлюзов и DNS-серверов, время истечения срока аренды, значения T1 и T2) в реестре, в ветви [HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\Interfaces]. Хотя без нужды туда лучше не лазить.

***

В этой части мы рассмотрели общие вопросы работы службы DHCP и наиболее популярных DHCP-клиентов. Следующая будет посвящена настройке DHCP-сервера и динамическим обновлениям DNS. EOF

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**:

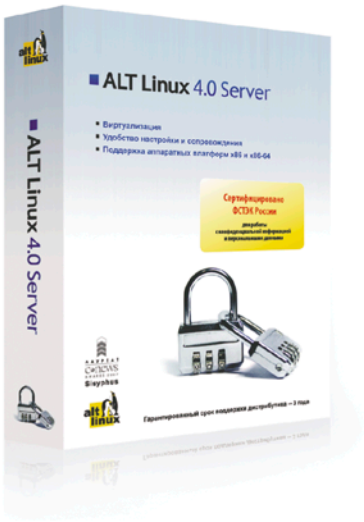
- Классификация по уровню контроля отсутствия недекларированных возможностей (НДВ) — **4 уровень**.
- Показатели защищённости от несанкционированного доступа к информации (СВТ) — по **5 классу защищённости**.

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

alt linux

Визитка

ИГОРЬ ШТОМПЕЛЬ, инженер, системный администратор. Сфера профессиональных интересов – GNU/Linux, функциональное программирование

Linux 2.6.30
выглядит неплохо!

Ядро – это сердце операционной системы. Оно изменяется от версии к версии, предоставляя все более широкие возможности. Что нового появилось в версии 2.6.30?

10 июня 2009 года Линус Торвальдс представил новый выпуск ядра операционной системы Linux – 2.6.30 [1]. 1334 разработчика подготовили более тринадцати тысяч исправлений (включено 1 096 994 строки кода, а 470 555 удалено) общим объемом 63 Мб [2].

Основными новшествами Linux 2.6.30 стали: добавление поддержки для файловых систем NILFS2, EXOFS и POHMELFS; протоколов RDS и IEEE 802.11w (предварительная); архитектуры Microblaze и подсистемы безопасности Tomoyo Linux; DRM (Direct Rendering Manager) для графических видеокарт Radeon R6xx/R7xx; появление асинхронной проверки устройств и разделов для ускорения загрузки (faster bootup); локальное кэширование данных, передаваемых с использованием сетевых файловых систем, и начальная поддержка NFS 4.1; добавлены системные вызовы preadv/pwritev и ряд новшеств в поддержке RAID.

Файловые системы NILFS2, EXOFS и POHMELFS

Как было сказано, новый выпуск ядра получил поддержку ряда новых файловых систем. Одной из них стала NILFS2, которая создана и активно разрабатывается NTT Lab (Nippon Telegraph and Telephone Corporation) [3]. NILFS2 – это файловая система с лог-структурированием (log-structures). В представлении файловой системы весь жесткий диск – это последовательность списка блоков, называемых log. Все операции по добавлению данных осуществляются в конец log. При этом блоки никогда не перезаписываются, за исключением случаев, когда на носителе информации не остается места (новые блоки будут добавлены в начало log).

Преимуществом данного подхода является то, что все изменения преобразуются в последовательность операций. А сами сбои (crashes) не могут повредить файловую систему, так как файловая система определяет конец log и продолжает работу. Кроме того, NILFS2 позволяет регулярно делать снимки изменений файловой системы – непрерывный snapshotting (continuous snapshotting). Последний не требует вмешательства системного администратора. NILFS2 дает возможность смонтировать эти снимки в режиме для чтения (on read-only mode). Указанная особенность позволяет пользователям восстанавливать уничтоженные данные.

Другой файловой системой, поддержка которой появилась в ядре версии 2.6.30, стала EXOFS (раннее известная как osdfs). Данная файловая система была разработана Avisha Traeger для IBM и основывалась на ext2. С 2008 года разработкой и поддержкой файловой системы занимается компания Panasas Inc (www.panasas.com), которая специализируется на создании высокопроизводительных вычислительных хранилищ, оптимизированных под кластеры под управлением операционной системы Linux. Данная файловая система работает поверх хранилищ объектов OSD (Object-based Storage Device). OSD – это абстракция, которая вместо логического массива не связанных между собой блоков (LBA – Logical block addressing) привносит идею хранения объекта как части коллекции (набора) объектов (collection of objects). Любой объект представляет собой контейнер для хранения данных и является массивом байт, индексирующимся от нуля до бесконечности [4]. В свою очередь EXOFS является объектно-основанной файловой системой (object-based file system), реализованной на вершине внешнего хранилища объекта. Данная особенность нашла отражение в ее названии – EXtended Object File Fystem, так как файловая система использует ext2-основанные метаданные и объектное хранилище устройств (object storage device). EXOFS поддерживает протокол T10 OSD, который является расширением SCSI [5]. Протокол дает возможность передавать данные объектами, например файлами, а не блоками, при этом передача данных и метаданных происходит раздельно.

POHMELFS (Parallel Optimized Host Message Exchange Layered File System) еще одна файловая система, получившая поддержку ядра версии 2.6.30, разрабатывается Евгением Поляковым. Она является высокопроизводительной распределенной файловой системой и дает возможность читать данные с удаленных узлов и одновременно записывать данные на удаленные узлы. POHMELFS позволяет осуществлять локальное кэширование данных и метаданных, что значительно ускоряет операции ввода-вывода (превосходит по быстродействию NFS в большинстве операций).

С разработкой POHMELFS тесно связан проект, который используется для создания распределенных хранилищ данных. Он представляет собой драйвер сетевого устройства – DST (Distributed (network) STrorage), работающий в ядре на уровне блочного устройства. DST позволяет шифровать канал передачи данных и поддерживает проверку целостности последних.

Протоколы RDS и IEEE 802.11w

Ядро версии 2.6.30, как было сказано выше, принесло поддержку новых протоколов в операционную систему Linux: RDS и IEEE 802.11w (предварительная). RDS (Reliable Datgram Sockets) – это протокол, ориентированный на обеспечение высокоскоростного обмена и низких задержек в транспортной системе серверов кластера. Разработчиком протокола является OpenFabrics Alliance (http://www.openfabrics.org). Зрелость проекта характеризует то, что на сегодняшний день RDS уже используется рядом продуктов (например, Oracle и Quicksilver от Silverstorm).

Протокол IEEE 802.11w Protected Management Frames (Защищенные Управляющие Фреймы) является частью набора стандартов, определяющих порядок беспроводной коммуникации в частотных диапазонах 2.4, 3.6 и 5 Ггц. Например, такие стандарты IEEE, как 802.11a, 802.11b, 802.11g и 802.11n, сегодня используются довольно широко. Кроме того, набор стандартов 802.11 ввел понятие типа «frame» для использования в сфере управления и контроля беспроводной связи. Результатом работы по усовершенствованию Medium Access Control layer набора стандартов IEEE 802.11 стало появление рассматриваемого протокола. Стоит отметить, что окончательный вариант стандарта IEEE 802.11w еще не утвержден, потому и поддержка его в ядре версии 2.6.30 носит предварительный характер.

Основная идея стандартизации протокола IEEE 802.11w заключается в необходимости внесения поправок в стандарт IEEE 802.11 с целью повышения уровня безопасности беспроводной связи за счет обеспечения конфиденциальности данных управленческих фреймов, механизмов интеграции данных и аутентификационных данных. Стандарт призван исправить ситуацию, когда в беспроводных локальных сетях системная управленческая информация отправляется в незащищенных фреймах и соответственно является уязвимой.

Архитектура MicroBlaze

MicroBlaze является микропроцессором с программным ядром (soft processor), созданным Xilinx для Xilinx FPGAs (FPGA – Field Programmable Gate Array, программируемая логическая интегральная схема) [6]. Разработку архитектуры осуществляет Михал Шимек (Michal Simek) с поддержкой PetaLogix and Xilinx. В основе MicroBlaze лежит 32-битный микропроцессор с программным ядром на базе RISC-архитектуры (RISC Harvard architecture). MicroBlaze позволяет комбинировать периферию, память и интерфейсы при создании разнообразных систем.

Ряд параметров MicroBlaze может быть сконфигурирован пользователем. Это размер кэша, блок управления памятью (memory management unit), встроенные периферийные устройства (embedded peripherals) и ряд других.

Без блока управления памятью с использованием MicroBlaze может быть запущена операционная система с упрощенной защитой и виртуальной моделью памяти (например, µClinux или FreeRTOS), а с блоком управления памятью возможен хостинг операционных систем, которым требуется основанная на аппаратной части защита (например, ядро Linux).

Tomoyo Linux

Tomoyo Linux – это новая подсистема безопасности (например, в Linux имеются SELinux, Smack), которая предлагает более правильную реализацию данного подхода в области достижения безопасности, что отличает ее от уже существующих. Программное обеспечение ориентировано на осуществление контроля доступа – MAC (Mandatory Access Control). Кроме того, подсистема безопасности может работать в режиме обучения (learning mode), когда она анализирует доступ к ядру и сохраняет результаты в качестве политики MAC. Tomoyo Linux разрабатывается NTT

DATA CORPORATION (Япония), которая распространяет его под лицензией GPL [7].

Direct Rendering Manager для Radeon R6xx/R7xx

Для обеспечения эффективной видеоакселерации (video acceleration), в особенности рендеринга 3D, в Linux (как, впрочем, на других UNIX-подобных операционных системах) используется DRM (Direct Rendering Manager). Последний является составной частью Direct Rendering Infrastructure и состоит из двух драйверов, реализованных как модули ядра Linux. Один из них – общий DRM-драйвер (generic drm driver), а другой отвечает за поддержку конкретного видеооборудования. Таким образом, ядро 2.6.30 получило поддержку DRM специфичного для видеокарт Radeon – R6xx/R7xx.

Fastboot

В рассматриваемое ядро были внесены изменения, призванные ускорить процесс загрузки. Компания Intel реализовала проект, использование которого дает возможность осуществления асинхронной проверки устройств и разделов. Так, например, ядро может продолжить загрузку остальной части, в то же время сканирование устройств хранения данных будет осуществляться параллельно. Как известно, ранее процесс сканирования был синхронным – сканировалось только одно устройство, а ядро находилось в состоянии ожидания. А это занимало достаточно много времени [8].

Кэширование для сетевых файловых систем и начальная поддержка NFS 4.1

Компания RedHat является разработчиком технологии локального кэширования данных, передаваемых с использованием сетевых файловых систем – FS-Cache. Данный процесс позволяет значительно ускорить осуществляемые операции. Реализация RedHat похожа на CacheFS, которую разработала компания Sun Microsystems и включила в ОС Solaris 2.3 [9]. Версия, включенная в ядро 2.6.30, получила поддержку файловых систем NFS и AFS.

Что касается NFS, то рассматриваемое ядро получило начальную поддержку этой файловой системы версии 4.1. NFS 4.1 разрабатывается в IETF (Internet Engineering Task Force, Специальная комиссия интернет-разработок – http://www.ietf.org). Основное поле деятельности организации – развитие протоколов и архитектуры Интернета. Важными новшествами, реализованными в данной файловой системе, стали обязательные для выполнения (mandatory-to-implement) сессии NFS 4.1, в то же время включение исходного кода Parallel NFS (http://pnfs.com) должно произойти в одной из следующих версий ядра.

Системные вызовы preadv()/pwritev()

В ядро версии 2.6.30 добавлена поддержка системных вызовов preadv()/pwritev(), разработчиком которых для операционной системы Linux является компания RedHat. Данные системные вызовы имеются в BSD-системах (например, NetBSD). Они предназначены для чтения из файлового дескриптора или записи в него по определенному смещению. Включение системных вызовов в ядро стало логичным шагом вперед, так как системные вызовы pread и pwrite появились в ядре Linux версии 2.1.60.

Изменения в поддержке RAID

Основным новшеством, затрагивающим поддержку RAID в рассматриваемой версии ядра, стало добавление проверки контроля целостности данных для переключения между режимами RAID5/6. Кроме того, внесено большое количество изменений в код MD (Multiple Device) реализации программного RAID. Так, RAID5 может быть конвертирован в RAID6 и наоборот, а также RAID1 в RAID5. Хотя стоит отметить, что текущая версия программы mdadm (ориентирована на создание программных RAID-массивов в Linux, раннее называлась – mdctl) не поддерживает эти изменения.

Новые драйверы

Среди большого количества изменений, внесенных в ядро 2.6.30, можно отметить появление новых драйверов. Так, звуковая подсистема получила поддержку ISA-драйвера для различных звуковых карт серии Turtle Beach MultiSound. Подсистема V4L/DVB стала поддерживать TV-устройства Conextant (с чипами серии cx231xx), которые подключаются через USB. Благодаря новому драйверу hdpvr добавлена возможность работать в Linux с устройствами Hauppauge HD PVR (ориентированы на запись видео с компьютера, телевизора или PlayStation 3 в качестве H.264). Также включены три драйвера (sq905, sq905c и mr97310a) для поддержки чипов, используемых в вебкамерах различных производителей.

В подсистему FireWire добавлена поддержка трансляции каналов (broadcasting channel) и асинхронного потока передачи. Разработчики удалили драйвер phidgets (предназначен для хранилищ (storage), работающих через USB), а вместо него предложили драйвер пространства пользователя (userspace), который имеет более широкую поддержку компонентов phidgets.

Подсистема I2C стала работать с рядом последних версий чипсетов для материнских плат Nvidia - MCP67, MCP73, MCP79 и MCP78S, AMD - SB800, Broadcom - HT1100. Подсистема аппаратного мониторинга обзавелась поддержкой чипов FSC Syleus, Hades, Nuvoton и Winbond Nuvoton.

В Linux 2.6.30 включен wmi-драйвер для ноутбуков Dell, который ответственен за обработку нажатий «горячих клавиш» (hotkeys). Поддержка лэптопов Sony и драйверов Thinkpad-acpi подверглась серьезной переработке (появилась поддержка большего количества моделей данных устройств).

***

Рассмотрение новшеств было сконцентрировано на основных моментах и не охватывает всего перечня изменений. Но ознакомления с ними достаточно, чтобы понять пути и масштабы совершенствования ядра одной из самых свободных операционных систем. EOF

1. http://permalink.gmane.org/gmane.linux.kernel/849020.
2. http://www.opennet.ru/opennews/art.shtml?num=22084.
3. http://www.nilfs.org/en/current_status.html.
4. http://en.wikipedia.org/wiki/Object_storage_device.
5. http://www.t10.org/intro.htm.
6. http://www.xilinx.com/tools/microblaze.htm.
7. http://tomoyo.sourceforge.jp/wiki-e.
8. http://lwn.net/Articles/299483.
9. http://en.wikipedia.org/wiki/CacheFS.

Решите проблемы **лицензирования ПО** с помощью профессионалов!

Операционная система GNU/Linux и свободное программное обеспечение помогут вам с минимальными затратами решить проблему лицензирования программного обеспечения, повысить безопасность и надежность вашей компьютерной сети.

Компания ГНУ/Линуксцентр предлагает вам внедрение ОС GNU/Linux и свободного программного обеспечения, реализацию и техническую поддержку сложных технических решений на базе свободного ПО, обучение ваших сотрудников — как пользователей, так и технических специалистов.

С НАШЕЙ ПОМОЩЬЮ ВЫ СМОЖЕТЕ:

- оптимизировать затраты на лицензирование ПО за счет максимально возможного использования свободного ПО;
- существенно сократить время системных администраторов, затрачиваемое на устранение последствий деятельности вирусов и сбоев в программном обеспечении.

ТИПОВЫЕ ПРОЕКТЫ:

- миграция рабочих станций и серверов с Microsoft Windows на GNU/Linux;
- установка 1С на серверах и рабочих станциях под управлением GNU/Linux;
- миграция с Microsoft Windows Active Directory на Mandriva Directory Server;
- миграция с Microsoft Exchange на Zimbra;
- внедрение интернет-телефонии на базе Asterisk;
- внедрение свободной CRM-системы SugarCRM;
- создание кластеров высокой доступности;
- реализация терминальных решений;
- создание порталов любой сложности на базе свободных CMS-систем — Joomla, Drupal, Plone;
- внедрение защищенных систем на основе сертифицированного ФСТЭК ПО.

СРЕДИ НАШИХ КЛИЕНТОВ:

- Правительство Московской области;
- Правительство Нижегородской области;
- администрация Черниговского района Приморского края;
- Министерство финансов республики Саха (Якутия);
- Владивостокский государственный университет экономики и сервиса;
- группа компаний «ИМАГ»;
- компания «Азбука мебели»;
- компания «Бестли — выставочные материалы»

и другие организации различного профиля.

Наш опыт внедрения свободного программного обеспечения в компаниях различного профиля поможет выбрать оптимальное сочетание свободного и коммерческого программного обеспечения, подходящее именно для вашей организации, а также поможет избежать техничеких и организационных проблем при внедрении свободного ПО.

Linux center www.linuxcenter.ru

Департамент внедрений компании ГНУ/Линуксцентр
Телефон в Москве: (499) 271-49-54,
в Санкт-Петербурге: (812) 309-06-86

ЗВОНИТЕ СЕЙЧАС!

Реклама

Визитка

ВЛАДИМИР ВАСИЛЬКИН, инженер, занимается администрированием информационных систем и сервисов

Sun OpenBoot Prom
между железом и софтом

Что может скрываться за буквами «ок» на белом экране?

OpenBoot Prom (OBP) – одна из айтишных «вкусностей», рожденная в лабораториях Sun Microsystems и широко используемая в настоящее время разными производителями аппаратного обеспечения. Можно сказать, что OBP – это аналог BIOS на платформах, отличных от x86, таких как sparc, powerpc и, возможно, других [1]. Основное предназначение данной программы – firmware[1] – загрузка и запуск других, более сложных программ и передача этим программам управления системой. «Другими» программами могут являться ОС, средства диагностики, отладки и т.п.

В процессе работы мне практически не приходилось сталкиваться с оборудованием, отличным от sparc и x86-подобных архитектур. OpenBoot на PC-совместимых компьютерах не встречал, все примеры в статье работают на архитектуре sparc sun4u.

В то же время одной из особенностей OBP является кроссплатформенность[2] – на разном аппаратном обеспечении ожидается похожее поведение системы. Чем-то напоминает «написано раз – используешь везде» – лозунг Java. Дело в том, что в компании всегда производились машины нескольких архитектур, отличных от x86. Сейчас это – sun4u (ultrasparc), sun4v (niagara), раньше были и другие.

Загружать операционную систему приходилось с целого ряда устройств: дисков различных типов, по сети через разные адаптеры и т.п. Вместо того чтобы писать свой загрузчик для каждого устройства ввода-вывода (см. пример BIOS), инженеры Sun пошли другим путем. Поставщикам оборудования была предоставлена возможность размещать загрузчики на самих устройствах – так называемые plug-in-драйверы устройств.

Драйверы должны быть написаны на языке Forth – OBP включает в себя интерпретатор этого языка. Храниться драйверы могут как на самих устройствах, так и на свободном месте в OBP. То есть любой сторонний производитель может выпустить свое абсолютно новое устройство и «подружить» его с остальной системой, не перекраивая firmware.

Но OBP – это не только загрузчик ОС. Он может еще использоваться для диагностики и отладки как железа, так и ядра операционной системы. Что является еще одним отличием OBP от BIOS для x86. Средства диагностики еще можно встретить на некоторых материнских платах, но вот с возможностями отладки мне сталкиваться не приходилось.

Наличие интерпретатора forth предоставляет возможность для составления сложных программ из простых, доступных изначально команд. Вообще работа с OBP происходит в оболочке интерпретатора forth, что напоминает привычный shell.

Приглашение для ввода команд обычно выглядит так:

```
ok
```

Далее по тексту это приглашение используется в примерах команд. Внимание – если приглашение выглядит так:

```
sc>
```

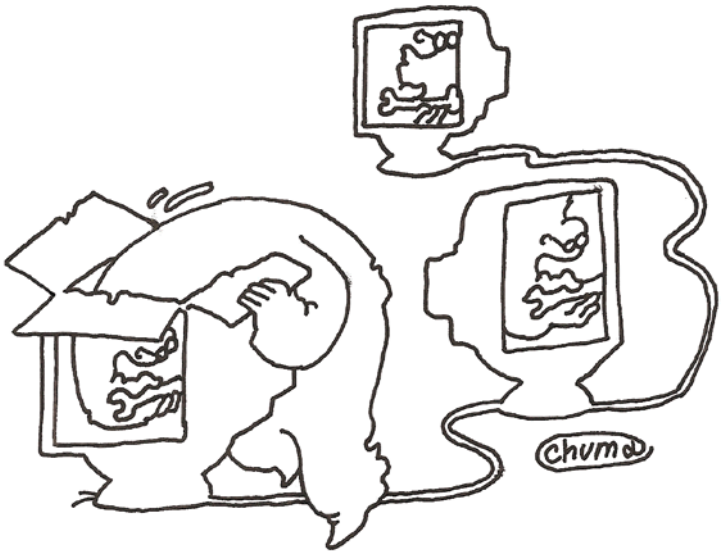
значит, управление передано не OBP, а сервисному контроллеру. Как работать с сервисным контроллером – отдельная тема [9].

Обычно достаточно помнить, что передать управление к OBP можно командой console. Попасть обратно в sc – сочетанием #., как показано в примере:

```
sc> console
Enter #. to return to ALOM.
```

Интерфейс командной строки мне хотелось бы выделить отдельно – это свойство может быть очень полезно в работе для «убийства рутины» – путем программирования часто повторяющихся действий. Например, при отладке. В слу-

1. Firmware – «микрокод» – говорит StarDict, или «ППЗУ» – подсказывают на сайте gentoo [7].
2. Для ряда платформ драйверы могут работать одинаково, но гарантировать полную идентичность поведения OBP на этих платформах не могу – не проверял.



чае же удаленного управления кучей серверов никакая графика не заменит возможностей expect и интерфейса командной строки OBP.

Пользовательский интерфейс основан на командном интерпретаторе, который предоставляет доступ к обширному набору команд для управления аппаратными средствами, программирования, изоляции проблемных мест и отладки. Набор доступных команд зависит от реализации – версий систем, используемых в OBP. Эта информация доступна по команде:

```
ok .version
```

```
Release 4.22.33  created 2007/06/18 12:45
OBP 4.22.33 2007/06/18 12:45 Sun Fire V210/V240,Netra 210/240
OBDIAG 4.22.33 2007/06/18 12:58
POST 4.22.33 2007/06/18 13:07
```

Далее набираем в поиске [2], к примеру, «OBP 4» и смотрим доступные документы. Также может быть полезен поиск по названию сервера.

Начало работы

Начать работать с OBP очень просто – нужно лишь послать сигнал break системе. Как – зависит от настроек консоли.

Часть систем управляется через COM-порт, часть – с помощью монитора и клавиатуры и т.п. В OBP можно переназначить console – управляющее устройство – об этом далее.

Самое популярное средство управления, конечно же, удаленная консоль. В таком случае процедура отправки сигнала break системе зависит от консольного клиента и от всей цепочки устройств до требуемого. Нередко доступ к консоли можно получить, лишь подключившись через цепочку серверов. Некоторые машины в цепочке также могут реагировать на сигнал break – т.е. прерывать свою работу. Следует быть аккуратным – бывают случаи, когда по невнимательности выключаются транзитные серверы.

Внимательно смотрим документацию на свой терминальный клиент (ssh, telnet – нужное подчеркнуть) и жмем соответствующие клавиши или кнопки мыши.

Например, подключившись через стандартный telnet-клиент, можно нажать <Ctrl>+<]>». После чего ввести два слова: «send break» и нажать <Enter>.

Кроме удаленного управления рабочие станции Sun на платформе sparc могут управляться с клавиатуры. В таком случае сигнал break системе можно послать, нажав одновременно <Stop>+<a> или <Stop>+<q> – в зависимости от типа клавиатуры: qwerty или azerty. На последних USB-клавиатурах порядок действий может отличаться – я с этим не сталкивался, но в документации так написано.

Также в OBP можно попасть из ОС, например, по команде:

```
# halt
```

Отличие от сигнала break в том, что halt прекращает работу ОС и передает управление в OBP, тогда как break прерывает работу ОС или других программ. Во многих случаях после «прерывания» можно опять запустить ОС в том же месте командой go. После команды halt (из ОС) будет работать только команда boot – загрузка ОС заново.

Кроме двух относительно нормальных способов, существует еще парочка.

Первый – отключение и включение питания сервера. Если система не сконфигурирована на автоматическую загрузку, после пропадания питания управление будет передано OBP.

Еще один нестандартный способ – когда OBP в момент загрузки ОС обнаруживает ошибки, которые разрешить не может. Например, часто встречающаяся ошибка – неправильно назначенно загрузочное устройство.

Дерево устройств – адресация

Для понимания работы OBP стоит разобрать понятие Device Tree – дерево устройств. Устройства могут подключаться к системе разными способами – используя различные шины, контроллеры, протоколы. OBP представляет все устройства в виде иерархической структуры типа «дерево», что очень похоже на файловую систему. У каждого устройства может быть родительское и ряд дочерних устройств – соответственно к чему подключено устройство

и что подключено через него. В основном родительскими являются шины, контроллеры и т.п.

Полный путь к каждому устройству обозначается как перечень родительских, разделенных прямой косой чертой – совсем как в UNIX-подобных файловых системах. Первая черта обозначает саму машину, «корень» всех устройств.

В Solaris тоже можно получить доступ к Device Tree через специальный каталог /devices. Внешний вид дерева устройств будет выглядеть так же, как в OBP.

Вывод команды ls в ОС Solaris на Netra210:

```
# uname -sir
SunOS 5.10 SUNW,Sun-Fire-V210
# pwd
/devices
# ls -1
iscsi
iscsi:devctl
memory-controller@0,0
memory-controller@0,0:mc-us3i
memory-controller@1,0
memory-controller@1,0:mc-us3i
options
pci@1c,600000
pci@1c,600000:devctl
pci@1c,600000:intr
pci@1c,600000:reg
pci@1d,700000
pci@1d,700000:devctl
pci@1d,700000:intr
pci@1d,700000:reg
pci@1e,600000
pci@1e,600000:devctl
pci@1e,600000:intr
pci@1e,600000:reg
pci@1f,700000
pci@1f,700000:devctl
pci@1f,700000:intr
pci@1f,700000:reg
pseudo
pseudo:devctl
ramdisk-root
ramdisk-root:a
ramdisk-root:a,raw
scsi_vhci
scsi_vhci:devctl
```

Начало ввывода show-devs на Netra210:

```
ok show-devs
/pci@1d,700000
/pci@1c,600000
/pci@1e,600000
/pci@1f,700000
/memory-controller@1,0
/SUNW,UltraSPARC-IIIi@1,0
/memory-controller@0,0
/SUNW,UltraSPARC-IIIi@0,0
/virtual-memory
/memory@m0,0
/aliases
/options
/openprom
/chosen
/packages
/pci@1d,700000/network@2,1
/pci@1d,700000/network@2
/pci@1c,600000/LSILogic,sas@1
/pci@1c,600000/scsi@2,1
/pci@1c,600000/scsi@2
/pci@1c,600000/LSILogic,sas@1/disk
/pci@1c,600000/LSILogic,sas@1/tape
/pci@1c,600000/scsi@2,1/tape
/pci@1c,600000/scsi@2,1/disk
```

Имя каждого устройства представлено в следующем виде: device-name@unit-address:device-arguments, где:

device-name – имя (название) устройства. В официальной документации сказано «для людей» – human-readable. Я бы подчеркнул, что понятны эти названия будут лишь подготовленным читателям;

unit-address – адрес устройства, текстовая строка, обозначающая физический адрес устройства в родительском пуле адресов. Формат написания зависит от шины (родительского устройства);

device-arguments – аргументы, зависящие уже от конкретного устройства данные, которые могут быть полезны при дальнейшей работе.

Хороший пример адресации устройства:

```
/sbus@1f,0/esp@0,40000/sd@3,0:a
```

Эта строчка говорит о том, что шина SBus подключена непосредственно к основной системной шине, адрес 1f,0. 0,40000 – слот в Sbus (в нашем случае – 0), и смещение 40000. Далее можно понять, что подключен SCSI Disk (sd) по адресу 3,0, партиция «a». В документации именование устройств расписано довольно подробно.

Псевдонимы

Все это выглядит очень интересно, но, мягко говоря, нечитабельно, если, конечно, читатель не имеет отношения к поддержке оборудования или разработке драйверов устройств.

Для более простого восприятия OBP предоставляет систему алиасов – псевдонимов устройств. Так что всем привычное net из команды:

```
ok boot net
```

обычно раскладывается во что-нибудь вроде:

```
/pci@1d,700000/network@2,1
```

Управлять псевдонимами устройств можно:

- на время текущей сессии – до перезагрузки по питанию или сброса параметров OBP (не путать с перезагрузкой ОС – на OBP никак не влияет).
- записать в NVRAM – энергонезависимую память OBP. Если быть более точным, то nvramrc – это часть NVRAM, доступная для хранения пользовательских команд, программ и псевдонимов устройств.

Команда devalias по своему синтаксису похожа на alias оболочки bash (или подобных интерпретаторов) и имеет три формы:

devalias – показывает список определенных алиасов устройств;

devalias ALIAS – показывает полный путь к устройству, доступному по указанному псевдониму;

devalias ALIAS ПУТЬ_К_УСТРОЙСТВУ – определяет новый псевдоним для указанного устройства.

Поведение команды nvramrc очень напоминает файл .bash_rc или другой подобный, выполняемый при старте сис-

темы или пользовательской сессии. Все команды, хранимые в nvramrc, записываются в текстовой форме. Причем может быть использован почти весь набор команд, доступный из командной оболочки. Исключений немного, это команды: banner, boot, nvedit, password, reset, setenv security-mode.

Для создания псевдонима устройства, доступного после перезагрузки, можно воспользоваться командой:

```
nvalias ALIAS ПУТЬ_К_УСТРОЙСТВУ
```

Действие команды аналогично devalias, что легко проверить. Набрав nvedit, мы увидим:

```
devalias ALIAS ПУТЬ_К_УСТРОЙСТВУ
```

Как нетрудно догадаться, nvedit – встроенный редактор, с помощью которого можно управлять nvramrc. Синтаксис немного похож на синтаксис Emacs. Подробное описание смотрите в документации, отмечу лишь, что выйти из редактора можно по <Ctrl>+<C>. Нужно помнить, что nvedit работает только с временным буфером. Чтобы изменения вступили в силу, после редактирования нужно выполнить команду nvstore. Проверить работу команд в буфере можно, выполнив nvrun.

В nvramrc можно также определять свои программы, как показано в примере:

```
ok nvedit
0: : hello ( -- )
1: ." Hello, world. " cr
2: ;
3: ^-C
ok nvstore
ok setenv use-nvramrc? true
ok reset
  ....
ok hello
```

```
Hello, world.
```

Понятно, что напрограммировать в nvramrc можно многое, но я в своей работе ни разу этот функционал не использовал. Похоже, он бывает больше полезен разработчикам и сервисным инженерам, которым приходится диагностировать проблемы в работе оборудования.

От себя добавлю лишь, что отключить использование nvramrc можно командой:

```
ok setenv use-nvramrc? false
```

Теперь мы знаем, что такое адресация и псевдонимы устройств, но не знаем, что с ними делать. Все просто.

Работа с устройствами

В терминологии OBP все устройства называются нодами. Конечные устройства (которые не имеют «потомков») называются «листьями» – leaf. Обычно это и есть «настоящие устройства», а не контроллеры, шины и другие связующие звенья. Каждая нода может предоставлять о себе следующую информацию:

свойства – структура данных, описывающая устройство;

методы – набор команд, доступных при работе с этим устройством;

данные – значения, используемые при инициализации и дальнейшей работе с устройством.

Существуют стандарты на название и наличие свойств и методов в драйверах устройств. Некоторые свойства и методы должны обязательно поддерживаться драйвером устройства, поддержка других – рекомендована. Что-то производители «железа» добавляют самостоятельно.

При работе с OBP в каждый момент времени у нас есть так называемое текущее устройство – current node.

Мы можем выбирать текущее устройство командой dev с параметром, где параметром может быть:

- полное имя устройства;
- неполное имя устройства. В таком случае среди всего дерева устройств-потомков ищется совпадающая по имени нода;
- «..» и «/» – две точки и слеш ведут себя совсем как в файловой системе и обозначают, соответственно, выбор родительского устройства и корень всех устройств – саму машину.

Чтобы интерфейс стал совсем узнаваемым – используются команды ls и pwd, поведение которых такое же, как в любой UNIX-подобной файловой системе. Они показывают, соответственно, «список потомков» и «текущее устройство».

Более того, во многих реализациях OBP для команды dev используется алиас cd – наверно, чтобы системные администраторы чувствовали себя «совсем как дома».

Вот еще полезные команды для работы с устройствами:

ok device-end – показывает список всех «листьев» «дерева»;

ok show-devs – показывает список всех устройств «дерева»;

ok .properties – показывает различные свойства устройства. Например, производитель, модель и текущие параметры сетевой карты;

ok words – показывает имена методов, применимые к указанному устройству;

ok see WORDNAME – показывает, что означает слово FORTH. Например, из каких команд состоит указанная программа;

ok unselect-dev – делает текущим предыдущее устройство или корень. Подобно cd $OLDPWD в bash.

Каждому устройству рекомендуется иметь работающий метод selftest. Он вызывается командой test и используется для диагностики. Как несложно догадаться, метод должен возвращать сообщение об обнаруженных проблемах в устройстве или не выводить ничего в случае корректной работы. Некоторые несознательные драйверы все же выводят сообщение об успешно проведенных тестах. Славятся подобным поведением драйверы сетевых карт. Если метод selftest не описан – система выведет сообщение об ошибке.

Команда test-all вызовет test для всех устройств в системе.

Кроме команды test, применимой, в принципе, ко всем устройствам, пользователю доступны еще несколько команд диагностики. Они различаются по типам проверяемых устройств и по типу предоставляемой информации. Все команды простые, не вижу смысла заострять внимание на их описании – смотрите документацию к своей версии OBP.

Если в процессе работы вы забыли название или синтаксис команд – всегда на помощь придет help:

ok help – выдаст список категорий помощи;

ok help КАТЕГОРИЯ – покажет краткое описание всех команд указанной категории. Категория определяется только по первому слову в названии;

ok help КОМАНДА – покажет справочную информацию о конкретной команде.

К сожалению, help доступен не для всех команд. Официальная причина – команд слишком много, и справка доступна лишь для самых популярных. Похоже на правду, если учесть ограниченный объем NVRAM.

Для получения помощи в OBP также можно использовать команду sifting:

ok sifting ARG – выведет все команды, которые содержат последовательность ARG.

```
ok sifting boot
```

```
network-boot-arguments(0x11bd) boot(0x10a2) auto-boot-
timeout(0x1075)

auto-boot?(0x1074) boot-command(0x1073) boot-file(0x1070)
boot-device(0x106f)

/openprom/client-services:boot(0x120d)
```

Конфигурация системы

Кроме набора команд и дерева устройств, каждая система имеет ряд настраиваемых параметров конфигурации. На один из них мы уже обращали внимание – use-nvramrc?.

Вопросительный знак в конце имени переменной значит, что значений может быть два: false или true. Значения остальных переменных – текстовые. Пожалуй, исключение составляет oem-logo – логотип, отображаемый командой banner (часто – при загрузке системы).

Логотип – это массив пикселей 64x64, поменять его проще всего командой eeprom из ОС.

Можно и средствами OBP, немного попрограммировав на FORTH или вбивая массив пикселей руками. В документации есть пример.

В основном вся работа с переменными производится с помощью 5 команд:

printenv [VARIABLE] – показывает значение одной переменной, если указана, или весь список имен и значений – в противном случае;

setenv [VARIABLE] [VALUE] – присваивает указанной переменной заданное значение. Часто вступления изменений в силу потребуется reset системы;

set-default [VARIABLE] – сбрасывает переменную в значение по умолчанию;

set-defaults – присваивает всем переменным значения по умолчанию;

password – присваивает пароль на управление системой.

В Solaris присутствует команда eeprom, которая позволяет менять некоторые переменные OBP. Самые ленивые администраторы переставляют ОС, не подключаясь к консоли – лишь используя eeprom и reboot с аргументами.

Уделим немного внимания встроенным средствам безопасности. OBP может работать в трех режимах безопасности (значения переменной security-mode):

full – все команды, кроме go, будут требовать ввода пароля;

command – все команды, кроме boot и go, будут требовать ввода пароля. Причем команда boot с аргументами (попытка загрузиться с устройства не по умолчанию) тоже запросит пароль;

none – значение по умолчанию – пароль не будет требоваться в любом случае.

Не удержусь от напоминания, что следует быть внимательным при назначении режима безопасности и при смене пароля – сбросить его своими силами вряд ли получится – придется вызывать сервис-инженера.

Ряд переменных отвечает за параметры ввода-вывода OBP – их конфигурацию называют еще «управление консолью»:

- input-device;
- output-device;
- screen-#columns;
- screen-#rows.

За что отвечают эти настройки – понятно из названия. Изменять их следует внимательно – можно «потерять консоль», что не светит ничем хорошим. В случае недоступности ввода или вывода после перезагрузки по питанию придется искать консоль на fall-back устройствах.

Основная задача системного администратора в OBP – загрузить систему. За поведение OBP в момент загрузки отвечают несколько переменных.

Во-первых, значение переменной auto-boot? говорит нам о том, будет ли система пытаться загрузиться при включении. Если да, то будет проверяться переменная boot-command, значение по умолчанию которой – boot.

Далее проверяется переменная diagnostic-mode?.

Если значение равно false, система будет пытаться загрузиться с устройств, перечисленных в переменной boot-device и искать там файл boot-file для запуска.

В противном случае процедура загрузки системы усложнится. Сначала будет запущен selftest в порядке, зависящем от переменной diag-level. Далее может последовать вывод дополнительной информации о статусе системы – зависит от реализации. Последнее отличие – для загрузки будут использованы другие переменные: diag-device и diag-file.

Нетрудно догадаться, что переменная boot-file – не что иное, как ядро операционной системы. По умолчанию система будет пытаться загрузить Solaris из файла kernel/unix, которому также можно передать параметры.

Подробное рассмотрение процесса загрузки и запуска программ в различных режимах выходит за рамки данной статьи наряду с возможностями отладки (debugging) и программирования на FORTH.

В повседневной работе системный администратор обычно сталкивается с задачами определения и конфигурации устройств, инсталляции и загрузки ОС.

После чего OBP на настроенной машине используется редко.

Работа с OBP хорошо документирована, информацию найти легко для всех, даже не самых простых, задач. EOF

1. http://wikipedia.org.
2. http://docs.sun.com.
3. OpenBoot™ 4.x Command Reference Manual, Sun P/N: 816-1177-10.
4. Writing FCode 3.x Programs, Sun P/N: 806-1379-10.
5. Working with the Openboot – http://tldp.org/HOWTO/SPARC-HOWTO-14.html.
6. Questions and answers on OpenBoot – http://www.itworld.com/print/34644.
7. Справочное руководство по ППЗУ OpenBoot PROM (OBP) – http://www.gentoo.org/doc/ru/gentoo-sparc-obpreference.xml.
8. TN105 – Sun OpenBoot Prom – http://www.marchansen.com/tn105.
9. Sun Advanced Lights Out Manager 1.6 (ALOM) – http://www.sun.com/servers/alom.html.

Множественные уязвимости в Wireshark

Программа: Wireshark версии до 1.2.1.
Опасность: Средняя.
Наличие эксплоита: Нет.
Описание: 1. Уязвимость существует из-за ошибки индексации массива в диссекторе IPMI. Удаленный пользователь может с помощью специально сформированного сетевого пакета вызвать отказ в обслуживании приложения. Уязвимости подвержена версия 1.2.0.

2. Уязвимость существует из-за ошибки в диссекторах Bluetooth L2CAP, RADIUS, MIOP и sFlow. Удаленный пользователь может с помощью специально сформированного сетевого пакета вызвать отказ в обслуживании приложения. Уязвимости подвержена версия 1.2.0.

3. Уязвимость существует из-за ошибки в диссекторе AFS. Удаленный пользователь может с помощью специально сформированного сетевого пакета вызвать отказ в обслуживании приложения. Уязвимости подвержены версии с 0.9.2 по 1.2.0.

4. Уязвимость существует из-за ошибки в Infiniband диссекторе. Удаленный пользователь может с помощью специально сформированного сетевого пакета вызвать отказ в обслуживании приложения. Уязвимости подвержены версии с 1.0.6 по 1.2.0.
URL производителя: www.wireshark.org.
Решение: Установите последнюю версию 1.2.1 с сайта производителя.

Переполнение буфера в реализации SHA2 в NetBSD

Программа: NetBSD 4.0.
Опасность: Низкая.
Наличие эксплоита: Нет.
Описание: Уязвимость существует из-за ошибки проверки границ данных в реализации SHA2. Удаленный пользователь может вызвать четырех- или восьмибайтное переполнение буфера, что может привести к переполнению динамической памяти в библиотеке libssh и к переполнению стека в pkg_install.
URL производителя: www.netbsd.org/releases/formal-4/NetBSD-4.0.html.
Решение: Установите исправление из CVS-репозитория производителя.

Отказ в обслуживании в IP Filter в Sun Solaris

Программа: Sun Solaris 10.
Опасность: Средняя.
Наличие эксплоита: Нет.
Описание: Уязвимость существует из-за неизвестной ошибки в Solaris IP Filter. Удаленный пользователь может вызвать панику ядра системы.
URL производителя: www.sun.com.
Решение: Установите исправление с сайта производителя.

Уязвимости в eCryptfs в ядре Linux

Программа: Linux kernel 2.6.30.3, возможно, другие версии.
Опасность: Низкая.
Наличие эксплоита: Нет.
Описание: 1. Уязвимость существует из-за ошибки проверки границ данных при обработке tag 11-пакетов. Удаленный пользователь может с помощью eCryptfs-файла, содержащего специально сформированную секцию метаданных, вызвать переполнение стека и выполнить произвольный код на целевой системе. Для успешной эксплуатации уязвимости злоумышленник должен обманом заставить пользователя открыть специально сформированный eCryptfs-файл.

2. Уязвимость существует из-за ошибки проверки границ данных в функции parse_tag_3_packet(). Удаленный пользователь может с помощью tag 3-пакета, содержащего слишком большой размер ключа шифрования, вызвать переполнение динамической памяти и выполнить произвольный код на целевой системе. Для успешной эксплуатации уязвимости злоумышленник должен обманом заставить пользователя открыть специально сформированный eCryptfs-файл.
URL производителя: www.kernel.org.
Решение: Установите исправление из GIT-репозитория производителя.

Отказ в обслуживании в MySQL

Программа: MySQL 5.0.83 и более ранние версии.
Опасность: Низкая.
Наличие эксплоита: Нет.
Описание: Уязвимость существует из-за ошибки форматной строки в функции dispatch_command() в файле sql_parse.cc. Удаленный пользователь может с помощью специально сформированных COM_CREATE_DB- или COM_DROP_DB-запросов аварийно завершить работу приложения.
URL производителя: www.mysql.com.
Решение: Установите последнюю версию 5.1.36 с сайта производителя.

Обход ограничений безопасности в Microsoft ISA Server 2006

Программа: Microsoft ISA Server 2006.
Опасность: Средняя.
Наличие эксплоита: Нет.
Описание: Уязвимость существует из-за ошибки при использовании Radius OTP (One Time Password)-аутентификации. Удаленный неавторизованный пользователь, знающий имя учетной записи администратора, может получить полный контроль над целевой системой.
URL производителя: www.microsoft.com.
Решение: Установите исправление с сайта производителя.

Составил Александр Антипов

Визитка

СЕРГЕЙ ЯРЕМЧУК,
наш постоянный автор

CrossBow

Сетевые технологии OpenSolaris

В OpenSolaris 2009.06 анонсирована поддержка технологии виртуальных сетей CrossBow, с возможностями которой и познакомимся сегодня

Мощности современных систем уже давно достигли такого уровня, что на одном компьютере могут без проблем работать несколько систем. Поэтому не удивительно, что темой номер один в ИТ-публикациях последних лет является виртуализация. Часто под термином «виртуализация» подразумевают виртуальные системы, реже говорят о приложениях. С реализацией нового сетевого стека в Solaris 10, а затем и в OpenSolaris 2009.06 в этих системах стала доступна технология сетевой виртуализации (Network Virtualization), позволяющей скомбинировать все сетевые ресурсы системы в единую виртуальную сеть, имеющую один центр управления. Такой подход упрощает администрирование, администратор получает вместо разрозненной целостную структуру, которая легко масштабируется, настройки проще переносятся в другую систему, с минимумом переделок и без потери функциональности. Виртуальные сети могут быть внешними (например, VLAN) или внутренними, по сути являющимися сетью в отдельной системе (network in a box). Проект CrossBow [1] позволяет реализовать в одном компьютере, даже имеющем одну сетевую карту, целые внутренние виртуальные сети с коммутаторами.

Возможности CrossBow

Возможности CrossBow заложены в трех основных функциях:

VNIC (Virtualized Network Interface) – виртуализированные сетевые интерфейсы, которые настраиваются поверх физических, предоставляя аналогичные возможности;

IP instances – выделенные копии TCP/IP-стека для выполнения задачи в отдельной зоне, с возможностью использования своего IP-адреса, таблицы маршрутизации, управления QoS, ограничения скорости передачи между зонами и контроля;

Bandwidth management and flow control – управление пропускной способностью и потоком для каждого VNIC-интерфейса.

VNIC-устройство создается при помощи специального драйвера псевдоустройства Nemo/GLDv3 [2], работающего на так называемом MAC-уровне, который находится между драйвером сетевого адаптера и стеком. Все клиенты, обращающиеся через MAC-уровень, получают доступ к нужному устройству, при этом каждому назначаются аппаратные ресурсы, полоса пропускания, приоритет, потоки и так далее. Один физический интерфейс может иметь несколько VNIC, каждый VNIC при создании получает собственный MAC-адрес. Для системных утилит VNIC выглядят, как реальные сетевые карты, и могут быть назначены зонам и гостевым системам. Всего можно создать 899 VNIC (1-899), номера 900-999 зарезервированы для подсистем Xen.

Максимальное количество IP Instances соответствует возможному количеству неглобальных зон – 8191. Обмен данными между VNIC проходит на системном уровне, не затрагивая физический интерфейс.

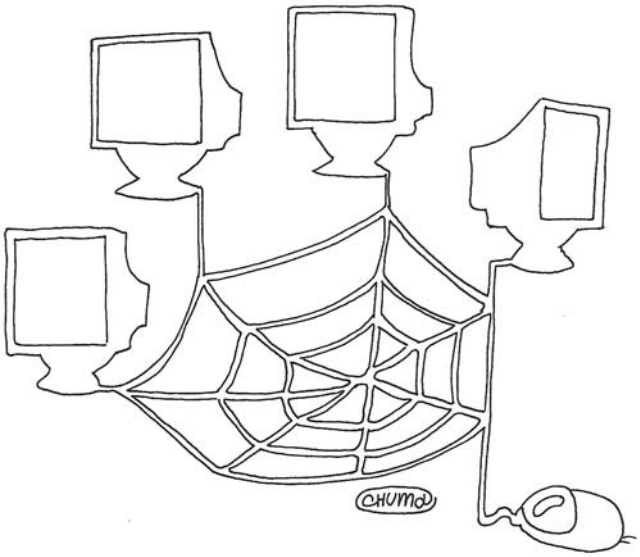
Кроме виртуальных адаптеров CrossBow позволяет создавать VLAN со всеми возможностями для его управления и виртуальный коммутатор Etherstub, при помощи которого можно связывать различные VNIC в сеть. По сути Etherstub представляет собой VNIC, которому нельзя присвоить IP-адрес.

CrossBow может быть использован для настройки системы и сетевых сервисов, изоляции зон Solaris и повышения безопасности. Например, атака на один из сервисов, работающих на виртуальном интерфейсе, будет иметь влияние только на атакуемый сервис, на остальные зоны она не распространится.

Создание виртуальной сети

Управление Crossbow производится при помощи утилиты dladm, для настройки полосы пропускания, приоритета трафика используется flowadm. Параметры dladm просты и понятны. Каждая состоит из двух частей: в первой заложено действие, во второй – объект, на который оно направлено. Так, например, для просмотра информации используется группа команд show-*, создания create-*, удаления – delete-*. Поэтому освоиться в них очень легко.

Для начала получим список datalink идентификаторов сетевых устройств:



```
# dladm show-link
```

```
LINK        CLASS     MTU    STATE    OVER
e1000g0     phys      1500   up       --
pcn0        phys      1500   unknown  --
```

Поле CLASS покажет класс устройства, который может принимать одно из четырех значений – phys, aggr, vlan и vnic. В данном случае это физическое устройство.

Другие команды, начинающиеся на show, покажут: show-phys (физические устройства), show-ether (Ethernet-устройства), show-wifi, show-vlan и так далее. В последних версиях OpenSolaris в dladm появилась подкоманда rename-link, при помощи которой можно изменить data-link и имя устройства на более удобное или единое, чтобы затем использовать в скриптах:

```
# dladm rename-link e1000g0 eth0
```

Виртуальный интерфейс создается при помощи подкоманды create-vnic в качестве параметра, принимающего имя интерфейса и присваиваемого номера vnic. В качестве имени интерфейса может выступать название физического устройства или виртуального коммутатора. Для примера создадим по одному VNIC для каждого физического устройства:

```
# dladm create-vnic -l e1000g0 vnic1
# dladm create-vnic -l pcn0 vnic2
```

Для создания виртуального коммутатора достаточно указать его имя:

```
# dladm create-etherstub etherstub0
# dladm create-etherstub etherstub1
```

Теперь создадим VNIC поверх виртуального коммутатора:

```
# dladm create-vnic -l etherstub0 vnic3
# dladm create-vnic -l etherstub0 vnic4
```

Для etherstub1 по аналогии. По умолчанию MAC-адрес генерируется автоматически, но при необходимости его можно указать вручную при помощи параметра -m, принадлежность к VLAN (-v) и ряд других параметров. Смотрим, что получилось:

```
# dladm show-link
```

```
LINK        CLASS     MTU    STATE    OVER
e1000g0     phys      1500   up       --
pcn0        phys      1500   unknown  --
vnic1       vnic      1500   up       e1000g0
vnic2       vnic      1500   up       pcn0
etherstub0  etherstub 9000   unknown  --
vnic3       vnic      9000   up       etherstub0
vnic4       vnic      9000   up       etherstub0
```

```
# dladm show-vnic
```

```
LINK    OVER        SPEED  MACADDRESS        MACADDRTYPE  VID
vnic0   e1000g0     1000   2:8:20:e5:e4:af   random       0
vnic1   etherstub0  0      2:8:20:b7:c8:41   random       0
vnic2   etherstub0  0      2:8:20:98:32:e6   random       0
vnic3   etherstub1  0      2:8:20:83:d6:32   random       0
vnic4   etherstub1  0      2:8:20:1c:d4:9e   random       0
vnic6   pcn0        0      2:8:20:b2:dd:fa   random       0
vnic7   etherstub0  0      2:8:20:87:d:45    random       0
```

Список параметров и их значения, установленные для каналов, можно получить при помощи команды dladm show-linkprop. Выведем для одного из них:

```
# dladm show-linkprop vnic0
```

```
LINK    PROPERTY   PERM VALUE     DEFAULT   POSSIBLE
vnic0   autopush   -w   --        --        --
vnic0   zone       rw   --        --        --
vnic0   state      r-   unknown   up        up,down
vnic0   mtu        r-   1500      1500      --
vnic0   maxbw      rw   --        --        --
vnic0   cpus       rw   --        --        --
vnic0   priority   rw   high      high      low,medium,high
vnic0   tagmode    rw   vlanonly  vlanonly  normal,vlanonly
```

Столбец PROPERTY показывает свойства адаптера, установленное значение выведено в VALUE, в POSSIBLE даны возможные варианты. Чтобы указать свое значение следует использовать параметр -p в вызове команды dladm create-vnic. Например, maxbw позволяет установить максимальную скорость интерфейса, cpus – использование CPU. Поэтому полная команда на создание VNIC может выглядеть так:

```
# dladm create-vnic -l etherstub0 ↵
        -p maxbw=50,priority=high,cpus=2,3,4 vnic5
# dladm show-linkprop vnic5
```

```
…
vnic5         maxbw           rw       50         --         --
vnic5         cpus            rw    2,3,4         --         --
…
```

Интерфейсы созданы, но в выводе ifconfig они пока отсутствуют. Подключаем и присваиваем IP-адрес. Эта процедура ничем не отличается от работы с физическим устройством. Например, для интерфейса vnic1:

```
# ifconfig vnic1 plumb
# ifconfig vnic1 dhcp start
# ifconfig vnic1
```

Управление потоком

В свойствах VNIC можно задать общие установки, характерные для обычной сетевой карты, например, указать определенную скорость интерфейса. Управление потоком дает возможность устанавливать пропускную способность и ресурсы для конкретного сервиса, протокола, номера порта или виртуальной машины. Установки управления потоком осуществляются при помощи утилиты flowadm. С ее помощью можно указать ряд атрибутов и параметров, все требования и параметры расписаны в man flowadm. Так, в правило можно добавить следующие атрибуты: локальный (local_ip) и удаленный адрес (remote_ip), локальный (local_port) и удаленный порт (remote_port), версию IP-протокола (ip_version) и ряд других. Создадим сопоставленный vnic1 поток, описывающий транспорт TCP, локальный порт 80 и присвоим ему ссылку http-1:

```
# flowadm add-flow -l vnic1 ↵
        -a transport=TCP,local_port=80 http-1
```

Второе правило будет содержать атрибуты версии IP-протокола и IP-адреса:

```
# flowadm add-flow -l vnic2 ↵
        -a ip_version=4,local_ip=10.4.0.16 v4flow
```

Кроме атрибутов, поток может принимать и параметры, некоторые из установок (пропускная способность, приоритет, привязка к CPU и т.д.) совпадают с create-vnic:

```
# flowadm set-flowprop ↵
        -p maxbw=30,priority=high,cpus=2  http-1
```

Проверяем:

```
# flowadm show-flowprop http-1
```

```
FLOW      PROPERTY     VALUE     DEFAULT     POSSIBLE
http-1    maxbw        30        --          30
http-1    priority     high      --          high
```

Теперь осталось подключить интерфейс к одной из зон Solaris (подробнее [3]):

```
# zonecfg -z zone1
```

```
zone1: No such zone configured
Use 'create' to begin configuring a new zone.
```

```
zonecfg:zone1> create

// Эксклюзивный IP
zonecfg:zone1> set ip-type=exclusive

// Добавляем сетевой интерфейс, подключим к  vnic1
zonecfg:zone1> add net
zonecfg:zone1:net> set physical=vnic1
zonecfg:zone1:net> info
```

```
net:
        address not specified
        physical: vnic0
        defrouter not specified
```

```
zonecfg:zone1:net> end
zonecfg:zone1:net> verify
zonecfg:zone1:net> commit
zonecfg:zone1:net> exit
```

Теперь зона zone1 будет использовать vnic1 и управление потока http-1.

Объединение интерфейсов

При помощи dladm очень просто физические устройства, поддерживающие GLDv3, объединить в одно логиче-

Рисунок 1. Список параметров каналов

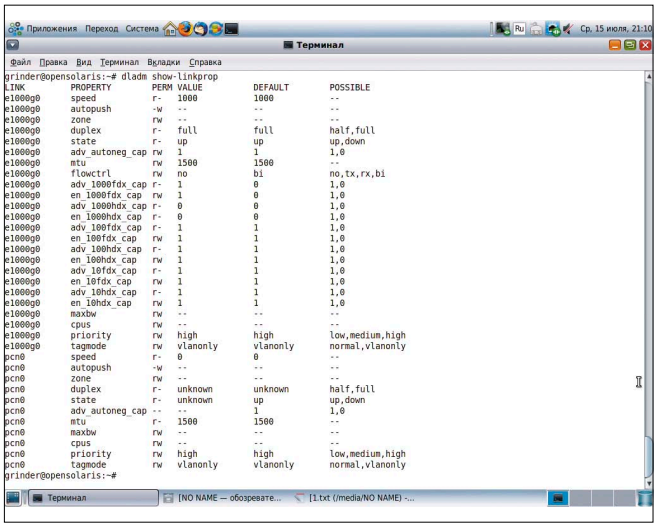
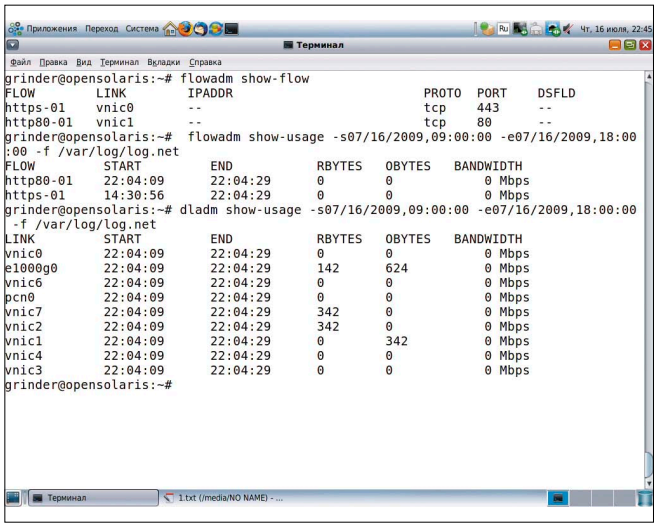


Рисунок 2. Полученная статистика



ское (link aggregations). Такая возможность востребована для возможности резервирования каналов, увеличения пропускной способности сети, балансировки нагрузки.

В случае необходимости объединения интерфейсов лучше выбрать две одинаковые сетевые карты, работающие в режиме full duplex с одной скоростью, сетевые коммутаторы должны поддерживать протокол LACP (link aggregation control protocol). Процесс достаточно прост. Останавливаем сетевые интерфейсы:

```
# ifconfig e1000g0 unplumb
# ifconfig e1000g1 unplumb
```

Объединяем интерфейсы:

```
# dladm create-aggr -l e1000g1 -l e1000g2 default0
```

Проверяем, что получилось:

```
# dladm show-aggr
# dladm show-link
```

После этого включаем интерфейс обычным образом:

```
# ifconfig default0 plumb 10.0.17.1 up
```

Далее поверх интерфейса default0 можно настраивать VLAN:

```
# dladm create-vlan -v 2 -l default0 vlan0
# dladm create-vlan -v 3 -l default0 vlan2
```

Удаление виртуальных интерфейсов

Удаляются виртуальные интерфейсы и коммутаторы при помощи команд delete-vnic и delete-etherstub. Перед удалением коммутатора следует удалить все связанные VNIC, при наличии хотя бы одного активного VNIC команда завершится с ошибкой:

```
# dladm delete-etherstub etherstub1
dladm: vnic deletion failed: link busy
```

Виртуальные сетевые интерфейсы вначале следует остановить и удалить управление потоком:

```
# dladm delete-vnic vnic1
dladm: vnic deletion failed: link still has flows
# flowadm remove-flow http-1
# ifconfig vnic1 umplumb
# dladm delete-vnic1
```

Получаем статистику

Утилиты dladm и flowadm умеют считывать статистику из внешнего файла, созданного при помощи команды acctadm.

Активируем сетевую статистику:

```
# acctadm -e extended -f /var/log/net.log net
```

Проверим:

```
# acctadm net
            Network accounting: active
            Network accounting file: /var/log/net.log
            Tracked Network resources: extended
            Untracked Network resources: none
```

Просмотр осуществляется при помощи команды flowadm show-usage, в качестве параметра принимающей созданный файл:

```
# flowadm show-usage -f /var/log/net.log
```

Дополнительные параметры позволяют отобрать статистику по дате, времени и потоку. Получим список дат из файла.

```
# flowadm show-usage -d -f /var/log/net.log
07/16/2009
```

Теперь просмотрим статистику за рабочий день (09:00-18:00):

```
# flowadm show-usage -s07/16/2009,09:00:00 ↵
        -e07/16/2009,18:00:00 -f /var/log/log.net
FLOW     START      END        RBYTES   OBYTES   BANDWIDTH
http-1   22:04:09   22:04:29   6586     896      1 Mbps
```

Заменив в вызове команду flowadm на dladm, узнаем статистику по виртуальным интерфейсам:

```
# dladm show-usage  -f /var/log/log.net
LINK     DURATION IPACKETS RBYTES OPACKETS OBYTES BANDWIDTH
vnic0    2678     10       420    21       882    1 Mbps
e1000g0  2678     55       3530   112      9841   2 Mbps
```

***

CrossBow в OpenSolaris – гибкий и простой инструмент для системного администратора, позволяющий управлять сетевыми настройками. Параметры для отдельного сервиса можно выставить индивидуально, при любых изменениях созданная структура легко переносится. EOF

1. Страница проекта CrossBow – http://ru.opensolaris.org/os/project/crossbow.
2. Страница проекта Nemo - http://ru.opensolaris.org/os/project/nemo.
3. Руководство по системному администрированию: контейнеры в Solaris – управление ресурсами и зонами – http://dlc.sun.com/pdf/820-2979/820-2979.pdf.
4. Man Pages – dladm, flowadm, acctadm, zonecfg, ifconfig.

Визитка

ИВАН КОРОБКО, сертифицированный специалист MCP, автор более 50 статей и двух книг. Занимается созданием различных приложений для Active Directory

Управление корзиной

Новый сервис в Active Directory

В Windows Server 2008 R2 реализовано несколько очень важных нововведений. Одно из них — корзина для восстановления учетных записей пользователей в Active Directory

Наряду с новой версией DFS, расширением схемы в Active Directory и многим другим в Windows Server 2008 R2, бета-версия которого уже доступна на сайте компании Microsoft [1], не только системный администратор, но и программист найдет один очень интересный сервис, с помощью которого можно восстанавливать удаленные объекты из каталога Active Directory. Создание такого сервиса потребовало от программистов Microsoft серьезной доработки основного инструмента управления этим сервисом – программной оболочки PowerShell и создания модуля для управления каталогом Active Directory (Windows PowerShell Integrated Scripting Environment). С его помощью реализовано управление учетными записями пользователей, групп, контейнеров, корзиной и другими объектами. По умолчанию этот сервис отключен.

Для включения этого сервиса необходимо выполнение следующих условий:

- Операционная система Windows Server 2008 R2 (Standard, Enterprise, DataCenter).
- Домен, функционирующий в режиме Windows Server 2008 R2.
- Windows PowerShell Integrated Scripting Environment (ISE).
- .NET Framework 3.5.1. Устанавливается вместе с операционной системой Windows Server 2008 R2. Необходим для работы Windows PowerShell ISE.

Активировать сервис можно из операционной системы семейства Windows Server 2008 R2 или Windows 7.

Установка PowerShell

Программное управление корзиной (Recycle Bin) и каталогом Active Directory в целом осуществляется с помощью модуля PowerShell [2] для управления Active Directory. В комплект Windows Server 2008 R2 входит Windows PowerShell Integrated Scripting Environment, в который включен этот модуль. По умолчанию PowerShell ISE не установлен.

Для его установки необходимо войти в оснастку Server Manager и в разделе Features (см. рис. 1) вызвать список доступных компонентов, нажав на кнопку Add Features. В появившемся окне необходимо в списке доступных для установки сервисов найти Windows PowerShell Integrated Scripting Environment (ISE) и установить флажок напротив него. Затем нажать на кнопку Next и, отвечая на вопросы мастера, установить выбранный компонент.

После завершения процесса установки приложения в папке %SystemRoot%\system32\WindowsPowerShell\v1.0\Modules будут расположены дополнительные модули. В частности, в подпапке ActiveDirectory находится модуль управления объектами каталога Active Directory. Привязка модуля к оболочке осуществляется с помощью команды:

```
%SystemRoot%\system32\WindowsPowerShell\v1.0\ ↵
        powershell.exe -NoExit -ImportSystemModule
```

По умолчанию выполнение сценариев в PowerShell отключено, поэтому попытка импортировать нужный модуль с установленным по умолчанию уровнем доступа не увенчается успехом.

Существует четыре уровня безопасности запуска сценариев:

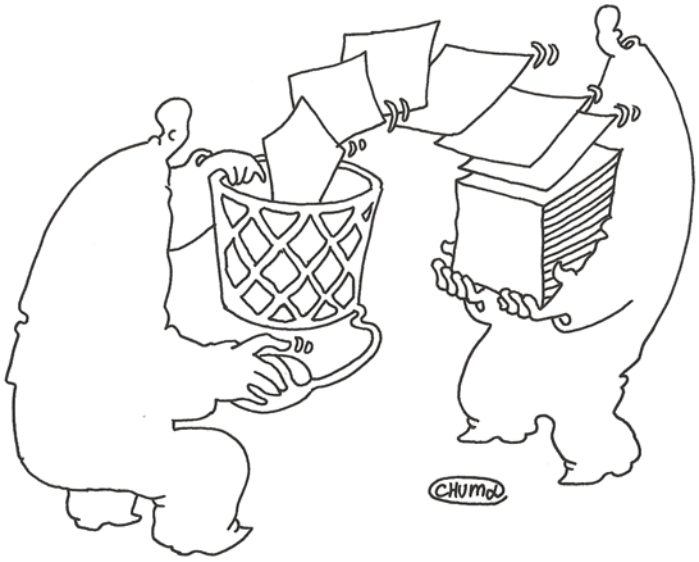
AllSigned – все файлы, в том числе и на локальной машине, содержащие сценарии на языке PowerShell, должны иметь цифровую подпись. При запуске файла оболочка задаст вопрос о том, доверяете ли вы данному издателю и можно ли доверять в дальнейшем файлам с этой подписью.

RemoteSigned – все сценарии, находящиеся в сети, должны быть подписаны. Файлы, запускаемые с локальной машины, могут не иметь цифровой подписи.

Restricted (по умолчанию) – выполнение сценариев запрещено.

Unrestricted – все сценарии, запускаемые с локального диска или из сети, могут не иметь цифровой подписи. Запуск файлов из сети сопровождается соответствующим предупреждением. Для его подавления необходимо в свойствах файла выбрать Unblock (разблокировать).

По умолчанию установлен режим Restricted, позволяющий работать с консолью только в интерактивном режиме.



Уровень безопасности задается с помощью параметра реестра ExecutionPolicy. Значение параметра соответствует названию уровня безопасности (см. листинг 1) или командлета Set-ExecutionPolicy, аргументом которого является одно из перечисленных в списке значений (см. рис. 2).

Листинг 1. Настройка параметра безопасности PowerShell по умолчанию

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE/SOFTWARE/Microsoft/PowerShell1/ ↵
       Shell/Ids/Microsoft.PowerShell]
"ExecutionPolicy"="Restricted"
```

Сценарий, подключающий Integrated Scripting Environment (ISE), запускается каждый раз при запуске оболочки PowerShell. На серверах рекомендуется использовать уровень безопасности AllSigned.

Управление режимом функционирования домена

Чтобы активировать новые функции, реализованные в домене, необходимо установить (обновить) новую версию операционной системы на всех контроллерах домена, в данном случае Windows Server 2008 R2, а затем изменить режим функционирования леса на Windows 2008 R2.

Для смены режима функционирования можно воспользоваться одним из способов:

- с помощью командлета Set-ADForestMode в Power Shell ISE;
- с помощью стандартной оснастки.

Изменение режима с помощью PowerShell

Для изменения режима необходимо запустить PowerShell с модулем управления каталогом Active Directory. При выполнении этих условий будет доступен командлет Set-ADForestMode, имеющий следующий синтаксис:

```
Set-ADForestMode -Identity <ADForest> -ForestMode ↵
        <ADForestMode>
```

где ADForest – DNS-имя домена, а ADForestMode – режим работы леса. В данном случае Windows2008R2Forest (см. рис. 3).

Рисунок 1. Установка PowerShell ISE

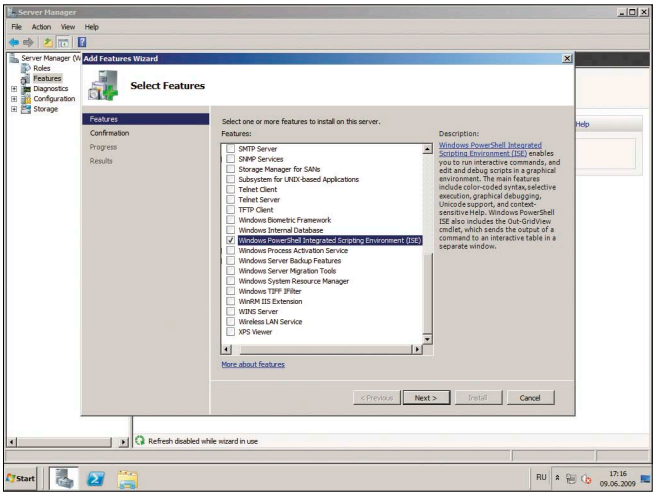
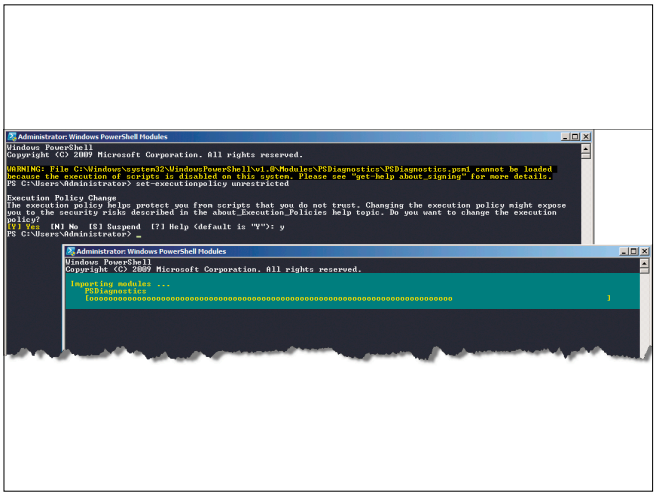


Рисунок 2. Запуск модуля для Active Directory



Замечание: переход леса на новый уровень функционирования необратим.

Изменение режима с помощью графического интерфейса

Для смены режима можно воспользоваться одной из оснасток управления каталогом: Active Directory Users and Computer или Active Directory Domain and Trusts. В появившейся оснастке необходимо вызвать контекстное меню домена и выбрать пункт Raise Domain Functional Level. В выведенном на экран диалогом окне необходимо выбрать нужный уровень домена, например Windows Server 2008 R2, и нажать «Изменить». После завершения работы мастера необходимо перезагрузить контроллер домена.

Включение Recycle Bin

Для активации корзины используется командлет Enable-ADOptionalFeature, имеющий три атрибута (см. рис. 5):

Identity – значением параметра является составной путь CN=Recycle Bin Feature,CN=Optional Features, CN=Directory Service,CN=Windows NT,CN=Services,CN=Configuration, DC=tasmania,DC=ru в домене tasmania.ru.

Scope – область действия корзины. Значение параметра Scope принимает один из трех параметров: Unknown, Domain, ForestOrConfigurationSet. Если домен в лесу один, то необходимо указать наибольшую из областей по смыслу, а именно лес – ForestOrConfigurationSet. Если в качестве области будет указан domain, то при выполнении командлета в этом случае будет выведено сообщение об ошибке.

Target – DNS-имя домена или леса в зависимости от области применения. В данном случае tasmania.ru.

Полный список доступных в модуле командлетов приведен в [2].

Анатомия удаленного объекта

Удаление объекта в каталоге Active Directory осуществляется традиционным образом: с помощью контекстного меню объекта необходимо выбрать пункт Delete и подтвердить выполнение желаемой операции в появившемся окне.

После включения корзины объект попадает в каталог CN=Deleted Objects,DC=tasmania,DC=ru. На рис. 6 приведен пример удаленной группы test. При удалении учетной

Рисунок 3. Изменение уровня функционирования леса

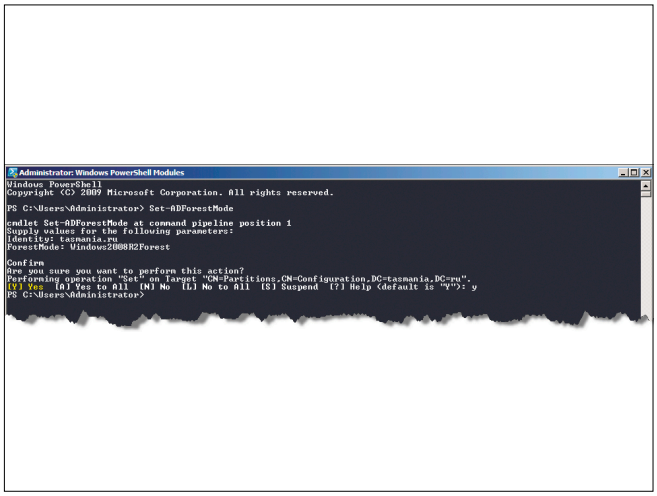


Рисунок 4. Изменение уровня функционирования домена

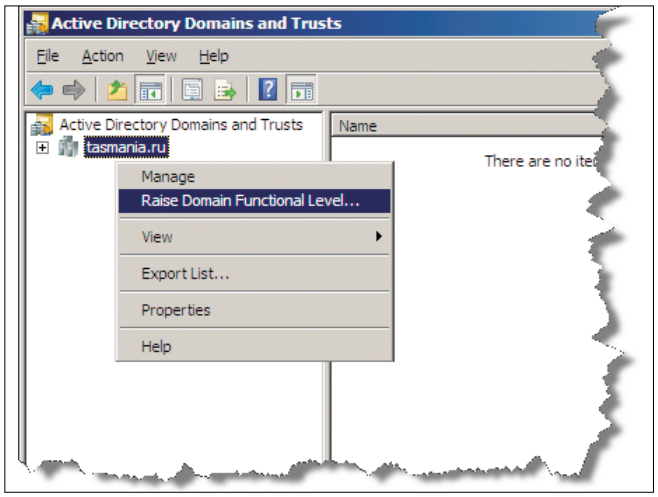


Рисунок 5. Включение корзины в Active Directory

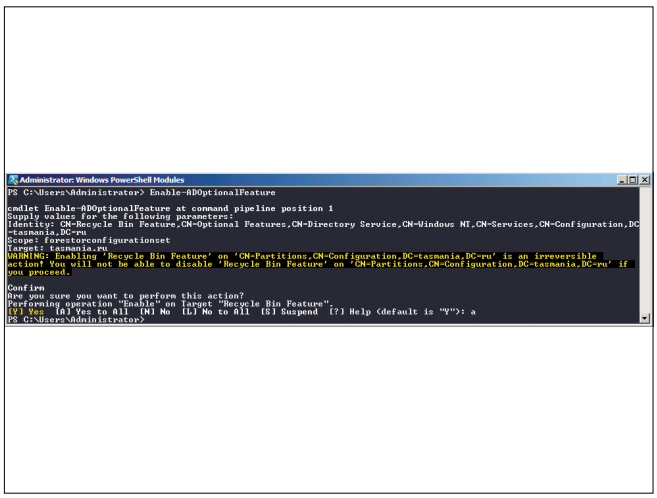
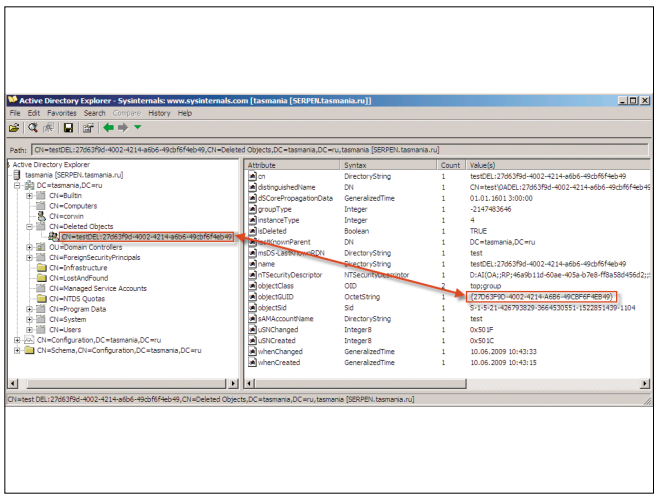


Рисунок 6. Удаленный в корзину объект Active Directory



записи со свойствами объекта происходят следующие преобразования:

- к имени объекта добавляется DEL:xxxxxxxx-xxxx-xxxx-xxxxxxxxxxxx (см. рис. 6), где xxxxxxxx-xxxx-xxxx-xxxxxxxxxxxx – GUID объекта;
- параметру isDelete присваивается значение TRUE. С помощью этого атрибута помечаются удаленные объекты;
- первоначальное местоположение объекта является значением атрибута lastKnownParent.

Все остальные параметры остаются без изменения.

Управление объектами корзины

Осуществляется с помощью PowerShell или какой-либо графической оболочки, например, ADExplorer [3], Softerra LDAP Browser [4] или Softerra LDAP Administrator [5]. В рамках этой статьи уделим внимание управлению объектов только с помощью PowerShell. Управление корзиной подразумевает просмотр содержимого и восстановление удаленных объектов.

Просмотр содержимого корзины

После включения корзины в Active Directory появляется объект CN=Deleted Objects,DC=tasmania,DC=ru. Как видно из составного пути, он расположен в корне домена. Для просмотра содержимого указанного объекта используется командлет Get-ADObject (см. рис. 7), который имеет два атрибута:

SearchBase – значением этого ключа является составной путь к контейнеру Deleted Objects, который располагается в корневом каталоге пространства defaultNamingContext. Для домена tasmania.ru путь к контейнеру CN=Deleted Objects,dc=tasmania,DC=ru.

IncludeDeletedobjects – присутствие ключа указывает на необходимость вывести объекты, атрибут которых isDeleted=TRUE.

Filter – обязательный ключ. С его помощью задаются критерии поиска. Если необходимо найти все объекты, то в качестве значения необходимо указать звездочку «*».

ldapFilter – применяется, если необходимо использовать традиционный фильтр, например (&(objectClass=group)). Правила написания запросов для поиска в Active Directory см. в [6].

В листинге 2 приведен пример вывода всех учетных записей, имеющих атрибут isDeleted=TRUE. Корзина также имеет этот атрибут, поэтому первой записью в числе найденных будет учетная запись корзины.

Листинг 2. Вывод списка удаленных пользователей

```
Get-ADObject -SearchBase "CN=Deleted Objects,DC=tasmania, ↵
        DC=ru" -includeDeletedObjects -filter * | ↵
        format-table -autosize -property name, ↵
        distinguishedname
```

В приведенном примере для удобства восприятия информации использован форматирующий вывод командлет format-table, располагающий выводимые данные в таблице.

С помощью ключа autosize осуществляется «укладывание» информации, а с помощью ключа property осуществляется вывод колонки name, а затем distinguishedname.

Восстановление удаленных объектов

Восстановление объектов осуществляется с помощью совместного использования командлета Restore-ADObject. В некоторых случаях, когда необходимо восстановить группу объектов по указанным критериям, используется командлет Get-ADObject в сочетании с Restore-ADObject.

Для восстановления одиночного объекта используется Restore-ADObject. Для однозначной идентификации объекта рекомендуется указать GUID объекта – уникальное 128-битное число (см. листинг 3).

Листинг 3. Восстановление удаленного объекта по его GUID

```
Restore-ADObject -Identity 27d63f9d-4002-4214-a6b6-49cbf6f4eb49
```

Для восстановления группы объектов необходимо создать фильтр, это можно сделать двумя способами.

В первом способе используется обычный фильтр PowerShell. Для вызова этого фильтра указывают параметр ldapFilter, после которого в фигурных скобках {...} записывается критерий поиска. При его составлении используются операторы сравнения (см. таблицу 1) и логические операторы (см. таблицу 2). Критерий поиска формируется по следующему шаблону:

```
{AD_Attribute EQ_Operator 'AD_Value' LOG_Operator ...}
```

AD_Attribute – название атрибута;
EQ_operator – оператор сравнения;
AD_Value – значение атрибута, заключаемое в одинарные кавычки;
LOG_Operator – логический оператор.

В листинге 4а приведен пример поиска всех учетных записей групп и их восстановления в соответствующие папки. Эта же операция для группы объектов осуществляется с помощью двух командлетов. Командлет Get-ADObject используется для поиска объектов по указанным параметрам, а затем с помощью оператора конвейера (|) осуществляется восстановление отобранных объектов.

Листинг 4а. Восстановление группы удаленных объектов (использование параметра Filter)

```
Get-ADObject -SearchBase "CN=Deleted Objects,DC=tasmania, ↵
        DC=ru" -includeDeletedObjects -Filter ↵
        {objectClass -eq 'group'} | Restore-ADObject
```

Рассмотрим второй способ – создание фильтра. Для тех администраторов, которые сталкивались с программированием Active Directory, он будет более понятен, поскольку для него используется LDAP-фильтр, признаком которого служит ключ ldapFilter. В листинге 4б приведен аналогичный пример с использованием другого фильтра [6].

Листинг 4б. Восстановление группы удаленных объектов (использование параметра ldapFilter)

```
Get-ADObject -SearchBase "CN=Deleted Objects,DC=tasmania, ↵
        DC=ru" -includeDeletedObjects -ldapFilter ↵
        "objectClass=group" | Restore-ADObject
```

В зависимости от поставленной задачи рекомендуется применять тот или иной фильтр. Например, для создания сценария (см. листинг 5), который восстанавливает все объекты, находившиеся в какой-либо папке, лучше всего использовать первый способ, поскольку в формировании фильтра используется значение атрибута lastKnownParent – составного пути к контейнеру, в котором хранился объект до удаления.

Листинг 5. Восстановление группы объектов удаленных из указанной папки

```
Get-ADObject -SearchBase "CN=Deleted Objects,DC=tasmania, ↵
        DC=ru" -includeDeletedObjects -Filter ↵
        {lastKnownParent -eq 'OU=WorkSpace,DC=tasmania, ↵
        DC=ru'}
```

***

В последние годы Active Directory претерпевает множество значительных изменений, однако их реализация, в частности, корзина – частичная. Ее может использовать только опытный системный администратор, владеющий навыками программирования на PowerShell, который не так давно появился. Встроенный стандартный графический интерфейс для управления этими объектами отсутствует. Будем надеяться, что к выходу операционной системы в свет Microsoft исправит эти недочеты. EOF

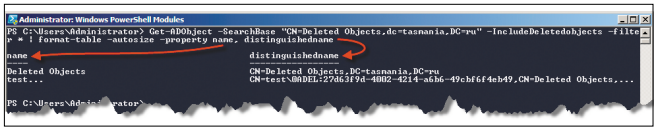
Таблица 1. Операторы сравнения в PowerShell

Оператор	Значение	Оператор	Значение
-eq	равно	-ne	не равно
-lt	меньше	-gt	больше
-le	меньше или равно	-gt	больше или равно
-contains	содержит	-not contains	не содержит

Таблица 2. Логические операторы в PowerShell

Оператор	Значение	Оператор	Значение
-and	И	-not	НЕ
-or	ИЛИ	!	НЕ

Рисунок 7. Просмотр содержимого корзины



1. Дистрибутив Release Candidate Windows Server 2008 R2 – http://www.microsoft.com/windowsserver2008/en/us/R2-Download.aspx.
2. Список командлетов PowerShell в модуле для Active Directory – http://go.microsoft.com/fwlink/?LinkID=140056.
3. Active Directory Explorer v1.2 (freeware) – http://download.sysinternals.com/Files/AdExplorer.zip.
4. Softerra Ldap Browser 2.6 (freeware) – http://www.ldapadministrator.com/download.htm.
5. Softerra Ldap Administrator (shareware) – http://www.ldapadministrator.com/download.htm.
6. Правила написания фильтров поиска – http://msdn.microsoft.com/ru-ru/library/system.directoryservices.directorysearcher.filter.aspx.

Визитка

СЕРГЕЙ ЯРЕМЧУК,
наш постоянный автор

QAD-командлеты

Простые команды вместо сложных конструкций

Quest AD PowerShell cmdlets (QAD cmdlets) разработаны Quest Software, скачать их можно со страницы http://www.quest.com/activeroles-server/arms.aspx. Командлеты вместо сложных конструкций реализуют простые команды. Чтобы получить список всех QAD-командлетов, введите:

```
PS> Get-QCommand
```

Подключимся к контроллеру домена:

```
PS> $pw = read-host "Enter password" -AsSecureString
PS> Connect-QADService -service 'domain.ru' -proxy ↵
        -ConnectionAccount 'domain\administrator' ↵
        -ConnectionPassword $pw
```

Теперь получим список пользователей и компьютеров:

```
PS> Get-QADUser
PS> Get-QADComputer
```

По сравнению с ADSI команды выглядят очень просто, хотя дополнительных параметров в команде может быть очень много. При запросе будут отображены только некоторые из свойств объектов. По умолчанию это Name, Type и DN. Поэтому свойства, которые необходимо получить, перечисляем после -IncludedProperties, все свойства объекта можно получить при помощи -Include AllProperties. Чтобы узнать информацию по отдельному пользователю и параметру, подставляем его в вызов:

```
PS> Get-QADUser -Name User -IncludeAllProperties | ↵
        Format-List *
```

Format-List требуется, чтобы вывести все полученные свойства. Список параметров объекта выводится по умолчанию при помощи команды:

```
PS> Set-QADPSSnapinSettings ↵
    -DefaultOutputPropertiesForUserObject Name,LastLogon
```

Получаем значение одного из свойств:

```
PS> (Get-QADUSer -Name "User").AccountIsDisabled
```

Узнаем, отключена ли учетная запись пользователя. Также получаем информацию о группах, например, об их членах:

```
PS> (Get-QADGroup "GroupName").members | ↵
        Get-MemberName | Export-Csv "C:\GroupMembers.csv"
```

Первую строку в этом примере можно заменить командой:

```
Get-QADGroupMember 'domain\group'
```

Также просто производятся и остальные действия. Для примера создадим новую доменную учетную запись.

```
PS> New-QADUser -name 'Ivanov' -ParentContainer ↵
        'OU=TestOU,DC=domain,DC=ru' -UserPassword 'Passw0rd'
```

Соответственно, чтобы отключить, включить или разблокировать учетную запись, используем: Disable-QADUser, Enable-QADUser и Unlock-QADUser. Командлеты, начинающиеся на Set, используются для установки и изменения параметров, их часто используют в скриптах.

Например:

```
PS> Get-QADUser -Department Sales | Set-QADUser ↵
        -ObjectAttributes @{"Department"="Product"; ↵
        "Description"="Product"}
```

Также просто создавать и новые объекты:

```
PS> New-QADObject -type OrganizationUnit ↵
        -ParentContainer domain -Name Product
```

При установке редактора PowerGUI (powergui.org) будут запрошены QAD-командлеты. Есть, конечно, в QAD минус. Так, командлеты не являются частью операционной системы и не поддерживается Microsoft, для их работы необходимо обязательное присутствие соответствующего провайдера.

Дополнительно можно отметить, что в Windows 2008 Server R2 и Windows 7 появились ADPowershell (Active Directory Module for Windows PowerShell) командлеты, имеющие аналогичный синтаксис – Get-ADDomain, Get-ADUser, New-ADObject и так далее.

Получить список всех команд можно введя:

```
Get-Command -Module ActiveDirectory
```

В Active Directory Powershell Blog (http://blogs.msdn.com/adpowershell) описана возможность использования ADPowershell в Windows 2003/2008. Но очевидно, что QAD-командлеты более универсальны. EOF

Визитка

АЛЕКСЕЙ БЕРЕЖНОЙ, системный администратор, главные направления деятельности: виртуализация и гетерогенные сети. Еще одно увлечение, помимо написания статей, – популяризация бесплатного ПО

NTI Shadow for ReadyNAS:
проводим резервное копирование данных *

Сетевое хранилище предоставляет интересные возможности для организации этого процесса

Настройка резервного копирования рабочих станций пользователей

В идеале все рабочие файлы пользователей должны храниться на сервере. К сожалению, далеко не всегда этого удается достичь на практике. Все зависит от специфики работы, привычек пользователей и других обстоятельств, которые трудно изменить в кратчайшие сроки. В связи с этим неплохо иметь инструмент, который позволил бы деликатно копировать содержимое файлов и каталогов на компьютерах пользователей в централизованное место хранения.

Благодаря наличию сетевого хранилища у нас появляется инструмент, способный реализовать данную функцию, – программа NTI Shadow for ReadyNAS. Данный продукт входит в комплект поставки сетевого хранилища и находится на прилагаемом CD в директории ...bin/shadow. Установка программы происходит достаточно просто. Запускаем файл setup.exe, принимаем лицензионное соглашение, указываем имя пользователя, название организации, нужно ли производить установку для всех пользователей или только для текущего – вот и весь процесс установки. После инсталляции появляется окно программы, и можно производить настройку резервного копирования. Так как невозможно охватить все ситуации, при которых может понадобиться теневое копирование, продемонстрируем на примере сохранения папки «Мои документы».

Итак, в основном окне программы нажимаем кнопку «Создать задание резервирования». В появившемся окне «Выбор файлов и папок» выбираем объекты для резервирования.

Дополнительно, нажав кнопку «Настройки», можно вызвать окно задания дополнительных параметров, в котором задаются фильтры по расширению для копируемых или игнорируемых файлов (см. рис. 1).

В следующем окне – «Где и когда резервировать» – указывается ресурс для хранения резервных копий (каталог на сетевом хранилище ReadyNAS) и задается расписание создания резервных копий.

В данном примере указан параметр «Сохранить изменение папки/файла в месте назначения каждый раз при сохранении их на компьютере». Преимуществом этого метода является то, что в данном случае резервирование происходит автоматически, как только файл закрывается пользователем (становится доступным другим приложениям), вне зависимости от того, является ли это изменением в старом файле или создан новый.

Для наших условий (при отсутствии выделенной должности системного администратора) это очень удобно, так как пользователям нет необходимости следить за актуальностью резервных копий или же выделять специально время, когда будет производиться резервирование, в течение которого обычно «тормозит» вся система, – в данном случае копируется только то, что появилось или изменилось.

В качестве альтернативы можно выбрать сохранение файла через определенный интервал или еженедельный бэкап в заданное время (см. рис. 2).

Далее следует указать количество предыдущих версий для сохранения. В данном примере указано число «3» (то есть сохраняются три последние версии файла). Альтернативой выбору фиксированного числа версий может быть сохранение абсолютно всех версий или отказ от сохранения предыдущих версий файла (см. рис. 3).

В заключительном окне – «Обзор задания резервирования» – будет предложено ознакомиться с параметрами вновь созданного задания. В случае необходимости можно будет вернуться назад, воспользовавшись соответствующей кнопкой, чтобы изменить свой выбор. И в самом конце программа в небольшом окошке «Начать резервирование»

* В первой части статьи (см. №7 за 2009 г.) читатели узнали о процедуре начальной установки сетевого хранилища NETGEAR ReadyNAS Pro, создании общих ресурсов и учетных записей пользователей.

предлагает либо немедленно запустить процесс резервного копирования, либо просто включить данное задание (т.е. сделать его активным).

Задание создано, теперь проверим возможность восстановления. Нажимаем кнопку «Ускоренное восстановление», перед нами появляется окно с аналогичным названием, в котором нам советуют использовать правую кнопку мыши для выбора восстановления либо в предыдущее расположение, либо в другое место. После нажатия кнопки «Открыть» мы попадаем в обычное окно Проводника Windows, в котором нам предлагают выбрать файлы для восстановления (см. рис. 4).

В случае выбора другого местоположения будет предложено выбрать, куда восстанавливать файлы, и появится окошко, в котором можно будет проследить процесс восстановления файлов. Как видно из примера, операции резервного копирования и восстановления при помощи NTI Shadow for ReadyNAS выполняются очень просто.

Настройка резервного копирования содержимого хранилища

Для обеспечения сохранности информации в случае возникновения аварийной ситуации необходима нормально функционирующая backup-система. Для решения этой задачи наше сетевое хранилище обладает соответствующим встроенным функционалом.

Для обеспечения надлежащей сохранности информации было принято решение использовать два съемных диска емкостью по 1 Тб, подключаемых по USB-интерфейсу, которые впоследствии будут выноситься за территорию предприятия. Таким образом, в случае возникновения серьезной форс-мажорной ситуации, например пожара, один USB-диск всегда будет находиться в безопасном месте. В данном случае нет смысла копировать абсолютно все содержимое нашего хранилища на резервный носитель, достаточно сохранить только файлы, содержащие критичную для бизнеса информацию.

Предполагаемый график копирования: раз в неделю выполняется полный бэкап, потом инкрементный, далее носители заменяются.

Управление процессами резервного копирования содержимого хранилища ReadyNAS, как и все остальные операции, выполняется посредством FrontView (веб-интерфейс администрирования по адресу http://_адрес_хранилища_/admin/).

Для этого перейдем в раздел Backup – Add a New Backup Job. Здесь нам будет предложено в несколько шагов создать задание по резервному копированию.

STEP 1 – Select backup source (Шаг первый – выбор ресурса для копирования). Предлагается выбрать, что именно мы собираемся копировать. Причем возможно выбрать не только каталоги на данном сетевом хранилище, но и расположенные удаленно, например на FTP-сервере (см. рис. 5).

STEP 2 – Select backup destination (Шаг второй – выбор местоположения для резервной копии). На этом этапе выбираем цель, куда будем осуществлять резервное копирование. В данном случае в качестве цели выбран USB-порт, к которому подключен жесткий диск (см. рис. 6).

STEP 3 – Choose backup schedule (Шаг третий – выбор расписания резервного копирования). В основном идет привязка к суточному и недельному графику. В нашем случае для маленькой компании этих возможностей вполне хватает, хотя для крупного предприятия может понадобиться функция планирования задач на месяц или даже на год вперед.

STEP 4 – Choose backup options (Шаг четвертый – выбор дополнительных параметров). Далее следует ряд параметров:

Schedule full backup. В ниспадающем меню предлагается выбрать «Every time», (т.е. каждый раз). Альтернативой является выбор одного из следующих пунктов: First time («Первый раз»), Every week («Каждую неделю»), Every 2 weeks («Каждые 2 недели»), Every 3 weeks («Каждые 3 недели»), Every 4 weeks («Каждые 4 недели»).

On backup completion, send (errors only / full backup logs / status and errors) to the alert email address. the alert email address. Выбор типа уведомления

Рисунок 1. Окно «Выбор файлов и папок» программы NTI Shadow for ReadyNAS с открытым окном настроек

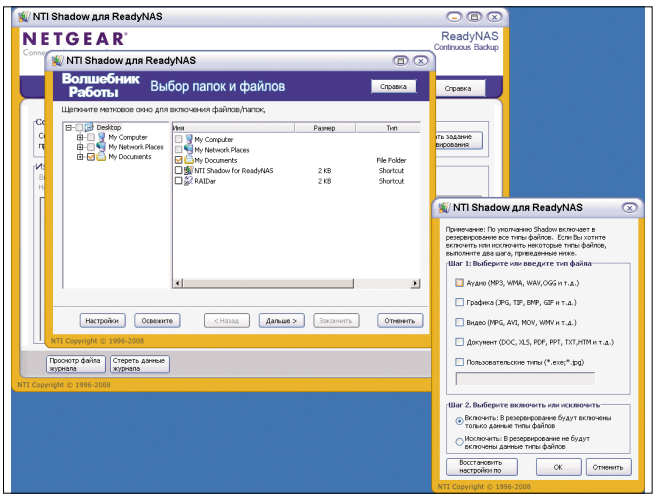
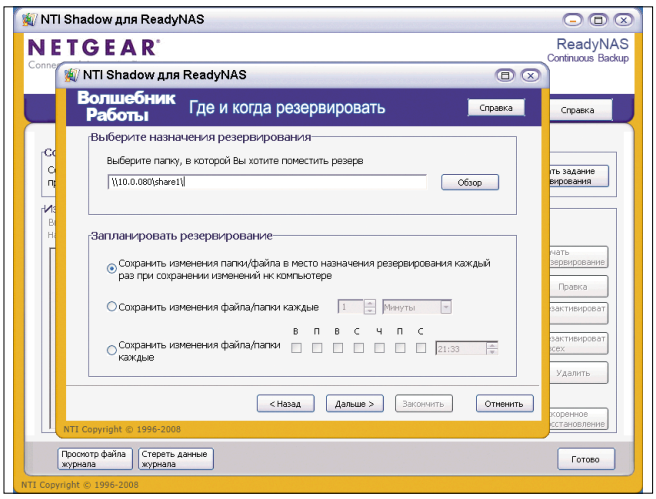


Рисунок 2. Окно «Где и когда резервировать» программы NTI Shadow for ReadyNAS



по e-mail: выслать только ошибки, полный журнал событий резервного копирования или статус и ошибки. В нашем случае было выбрано «статус и ошибки» как некое компромиссное решение.

Remove the contents of the backup destination before a full backup is performed... Данная функция удаляет файлы старой резервной копии при выполнении способа Full Backup (полного копирования) По умолчанию данный флажок снят. В нашем случае, учитывая тот факт, что в организации нет собственного системного администратора, установка данной функции даст некоторые гарантии, что на USB-диске хватит места.

Remove deleted files on backup target (rsync only). Данная функция актуальна только в случае копирования на другое сетевое хранилище ReadyNAS.

After backup is complete, change ownership of files in the backup destination to the share owner if the destination is a ReadyNAS share... Сменить владельца после выполнения резервного копирования, если для сохранения резервной копии используется общий ресурс ReadyNAS. В нашем случае в качестве сменных носителей используются USB-диски с файловой системой FAT32, поэтому данная функция не имеет для нас никакого значения.

Остается только запустить резервное копирование, проверить его состояние (см. рис. 6).

Для восстановления файлов необходимо подключить USB-диск к любому компьютеру, умеющему работать с FAT32, и скопировать информацию.

***

Сетевое хранилище ReadyNAS Pro предоставляет неплохие возможности для реализации резервного копирования информации, хранящейся как на рабочих станциях пользователей, так и непосредственно на самом сетевом хранилище. Это позволяет значительно повысить степень сохранности информации и облегчить трудовые будни системного администратора. EOF

1. Сайт русскоязычного сообщества ReadyNAS – http://www.readynas.su.
2. То же, но в международном масштабе – http://www.readynas.com.

Рисунок 3. Окно «файловых версий» программы NTI Shadow for ReadyNAS

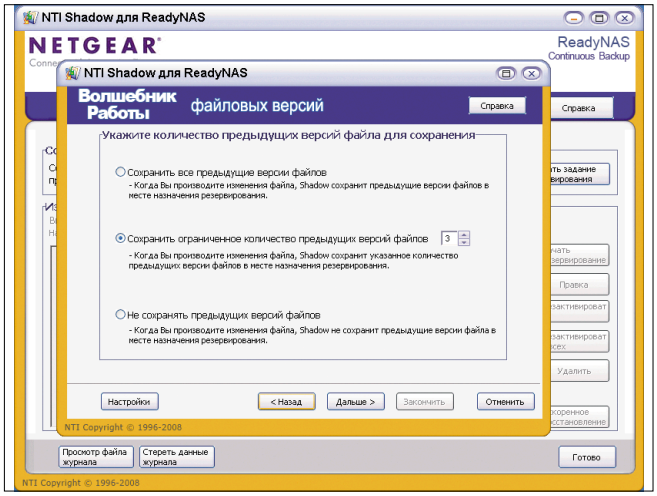


Рисунок 4. Выбор файла для восстановления

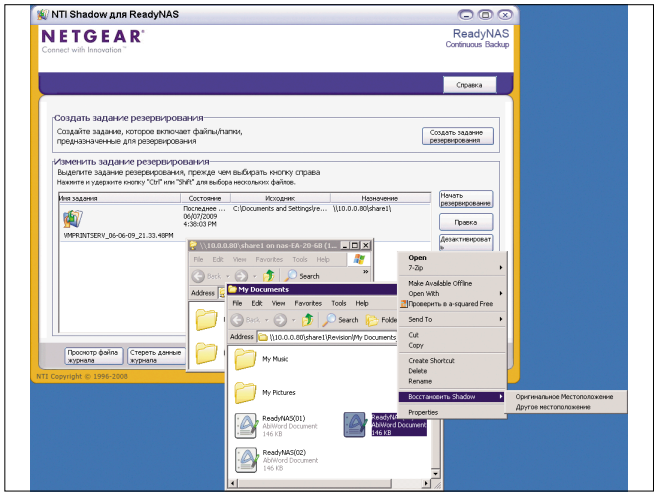


Рисунок 5. Окно «файловых версий» программы NTI Shadow for ReadyNAS

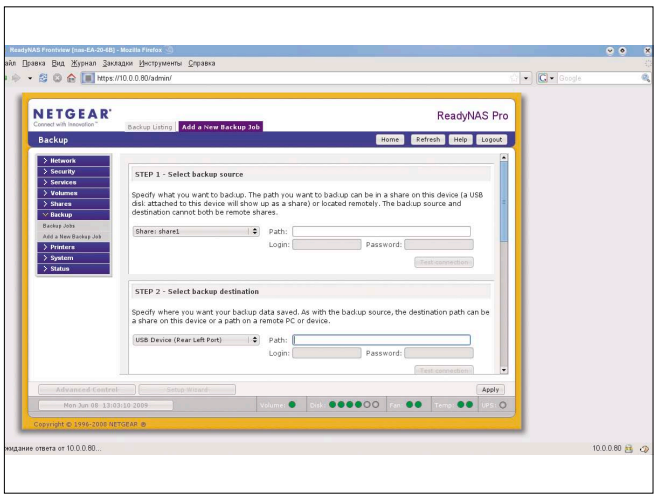
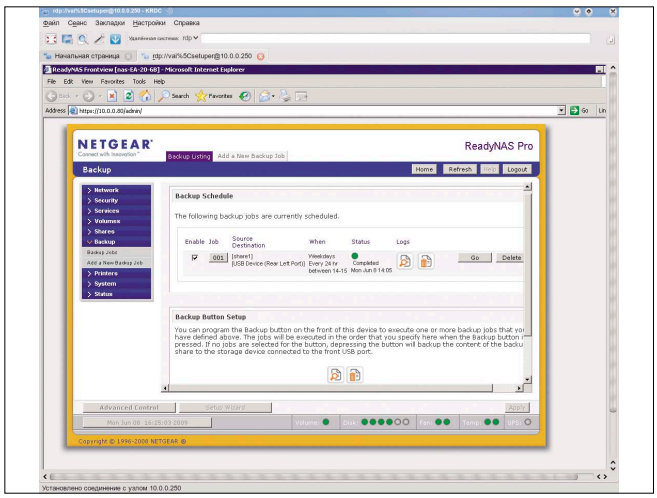


Рисунок 6. Выбор файла для восстановления



Визитка

ДМИТРИЙ БУТЯНОВ, консультант по решениям компании Microsoft в области портальных технологий и BI, специализируется на консультациях ключевых заказчиков компании. Опыт работы в области ИТ более 10 лет

Расчет на салфетке

Как продать ИТ-проект с помощью математики

В наши трудные времена выделение бюджета на ИТ-проект превращается в непростую задачу. Попробуем разобраться, как ее можно решить

Как же много всего поменялось на ИТ-рынке в целом и ИТ-отделах в частности за последнее время! Как только разговор заходит о докризисных временах, на лицах ИТ-специалистов появляются добрые и немного грустные улыбки. Ведь было же время! И бюджеты давали по первому требованию, и в работу никто особенно не лез – лишь бы все функционировало и можно было работать с новыми технологиями, сколько душа пожелает. А сейчас – лишь следы былой роскоши. Ни тебе бюджетов, ни роста… Конечно, сейчас жизнь не сахар, но давайте-ка вспомним, так ли всё было замечательно в докризисные времена?

Так ли хорошо было?

Ещё год назад большинство предприятий находилось на различных этапах экономического подъёма, а капиталы были доступны, например, в виде кредитов с небольшой процентной ставкой. Хорошо ли было при этом ИТ-отделу? Я бы сказал, что относительно. Обращается, скажем, ИТ-директор к генеральному с предложением внедрить… CRM-систему. И говорит, что внедрение этой системы позволит уменьшить величину оттока клиентов на 2%. Какой могла быть реакция гендиректора, у которого база клиентов росла на 10-15% в месяц, а объемы продаж – на 20% и без всяких CRM?

Интересная картина получалась. Особое внимание бизнес-пользователи уделяли специфическим ИТ-проектам.

Во-первых, главной целью их реализации было повышение капитализации компании. Это замечательно увеличивало стоимость компании на рынке, например, перед её продажей или перед публичным размещением акций (IPO). И было абсолютно не важно, принесет ли прибыль такой проект, так как главным в нем оставалась сумма потраченных средств. При упоминании таких проектов ИТ-директор, как правило, теперь хватается за голову, так как висят они на нем мертвым или полумертвым грузом.

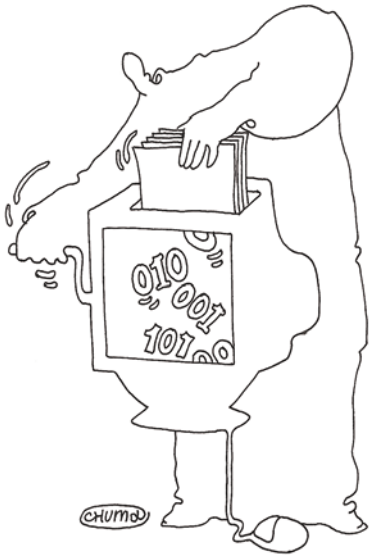
Во-вторых, «зеленый свет» получали ИТ-системы, которые были своеобразным дресс-кодом для компании. Под влиянием тусовки, семинаров и многочисленных рекламных акций, которые проводят производители программного обеспечения, рождался определенный набор стереотипов, которым бизнес часто следовал. Внедрение подобных систем происходило не потому, что они были действительно нужны, а потому что «у них есть, почему у нас нет?!» или «у всех уже есть, и нам тоже обязательно надо».

В-третьих, часть проектов реализовывалась благодаря активности ИТ-отделов. В подавляющем своём большинстве это были новые, интересные ИТ-специалистам продукты и технологии, внедряемые «потому что интересно покопаться». Зачастую эти внедрения выполнялись силами самого ИТ-отдела, а процент успеха был средний и очень зависел от особенностей продукта. И если с инфраструктурными решениями всё было более-менее хорошо, то с бизнес-системами, такими как системы документооборота или CRM, были трудности. В ИТ-отделе просто не хватало специалистов по таким решениям. Деньги на эти проекты выделялись достаточно хорошо. Если еще и бизнес-менеджер был гиком и ему тоже «было интересно», то проблем с финансированием не возникало вообще.

Заметили, что общего в этих проектах? Решение о начале проекта принималось на основе каких угодно соображений, только не его финансовых параметров (в первую очередь финансовой эффективности) или его полезности. В самом деле, когда с бизнесом всё хорошо, с рентабельностью всё в порядке, а прогнозы продаж устремлены ввысь, зачем возиться с ИТ? Хлопотно это и малоэффективно. Роль ИТ-отдела сводилась к роли обслуживающего подразделения. Эдакий чёрный ящик, с большим аппетитом потребляющий деньги. ИТ-директор ничего не решал, его даже редко звали на совет директоров.

Так ли плохо сейчас?

И вот осенью прошлого года грянул гром. Только ленивый не писал еще про сущность, причины и перспективы кризиса. Но всё-таки напомню о нескольких важных вещах, влияющих на судьбу ИТ-проектов на предприятии. Компании потеряли темпы роста, доступ к большому количеству дешевых кредитов, стали более внимательно смотреть



на расходы, и сейчас в качестве приоритетных выступают ИТ-проекты с совершенно другими характеристиками, нежели ранее. Что стало самым главным? Достижение результата!

Обратите внимание на то, что реализация проекта должна приводить к получению результата, хорошо понятного менеджерам, который можно посчитать: рубли, штуки товара, киловатты, километры. Это проект, внедрение которого приведет к экономии или к заработку средств, причем, разумеется, величина заработка или экономии должна быть выше затрат на реализацию. Проекты ради проектов, абстрактно повышающие непонятные параметры, не являются приоритетными сегодня. Из-за непростой экономической ситуации компании рассматривают ИТ-проекты, окупаемость которых является очень быстрой. Сегодня вероятность получить положительное решение о выделении средств, на мой взгляд, имеют проекты со сроками окупаемости до года, еще лучше – шести месяцев. И, разумеется, средств выделяют мало и неохотно – их и так немного осталось. Соответственно любые инициативы по снижению себестоимости проекта приветствуются. Одной из таких инициатив является комплекс мероприятий по снижению рисков внутри проекта, так как подавляющее большинство рисков приводит к росту затрат в проекте. Вариантов здесь немало, например, работа только с уже зарекомендовавшими себя технологиями, производителями и партнёрами.

Поскольку выделение средств сейчас происходит с очень большим скрипом, бюджеты, в том числе ИТ, режут, внимательно рассматривают каждый рубль, который тратится на ИТ. Средства на развитие часто вообще не выделяются, не потому, что их совсем нет, а потому, что руководство ИТ-отдела не может предоставить грамотную основу для принятия решения. Привыкли, что средства выделяют «чуть меньше, чем попросил», и к встречным вопросам типа «что это нам может дать» оказались совершенно не готовы. Переход от затрат на ИТ к инвестированию в ИТ оказался неожиданным: что с этим делать и как теперь говорить про деньги, для большого числа ИТ-специалистов оказалось непонятно. Вы думаете, это плохо? Отнюдь. Это замечательно, так как позволяет не только поддержать уровень финансирования ИТ-отдела с учётом ведущихся проектов, но и увеличить политический вес и уровень влияния ИТ-руководителя на предприятии. Много для этого не надо: научиться считать деньги и смотреть на ИТ с точки зрения бизнес-руководителя и финансиста.

Идея очень проста. Если вложения в ИТ-проекты сейчас рассматриваются как инвестиции, то на них распространяются действия инвестиционных законов. А значит, на основании этих же законов средства могут выделяться (инвестироваться). Но в то же время отрадно, что эти траты стали рассматриваться как инвестиции, и руководство теперь рассматривает вложения в ИТ как инвестирование. Это хорошо, так как проще стало получить деньги – достаточно обосновать траты и показать, как эти деньги заработают и что компания получит, выделив соответствующую сумму. Однако у этой медали есть и обратная сторона – процесс принятия решения о выделении средств стал длиннее, и сейчас расходы на ИТ должны одобрить инвестиционные комитеты или менеджеры, отвечающие за финансы и инвестиции. Этих людей надо убедить, они редко бывают доверчивы и не будут внедрять новые технологии ради самих технологий или по другим неэкономическим причинам.

Что считать?

В качестве основы принятия решения о начале финансирования ИТ-проекта часто рассматриваются два параметра, которые можно назвать классическими для экономики – это коэффициент возврата инвестиций (ROI) и срок окупаемости инвестиций. Первый параметр (ROI) показывает размер прибыли на рубль вложений. Иными словами, сколько рублей (копеек) мы можем получить за заданный период, если вложим в проект один рубль. ROI 200% – это означает, что доходы от проекта в два раза превышают расходы на него, и каждый вложенный рубль дает два рубля чистой прибыли. На бумаге считается ROI довольно просто – это отношение прибыли, полученной в результате проекта,

к совокупным затратам на этот проект за тот же период. Как происходит на практике – читайте ниже.

Не менее важным параметром является время, которое потребуется для того, чтобы полностью вернуть вложенные средства (срок окупаемости инвестиций). Разумеется, я рассматриваю проект, который приносит какую-то прибыль.

Вначале затраты на проект превышают доходы от него, однако далее ситуация меняется, и доходы от реализации проекта начинают превышать расходы на него. Величина времени, прошедшая от начала реализации проекта до момента, когда потраченные на него деньги вернулись, – и есть период окупаемости проекта. Иными словами, это период времени, спустя который потраченные на проект деньги возвращаются.

Бытует мнение, что посчитать экономический эффект ИТ-проекта невозможно. Это мнение культивируется людьми, для которых принятие решения о том или ином ИТ-проекте лежит не в области его экономической эффективности или оправданности, а в какой-то иной: например, в области идеологии или личных предпочтений. На самом деле подсчет экономической эффективности ИТ-проекта является выполнимой задачей. Для её решения существует несколько путей.

Таблица 1. Временные затраты на согласования документов

Этапы	Сейчас (человеко-часы)	После (человеко-часы)
Согласование документов		
Суммарное время на процесс запуска согласования договора включает в себя:	12,4	5,9
время на поиск шаблона договора	1	0,4
время на приложения к существующему договору (поиск в архиве и т.п.)	2	0,3
время на присвоение договору уникального номера	0,2	0
время на заполнение карточки документа	0,2	0,2
время на согласование договора с контрагентом	4	2
другие временные расходы	5	3
Согласование с владельцем бюджета		
Суммарное время на процесс согласования с владельцем бюджета включает в себя:	7	2,8
время на поиск сопроводительных документов	1	0,4
время на согласование изменений договора	4	2
прочие временные расходы согласования	2	0,4
Согласование с отделом закупок		
Суммарное время на процесс согласования с отделом закупок включает в себя:	8	3,1
время на поиск документов по каждому договору	1	0,1
время на редактирование и комментирование договора	4	1
прочие временные расходы согласования	3	2

Первый путь – это привлечение экспертов, людей, для которых расчет экономической эффективности является работой. Итоговые результаты будут очень точными, так как используются наработанные методики, модели и опыт. Однако есть и обратная сторона медали.

Во-первых, экспертам надо будет раскрыть финансовую информацию о работе компании, а это зачастую является коммерческой тайной.

Во-вторых, это достаточно долго, так как требуется выполнить большой объём работ.

В-третьих, это недёшево. Поэтому такой путь поиска экономической эффективности предпочитают крупные компании, или подобные расчёты выполняются для масштабных проектов с большими бюджетами. Да и не хватает таких экспертов, так как работают они в крупных интеграторах и живут в крупных городах.

Еще одним способом расчета являются так называемые «Большие калькуляторы» – типически это файлы Excel или другие решения, которые представляют собой анкеты, заполнив их, можно получить оценку экономической эффективности проекта. Большое число производителей имеют такие, кроме того, вы можете найти в Интернете независимые аналитические агентства, которые также формируют подобный инструментарий (как платный, так и бесплатный).

К сожалению, бытует мнение, что эти калькуляторы не очень точные, так как они разрабатывались для Запада, а в России своя специфика в ИТ. Я не могу поручиться за все калькуляторы на свете, но наши корпоративные сам проверял.

Однако у калькуляторов есть еще и минусы – заполнять их достаточно долго и непросто в том плане, что, если нужно получить относительно точный ответ, необходимо ответить на большое количество вопросов, а их там сотни. Зачастую люди не готовы отвечать на огромное количество вопросов – это долго и утомительно. Они хотят ответить на небольшое количество вопросов и получить оценку, которую с некоторой долей погрешности можно считать основой для принятия решений.

Чтобы решить эту задачу, существует расчет, который я называю «расчетом на салфетке». Основная идея – исключить из расчёта статьи расходов и доходов, не оказывающих большого воздействия на конечный результат. Наверное, кто-то удивлённо поднимет брови. Как это не рассматривать в расчетах стоимость аренды занимаемой сервером площади и изменение амортизации клавиатур?! Это ведь снизит точность расчёта на 0,01%!!!

Коллеги, мне понятны ваши чувства, но помните: наша задача – не точный расчёт ROI или TCO, а формирование основы для принятия решения о финансировании проекта. И если вы знаете, что в расходах на проект пять статей составляют 90% всех расходов, то остальное – отбрасывайте. Это мелочь, которая отнимет массу сил и времени и в принятии решения не играет никакой роли. Так что смело оставляйте только самое важное и делайте вид, что остального не существует.

Важна также проблема входных данных для расчётов. Приступать к определению экономических параметров внедрений можно в трех различных фазах: до начала проекта,

во время его выполнения и после его завершения. Разумеется, идеальным вариантом является тот, при котором можно сделать «снимок» ситуации до внедрения решения и после, потом сравнить два снимка. На практике такой расчет очень редок, по причинам, сами понимаете каким. Так что если расчёты ведутся до начала проекта, то можно сделать снимок текущего состояния подразделения (предприятия), а состояние «после внедрения» придется прогнозировать. Аналогично – если внедрение закончено, то можно сделать снимок «после внедрения», а состояние «до внедрения» надо будет вспоминать. И так далее – суть в том, что одно из состояний будет формироваться не как результат наблюдений, а как результат анализа или прогнозирования. Данные для таких операций можно рассчитать самим или взять примеры реализаций аналогичных проектов, каких на сайтах производителей много. И посмотреть, какие параметры и насколько изменились, у каждой технологии они, скорее всего, свои.

Как считать?

Давайте рассмотрим конкретный пример[1]. Предположим, что мы работаем в торговой компании, у которой есть бумажный документооборот, поддерживающий систему ведения договоров с партнёрами. Партнерская сеть росла, проблемы документооборота также множились и расширялись, но до кризиса на это закрывали глаза – на фоне высоких темпов роста буксующий документооборот поддерживали экстенсивно (наймом дополнительного персонала). Сейчас, в кризис, компания вплотную занялась решением задач снижения себестоимости бизнеса, удержания партнерской сети и так далее. Руководство с надеждой смотрит на нас, ожидая нашего вклада в общее дело. Поразмыслив на досуге, понимаем, что удержание объёмов продаж – наше всё. Проблема документооборота известна, вот тут-то мы можем попытаться что-то сделать, переведя его из бумажного в электронный вид и немного оптимизировав в процессе перевода.

Итак, начинаем исследовать систему заключения договоров и получаем следующие данные:

- В среднем через систему сейчас проходит 100 договоров в месяц от 100 партнеров.
- Согласующих договор с нашей стороны – 25 человек (для каждого договора!).
- Средний срок согласования договора – 10 дней.

Эти цифры помогут посчитать экономические параметры.

Теперь надо узнать, какие проблемы являются животрепещущими для пользователей. Самый простой вариант – беседы с пользователями. Можно еще проанализировать статистику обращений в службу поддержки, провести анкетирование и так далее. В данном примере, проведя несколько бесед с работниками различного уровня, выясняем, чем именно не устраивает их существующий документооборот.

Получаем следующий список, ранжированный по степени важности:

Утеря договоров. Поскольку документы бумажные, они довольно часто теряются, и тогда весь отдел стоит на ушах. Сколько договоров теряется, никто точно не знает, но много. Коммерческий директор оценил убытки от таких потерь примерно в 200 тысяч в год.

Слишком долгие сроки согласования документов. Руководству хотелось бы сократить это время примерно на 30%.

Мы сами не лыком шиты и кое-что про документооборот прочитали. И о типичных проблемах «бумажных» систем тоже. В разговорах с респондентами выясняем, что у них они, оказывается, тоже есть, причем довольно острые.

Поиск документов. Каждый договор с контрагентом сопровождает пачка других документов. При перезаключении договора они нужны, их поиск занимает немало времени.

Таким образом выявили три наиболее важные проблемы. Считаем, что их решение может дать наибольший экономический эффект, и остальными плюсами системы (типа экономии бумаги) пренебрегаем, чтобы не усложнять расчёты.

Начинается самое сложное – перевод абстрактных понятий в их конкретное денежное выражение. Чтобы это выполнить, сделаем общий снимок процесса согласования документов с неглубокой детализацией и расчетом времени. Результаты поместим в таблицу (см. таблицу 1, колонка «Сейчас»). Обратите внимание на то, что детализация снимка напрямую зависит от тех самых трёх проблем, которые мы вывели ранее, и «лишних» данных мы не собираем.

Теперь надо представить, каковы будут параметры системы после окончания проекта, то есть займёмся прогнозированием. В этом нам помогут производители программного обеспечения, которые публикуют необходимые оценки и примеры на своих сайтах, плюс мы сами тоже прикинем, что и как может быть в будущем. Опять же исходим из принципа решения трёх проблем.

Предполагаем, что:

- Утеря договоров прекратится, так как всё будет в электронном виде.

Таблица 2. Денежные затраты

Позиции	Сейчас	После
Стоимость запуска согласования одного договора	4 429 р.	2 107 р.
Согласование с владельцем бюджета (один договор)	3 750 р.	1 500р.
Согласование с отделом закупок (один договор)	4 286 р.	1 661 р.
Общая стоимость процесса запуска в месяц	442 857 р.	295 000 р.
Согласование с владельцем бюджета в месяц	375 000 р.	210 000 р.
Согласование с отделом закупок в месяц	428 571 р.	232 500 р.
Общая стоимость процесса в месяц	1 246 429 р.	737 500 р.
Стоимость сэкономленного времени в месяц		508 929 р.
Общая стоимость экономии в год (с учетом потерь договоров)		6 307 143 р.

1. Здесь и далее рассмотрен реально существующий и успешно завершенный проект. Все цифры не являются симуляцией. Все параметры проекта – результаты измерений.

- Сроки согласования сократятся примерно на 30-40% (в среднем замена бумаги на электронку даст такой эффект).
- Поиск документов будет автоматизирован, и его время сократится в разы, так как на смену поиска по картотеке и ходьбе по помещениям со стеллажами придет простой запрос к электронному архиву.

Понятно, что этот проект, по своей сути, является переходом от бумажного документооборота к системе СЭД в рамках одного отдела. Не буду вдаваться в подробности и тонкости – скажу лишь, что такой переход вполне возможен и легитимен при развертывании системы ЭЦП (договор в электронной форме, «подписанный» ЭЦП, имеет силу бумажного договора с синими печатями).

Для расчёта прибыли по проекту пользуемся принципом «что сэкономили, то заработали». Непосредственно система документооборота денег не заработает, но позволит исключить убытки от утери договоров и сэкономить некоторое количество рабочего времени. Зная себестоимость сотрудника в месяц (зарплата + налоги), легко подсчитать себестоимость часа его работы. Зная, сколько часов сможет сэкономить система документооборота, легко превратить это в деньги.

И не надо заниматься вопросами типа «как будут использоваться сэкономленные часы» и так далее. Это не ваши вопросы. Вы даёте директору возможность сэкономить N часов рабочего времени, которое стоит M рублей. Пусть он решает, как этим распорядиться – а он решит, вы не переживайте.

Итак, исходные данные для расчёта прибыли у нас есть и сведены для наглядности в таблицу 1. Колонка «Сейчас» показывает текущее состояние процесса, колонка «После решения» показывает наш прогноз ситуации после реализации проекта.

Нехитрые вычисления позволяют определить стоимость процессов согласования документов. Результаты – в таблице 2. Там вы можете увидеть общую цифру дохода от реализации проекта. Это не прибыль, так как из этой суммы еще надо вычесть затраты.

Затраты на проект складываются из стоимости приобретения и стоимости владения. Стоимость приобретения (совокупная) – это сумма средств, которые надо потратить для того, чтобы успешно реализовать проект.

Список статей может быть очень обширным, но опять же выкидываем всё неважное и составляем краткий список (см. таблицу 3).

Совокупная стоимость владения тоже денег стоит, но в данном случае сводим ее к затратам на персонал, как к самой большой статье затрат. Соответствующие данные представлены в таблице 4.

А теперь под звук труб и фанфар мы определяем общую прибыль от проекта за 12 месяцев – примерно 4 млн руб в первый год. При этом ROI проекта за первый год составляет 242%, а срок окупаемости 93 дня.

Фантастично? Нет. Ведь речь идет об автоматизации «бумажного» процесса с большой себестоимостью и многими типичными для него проблемами. Разумеется, при расчёте других проектов могут получаться иные цифры – и срок окупаемости больше, и ROI ниже.Но в любом случае полученные результаты являются отличным поводом поговорить о проекте с директором, например. Это оценочные цифры, их можно уточнять и уточнять. Никто с этим не спорит. При всех своих минусах этот метод расчёта даёт информацию к размышлению и позволяет оценить эффективность ИТ-проекта. Точность расчёта вполне позволяет принять решение о выделении или невыделении средств на его реализацию.

Аналогичные методики можно применять и для расчёта эффективности развёртывания других технологий. Помните о двух принципах: «отбрасывание всего лишнего» и «то, что сэкономили, то заработали». Например, технологии Unified Communications позволят сэкономить на стоимости использования фиксированной и мобильной связи (в меньшей степени) и на расходах на командировки сотрудников (в большей степени), а также на количестве и длительности совещаний.

Структура затрат при этом будет почти такая же, как в приведенном примере, только добавится статья расходов на оборудование. И перед «не ориентированными на бизнес» технологиями тоже пасовать не надо.

Внедрение того же System Center позволит сэкономить рабочее время работников ИТ-отдела, рабочее время сотрудников компании (ускорение операций восстановления данных), а также уменьшит стоимость аппаратного обеспечения за счёт виртуализации.

И главное – попробуйте взглянуть на ИТ-проект глазами того, кто платит. У этого человека масса требующих решения проблем. Если вы станете для него человеком, способным разрешить хотя бы часть этих проблем, – у вас всё получится.

Удачи! EOF

Таблица 3. Совокупная стоимость приобретения (TCA)

Общая стоимость ПО	450 000 р.
Общая стоимость контракта с партнером (минус ПО)	780 000 р.
Стоимость закупленных аппаратных средств	100 000 р.
Количество консультантов от заказчика	8
Средняя себестоимость услуг консультанта для заказчика, в месяц	90 000 р.
Количество консультаций (на одного консультанта)	4
Средняя продолжительность консультаций, часов	2
Продолжительность курсов обучения пользователей, часов	8
Количество обученных работе в системе пользователей	30
Средняя себестоимость обучения 1 пользователя для компании	700 р.
Итого:	**1 385 286 р.**

Таблица 4. Совокупная стоимость владения (TCO)

Количество обслуживающего персонала системы (включая Helpdesk)	1
Средняя себестоимость услуг одного человека обслуживающего персонала (в месяц)	50 000 р.
Длительность обслуживания системы, часов (в месяц)	40
Стоимость контракта постпроектной поддержки партнера (в месяц)	60 000 р.
Итого, в год:	**862 857 р.**

Повышение привилегий в ядре Linux

Программа: Linux kernel 2.6.30.
Опасность: Низкая.
Наличие эксплоита: Да.
Описание: Уязвимость существует из-за ошибки разыменования нулевого указателя в функции tun_chr_pool() в файле drivers/net/tun.c. Локальный пользователь может выполнить произвольный код на целевой системе с привилегиями учетной записи root. Для успешной эксплуатации уязвимости ядро должно быть собрано с опцией GCC -fdelete-null-pointer-checks.
URL производителя: www.kernel.org.
Решение: Установите исправление из GIT-репозитория производителя.

Уязвимость при обработке ASN.1-строк в strongSwan

Программа: strongSwan версии до 2.8.10, 4.2.16 и 4.3.2.
Опасность: Средняя.
Наличие эксплоита: Нет.
Описание: 1. Уязвимость существует из-за ошибки при обработке ASN.1 Relative Distinguished Names. Удаленный пользователь может с помощью специально сформированного X.509-сертификата аварийно завершить работу pluto IKE-демона.

2. Уязвимость существует из-за ошибки при обработке ASN.1 UTCTIME- и GENERALIZEDTIME-строк. Удаленный пользователь может с помощью специально сформированного X.509-сертификата аварийно завершить работу pluto IKE-демона.
URL производителя: strongswan.org.
Решение: Установите последнюю версию 2.8.10, 4.2.16 или 4.3.2 с сайта производителя.

Переполнение буфера в stftp

Программа: stftp 1.1.0, возможно, другие версии.
Опасность: Средняя.
Наличие эксплоита: Да.
Описание: Уязвимость существует из-за ошибки проверки границ данных в функции p_header() в файле misc.c. Удаленный пользователь может с помощью слишком длинного PWD-ответа, отправленного вредоносным FTP-сервером, вызвать переполнение динамической памяти и выполнить произвольный код на целевой системе.
URL производителя: sourceforge.net/projects/stftp.
Решение: В настоящее время способов устранения уязвимости не существует.

Отказ в обслуживании в реализации TCP/IP в Sun Solaris

Программа: Sun Solaris 10.
Опасность: Низкая.
Наличие эксплоита: Нет.
Описание: Уязвимость существует из-за ошибки в реализации сетевого стека TCP/IP при обработке jumbo-фреймов в драйвере устройств Cassini Gigabit-Ethernet. Удаленный пользователь может аварийно завершить работу системы. Для успешной эксплуатации на системе должен быть сконфигурирован GigaSwift Ethernet Adapter-интерфейс для принятия jumbo-фреймов с включенной аппаратной проверкой контрольных сумм.
URL производителя: www.sun.com.
Решение: Установите исправление с сайта производителя.

Повышение привилегий в Microsoft Virtual PC и Virtual Server

Программа: Microsoft Virtual PC 2004; Microsoft Virtual Server 2005; Microsoft Virtual PC 2007.
Опасность: Низкая.
Наличие эксплоита: Нет.
Описание: Уязвимость существует из-за ошибки при обработке уровней привилегий в Microsoft Virtual PC и Microsoft Virtual Server при выполнении определенных инструкций в Virtual Machine Monitor. Локальный авторизованный пользователь гостевой ОС может выполнить произвольный код в пределах гостевой ОС с повышенными привилегиями.
URL производителя: www.microsoft.com.
Решение: Установите исправление с сайта производителя.

Переполнение буфера в ISC DHCP

Программа: ISC DHCP версии 2.0 по 4.1.
Опасность: Средняя.
Наличие эксплоита: Нет.
Описание: Уязвимость существует из-за ошибки проверки границ данных в функции script_write_params() в файле client/dhclient.c. Удаленный пользователь, контролирующий DHCP-сервер, может отправить слишком длинную опцию subnet-mask, вызвать переполнение стека и выполнить произвольный код с привилегиями учетной записи root на клиентской системе.
URL производителя: www.isc.org/products/DHCP.
Решение: Установите последнюю версию 3.1.2p1, 4.0.1p1 или 4.1.0p1 с сайта производителя.

Составил Александр Антипов

Михаил Кристев:
«Кризис не время для уныния»

На вопросы «Системного администратора» отвечает директор по развитию бизнеса Cisco в России, руководитель направления перспективных технологий Михаил Кристев

Алексей Алексеев

– Михаил, как мировой финансовый кризис повлиял на работу вашей компании? Что вам помогает держаться на плаву сегодня?

– Кризис коснулся всех. Естественно, он не мог не сказаться и на нашей компании. Предыдущий, 2008 финансовый год мы закончили с очень хорошим показателем – 39,5 млрд долларов оборота. В только что завершившемся 2009 финансовом году оборот Cisco снизился, но не так сильно, как у большинства наших конкурентов.

Есть ли у нас секреты? Мы считаем, что кризис не время для уныния, а отличная возможность улучшить свое положение на рынке. Сегодня мы более внимательно управляем своими финансовыми расходами, следим, чтобы они соответствовали изменившемуся уровню оборотов и продажи. Компания остается прибыльной, и согласно нашей стратегии мы не прекращаем инвестиций в новые разработки. В отличие от многих наших конкурентов мы не топчемся на месте и уж тем более не отступаем.

Наши основные направления – это работа с партнерами, с которыми заключаем прямые договорные отношения, и прямое финансирование отдельных проектов заказчика.

К маю этого года наша компания накопила солидный объем свободных финансовых средств – 33,5 миллиар-

да долларов. Для нас это большой козырь, и мы используем его, в том числе, для финансирования наших партнеров и заказчиков в период, когда привлекать заемные средства становится все сложнее, тем более в России.

Кстати, в июне 10-летие успешной деятельности в России и других странах СНГ отметила Cisco Capital – дочерняя компания Cisco, один из мировых лидеров в сфере финансирования сетевых технологий и оборудования для Интернета. В 2008 году она организовала региональную финансовую структуру ООО «Сиско Кэпитал СНГ» (www.ciscocapital.ru), которая с тех пор обслуживает локальных заказчиков и партнеров. Осенью прошлого года мы предоставили большинству наших партнеров 90 дней отсрочки платежа, а общий объем кредитных линий в России достигает 200 млн долларов. Это ощутимая помощь клиентам в условиях финансовой нестабильности и дороговизны кредитных предложений в банковской сфере.

– Значит, любая компания, которая желает внедрить решение Cisco, если ей не хватает средств, может обратиться к вам за кредитом на внедрение этих решений?

– Да. Вначале, конечно, будет изучено финансовое положение такой компании, ее баланс, и после положительного решения нашего кредитного комитета мы сможем перейти к финансированию проекта клиента. Кстати, мы предлагаем более выгодные для заказчиков и партнеров условия по сравнению с существующими на свободном кредитном рынке.

– Предпринимаете ли вы какие-нибудь меры для расширения своего присутствия на российском рынке?

– Первое, что мы сделали с наступлением кризиса, чтобы не растерять, а наоборот, укрепить наши позиции на рынке, – мы не стали сокращать своих сотрудников и постарались сохранить всех наших партнеров и заказчиков. Уверен, что сегодня это одно из наших конкурентных преимуществ. Кроме этого, в конце 2008 г. мы открыли новый офис в Новосибирске, третий по счету после Москвы и Санкт-Петербурга. Всевозможная локализация – одна из ключевых стратегий нашей деятельности в России.

– Возможно ли сейчас устроиться в компанию, есть ли у вас какие-то особые требования к вашим претендентам?

– Подбором кадров у нас занимается рекрутинговый департамент. Разумеется, мы предъявляем весьма строгие требования к желающим работать в Cisco специалистам как по уровню знаний, так и по опыту работы. Кроме того, мы придаем очень большое значение тому, чтобы кандидат вписался в нашу команду.

Мы оцениваем специалистов по самым разным критериям и проводим не менее 5-6 собеседований с соискателем, прежде чем будет принято решение о его трудоустройстве. Кстати, в прошлом году мы впервые приняли участие в исследовании «Лучшие работодатели России», которое ежегодно проводит компания Hewitt Associates, и сразу же вошли в первую тройку.

– В России активно расширяется русскоязычная служба техподдержки. Раньше клиенты, столкнувшиеся с технической проблемой, должны были общаться с инженерами в Брюсселе на английском языке. Не так давно у меня возник вопрос по поводу довольно сложного оборудования Cisco CRS-1, и я с удивлением получил ответ на русском языке от русских инженеров. Это тоже часть стратегии компании – развивать русскоязычную службу техподдержки?

– Совершенно верно. В 2006 году мы открыли в Москве центр круглосуточной обработки заявок и технического обслуживания, позволяющий предоставлять телефонные консультации на русском языке. Добавлю, что во всем мире существует лишь 9 таких центров Cisco.

– Правда ли, что полтора-два года назад произошли серьезные изменения в политике Cisco, касающейся замены вышедшего из строя оборудования? Во многих городах-миллионниках появились склады, позволяющие производить замену в более короткие сроки.

– Да, теперь замена вышедшего из строя оборудования производится в течение четырех часов. Во многом это результат того, что в ключевых регионах РФ теперь действуют 12 быстро пополняемых складов Cisco, где всегда есть именно то оборудование, которое обычно спрашивают в данном регионе заказчики. Это не только еще одно наше конкурентное преимущество, но и возможность отличить «серого» дилера от своего партнера. Когда все закуплено по правилам, заказчик получает доступ к нашему центру сервис-

Мы не стали сокращать сотрудников и постарались сохранить всех наших партнеров и заказчиков. Уверен, что сегодня это наше конкурентное преимущество

Михаил Кристев отвечает за разработку и реализацию стратегии Cisco по продажам всех решений системы унифицированных коммуникаций, систем обеспечения информационной безопасности, беспроводных решений, продукции для центров обработки данных, решений для построения оптических сетей, а также инновационных решений корпорации в России, Украине, Казахстане, Белоруссии, Узбекистане, Азербайджане, Армении, Туркменистане, Грузии и Таджикистане.

Ранее Михаил возглавлял подразделение технического обеспечения деятельности корпорации Cisco в России и странах СНГ. Он начал работать в Cisco в 1996 году в должности системного инженера в московском офисе. До начала работы в Cisco Михаил занимал технические и руководящие должности в российских компаниях, занимающихся системной интеграцией. Стаж работы Михаила в сфере информационных технологий составляет более 20 лет.

ной поддержки. Если же оборудование было куплено непонятно где, заказчик не вправе рассчитывать на высокий уровень сервисной поддержки. Это один из способов провести четкую грань между ввозом оборудования законным путем и всевозможными махинациями.

По результатам прошлогоднего опроса, который проводила компания Hewitt Associates, компания Cisco вошла в тройку лучших работодателей в России

– Не секрет, что сейчас в Интернете многие получают пиратские версии операционных систем IOS, которые могут стоить десятки тысяч долларов. Иностранные компании создают антипиратские коалиции. А как действует Cisco?

– Мы находимся не в столь сложной ситуации, как производители исключительно программных продуктов, так что размер бедствия для нас несколько меньше. Тем не менее нас, естественно, не устраивает, когда программные продукты компании, в частности, операционная система Cisco IOS, используются несанкционированно, и мы всячески с этим боремся. Активно работаем над тем, чтобы была очень четкая связь между аппаратной платформой и программным обеспечением, закупленным заказчиком.

В будущем, наверное, можно будет говорить о том, что на «коробке», приобретенной заказчиком, будет работать только тот экземпляр программного обеспечения, на который покупатель имеет право.

– У вас в компании сейчас меняется политика ввоза оборудования. Есть некие трудности с ввозом оборудования с шифрованием. В чем дело?

– Мы сейчас переводим наших партнеров на новую модель ввоза оборудования, которая называется DDU (Delivered duty unpaid). Непосредственно она касается только тех партнеров, с кем у нас есть прямые контракты. Перевод на эту модель соответствует задаче, поставленной российским правительством, которое хочет видеть полностью прозрачный и понятный алгоритм ввоза оборудования из-за рубежа.

Что касается наличия оборудования на складах наших дистрибьюторов-партнеров, то с этим проблем нет. Мы готовились к переходу больше года и, надеюсь, большинство проблем заранее предусмотрели, решив их еще до того, как они возникли.

Ввоз шифровальных средств согласно российскому законодательству осуществляется по лицензии, выданной Минэкономразвития, на основании разрешения ФСБ России. Чтобы ввезти шифровальные средства в полном соответствии с законом, нужно пройти очень большой путь.

Мы его стали проходить, наверное, раньше многих наших конкурентов. И, несмотря на определенные сложности, думаю, нам удастся выйти на рабочий режим ввоза криптосредств в полном соответствии с требованиями российского законодательства существенно раньше, чем нашим конкурентам, потому что многие из них этим вопросом еще даже не озадачились.

Мы неоднократно слышали призывы к тому, чтобы компания Cisco интегрировала в свои продукты российские алгоритмы шифрования. И мы это сделали, разработав аппаратную платформу – VPN-модули, которые устанавливаются в маршрутизаторы серии ISR. На эти модули ставится российское программное обеспечение с ГОСТовским шифрованием. Таким образом, мы постарались решить проблему ввоза оборудования, которое используется именно для создания VPN. У тех, кто знаком с деталями регулирования ввоза криптосредств, наибольшие сложности возникают именно тогда, когда аппаратные и программные средства используются для создания VPN, для шифрования про-

Добро пожаловать в Сетевую Академию

Компания Cisco расширяет свое присутствие на рынке России еще и за счет бесплатных образовательных инициатив, прежде всего за счет глобальной программы Сетевых Академий Cisco, в которую наша компания вложила уже более 300 млн долларов. Эта программа призвана способствовать росту квалифицированных ИТ-кадров в нашей стране. Сейчас при российских вузах, школах и других образовательных учреждениях действуют 125 таких академий, где обучаются 5078 студентов. Планируется, что в ближайшие годы число Сетевых академий Cisco в России будет доведено до 350, что позволит дополнительно обучить 22 тысячи специалистов по информационно-коммуникационным технологиям.

После обучения в Сетевой Академии выпускники могут сдать экзамен на сертификат CCNA (Cisco Certified Network Associate). Это базовый уровень сертификации. В дальнейшем можно получить следующий уровень сертификации – CCNP (Cisco Certified Network Professional), и так далее, вплоть до введенной недавно высшей ступени сертификации – «Архитектор», на которую вправе претендовать специалисты, занимающиеся проектированием сетей. Замечу, что, по данным рекрутинговых компаний, в России сертифицированный компанией Cisco специалист находит престижную высокооплачиваемую работу в среднем в 5 раз быстрее, чем несертифицированный, а теряет работу в 9 раз реже.

Кроме того, в феврале 2009 года мы ввели в действие программу Cisco Expo Learning Club, направленную на повышение квалификации российских ИТ-специалистов. В рамках этой инициативы к августу были проведены 48 бесплатных семинаров и тренингов. Благодаря уникальному интернет-сервису WebEx, который позволяет одним щелчком компьютерной мыши устроить виртуальное совещание в режиме реального времени, мы обеспечили регулярное участие в этих мероприятиях ИТ-специалистам из десятков городов России и ближнего зарубежья, а недавно предоставили такую возможность и студентам, преподавателям и выпускникам 250 Сетевых Академий Cisco, действующих на территории СНГ. Тем временем количество членов Cisco Expo Learning Club выросло с нуля до 3760. Многие из них наверняка примут участие в юбилейной, уже десятой по счету конференции Cisco Expo, которая пройдет 12-14 октября в московском Центре международной торговли.

Александр Палладин,

глава пресс-службы ООО «Сиско системс»

ходящего трафика. Есть различные исключения, под них подпадают, например, средства беспроводного доступа короткого радиуса действия и некоторые другие.

От этого функционала в нашем программном обеспечении уйти никак нельзя, иначе оно станет не столь привлекательным для наших заказчиков. Задачу же создания VPN мы собираемся в перспективе решать за счет ГОСТовских алгоритмов и ГОСТовского шифрования.

– В этом году компании Cisco исполняется 25 лет. Каким вы видите будущее лет эдак через 25?

– Нужно быть писателем-фантастом, чтобы представить, как мир будет выглядеть спустя четверть века, но уже очевидно, что информационные коммуникации будут использоваться всюду. Скорость как проводных, так и беспроводных коммуникаций будет, по сегодняшним меркам, просто невообразимой. Помимо передачи видео и голоса по сетям будут передаваться запахи, тактильные ощущения. Сегодня это кажется фантастикой, но лет через 25 станет настолько обыденным, что люди будут воспринимать это как должное. 25 лет назад создатели компании Cisco и те, кто их окружал, вряд ли представляли себе, как мир сетей, телекоммуникаций будет выглядеть сегодня. Точно так же и нам сейчас сложно предсказать, какие технологии появятся через четверть века. В одном, впрочем, я уверен: Cisco и через 25 лет останется компанией, на наших глазах меняющей образ жизни, работы, методы обучения и общения. EOF

Только факты

Cisco изначально позиционировала себя как компания, у которой большое будущее и большие задачи. И действительно, за четверть века она прошла серьезный путь от разработки первого маршрутизатора до статуса лидера телекоммуникационного рынка.

Сегодня в десятках офисов Cisco на всех континентах работают более 66,5 тысяч человек, которые разрабатывают и производят оборудование для крупнейших операторских сетей и сетей домашнего использования, занимаются вопросами организации передачи информации, начиная от передачи данных в корпоративных сетях и заканчивая передачей видео и голоса через беспроводные технологии.

Ежегодно компания выделяет на НИОКР более 5 млрд долларов. Только на исследования и разработки в области сетевой безопасности она тратит около 500 млн долларов, что сравнимо с уровнем оборота большинства компаний, специализирующихся исключительно на решениях безопасности.

Визитка

АНДРЕЙ ЛУКОНЬКИН, ведущий инженер-программист ОАО «НижегородАвтоДор». Занимается автоматизацией производства, бухгалтерского, управленческого и кадрового учета

Углубляемся в код
управляемого приложения

Кроме визуальной настройки интерфейса, необходимо кардинально менять код модуля управляемой формы, чтобы добиться нужной функциональности

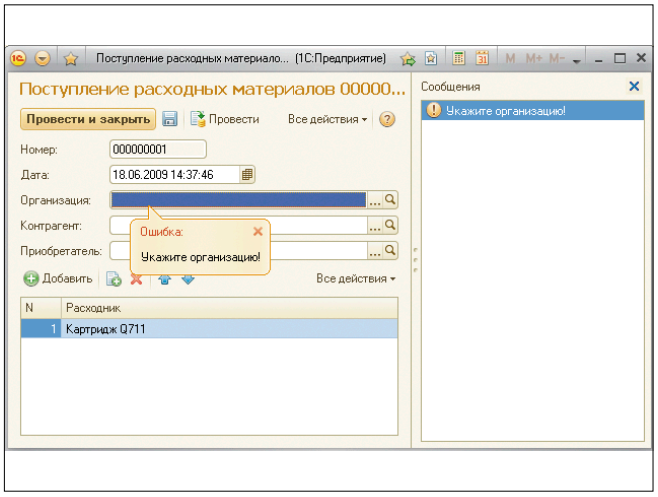
Помимо визуальной картинки, часто необходимо программно описывать события формы. Методология написания программного кода для тонкого клиента значительно отличается от программирования на платформе 8.1. Вся сложность заключается в том, что система должна суметь автоматически транслировать клиентские модули из встроенного языка «1С:Предприятия» в Java Script. Поэтому перед каждой процедурой, функцией или объявлением переменной модуля формы указывается одна из директив компиляции (см. таблицу 1).

Директивой по умолчанию является «&НаСервере».

Разработчики утверждают, что применение внеконтекстных методов позволяет существенно уменьшить объем передаваемых данных при вызове серверной процедуры из среды клиентского приложения, что положительно сказывается на скорости работы (см. таблицу 2).

Текст программы при переходе с 8.1 пришлось кардинально изменить: указывать директивы препроцессору, изменять логику построения функций и процедур.

Рисунок. Сообщение об ошибке привязывается к конкретному реквизиту формы



В качестве примера рассмотрим событие обработки выбора организации на форме справочника.

```
&НаСервере
Функция ОпределитьИнвНомер(Орг)
    ВидТехники = Перечисления.ВидТехники.Компьютеры;
    …
    НаборЗаписей = РегистрыСведений.ИнвентарныеНомера. ↵
        СоздатьНаборЗаписей();
    …
    возврат ИнвНомер;
КонецФункции

&НаКлиенте
Процедура ОрганизацияОбработкаВыбора(Элемент, ↵
        ВыбранноеЗначение,  СтандартнаяОбработка)
    Если Объект.Организация <> ВыбранноеЗначение Тогда
        Объект.ИнвНомер = ↵
                ОпределитьИнвНомер(ВыбранноеЗначение);
    КонецЕсли;
КонецПроцедуры
```

Здесь мы видим, что есть существенные ограничения в работе клиентских процедур. Обращения возможны только к объектам формы, а чтобы получить какие-либо объекты конфигурации, нужно обращаться к серверным функциям (именно функциям, т.к. они имеют возвращаемое значение). Такая логическая структура построения программы достаточно прозрачна и понятна, хотя и требует некоторого переосмысления после программирования на платформе 8.1.

Использование перечислений в клиентских процедурах возможно двумя способами.

> Используя функцию, выполняемую на сервере.

```
&НаСервере
Функция ВернутьЗначениеВидаТехники()
    возврат Перечисления.ВидТехники.Компьютеры;
КонецФункции

&НаКлиенте
Процедура ОрганизацияПриИзменении(Элемент)
    ВидТехники = ВернутьЗначениеВидаТехники();
КонецПроцедуры
```

> Используя ссылку на предопределенный элемент из предопределенных данных или прикладных перечислений.


```
&НаКлиенте
Процедура ОрганизацияПриИзменении(Элемент)
    ВидТехники = ПредопределенноеЗначение( ↵
        "Перечисление.ВидТехники.Компьютеры");
КонецПроцедуры
```

Таким образом, нужно пересмотреть логику программных модулей форм объектов конфигурации. Главное – понять, какие действия выполняются на стороне клиента, а какие на стороне сервера.

Также хочется сказать пару слов об интерактивных сообщениях, выводимых пользователю. Например, объект «СообщениеПользователю()» предназначен для хранения параметров сообщения, которые необходимо вывести пользователю.

Допустим, нам нужно добавить проверку на заполнение реквизита. Это возможно двумя способами: свойство реквизита «Проверка заполнения» и программно.

Рассмотрим второй способ для демонстрации работы с сообщениями. В процедуре обработки проведения документа зададим проверку и укажем причину невозможности проведения.

```
Если НЕ ЗначениеЗаполнено(Организация) Тогда
Сообщение = Новый СообщениеПользователю();
Сообщение.Текст = "Укажите организацию!";
Сообщение.Поле = "Организация";
Сообщение.УстановитьДанные(ЭтотОбъект);
Сообщение.Сообщить();
    Отказ=Истина;
КонецЕсли;
```

На рисунке видно, что сообщение визуально привязывается к определенному реквизиту формы, что очень удобно использовать для указания на совершенные ошибки при заполнении.

Новая платформа таит в себе еще много других возможностей и отличий, которые я постараюсь раскрыть в следующих статьях. Хорошей новостью является то, что 30 июня 2009 года уже выпущена тестовая платформа управляемого приложения, не предполагающая развития и дополнения функционала, а это значит, что в скором будущем (ориентировочно в третьем квартале 2009 года) выйдет финальная версия платформы. EOF

1. Луконькин А. Управляемое приложение. Первые осторожные шаги. //Системный администратор, №7, 2009 г. С. 64-65.

Таблица 1. Директивы компиляции модуля управляемой формы

&НаКлиенте	Метод выполняется на стороне клиента, а переменная существует все время жизни клиентской части управляемой формы. Из клиентского метода допустимыми являются вызовы клиентских, серверных и серверных внеконтекстных методов
&НаСервере	Метод выполняется на стороне сервера, а переменная существует только во время вызова выполнения серверного или серверного внеконтекстного вызова. Для серверных методов допустимыми являются вызовы серверных и серверных внеконтекстных методов
&НаСервереБезКонтекста	Метод исполняется на сервере вне контекста формы. Переменные не могут быть внеконтекстными. В таких методах недоступен контекст формы (включая данные формы). Допустимыми являются вызовы только других внеконтекстных методов. При вызове этих методов не выполняется передача данных формы на сервер и обратно

Таблица 2. Применимость директив компиляции в модулях системы «1С:Предприятие»

	НаКлиенте	НаСервере	НаСервереБезКонтекста
Модуль формы	+	+	+
Модуль команды	+	+	–
Общий модуль	+	+	–

Визитка

ИВАН ПАНИН, инженер по технической информационной безопасности.
Сфера интересов: сетевые технологии, защита информации

Эффективный инструмент
для создания единой корпоративной сети

Сокращаем затраты на организацию межсетевого взаимодействия в части бизнес-процессов для территориально распределенной компании с помощью Virtual Private Network

Экономическая выгода от использования технологии VPN довольно ощутима. Нет необходимости в дорогостоящих «чистых» каналах для создания единой корпоративной среды. Пользователями VPN могут быть как небольшие компании с несколькими офисами или торговой сетью в черте города, так и крупные холдинговые компании. За счет шифрования создаются закрытые каналы, позволяющие объединить территориально разрозненные подразделения организации в единую сеть. Причем именно для крупных компаний наиболее востребовано эффективное и безопасное межсетевое взаимодействие, позволяющее создать оптимальную корпоративную сеть, как с технической, так и с экономической точек зрения. (Начало статьи читайте в предыдущих номерах [1, 2].)

Point-to-Point GRE over IPsec

На рис. 1 представлена p2p GRE over IPsec [3, 4] топология с двумя центральными маршрутизаторами – основным и резервным. На каждом центральном настроен отдельный туннельный интерфейс для каждого периферийного. На периферийных в свою очередь настроено по два туннельных интерфейса, к основному и резервному. Headend-1 – является активным и пропускает трафик, в то время как резервный поддерживает дополнительные p2p GRE (Generic Routing Encapsulation) [5] туннели. Посредством протокола динамической маршрутизации определяется, какой из тунелей является активным либо можно выполнить балансировку нагрузки. Число Headend может быть сколь угодно большим, и они могут быть территориально разнесены.

В качестве протокола динамической маршрутизации используется EIGRP (Enhanced Interior Gateway Routing Protocol) [6], можно применить и другой, например OSPF [7]. В случае если активный Headend стал недоступен, активным становится резервный туннель. Если метрика для туннелей к Headend-1 и 2 одинакова, то после восстановления работоспособности первого маршрутизатора активным он не станет. Для автоматического переключения на основной Headend, после его восстановления, необходимо уменьшить метрику на основном туннельном интерфейсе по сравнению с резервным. Например, увеличить задержку на резервном туннельном интерфейсе периферийного маршрутизатора. По умолчанию для подсчета метрики используются bandwidth и delay.

Настройка p2p GRE на Headend-1

Создаем туннельный интерфейс для взаимодействия с Branch-1:

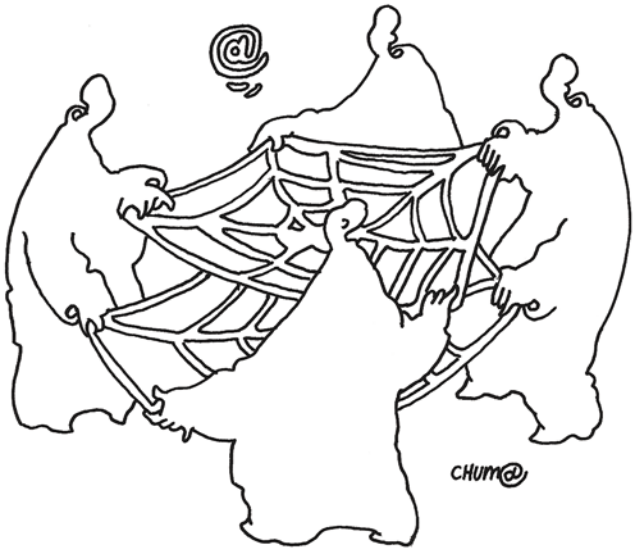
```
interface Tunnel1
 description Tunnel_to_Branch-1
 ! Полоса пропускания 10000 Кбит
 bandwidth 10000
 ip address 10.1.1.1 255.255.255.0
 ! Поместим в таблицу маршрутизации как внутренний маршрут
 ip summary-address eigrp 1 10.1.1.0 255.255.255.0
 ! Интервал 30 секунд для вычисления загрузки интерфейса,
 ! по умолчанию установлено значение 5 минут
 load-interval 30
 ! Настройка соответствия между туннельным интерфейсом
 ! и физическим. В качестве адреса отправителя
 ! в выходящем пакете будет использоваться IP-адрес
 ! физического интерфейса(source), адрес получателя
 ! указываем при помощи параметра destination
 tunnel source 172.16.1.1
 tunnel destination 172.16.1.101
```

Создаем туннельный интерфейс для Branch-2, для Branch-n действуем аналогично:

```
interface Tunnel2
 description Tunnel_to_Branch-2
 bandwidth 10000
 ip address 10.1.2.1 255.255.255.0
 ip summary-address eigrp 1 10.1.2.0 255.255.255.0
 tunnel source 172.16.1.1
 tunnel destination 172.16.1.102
```

Создаем политику ISAKMP, которая будет использоваться при подключении Branch.

```
crypto isakmp policy 1
 hash md5
 encryption 3des
 authentication pre-share
 group 2
crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0
```



Определяем список выполняемых операций для установки подлинности данных, конфиденциальности и сжатия:

```
crypto ipsec transform-set rtpset esp-des esp-md5-hmac
```

Создаем списки доступа для удаленных Branch. Весь трафик между сайтами инкапсулируется в p2p GRE-пакет дочпроцесса шифрования, поэтому необходимо открыть только GRE-протокол:

```
access-list 111 permit gre host 172.16.1.1 host 172.16.1.101
access-list 112 permit gre host 172.16.1.1 host 172.16.1.102
```

Для каждого Branch создаем динамическую крипто-карту rtp:

```
crypto map rtp 1 ipsec-isakmp
 set peer 172.16.1.101
 set transform-set rtpset
 match address 111

crypto map rtp 2 ipsec-isakmp
 set peer 172.16.1.102
 set transform-set rtpset
 match address 112
```

Внешний сетевой интерфейс: включаем VPN сервер, назначаем ACL, меняем значение MTU, MSS [8]:

```
access-list 101 remark 'External interface'
access-list 101 permit udp 172.16.1.0 0.0.0.255 ↵
       host 172.16.1.1 eq isakmp
access-list 101 permit esp 172.16.1.0 0.0.0.255 ↵
       host 172.16.1.1
access-list 101 permit ahp 172.16.1.0 0.0.0.255 ↵
       host 172.16.1.1
access-list 101 deny ip any any log

int fa0/0
 ip address 172.16.1.1 255.255.255.0
 ip access-group 101 in
 load-interval 30
 ip mtu 1300
 ip tcp adjust-mss 1260
 crypto map rtp
```

Рисунок 1. p2p GRE over IPsec Failover Headend topology

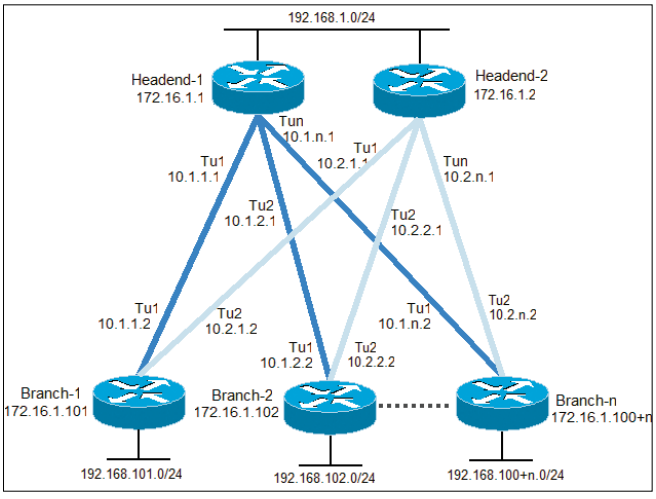
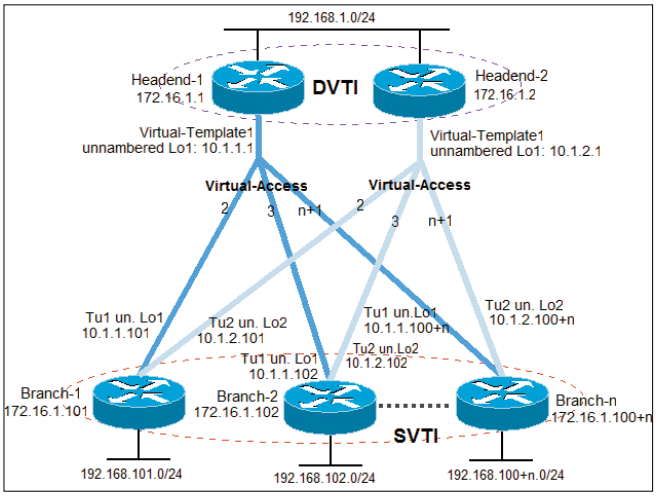


Рисунок 2. IPSec VTI Failover Headend topology



Динамическая маршрутизация:

```
router eigrp 1
 network 10.1.1.0 0.0.0.255
 network 10.1.2.0 0.0.0.255
 network 192.168.1.0 0.0.0.255
 no auto-summary
```

Конфигурация Headend-2 аналогична Headend-1, отличия лишь в IP-адресах, согласно рис. 1.

Настройка p2p GRE на Branch-1

Для задействования механизма автоматического переключения на основной маршрутизатор изменяем задержку пропускной способности туннельных интерфейсов. Для tunnel 1 установлено значение 100, а для tunnel 2 – 200, таким образом уменьшаем метрику к Headend-1 по сравнению с Headend-2.

```
crypto isakmp policy 1
 hash md5
 encryption 3des
 authentication pre-share
 group 2
crypto isakmp key cisco123 address 172.16.1.1
crypto isakmp key cisco123 address 172.16.1.2

crypto ipsec transform-set rtpset esp-des esp-md5-hmac

access-list 111 permit gre host 172.16.1.101 ↵
        host 172.16.1.1
access-list 112 permit gre host 172.16.1.101 ↵
        host 172.16.1.2

crypto map rtp 1 ipsec-isakmp
 set peer 172.16.1.1
 set transform-set rtpset
 match address 111

crypto map rtp 2 ipsec-isakmp
 set peer 172.16.1.2
 set transform-set rtpset
 match address 112

access-list 101 remark 'External interface'
access-list 101 permit udp 172.16.1.0 0.0.0.255 ↵
        host 172.16.1.101 eq isakmp
access-list 101 permit esp 172.16.1.0 0.0.0.255 ↵
        host 172.16.1.101
access-list 101 deny ip any any log

int fa0/0
 ip address 172.16.1.101 255.255.255.0
 ip access-group 101 in
 ip mtu 1400
 ip tcp adjust-mss 1360
 load-interval 30
 crypto map rtp

interface Tunnel1
 description Tunnel_to_Headend-1
 bandwidth 100
 ! Задержка пропускной способности интерфейса
 delay 100
 ip address 10.1.1.2 255.255.255.0
 ip summary-address eigrp 1 10.1.1.0 255.255.255.0
 tunnel source 172.16.1.101
 tunnel destination 172.16.1.1

interface Tunnel2
 description Tunnel_to_Headend-2
 bandwidth 1000
 delay 200
 ip address 10.2.1.2 255.255.255.0
 ip summary-address eigrp 1 10.2.1.0 255.255.255.0
 load-interval 30
 tunnel source 172.16.1.101
 tunnel destination 172.16.1.2

router eigrp 1
 network 10.1.1.0 0.0.0.255
 network 10.2.1.0 0.0.0.255
 network 192.168.101.0 0.0.0.255
 no auto-summary
```

Конфигурация Branch-2(n) аналогична Branch-1, отличия лишь в IP-адресах, согласно рис. 1.

Преимущества: Сеть может быть построена как с использованием одного, так и нескольких центральных узлов для обеспечения резервирования устройств и каналов связи. Пересылка информации об IP-сетях осуществляется по зашифрованным туннелям между подразделениями компании при помощи протоколов динамической маршрутизации. Поддерживается на всех IOS-маршрутизаторах. Возможность назначить отдельную QoS-политику для каждого туннеля. Обеспечивает передачу широковещательного и маршрутизируемого трафика через туннели. Основным преимуществом и отличием от технологии IPSec VPN Site-to-Site является поддержка протоколов динамической маршрутизации IP multicast-трафик может передаваться через VPN-туннель.

Недостатки: Основным недостатком является статическая конфигурация каждого p2p GRE-туннельного интерфейса, вследствие чего при добавлении нового Branch необходимо настраивать каждый Headend-маршрутизатор. То есть реализует функции, аналогичные DMVPN, но требует более объемной и детальной конфигурации.

IPSec Virtual Tunnel Interface

IPSec virtual tunnel interfaces (VTIs) [9] имеет множество преимуществ перед другими вариантами IPsec, включая динамическую маршрутизацию и передачу информации без дополнения p2p GRE и mGRE (используемого в DMVPN). При создании VPN мы должны четко разграничить центральный и периферийные узлы, так как их конфигурация может значительно различаться, а именно использование динамических и статических VTI.

Static VTI (SVTI) очень похож на реализацию point-to-point GRE туннеля. С технической точки зрения, у этого решения те же самые преимущества и недостатки, как и у реализации GRE, отличие заключается лишь в том, что VTIs поддерживает только IP (unicast и multicast), в то время как GRE поддерживает и другие протоколы (non -ip). С точки зрения конфигурации, отличие от p2p GRE, будет заключаться в другом способе настройки туннельного интерфейса.

Dynamic VTI (DVTI) реализован через virtual-templates, расширяющегося до индивидуальных virtual-access, и очень похож на реализацию DMVPN. Конфигурация virtual-access-интерфейса клонируется для каждого периферийного узла из virtual-template.

Статическая конфигурация туннелей требует наличия большого количества туннельных интерфейсов. Замена индивидуальных SVTI на DVTI на центральных узлах позволит значительно упростить конфигурацию. Комбинация DVTI-SVTI [9, 10] требует минимальной конфигурации по сравнению с p2p GRE и DMVPN. В таблице приведены дополнительные комбинации. Пример использования отказоустойчивой схемы DVTI [11, 12] на центральных узлах и SVTI на периферийных узлах представлен на рис. 2.

Настройка DVTI на Headend-1

Список контроля доступа для внешнего сетевого интерфейса. Открываем только необходимые порты: Authentication Header Protocol(AHP), ESP и UPD ISAKMP:

```
access-list 101 remark 'Ext int'
access-list 101 permit udp 172.16.1.0 0.0.0.255 ↵
       host 172.16.1.1 eq isakmp
access-list 101 permit esp 172.16.1.0 0.0.0.255 ↵
       host 172.16.1.1
access-list 101 permit ahp 172.16.1.0 0.0.0.255 ↵
       host 172.16.1.1
access-list 101 permit icmp 172.16.1.0 0.0.0.255 ↵
       172.16.1.0 0.0.0.255 echo
access-list 101 permit icmp 172.16.1.0 0.0.0.255 ↵
       172.16.1.0 0.0.0.255 echo-reply
```

Политика инспектирования трафика:

```
ip inspect name FW isakmp
ip inspect name FW icmp
ip inspect name FW udp
ip inspect name FW tcp
```

Внешний сетевой интерфейс: назначаем список доступа, устанавливаем значения MTU, MSS и интервал для вычисления загрузки интерфейса, ассоциируем политику инспектирования FW.

```
int fa0/0
ip address 172.16.1.1 255.255.255.0
 ip inspect FW out
 ip access-group 101 in
 load-interval 30
 ip mtu 1300
 ip tcp adjust-mss 1260
```

Для быстрой коммутации IP-пакетов необходимо включить Cisco Express Forwarding:

```
ip cef
```

Создаем политику ISAKMP, которая будет использоваться при подключении Branch.

```
crypto isakmp policy 1
 hash md5
 encryption 3des
 authentication pre-share
 group 2
crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0
crypto isakmp invalid-spi-recovery
crypto isakmp keepalive 120 30 periodic
```

Определяем группу Diffie-Hellman, указываем алгоритмы хеш-функции и шифрования, разрешаем аутентификацию с любого IP-адреса с ключом cisco123. Ресинхронизация базы SA в случае потери peer и keepalive, интервал для Dead Peer Detection (DPD):

Включаем виртуальные профили:

```
virtual-profile virtual-template 1
```

ISAKMP-профиль [13] необходим для ассоциации параметров с IPSEC-туннелем. Связываем динамический VTI-интерфейс с IP-адресом внешнего физического интерфейса.

```
crypto isakmp profile isakmp_prof
 keyring default
 match identity address 0.0.0.0
 virtual-template 1
 local-address 172.16.1.1
```

Определяем список выполняемых операций для установки подлинности данных, конфиденциальности и сжатия:

```
crypto ipsec transform-set rtp_set esp-des esp-md5-hmac
```

IPSec-профиль [11] определяет параметры, которые будут использоваться для шифрования между IPSEC-маршрутизаторами. Необходим для ассоциации isakmp-профиля, transform-set и Perfect Forward Secrecy (PFS)[11] с VTI:

```
crypto ipsec profile ipsec_prof
 set transform-set rtp_set
 set pfs group2
 set isakmp-profile isakmp_prof
```

Создание ключа для аутентификации EIGRP:

```
key chain vti_chain
 key 10
  key-string cisco101
```

Loopback-интерфейс для Virtual-Template. Каждый интерфейс в сети с последовательными линиями связи будет требовать отдельную подсеть. Так как каждая последовательная линия связи имеет лишь два узла, то остаются неиспользованными 252 адреса на каждой последовательной линии. Непронумерованные (unnumbered) IP позволяют «позаимствовать» адрес у интерфейса локальной сети для использования в качестве исходного адреса для маршрутизируемых обновлений и пакетов с этого интерфейса.

```
interface Loopback1
 ip address 10.1.1.1 255.255.255.255
```

Создаем Virtual-Template интерфейс:

```
interface Virtual-Template1 type tunnel
 ! Полоса пропускания
 bandwidth 10000
 ! Ассоциация с loopback
 ip unnumbered Loopback1
 ! Ассоциация с созданным ранее ключом vti_chain
 ! для аутентификации EIGRP-соседей
 ip authentication mode eigrp 1 md5
 ip authentication key-chain eigrp 1 vti_chain
 ! Добавляем в таблицу маршрутизации
 ! как внутренний маршрут
 ip summary-address eigrp 1 10.1.1.1 255.255.255.255
 ! Ведение журнала UPDOWN состояний подинтерфейсов
 logging event subif-link-status
 ! Соответствие между туннельным интерфейсом
 ! и физическим интерфесом
 tunnel source fa0/0
 ! Режим инкапсуляции туннеля
 tunnel mode ipsec ipv4
 ! Ассоциация с ipsec-профилем
 tunnel protection ipsec profile ipsec_prof
```

Таблица 1. Комбинации VTI

Центральный узел	Периферийный узел
Static VTI	Static VTI
Dynamic VTI	Static VTI
Dynamic VTI	Static crypto map
Dynamic VTI	Easy VPN remote

Динамическая маршрутизация:

```
router eigrp 1
 network 10.1.1.1 0.0.0.0
 network 192.168.1.0 0.0.0.255
 no auto-summary
```

Конфигурация Headend-2 аналогична Headend-1, отличия лишь в IP-адресах согласно рис. 2.

Настройка SVTI на Branch-1

Механизм переключения на основной Headend-маршрутизатор аналогичен реализованному в p2p GRE over IPsec:

```
access-list 101 remark 'Ext int'
access-list 101 permit udp 172.16.1.0 0.0.0.255 ↵
        host 172.16.1.101 eq isakmp
access-list 101 permit esp 172.16.1.0 0.0.0.255 ↵
        host 172.16.1.101
access-list 101 permit ahp 172.16.1.0 0.0.0.255 ↵
        host 172.16.1.101
access-list 101 permit icmp 172.16.1.0 0.0.0.255 ↵
        172.16.1.0 0.0.0.255 echo
access-list 101 permit icmp 172.16.1.0 0.0.0.255 ↵
        172.16.1.0 0.0.0.255 echo-reply

int fa0/0
 ip access-group 101 in
 ip access-group 101 in
 load-interval 30
 ip mtu 1300
 ip tcp adjust-mss 1260

key chain vti_chain
 key 10
  key-string cisco101

crypto isakmp policy 1
 hash md5
 encryption 3des
 authentication pre-share
 group 2

crypto isakmp key cisco123 address 172.16.1.1
crypto isakmp key cisco123 address 172.16.1.2
crypto isakmp invalid-spi-recovery
crypto isakmp keepalive 120 30 periodic

crypto ipsec transform-set rtp_set esp-des esp-md5-hmac

crypto ipsec profile ipsec_prof
 set transform-set rtp_set
 set pfs group2

interface Loopback1
 ip address 10.1.1.101 255.255.255.255

interface Loopback2
 ip address 10.1.2.101 255.255.255.255

interface Tunnel1
 description Tunnel_to_Headend-1
 bandwidth 1000
 delay 100
 ip unnumbered Loopback1
 ip authentication mode eigrp 1 md5
 ip authentication key-chain eigrp 1 vti_chain
 tunnel source fa0/0
 tunnel destination 172.16.1.1
 tunnel mode ipsec ipv4
 tunnel path-mtu-discovery
 tunnel protection ipsec profile ipsec_prof

interface Tunnel2
 description Tunnel_to_Headend-2
 bandwidth 1000
 delay 200
 ip unnumbered Loopback2
 ip authentication mode eigrp 1 md5
 ip authentication key-chain eigrp 1 vti_chain
 tunnel source fa0/0
 tunnel destination 172.16.1.2
 tunnel mode ipsec ipv4
 tunnel path-mtu-discovery
 tunnel protection ipsec profile ipsec_prof

router eigrp 1
 network 10.1.1.101 0.0.0.0
 network 10.1.2.101 0.0.0.0
 network 192.168.101.0 0.0.0.255
 no auto-summary
```

Конфигурация Branch-2(n) аналогична Branch-1, отличия лишь в IP-адресах согласно рис. 2.

Преимущества: Гибкость dynamic VTI в комбинациях с static crypto maps, static VTIs и Easy VPN, поддержка IP multicast, динамические протоколы маршрутизации, все туннели (основные и резервные) предустановленны. Работа VTI подобна работе реального интерфейса, т.е. могут быть применены QoS, firewall, ACL, Netflow. По сравнению с DMVPN конфигурация периферийных узлов проще, т.к. нет необходимости использовать mGRE и NHRP.

Недостатки: Отсутствует поддержка non-IP протоколов. Сложность поиска неисправностей по сравнению с p2p GRE over IPsec.

***

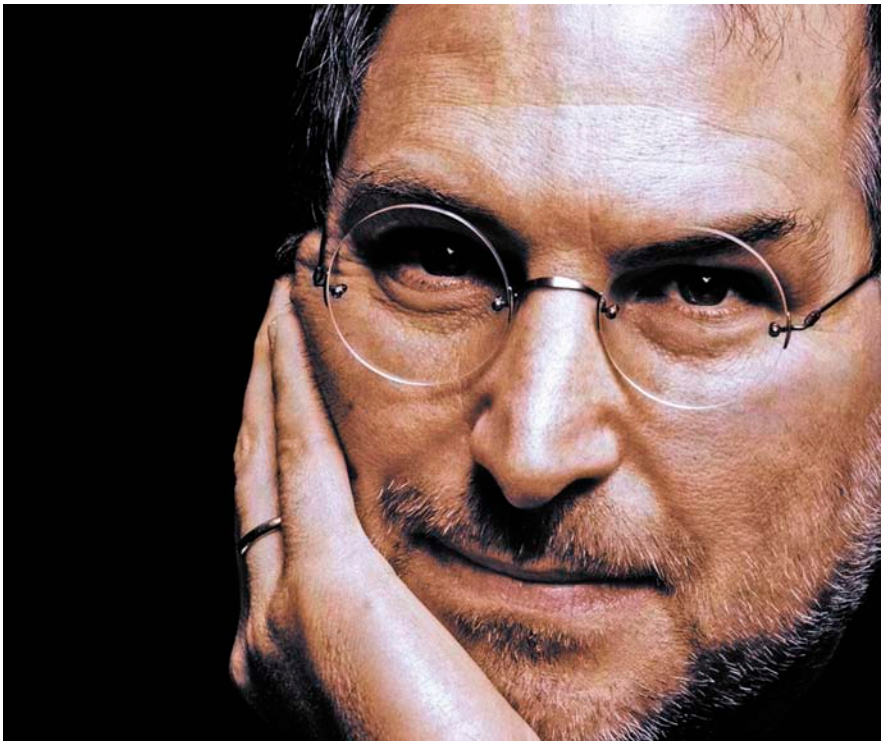
VTI – сравнительно новая технология, может быть использована при тех же требованиях, как p2p GRE over IPsec и DMVPN. Перечень платформ, поддерживающих технологию, доступен по адресу [3]. EOF

1. Панин И. Корпоративные VPN на базе Cisco. //Системный администратор, №6, 2009 г. – С. 78-84.
2. Панин И. WebVPN на базе Cisco IOS. //Системный администратор, №7, 2009 г. – С. 66-69.
3. IPsec VPN WAN Design Overview – http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/IPSec_Over.html.
4. Point-to-Point GRE over IPSec – http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/P2P_GRE_IPSec/p2pGRE.pdf.
5. Generic Routing Encapsulation – http://ru.wikipedia.org/wiki/GRE.
6. EIGRP – http://xgu.ru/wiki/EIGRP.
7. OSPF – http://xgu.ru/wiki/OSPF.
8. Resolve IP Fragmentation, MTU, MSS – http://www.cisco.com/en/US/tech/tk827/tk369/technologies_white_paper09186a00800d6979.shtml.
9. IPSec Virtual Tunnel Interface – http://www.cisco.com/en/US/docs/ios/12_3t/12_3t14/feature/guide/gtIPSctm.htm.
10. Configuring Cisco Easy VPN with IPSec Dynamic Virtual Tunnel Interface (DVTI) – https://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6635/prod_white_paper0900aecd803645b5.html.
11. Configuring Dual Tunnel with Cisco IOS Easy VPN Using Auto Configuration Update – http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6635/prod_white_paper0900aecd8039e301_ps6659_Products_White_Paper.html.
12. Hub and Spoke VPN with VTI, dual hubs, spokes with redundant internet access – http://inetpro.org/wiki/Hub_and_Spoke_VPN_with_VTI,_dual_hubs,_spokes_with_redundant_internet_access#Spoke_Internet_uplinks.
13. Cisco IOS Security Command Reference – http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html.

ВЛАДИМИР ГАКОВ, журналист, писатель-фантаст, лектор. Окончил физфак МГУ. Работал в НИИ. С 1984 г – на творческой работе. В 1990-91 гг. – Associate Professor, Central Michigan University. С 2003 г. преподает в Академии народного хозяйства. Автор 8 книг и более 1000 публикаций

Харизматик-искуситель

Стив Джобс — это гений креатива! Никто из писавших о его компании не смог обойтись без «яблочных» ассоциаций. Спасибо компьютерному гуру



Креативные провокации сопровождали историю компании Стива Джобса с того самого дня, 1 апреля 1976 года, когда в одном из калифорнийских клубов компьютерных фанатов два студента-недоучки презентовали друзьям по увлечению новый компьютер Apple I. Тогда, кстати, никто не воспринял новинку как первоапрельскую шутку. Наоборот, с тех пор к любой продукции, выходившей под торговой маркой Apple, компьютерный мир относится запредельно серьезно. Потому что где Джобс – так жди неожиданностей. С каким знаком – это уж как фишка ляжет.

Райское яблочко

За тридцать лет фирма с надкушенным разноцветным яблоком на эмблеме испытала не один взлет – и, наверное, столько же падений. А продолжающееся по сей день идейное противостояние между «яблочниками» (фанатами компьютеров Macintosh) и «писишниками» (соответственно пользователями персоналок, совместимых с IBM PC) по ожесточенности и непримиримости сравнимо разве что с войной «тупоконечников» с «остроконечниками», описанной Свифтом.

Для тех, кто позабыл: в придуманной великим английским сатириком Лилипутии веками не прекращалась политическая свара, в которой столкнулись лбами две партии – сторонников разбивать яйца всмятку с тупого конца и тех, кто принципиально лупил их с острого. Примерно то же самое вот уже более трех десятилетий происходит на рынке персональных компьютеров.

Первый залп этой войны прозвучал в середине 1970-х, когда два молодых человека, Стив Джобс и Стив Возняк, создали легендарную фирму Apple Computer. Они подружились еще в школе, поскольку питали одну общую страсть. Электроника занимала все свободное время – парочка вундеркиндов вечно что-то паяла и настраивала, игнорируя другие радости детства. Потом друзья одновременно поступили в университет и оба же в одночасье бросили учебу, не дождавшись диплома. Им захотелось заняться настоящим делом.

Под настоящим делом Джобс, бесспорный заводила в дуэте, понимал бизнес – не только конструирование компьютеров (в этом как раз больше преуспел Возняк), но и их продажу. Что казалось невероятным, потому что с детства Джобс был безнадежным интровертом и предпочитал делать все не так, как остальные. Для бизнеса – не самые лучшие качества, хотя порой они становятся поистине козырными.

Из жизни хулиганов-вундеркиндов

В школе Стив Джобс предпочитал общаться с учениками старших классов (одним из таких был Стив Возняк), в качестве учителя и наставника! Первым изобретением двух Стивов, а также успешным бизнес-проектом, стал прототип современного Blue Box (фильтра-шифратора, позволявшего скрывать от пристального ока телефонных компаний произведенные междугородние звонки). Во время учебы в Беркли Возняк начал «левое» производство таких аппаратов, а их продажей занимался школьник Джобс. Однажды Возняк даже дозвонился до Ватикана и, представившись госсекретарем США Генри Киссинджером (подделать его голос для юных «телефонных хакеров» труда не составило), попросил соединить его с самим папой. К счастью для обоих Стивов, понтифик в тот момент почивал, и «историческая телефонная беседа» была перенесена.

Прежде чем создать собственную фирму, друзья успели засветиться в популярном калифорнийском компьютерном клубе Homebrew (буквально – «Домашней перегонке»!). И поработать «на дядю», благо соответствующих фирм в пригороде Сан-Франциско, получившем название Силиконовой долины, было как секвой в окрестных лесах. Джобс получил место в фирме Atari, знаменитой своими игровыми приставками, а его друг – в тогда еще не раскрученной Hewlett Packard.

Там Возняк и начал в свободное время конструировать машину, превратившуюся к 1976 году в персональный компьютер Apple I. Появился он, как и многие высокотехнологичные американские чудеса той романтической эпохи, в старом гараже. Джобс, усмотрев в этом начинании приятеля сказочные потенции, посоветовал Возняку немедленно брать расчет, уволился сам, и они на пару быстро организовали фирму Apple Computer. Штаб-квартира ее разместилась в том же гараже.

Официальная дата рождения компании совпадает с днем рождения компьютера Apple I – 1 апреля 1976 года. Не самый удачный день для серьезного предприятия, однако, Джобс и Возняк не были суеверными. Их не смутил даже более чем прохладный прием первого «яблочного» продукта, который продавался по вызывающей цене $666,66 – она-то была провокационнее некуда!

Грубоватый ящик без дисплея (какой-то блок питания, а не компьютер!) оказался слишком маломощным и примитивным для специалистов и в то же время чересчур сложным и неудобным для пользователей-любителей. Фактически Джобс и Возняк продавали лишь готовую плату, а деревянный корпус счастливому покупателю приходилось мастерить самому в домашних условиях. Тем не менее, 1160 компьютеров все-таки разошлись по окрестным магазинам.

Друзья учли критические замечания и ровно через год порадовали мир уже настоящим шедевром – моделью Apple II, продававшейся по цене $1298. Ничего подобного рынок доселе не видел. Симпатичный пластмассовый корпус со встроенным дисплеем, удобная клавиатура, игровой порт, бытовой магнитофон в качестве жесткого диска, невиданная цветная графика… Короче, машина произвела сенсацию.

Друзья впервые представили новинку на региональной компьютерной ярмарке в апреле 1977 года, и вскоре от заказчиков не стало отбоя – особенно после того, как фирма выпустила дешевый и удобный дисковод для флоппи-дисков Apple Disc II. Без преувеличения можно сказать, что в те дни в американском компьютерном мире существовал один-единственный хит, приобрести который мечтали буквально все: Apple II.

Президент Apple считал Стива Джобса опасным бунтарем. Руководитель крупной корпорации позволял себе являться на работу небритым и босым!

Надкушенное яблоко

Дела двух Стивов шли лучше некуда: росли объемы продаж, а вместе с ними и фирма. К 1980 году штат Apple Computer превышал несколько тысяч человек, и «яблочники», завалив страну своей продукцией, начали бойко ее экспортировать. Инвестировать в Apple Computer считалось хорошим тоном в деловом мире, тем более что друзья сообразили ввести ряд наиболее важных инвесторов в состав правления. Будущее обоим Стивам представлялось безоблачным.

Однако и в компьютерном мире тоже действует закон моря: как назовешь корабль, так он и поплывет. Выбранное в качестве логотипа радужное яблоко с характерным надкусом оказалось пророческим – уже в 1981 году Apple Computer изрядно покусали. Причем сразу с нескольких сторон.

Компьютерный рынок переживал тогда не лучшие времена: Джобс с Возняком были вынуждены резко сократить численность персонала. Тут же последовал новый удар – Стив Возняк попал в авиакатастрофу. Получив тяжелые травмы, он отошел от дел. Как оказалось, навсегда. Оставшись в одиночестве, Джобс занял пост председателя правления Apple Computer, имея всего 11% акций. И тут же приступил к разработке одного из лучших своих проектов – серии легендарных персоналок Macintosh, сокращенное название которых (MAC) прочно вошло в сленг XX века.

Но это произойдет чуть позже. Пока же, в 1981 году, перчатку, брошенную Джобсом, поднял настоящий тяжеловес на рынке персональных компьютеров – компания IBM. В отличие от Apple Computer, «Голубой гигант» (как прозвали IBM за ее эмблему – голубой прямоугольник) располагал несравнимо большими ресурсами и выпустил свою версию персонального компьютера – модель 5150 Personal Computer, или сокращенно IBM PC. Фактически это и был первый в мире персональный компьютер, по крайней мере официально признанный таковым.

Ситуация становилась угрожающей. Джобс чувствовал, что его детищу нужно стремительно взрослеть, чтобы успешно конкурировать с таким зубром, как IBM. Для этого первым делом следовало подыскать себе достойную замену на административном посту, чтобы посвятить все время своему MAC'у.

В начале 1983 года, как пишут биографы, «Джобс начал настойчиво обхаживать тогдашнего президента компании Pepsi Джона Скалли – и к апрелю добился своего». Скалли пересел в президентское кресло Apple Computer, одновременно заняв пост исполнительного директора. Джобс, оставшись председателем правления, ликовал: пришел человек, который выведет компанию из порядком затянувшегося переходного возраста! Скалли действительно вдохнул жизнь в захиревшую компанию, хотя особой радости ее основателю это не доставило.

Новый президент Apple Computer был опытным и удачливым бизнесменом, но, как быстро выяснилось, плохо ориентировался в компьютерной отрасли. Неудивительно, что отношения между двумя руководителями Apple быстро испортились.

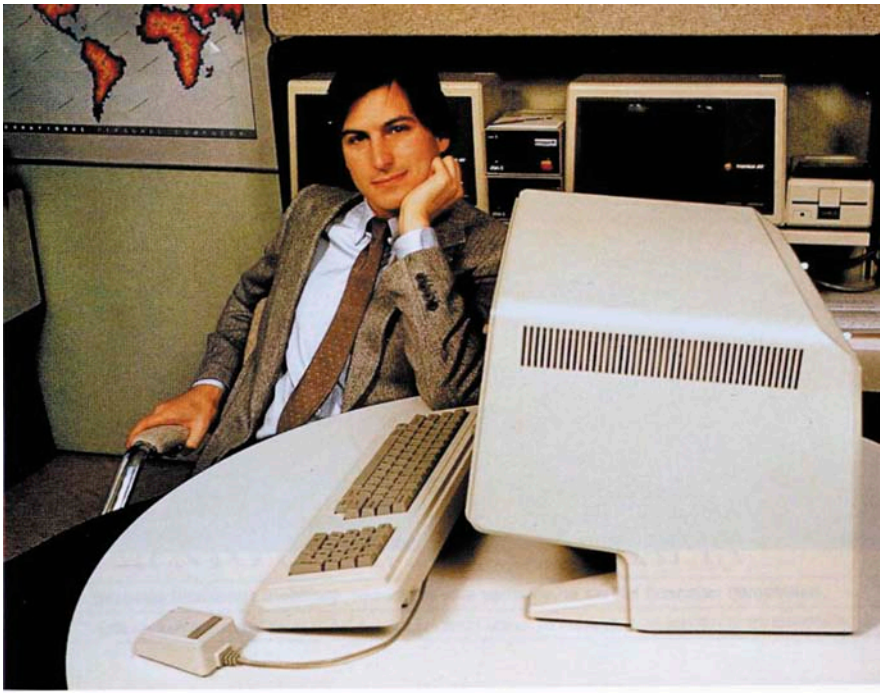
Все надежды Джобс по-прежнему связывал с MAC. Стремясь поскорее вывести его на рынок, он работал в сумасшедшем режиме, вникая в каждую мелочь, будь то «железо» или разрабатываемое специально для Macintosh программное обеспечение.

22 января 1984 года, во время финального матча чемпионата по американскому футболу (Super Bowl), за которым, естественно, следила вся страна, среди рекламных вставок появилась и 60-секундная «яблочная», да какая! Рекламный ролик создал творец культовых научно-фантастических фильмов «Чужой» и «Бегущий по лезвию» Ридли Скотт, поэтому реклама нового компьютера была облечена в соответствующую форму. Америка увидела мир-тюрьму, находившийся под неусыпным оком электронного Большого Брата (намек на Оруэлла), в котором трудно было не узнать корпорацию IBM. Но затем «царство тирании» буквально рассыпалось на части, и «свобода встречала радостно у входа». Свободу олицетворял, конечно, новый Macintosh.

Гнилые яблоки

Поначалу продажи новой модели превзошли самые смелые ожидания. Хотя ситуация быстро менялась невыгодным для Apple образом, MAC стал одним из важных атрибутов американской жизни.

Теперь аббревиатура из трех букв служила паролем, с помощью которого узнавали друг друга члены неформального «клуба избранных». Иметь у себя настольный MAC (портативные придут позже), читать MAC-журналы, играть в MAC-игры (это была самая сильная сторона нового компьютера), обмениваться MAC-информацией с такими же MAC-фанатами стала не просто модой, а свидетельством тогдашней крутизны в компьютерной среде.



С тех пор мир юзеров, как в Лилипутии Свифта, поделен на сторонников MAC и PC. Произведения каждого из соперников имели свои достоинства и недостатки. Творение Джобса обладало уникальным графическим интерфейсом. Вместо унылых строчек с текстом и символами перед лицом пользователя была образная и удобная картинка с «окнами», «иконками» и даже «корзиной», куда можно было сбрасывать накопившийся в процессе работы «мусор». Зато первым MAC явно не хватало памяти, имелся и ряд других технических недостатков.

Кроме того, MAC'и стоили дороже PC-совместимых машин, и американский пользователь разрешил спор, проголосовав «зеленым» рублем. За несколько лет IBM PC и его многочисленные версии заметно потеснили на рынке более изощренные и снобистские Macintosh. И хотя верные поклонники Apple продолжали покупать ее продукцию, массовый потребитель, далекий от баталий «тупоконечников» и «остроконечников», приобретал более доступные PC.

В 1985 году конфликт между Скалли и Джобсом достиг кульминации. Президент Apple считал председателя правления опасным, лишенным самоконтроля бунтарем. Что была истинная правда – виданное ли дело, чтобы руководитель крупной корпорации позволял себе являться на работу небритым и босым! Джобс в свою очередь утверждал, что Скалли, ничего не смысля в компьютерах, уверенно ведет компанию к краху (и это позднее

Угадать линию жизни

В колледже Рид, где учился Стив Джобс, одним из коньков были курсы каллиграфии. Уже бросив колледж, будущий глава Apple продолжал посещать занятия по этому древнему ремеслу «красивописания». Казалось бы, что за блажь? «Но спустя десять лет, – вспоминал Джобс, – когда мы разрабатывали первый Macintosh, всё это неожиданным образом пригодилось. Если бы я не бросил учебу, то никогда бы не записался на курс каллиграфии, и вполне вероятно, сегодня у компьютеров не было бы такой изумительной типографики, к которой все привыкли. Правда, я соединил все точки кривой моей жизни гораздо позже. Посему мораль – вы не можете выстроить линию жизни, соединив все ее точки, смотря вперед; соединить их можно, лишь оглядываясь в прошлое. Поэтому вам всегда приходится на что-то положиться, не имея всей информации в руках: на свой характер, судьбу, обстоятельства жизни, карму – на что угодно. Подобный подход никогда не подводил меня, сделав мою жизнь такой, какая есть».

Яблочная война

Проблем у компании Apple хватает. Чего стоит одна многолетняя тяжба за бренд со звукозаписывающей компанией Apple Corps, созданной в 1968 году участниками легендарной группы The Beatles! На все обвинения в «плагиате» (речь идет, конечно же, о самом названии фирмы) Джобс неизменно отвечал в том духе, что «тогда – в шестидесятых – все бредили музыкой The Beatles, и заимствование «яблочной» символики было простой случайностью». Переиначивая известное высказывание, «никакого бизнеса – только личное»…

Однако в 2006 году сэр Пол Маккартни и Ринго Стар, а также наследники покойных Джона Леннона и Джорджа Харрисона посчитали неправомерным вторжение компании Джобса в музыкальный бизнес вообще. На сей раз камнем преткновения стал популярный музыкальный интернет-магазин iTunes, созданный компанией Apple Computers. Экс-«битлы» обвинили компанию Джобса в нарушении соглашения от 1991 года, по которому производитель компьютеров не имеет права торговать музыкой. Ответчики утверждали, что подписанное соглашение позволяло им распространять данные в режиме он-лайн, а скачивание музыки, по сути, этим и является. В настоящее время Apple Corps переиздает записи The Beatles на современных носителях, но через Интернет музыку продавать не пытается, соблюдая договоренности с компанией Стива Джобса.

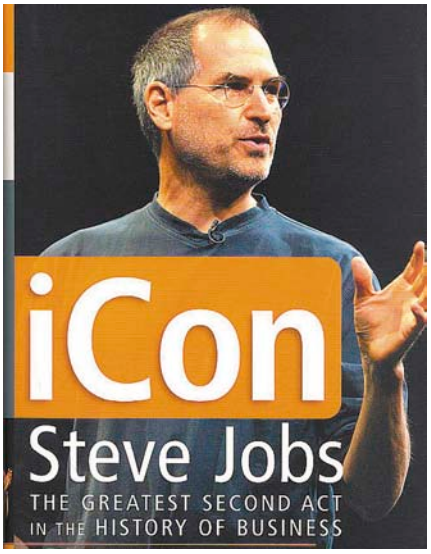
подтвердилось). В конце концов Джобс решил, что с него хватит! Устроив так, чтобы Скалли отправился в престижную командировку в Китай, Джобс намеревался в его отсутствие провести заседание правления, на котором предполагал осуществить «домашний» переворот.

Однако, как часто случается среди заговорщиков, в последний момент кто-то донес Скалли о бунте на корабле. Президент компании, отложив поездку, дал Джобсу открытый бой. Опытному администратору не составило труда выиграть эту битву – вопрос был поставлен на тайное голосование, и большинство членов правления поддержало Скалли. В тот же день Стив Джобс, написав заявление об отставке, покинул компанию.

В первый год «без Джобса» лишились работы почти 1200 человек, что составляло пятую часть всего штата Apple Computer. Первый в истории компании квартал был закончен с убытками. Ко всем бедам добавилась судебная тяжба с компанией Microsoft. Руководство Apple не без оснований углядело в новой операционной системе Билла Гейтса Windows 1.0 слишком много сходства с «яблочным» ноу-хау – операционной системой GUI. В конце концов, Гейтс согласился не использовать «яблочную» технологию в Windows 1.0, но в подписанном между Microsoft и Apple соглашении ничего не говорилось о будущих модификациях Windows! Со временем это привело к фактической потере монополии на графический интерфейс, которым так гордилась компания Apple и который обеспечивал ей поддержку пользователей.

Впрочем, потеряв одних приверженцев, компания неожиданно получила других. На сей раз под «яблочное» знамя встала бурно развивавшаяся издательская отрасль. Выпущенные на рынок лазерный принтер PostScript вкупе с уникальной пионерской программой настольного издательства PageMaker сделали Apple бесспорным лидером в области computer publishing.

Развивая успех, Apple Computer в 1987 году выпустила перспективную модель Mac II. Дела бодро пошли в гору, компания продавала 50 тысяч машин в месяц. По оценке журнала Rolling Stone, «на Уолл-стрит Apple снова стала душечкой». К концу 1980-х годов многим казалось, что золотые времена Windows миновали, фортуна вновь поворачивается лицом к Apple и в следующее десятилетие компания войдет единоличным лидером на рынке персоналок.



Яблочный спас

Однако этого не случилось. У компании началась новая полоса неудач, связанная главным образом с безудержным процессом PC-клонирования. Все компьютерные компании продавали фактически унифицированную продукцию с генеральной лицензией IBM. Этот процесс принял лавинообразный характер после выхода новой операционной системы Windows 3.0 в марте 1990 года. Apple же никого не подпускала к своему уникальному творению! Завод по производству компьютеров Macintosh в калифорнийском городе Кьюпертино был приравнен к секретному объекту.

Кроме того, не оправдал ожиданий и революционный «персональный электронный помощник» Newton: проект, на который делал ставку Джон Скалли, явно опередил свое время. Окончательно потеряв интерес к компьютерному бизнесу, президент Apple в июне 1987 года покинул компанию.

После его ухода дела в компании шли ни шатко, ни валко. Были успехи – например, новое семейство PowerMac на базе микропроцессора PowerPC, разработанного совместно с IBM и Motorola. Но затем следовали провалы. Apple проиграла новую тяжбу с Microsoft в связи с выходом на рынок операционной системы Windows'95, хотя в ней «яблочные мотивы» были видны, что называется, невооруженным взглядом.

В середине 1990-х годов компания терпела неудачу за неудачей, и многие решили, что на «яблочниках» можно ставить крест. Как оказалось, поспешили. Традиции есть традиции, даже тогда, когда традицией становятся нетрадиционные решения. Свой очеред-

ной нетривиальный ход руководство Apple сделало в 1996 году, купив фирму NeXT. Казалось бы, ну и что такого? Ничего, если не знать имени и фамилии тогдашнего владельца NeXT. А владельцем был… Правильно, Стив Джобс!

Так состоялось триумфальное возвращение в Apple блудного сына. Или, по мнению его самых горячих поклонников, непризнанного пророка. Как бы то ни было, неутомимый харизматик Джобс принялся реанимировать компанию с такой энергией и творческой фантазией, что компьютерному миру стало ясно – списывать вечно альтернативных «яблочников» со счетов по крайней мере рано. Первые же новации Джобса впечатляли: он пригласил в совет директоров главу фирмы Oracle Ларри Эллисона (еще один заслуженный харизматик компьютерного мира), запустил новое семейство полупрозрачных цветных iMac'ов, бивших все рекорды популярности.

Вроде бы мелочь – внешний дизайн («начинка» нового семейства не представляла ничего экстраординарного по сравнению с моделями, в то время бывшими на рынке), но Стив Джобс предугадал то, что позже сообразили и другие производители персоналок. Персональный компьютер перестал быть научным прибором и превратился в предмет домашней обстановки. Если не «членом семьи» – как наши песики и кошечки, рыбки и птички. А раз так, то внешний вид нового предмета интерьера менее всего должен был наводить мысль об офисе или лаборатории. Посему прочь черно-серо-белые «ящики» с прямыми углами, даешь палитру цветов и мягкие закругленные формы!

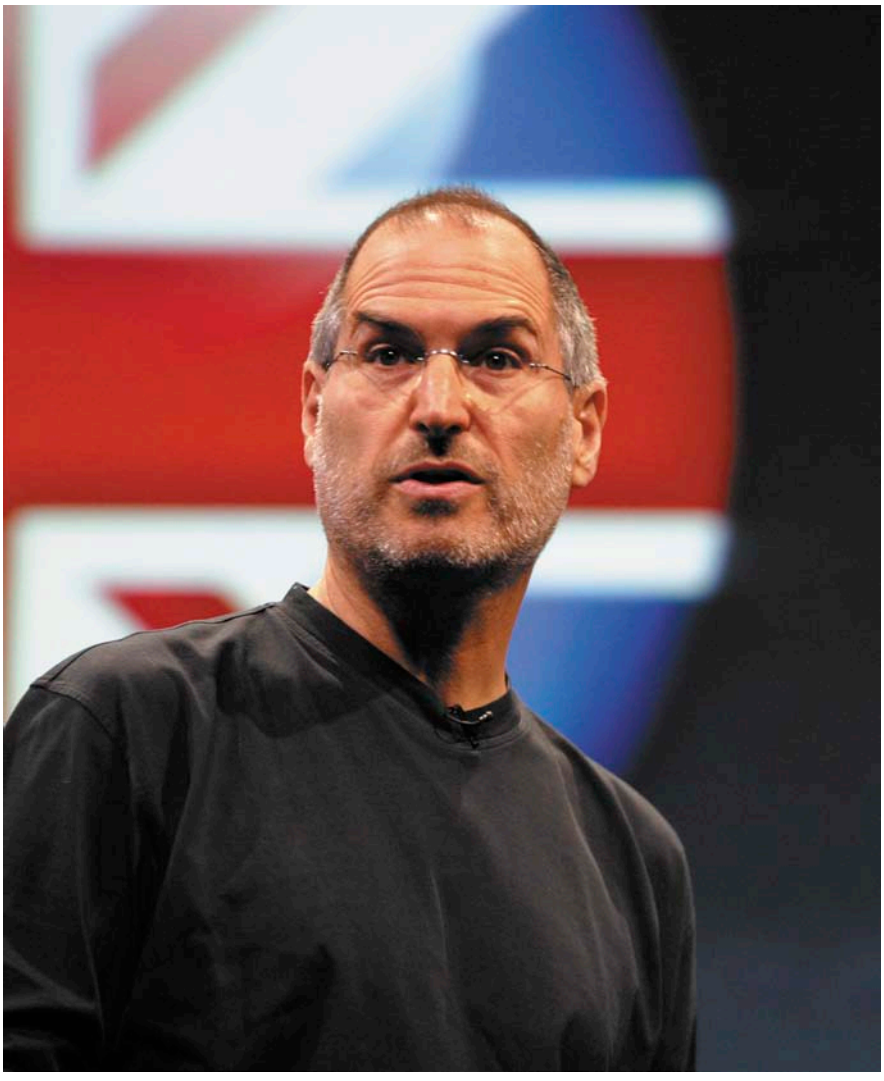
Кроме того, Джобс начал раздачу лицензий на «яблочные» клоны. Передал эксклюзивные права на розничную продажу MAC'ов «тяжеловесу» – компании CompUSA (которая успешно занимается этим делом и поныне). И, наконец, самым интригующим стал альянс между заклятыми врагами – Microsoft и Apple, заключенный в августе 1997 года. «Туконечники» и «остроконечники» обещали взаимно забыть старые обиды, мирным образом урегулировать взаимные претензии и на ближайшие пять лет даже предоставили друг другу все лицензии.

Кроме того, Джобс объявил об агрессивном вторжении Apple на перспективный рынок электронного бизнеса. Спустя считанные недели после создания электронный «яблочный» магазин (The Apple Store) превратился в третий по значению сайт в разделе «электронная коммерция». Компания Джобса вновь стала прибыльной, у нее опять появились стратегические инвесторы – в Apple, например, крупно вложились тот же Эллисон и некий арабский шейх. Позже Стив Джобс активно вторгся на сопредельные территории рынка – в музыкальную индустрию (первый музыкальный интернет-магазин iTunes) и анимационную (возглавил компанию Pixar). Впрочем, вопрос о том, удастся ли Стиву Джобсу вновь сделать свое «яблочное» хозяйство высокоурожайным в новом столетии, остается открытым. Новомодные креативные игрушки Apple и ее бессменного «рулевого» вроде коммуникатора iPhone – это уже обыденная повседневность людей XXI века. Однако новинка вызвала очередной приступ энтузиазма как у восторженных поклонников Джобса, так и у его не менее возбужденных хулителей. А конкуренты не замедлили с «ассиметричным ответом», результатом чего словосочетание «убийца iPhone» прочно вошло в современный сленг.

А кто сказал, что быть пророком легко? Богом – и подавно…

Шесть лет назад врачи нашли у Стива Джобса рак. В январе этого года гуру и пророк объявил, что уходит в полугодовой отпуск по состоянию здоровья. Но аналитики, точно спрогнозировавшие возвращение Джобса в Apple в конце девяностых, полагают, что Джобс еще вернется – чтобы воспитать преемника. В Истории он себе место зарезервировал, и это поважнее, чем какие-то там высокие посты даже в суперуспешных компаниях.

А пока суд да дело, идейное противостояние фанатов MAC и PC продолжается. Ну, действительно, сил нет терпеть, когда какие-то придурки разбивают яйца не с той стороны?! EOF



Визитка

АНДРЕЙ ДУГИН, системный администратор Группы Безопасности информационных систем «МТС-Украина». Специализируется на системах IDS и IPS. Интересы: системная и сетевая безопасность

Cisco IDS/IPS
Безопасная настройка

Системы обнаружения вторжений должны быть правильно сконфигурированы для предотвращения несанкционированного доступа

Самый первый этап защиты – информационный. Очень ограниченное количество специалистов знает о том, что существуют такие устройства, как IDS/IPS, и еще меньше догадывается о том, что они используются в той или иной корпоративной сети. Дальнейшая защита осуществляется технологическими методами.

Командная строка в Cisco IPS/IDS очень похожа на Cisco IOS CLI. В то же время Cisco IPS основаны на Linux RedHat, поэтому возможно управление как IPS, так и ОС.

Примечание: статья не является полным и универсальным руководством по настройке, эксплуатации и обеспечению безопасности систем обнаружения и предотвращения вторжений производства Cisco Systems. Более подробная информация доступна на сайте производителя [1].

Управление учетными записями пользователей

В Cisco IPS определены 4 уровня доступа пользователей:

Administrator – «суперпользователь» IPS. Имеет право на произведение любых действий в IPS CLI, но не имеет доступа в консоль операционной системы.

Operator – доступно большинство функций CLI IPS, кроме управления конфигурационными файлами, пользователями и рестарта/выключения системы.

Viewer – уровень доступа без возможности редактирования.

Service – пользователь консоли Linux.

Рекомендую создать хотя бы одну учетную запись пользователя с уровнем доступа service на случай сбоя mainApp-сенсора, и, как результат, отсутствия возможности входа в Cisco IPS CLI. Доступ в консоль операционной системы позволит диагностировать и, возможно, решить возникшую проблему. Как минимум будет инструмент для сбора необходимой для службы поддержки производителя информации (cidDump, tech-support, logs). Пароль пользователя уровня service используется также для перехода в режим суперпользователя root командой su консоли Linux. Производитель официально предупреждает о том, что вносить изменения, используя уровень доступа service, рекомендуется только в случае прямых указаний службы поддержки [2].

Создание учетной записи пользователя

Производится в режиме глобальной конфигурации. Пароль для пользователя можно ввести как в открытом виде:

```
ids(config)# username test privilege operator password ↵
        u$erp@$$
```

так и в безопасном:

```
ids# configure terminal
ids(config)# username test privilege operator

Enter new login password : **********
Re-enter new login password : **********
```

Увидеть всех пользователей в Cisco IPS CLI можно в режиме, аналогичном EXEC-режиму Cisco IOS, с помощью команды:

```
ids# show users all

    CLI ID   User      Privilege
*   12528    admin     administrator
             andrey    service
             cisco     administrator
             soc       viewer
             test      operator
```

Изменение пароля для учетной записи пользователя

Когда возникает необходимость изменить пароль пользователя, например, при компрометации или стандартной ситуации «забыл пароль», администратор IPS может осуществить операцию с помощью команды (в данном случае для пользователя test):

```
ids(config)# password test

Enter new login password : *********
Re-enter new login password : *********
```

Удаление учетной записи пользователя

В случае необходимости удалить учетную запись пользователя можно командой:

```
ids(config)# no username test
```

При попытке удалить встроенного пользователя cisco получим:

```
ids(config)# no username cisco
```

```
Error: this account cannot be removed.
Use the 'no password' command to disable account.
```

Парольная политика Cisco IPS не позволяет использовать «слабые» пароли для пользователей, однако для большей безопасности рекомендую создать пользователя с правами администратора IPS, а аккаунт cisco заблокировать:

```
ids(config)# no password cisco
```

Определить то, что пользователь cisco заблокирован, можно по круглым скобкам:

```
ids# show users all
```

```
    CLI ID   User      Privilege
*   12528    admin     administrator
             andrey    service
             (cisco)   administrator
             soc       viewer
```

Настройка парольной политики

Парольная политика Cisco IPS по умолчанию предъявляет строгие требования к паролям, однако если есть необходимость ужесточить ее – предоставляется возможность задать:

- длину пароля;
- количество символов верхнего и нижнего регистра в пароле;
- количество цифр и спецсимволов в пароле;
- количество старых паролей, которые помнит сенсор.

Настройки производятся через режим конфигурации службы аутентификации:

```
ids# configure terminal
ids(config)# service authentication
```

Сброс сессии

Определить, что пользователь в данный момент работает с Cisco IPS через CLI, возможно с помощью той же команды show users all. Звездочкой (*) обозначена сессия текущего пользователя:

```
ids# show users all
```

```
    CLI ID   User      Privilege
*   12528    admin     administrator
    14167    soc       viewer
             andrey    service
             (cisco)   administrator
```

Если возникает необходимость сбросить сессию другого пользователя, например, по причине зависания ssh-клиента, тайм-аута, принятия решения о нелегитимности сессии и т.п., определяем ее CLI ID (в данном случае для soc – 14167) и принудительно обрываем:

```
ids# clear line 14167
```

Изменение привилегий пользователя

При необходимости изменения уровня доступа пользователя администратор IPS может произвести эту операцию с существующими пользователями:

```
ids(config)# privilege user test viewer
```

```
Warning: The privilege change does not apply to current
CLI sessions. It will be applied to subsequent logins.
```

Как предупреждает IPS, если пользователь, которому переназначили права доступа, на момент их реконфигурации использует активную сессию, изменения коснутся его только после повторного логина. Соответственно, нужно либо сообщить пользователю о такой необходимости, либо сбросить его сессию.

Для аккаунта cisco также возможно изменение уровня доступа.

Настройки узла

Структура настроек Cisco IPS организована таким образом, что из знакомого всем по IOS режима global config возможен переход в режимы специфической конфигурации каждого сервиса:

```
ids# configure terminal
ids(config)# service host
```

Сетевой доступ

Достаточно важной частью обеспечения безопасности любого сетевого устройства является ограничение доступа по сети. Само собой разумеется, что IP-адрес интерфейса управления сенсора должен находиться в максимально защищенном корпоративными файерволами административном (management) VLAN. Однако для комплексности защиты не помешает настройка собственного брандмауэра IPS. Из режима конфигурации хоста переход в режим конфигурации доступа по сети к сенсору осуществляется так:

```
ids(config-hos)# network-settings
```

В режиме конфигурации любого сервиса возможен просмотр настроек, касающихся сугубо текущего специфического режима с помощью команды:

```
ids(config-hos-net)# show settings
```

```
   network-settings
   ------------------------------------------------
      host-ip: 10.0.1.50/24,10.0.1.1
      default: 192.168.1.2/24,192.168.1.1
      host-name: ids default: sensor
      telnet-option: disabled default: disabled
      access-list (min: 0, max: 512, current: 6)
      ------------------------------------------------
         network-address: 10.0.11.11/32
         ------------------------------------------------
         network-address: 10.0.16.154/32
         ------------------------------------------------
         network-address: 10.0.12.0/27
         ------------------------------------------------
      ------------------------------------------------
      ftp-timeout: 300 seconds <defaulted>
      login-banner-text:  <defaulted>
      dns-primary-server
      ------------------------------------------------
         enabled
         ------------------------------------------------
            address: 10.0.2.5
         ------------------------------------------------
      ------------------------------------------------
      dns-secondary-server
      ------------------------------------------------
         enabled
         ------------------------------------------------
            address: 10.0.2.6
         ------------------------------------------------
      ------------------------------------------------
      dns-tertiary-server
      ------------------------------------------------
         disabled
         ------------------------------------------------
         ------------------------------------------------
      ------------------------------------------------
      http-proxy
      ------------------------------------------------
         proxy-server
         ------------------------------------------------
            address: 10.0.2.7
            port: 3128
         ------------------------------------------------
      ------------------------------------------------
   ------------------------------------------------
```

В access-list указаны хосты и сети, с которых разрешен доступ на IPS по SSH, Telnet (если включен), HTTP (если включен), HTTPS, SNMP (если включен), ICMP.

Если обнаруживаем в списке доступа подсети или хосты, которым в данный момент не нужен доступ к management-интерфейсу и не понадобится в ближайшем будущем, либо в случае критической ситуации – удаляем:

```
ids(config-hos-net)# no access-list 10.0.16.154/32
```

Назначаем banner login

Для того, чтобы иметь возможность предупредить потенциального взломщика об уголовной ответственности, определяем текст баннера при логине, указывающий на преследование незаконных попыток подбора пароля:

```
ids(config-hos-net)# login-banner-text
```

```
This system is restricted to authorized users. Individuals
attempting unauthorized access will be prosecuted.
```

Отключение telnet

Telnet отключен по умолчанию, как требуют нормы безопасности. Если же он оказался включен предыдущим администратором, рекомендуется его отключить:

```
ids(config-hos-net)# telnet-option disabled
```

Автоматические обновления

Для поддержания в актуальном состоянии систем обнаружения вторжений необходимо периодическое обновление сигнатур и системы. Для этого нужна лицензия производителя. Когда в распоряжении администратора 1-2 сенсора, обновление вручную может не создавать особого труда, но если их гораздо больше, стоит настроить автоматическое обновление в целях экономии времени. Автоматическое обновление возможно по протоколам FTP, SCP, HTTP, HTTPS.

Рассмотрим обновление по SCP. Необходим UNIX-сервер обновлений, на котором только создается учетная запись для сенсора с минимальными привилегиями. Корпоративными файерволами обеспечивается доступ по порту 22 от управляющих интерфейсов IDS/IPS к серверу обновлений, если они находятся не в одной подсети. Администратором IPS по мере выхода обновлений и анализа их необходимости файлы выкладываются в определенную папку, а сенсоры рациональнее всего настроить на периодическую проверку наличия обновлений. Файлы, загруженные с сайта производителя, переименовывать категорически не рекомендуется. При обновлении по SCP на сервере, где будут располагаться обновления, должна быть включена поддержка SSHv1 в sshd_config.

На сенсоре для корректной работы обновлений по SCP необходимо добавить ssh-ключ сервера обновлений в список доверенных узлов сенсора:

```
ids# configure terminal
ids(config)# ssh host-key 10.0.105.50
```

```
MD5 fingerprint is
DE:0E:FE:AE:77:F9:4B:0D:69:49:D4:60:26:55:67:52
Bubble Babble is xulir-tyhoc-tehyb-dupez-byvat-tapiz-fepur-
povok-sadem-luhyt-taxux
Would you like to add this to the known hosts table for
this host?[yes]:
```

Затем можно приступать непосредственно к настройке автоапгрейда. Включаем обновление с сервера в корпоративной сети:

```
ids(config)# service host
ids(config-hos)# auto-upgrade
ids(config-hos-aut)# user-server enabled
```

Указываем IP-адрес сервера обновлений:

```
ids(config-hos-aut-ena)# ip-address 10.0.5.5
```

Указываем директорию, в которую будут выкладываться файлы обновлений, относительно пути /home/<username>:

```
ids(config-hos-aut-ena)# directory up
```

Имя пользователя на сервере обновлений:

```
ids(config-hos-aut-ena)# user-name ips
```

Указываем пароль учетной записи сенсора на сервере обновлений:

```
ids(config-hos-aut-ena)# password
```

Затем конфигурируем на обновление либо по календарю, либо периодическое обновление. Я предпочитаю последнее:

```
ids(config-hos-aut-ena)# schedule-option periodic-schedule
```

Задаем интервал в часах:

```
ids(config-hos-aut-ena-per)# interval 24
```

и время обновления. Поскольку в данном случае объем трафика в большинстве случаев будет генерироваться небольшой (объем файла сигнатур порядка 200-300 Кб), критичного влияния нет, я предпочел поставить дневное время, чтобы наблюдать за процессом:

```
ids(config-hos-aut-ena-per)# start-time 12:00
```

Рекомендую настраивать обновления на всех сенсорах в разное время с интервалом порядка 15 минут.

В случае обнаружения некорректной работы обновления сигнатур или движка (engine) либо принятия решения о возврате на предыдущую конфигурацию в CLI используется команда downgrade режима глобальной конфигурации:

```
ids(config)# downgrade
```

Производитель в своей онлайн-документации официально уведомляет о том, что возврат к предыдущей Minor- или Major-версии с помощью команды downgrade осуществить невозможно [3].

Настройка параметров времени

Для того чтобы время отработанных событий совпадало со всеми остальными информационными системами компании, рекомендую настроить синхронизацию времени с корпоративным NTP-сервером. Параметры времени сенсора настраиваются следующим образом:

```
ids(config-hos)# time-zone-settings
```

Указываем смещение в минутах относительно GMT:

```
ids(config-hos-tim)# offset 120
```

И название часового пояса:

```
# EET - название зоны
ids(config-hos-tim)# standard-time-zone-name EET
```

Настраиваем синхронизацию по NTP с сервером, не требующим аутентификации:

```
ids(config-hos)# ntp-option enabled-ntp-unauthenticated
ids(config-hos-ena)# ntp-server 10.0.2.123
ids(config-hos-ena)# exit
```

Настраиваем автоматический переход на летнее время:

```
ids(config-hos)# summertime-option recurring
ids(config-hos-rec)# offset 60
ids(config-hos-rec)# summertime-zone-name EEST
ids(config-hos-rec)# start-summertime
ids(config-hos-rec-sta)# month march
ids(config-hos-rec-sta)# week-of-month last
ids(config-hos-rec-sta)# day-of-week sunday
ids(config-hos-rec-sta)# time-of-day 03:00:00
ids(config-hos-rec-sta)# exit
ids(config-hos-rec)# end-summertime
ids(config-hos-rec-end)# month october
ids(config-hos-rec-end)# week-of-month last
ids(config-hos-rec-end)# day-of-week sunday
ids(config-hos-rec-end)# time-of-day 04:00:00
ids(config-hos-rec-end)# exit
```

Сохранение изменений

Сохраняются нововведения не сразу, а при выходе из подрежима конфигурации хоста в режим global config:

```
ids(config-hos)# exit
Apply Changes?[yes]:
```

Настройка SNMP

По умолчанию управление сенсором по SNMP отключено, но может возникнуть необходимость использования этого протокола для мониторинга и анализа работы сенсора. В этом случае стоит обратить внимание на то, что доступ по SNMP открывается и на чтение, и на запись, даже если нет необходимости в редактировании по SNMP – такова особенность работы Cisco IPS. Потенциальная опасность ясна: каждый, кто знает значения read-write community, имеет возможность конфигурировать сенсор с помощью set-команд. Отдельный access-list для SNMP не создается, используются общие ACL из настроек service host. Аутентификация и шифрование не поддерживаются, поэтому возможны варианты защиты:

- нетривиальные значения community, которые сложно подобрать;
- ограничение доступа по сети как на уровне корпоративных файерволов и ACL-роутеров, так и списков доступа service host;
- использование протокола транспортного уровня TCP, поскольку защита от spoofing в UDP не реализована;
- использование нестандартного порта.

Безопасная настройка производится следующим образом:

```
ids#configure terminal
ids(config)#service notification
ids(config-not)#enable-set-get true
ids(config-not)#read-only-community DlY@_$en$0r@
ids(config-not)#read-write-community DlY@_AdM1n@_$en$orA
ids(config-not)#snmp-agent-protocol tcp
ids(config-not)#snmp-agent-port 1961
ids(config-not)#exit
```

Настройка веб-вервера

Обезопасить веб-вервер необходимо включением TLS (активировано по умолчанию), также можно изменить порт,

на котором он слушает (по умолчанию назначен 443 порт):

```
ids(config)# service web-server
ids(config-web)# enable-tls true
ids(config-web)# port 7001
ids(config-web)# exit
```

```
Apply Changes?[yes]:
```

Настройка логгирования

По умолчанию уровень логгирования на каждую категорию системных событий установлен как warning. В случае необходимости, например, для диагностики возникших проблем, можно внести свои корректировки методом конфигурации service logger. Делать это необходимо очень аккуратно, во избежание перегрузок [4]:

```
ids(config-not)#exit
```

Настройка дампов

При использовании Cisco IDS/IPS может возникнуть необходимость записи дампов трафика определенного пользователя, сервера и т.п. Нужно учесть, что по умолчанию количество дампов, которые могут одновременно находиться на сенсоре, равно 20. Возможно увеличение до 100, однако необходимо обращать внимание на заполненность дискового пространства и загруженность процессоров IDS. Запись трафика может производиться как вручную, так и автоматически – как реакция на срабатывание сигнатуры.

Количество дампов конфигурируется так:

```
ids(config)# service analysis-engine
ids(config-ana)# global-parameters
ids(config-ana-glo)# ip-logging
ids(config-ana-glo-ip)# max-open-iplog-files 100
```

При записи дампа трафика вручную необходимо указать следующие параметры:

- виртуальный сенсор, на котором слушается трафик;
- IP-адрес, трафик которого пишется;
- количество байт для записи (опционально);
- количество пакетов для записи (опционально, по умолчанию 1000);
- длительность записи в минутах (опционально, по умолчанию 10).

При уточнении всех трех опциональных параметров запись трафика прекращается при достижении любого из указанных ограничений. Пример:

```
ids# iplog vs0 1.2.3.4 bytes 500000 duration 50 packets 10000
```

```
Logging started for virtual sensor vs0, IP address 1.2.3.4,
Log ID 1701737004
Warning: IP Logging will affect system performance.
```

Просмотреть состояние текущих записей дампов, на мой взгляд, удобнее всего с помощью команды:

```
ids# iplog-status brief
```

Если запись iplog вызвана срабатыванием сигнатуры, то в колонке Event ID будет отображаться ID отработанного события, взаимосвязь с которым можно увидеть в системе мониторинга IPS Manager Express.

По каждому отдельно iplog статус просматривается с помощью команды:

```
ids# iplog-status log-id 1701737004
```

Что немаловажно: можно отменить текущую запись одного или нескольких дампов с помощью команды no iplog, однако невозможно управлять iplog'ами в состоянии completed, их можно только скопировать на другой сервер с помощью CLI, либо скачать на ПК через веб-интерфейс или IPS Manager Express для дальнейшего анализа снифферром.

Конфигурация параметров автоматической записи трафика при срабатывании сигнатур производится так:

```
ids(config)# service signature-definition sig0
ids(config-sig)# ip-log
```

Настраиваются ограничения:

- время записи в секундах (от 30 по умолчанию до 300);
- количество пакетов (опционально);
- количество байт (опционально).

Пример:

```
ids(config-sig-ip)# ip-log-time 30
ids(config-sig-ip)# ip-log-bytes 5000
ids(config-sig-ip)# ip-log-packets 100
```

***

Подводя итоги, можно сказать, что защита и безопасная конфигурация IPS/IDS осуществляются следующими средствами:

- Административно-информационные меры. Чем меньше людей знает о наличии сенсоров, тем лучше.
- Расположение управляющего интерфейса в специальном, административном VLAN, защищенном корпоративными файерволами и списками доступа на маршрутизаторах.
- Управление пользователями и разграничение прав доступа. Блокировка встроенной учетной записи пользователя cisco, создание отдельных пользователей с правами администратора IPS и уровня service.
- Настройка парольной политики в соответствии с корпоративными нормами безопасности.
- Конфигурация параметров сетевого доступа. Разрешение доступа с ограниченного количества хостов/подсетей.
- Предупреждение потенциального взломщика с помощью баннера при логине.
- Отключение возможности администрирования сенсора с помощью telnet.
- Настройка автоматического обновления и синхронизации времени.
- В случае включения администрирования по SNMP назначить сложноугадываемые community и по возможности использовать протокол TCP и нестандартный порт.
- Включение шифрования TLS в веб-сервере и смена номера порта. EOF

1. http://www.cisco.com.
2. http://www.cisco.com/en/US/docs/security/ips/7.0/configuration/guide/cli/cli_setup.html#wp1073485.
3. http://www.cisco.com/en/US/docs/security/ips/7.0/configuration/guide/cli/cli_system_images.html#wp1044573.
4. http://www.cisco.com/en/US/docs/security/ips/7.0/configuration/guide/cli/cli_troubleshooting.html#wp1009781.

2009

www.infosecuritymoscow.com

infosecurity RUSSIA

6-я международная специализированная выставка-конференция по информационной безопасности

29 сентября – 1 октября 2009

МОСКВА, Экспоцентр на Красной Пресне
Павильон №7

Одновременно на одной площадке с Infosecurity Russia:

STORAGE EXPO

DOCUMATION

РАЗДЕЛЫ ВЫСТАВКИ

- Антиспам
- Антивирусы
- Безопасность приложений
- Биометрические системы
- Непрерывность бизнеса/восстановление бизнеса после катастроф
- Соответствие требованиям регуляторов и стандартам
- Системы мониторинга и фильтрации контента
- E-mail безопасность / Безопасность средств оперативной пересылки сообщений или Безопасность мгновенного обмена сообщениями (систем типа ICQ)
- Шифрование, PKI (инфраструктура открытых ключей), Цифровые сертификаты
- Межсетевые экраны (брандмауэры)
- Управление идентификацией и доступом
- Безопасность Интернет/сетевая безопасность
- Выявление и предупреждение вторжений
- Расследование компьютерных инцидентов
- Техническая поддержка/системы helpdesk
- Законодательство и стандарты/BS7799/Сертификация
- Сертификационные центры
- Управление внесением исправлений
- Тестирование безопасности системы путем имитации атак / Оценка риска и уязвимости
- Физическая безопасность
- Удаленный доступ
- Безопасность хранения данных
- Политика безопасности
- Маркеры доступа
- Обучение и повышение осведомленности в области безопасности
- Безопасность Веб-сервисов
- Система «Доступ за один шаг» (Single Sign-On)
- Смарт-карты
- Системы унифицированного управления защитой от угроз
- Безопасность IP телефонии
- VPN (виртуальные частные сети)
- Безопасность мобильных/беспроводных систем

ВЫСТАВОЧНОЕ ОБЪЕДИНЕНИЕ РЕСТЭК™

Reed Exhibitions®

Дирекция выставки:
Санкт-Петербург, Петрозаводская ул., д.12
Тел.: +7 (812) 320-8098, факс: +7 (812) 320-8090, E-mail: itcom@restec.ru

Визитка

ДМИТРИЙ ВАСИЛЬЕВ, более 10 лет профессионально занимается разработкой ПО. Принимает активное участие в различных проектах с открытым исходным кодом

Знакомьтесь, Erlang

Основы языка программирования

В 1981 году компания Ericsson запустила исследовательский проект, чтобы найти лучший способ программирования телекоммуникационных приложений. Не найдя подходящего, решили разработать новый язык

Первая версия языка программирования Erlang была представлена в 1986 году. До 1998 года язык и сопутствующие библиотеки развивались внутри компании Ericsson, но в 1998 году Erlang был выпущен как проект с открытым исходным кодом.

Основные особенности Erlang

Erlang – это язык программирования общего назначения и также среда выполнения. Хотя Erlang как язык привлекателен сам по себе, его реальная мощь проявляется при соединении со средой выполнения (виртуальной машиной) и поставляемыми с языком библиотеками. Рассмотрим его основные особенности:

Высокоуровневые конструкции языка. Erlang – это декларативный язык программирования, позволяющий описывать, что должно быть вычислено, вместо описания того, как это должно быть вычислено. Erlang также использует динамическую типизацию, что может ускорить разработку приложений.

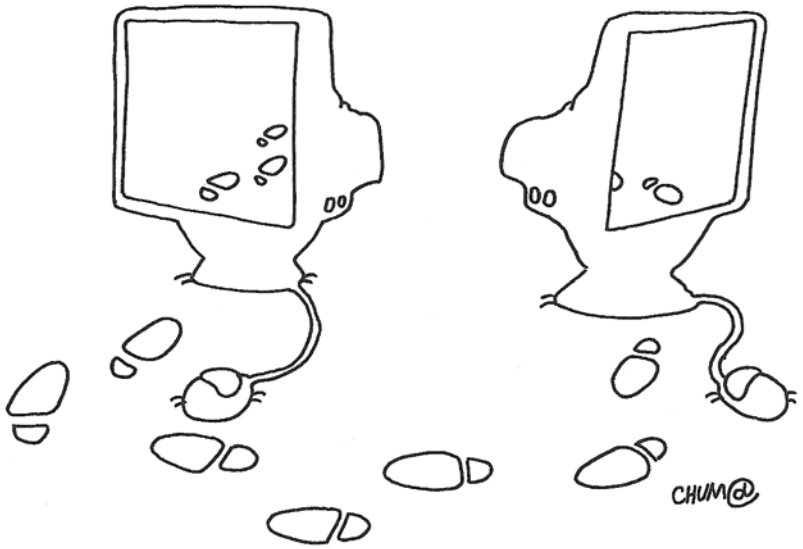
Параллельная обработка и передача сообщений. Вместо использования распространенной в настоящее время модели параллельного программирования, в которой используются потоки с разделяемой памятью, Erlang поддерживает параллельную модель, основанную на легковесных процессах с асинхронной передачей сообщений. Процессы в Erlang не имеют ничего общего с процессами операционной системы и называются процессами только потому, что код каждого процесса выполняется независимо от других процессов. При этом процессы Erlang за счет своей легковесности (время создания процесса составляет несколько микросекунд и не зависит от количества уже работающих процессов) работают даже эффективнее, чем потоки операционной системы, что позволяет работать с несколькими десятками тысяч процессов в одном приложении. Процессы общаются между собой посредством передачи сообщений (время передачи сообщения составляет несколько микросекунд, так как данные копируются из пространства одного процесса в пространство другого в рамках виртуальной машины), где сообщением может быть любое значение, используемое в языке. Сообщения передаются асинхронно, таким образом, сразу после посылки сообщения отправитель может продолжить работу. Входящие сообщения извлекаются из «почтового ящика» процесса выборочно, и, таким образом, нет необходимости извлекать сообщения по очереди.

Распределенная обработка. Так как процессы в Erlang не используют разделяемой памяти, а общаются только посредством передачи сообщений, язык позволяет достаточно легко превратить параллельное приложение в распределенное, где различные процессы выполняются на различных узлах сети.

Надежность. Erlang поддерживает различные подходы для построения высоконадежных систем. На низком уровне процессы могут быть связаны между собой и оповещаться посредством сообщений при завершении связанного процесса. На более высоком уровне при использовании OTP (см. врезку «Что такое OTP?») появляется возможность устанавливать различные политики мониторинга отдельных процессов и групп процессов. В распределенной системе резервные узлы могут автоматически заменять узлы, вышедшие из строя.

Работа в режиме мягкого реального времени (soft real-time). Хотя Erlang – это высокоуровневый язык, его можно использовать для систем, работающих в режиме мягкого реального времени (когда нарушение временных ограничений приводит только к снижению качества работы системы). Язык использует автоматическое управление памятью, при котором «сборка мусора» происходит отдельно для каждого процесса в системе. Это позволяет получать ответы системы в пределах нескольких микросекунд даже при наличии «сборки мусора», что в свою очередь позволяет работать в режиме высокой нагрузки практически без потери пропускной способности.

Работа приложений в течение долгого времени. Язык поддерживает «горячую» замену кода модулей в работающем приложении, при котором в один момент времени могут работать старая и новая версии кода. Это



необходимо для систем, которые не должны останавливаться для обновления кода, например, телефонных систем или систем контроля трафика.

Проекты, в которых используется Erlang

Много коммерческих компаний используют Erlang в своих проектах, например:

- Amazon использовал Erlang для создания SimpleDB, которая предоставляет сервис хранения данных для Amazon Elastic Compute Cloud (EC2).
- Erlang использовался при создании Delicious, сервиса социальных закладок от Yahoo!, в котором зарегистрировано больше чем 5 миллионов пользователей и больше чем 150 миллионов закладок.
- Facebook использовал Erlang для создания сервиса чата, обрабатывающего больше чем 100 миллионов активных пользователей.

Erlang также используется и в проектах с открытым исходным кодом, например:

- Ejabberd, сервис мгновенных сообщений, использующий XMPP-протокол, написан на Erlang.
- Erlang использовался для создания базы данных хранения документов CouchDB.

Начинаем работать

Перед началом изучения Erlang стоит убедиться, что он установлен в вашей операционной системе. Попробуйте набрать в командной строке команду erl:

```
$ erl
Erlang R13B01 (erts-5.7.2) [source] [rq:1]
[async-threads:0] [kernel-poll:false]

Eshell V5.7.2  (abort with ^G)
1>
```

Для Windows вызов erl из командной строки работает только, если в переменную среды PATH добавлен путь к программе. В случае стандартной установки для Windows интерпретатор команд Erlang можно запустить через меню Start → All Programs → Erlang OTP. Если Erlang установлен в вашей системе, то вы увидите приветствие, похожее на пример выше. В случае если при вызове erl вы получили сообщение о неизвестной команде, вам нужно установить Erlang. Для большинства систем Erlang может быть установлен с использованием стандартной системы управления пакетами. Для Windows инсталлятор может быть скачан с официального сайта: http://erlang.org/download.html. В других системах можно собрать Erlang с использованием исходного кода, который также можно скачать с официального сайта: http://erlang.org/download.html.

Командная оболочка

Командная оболочка Erlang может использоваться для интерактивных сессий и выполнения выражений языка. Запустим оболочку командой erl (или через меню Windows, как описано выше) и наберем несколько команд:

```
$ erl
Erlang R13B01 (erts-5.7.2) [source] [rq:1]
[async-threads:0] [kernel-poll:false]

Eshell V5.7.2  (abort with ^G)
1> % Это просто комментарий
1> 2 + 2.
4
2>
```

Рассмотрим нашу первую сессию подробнее:

- При старте командой erl оболочка выводит заголовок с информацией о версии и опциях, с которыми собран Erlang.
- После этого выводится приглашение для ввода команд 1>. После первого приглашения мы набрали комментарий. Комментарии в Erlang начинаются со знака «%» и продолжаются до конца строки. Оболочка игнорирует комментарии.
- Затем оболочка опять выводит «1>», так как мы не набрали законченной команды. Теперь мы набираем «2 + 2», затем точку и нажимаем <Enter>. Многие начи-

Почему язык назван Erlang?

Один из авторов языка Джо Армстронг (Joe Armstrong) говорит, что есть две версии происхождения названия. По одной версии название языка расшифровывается как Ericsson Language (язык Ericsson). По второй – язык назван в честь датского математика Агнера Крарупа Ерланга (Agner Krarup Erlang). И, кроме этого, авторам нравится поддерживать такое неоднозначное толкование названия.

нающие изучать Erlang забывают набрать точку в конце выражения, но в этом случае оболочка не сможет определить, что выражение закончено, и результат не будет выведен.

- Теперь оболочка вычисляет выражение и выводит результат (4, в нашем случае).
- После этого оболочка выводит приглашение в виде «2>». Где 2 – это номер команды, который увеличивается с каждой выполненной командой.

Оболочка является мощным инструментом при работе с Erlang. Кроме ввода выражений поддерживается история команд (например, комбинации клавиш <Ctrl>+<P> и <Ctrl>+<N> используются для передвижения по введенным прежде командам), различные возможности редактирования команд и множество вспомогательных функций, которые можно посмотреть командой help(). Кроме этого, оболочка позволяет присоединяться к запущенным программам Erlang даже на удаленных узлах (при этом также имеется возможность автоматического использования защищенного соединения через SSH) и многое другое. Надо заметить, что оболочка позволяет выполнять только выражения Erlang, но ее нельзя использовать для ввода других конструкций языка, которые мы будем рассматривать ниже.

Для выхода из оболочки можно использовать встроенную функцию halt():

```
1> halt().
```

В случае если оболочка не отвечает (или как другой способ нормального выхода), то можно прервать выполнение нажатием клавиш <Ctrl>+<C> (или <Ctrl>+<Break> на Windows), после чего на экран будет выведено:

```
BREAK: (a)bort (c)ontinue (p)roc info (i)nfo (l)oaded
       (v)ersion (k)ill (D)b-tables (d)istribution
```

И теперь для прерывания выполнения можно нажать клавишу <A>.

Базовые понятия

После того как мы научились работать в оболочке Erlang, рассмотрим основные конструкции языка.

Числа

Как и во многих языках, арифметические выражения Erlang следуют обычным правилам для арифметических выражений, например, «1 + 2 * 3» будет вычислено как 1+(2*3). Целые числа могут иметь произвольный размер, и нет необходимости беспокоиться об арифметических переполнениях.

Проверим это на практике:

```
1> 123456789 * 123456789 * 123456789 * 123456789.
232305722798259244150093798251441
```

Кроме этого, целые можно вводить в различных системах счисления, используя следующую форму:

```
1> 10#10.
10
2> 16#10.
16
3> 2#10.
2
```

Здесь мы ввели число 10 в десятичной, шестнадцатеричной и двоичной системах.

Для ввода кодов символов можно использовать нотацию, начинающуюся с символа $:

```
1> $a.
97
2> $%.
37
3> $0.
48
4> $\n.
10
```

Числа с плавающей точкой можно вводить в следующих форматах:

```
1> 1.25.
1.25
2> 2.0e-10.
2.0e-10
```

Для чисел с плавающей точкой Erlang использует 64-битное представление, соответствующее стандарту IEEE 754-1985.

Переменные и сравнение с шаблоном

Имена переменных в Erlang должны начинаться с большой буквы, как в следующем примере:

```
1> X = 123456789.
123456789
2> X.
123456789
3> X * X * X * X * X.
232305722798259244150093798251441
```

В первой строке мы присваиваем значение числа 123456789 переменной X, и затем значение выводится оболочкой.

После этого мы выводим значение переменной и используем ее в арифметической операции.

Но при этом значение переменной Erlang может быть присвоено только один раз. Продолжая следующий пример, мы увидим следующее:

```
4> X = 10.
** exception error: no match of right hand side value 10
```

Что здесь происходит? Строго говоря, оператор «=» в Erlang не является оператором присваивания, а является оператором сравнения с шаблоном. При этом, если переменной в текущей области видимости еще не присвоено значение, «=» действует как оператор присваивания, в противном случае = сравнивает значение с шаблоном.

При сравнении с шаблоном сначала вычисляется правая часть выражения, затем она сравнивается с шаблоном в левой части. В последнем примере переменная X является простейшей формой шаблона. В данном случае сравнение с шаблоном будет успешным только в случае, если значение правой части выражения равно 123456789:

```
5> X = 123456789.
123456789
6> X = 100000000 + 23456789.
123456789
```

Одноразовое присваивание избавляет разработчика от огромного класса ошибок, связанных с неверным значением переменной, которая в противном случае могла бы быть изменена где-то между первым присваиванием и выражением, в котором она используется. Плюс к этому такое поведение согласовывается с математической нотацией, где невозможна формула вида X=X+1.

Атомы

В Erlang атомы используются для представления глобальных нечисловых констант. При сравнении с другими языками можно представить атомы как элементы в перечисляемом типе данных. Значением атома является сам атом, и единственная операция над атомами – это сравнение.

Атомы должны начинаться с маленькой буквы (как мы уже рассмотрели выше, переменные должны начинаться с большой буквы, так что они не пересекаются с атомами), за которой могут следовать буквы, цифры, «@» и «_» (точка тоже может использоваться в атомах, хотя это является не поддерживаемым разработчиками расширением языка). При использовании одинарных кавычек (') для атома могут использоваться любые символы.

Примеры атомов:

```
1> hello.
hello
2> 'Hello, World!'.
'Hello, World!'
3> '1
3> 2
3> 3'.
'1\n2\n3'
```

Хотя Erlang не имеет отдельного булевского типа, по соглашению для этого используются атомы true и failse:

```
1> 1 > 2.
false
2> a < z.
true
3> is_boolean(1 > 2).
true
4> is_boolean(1 + 2).
false
```

Заметьте, что во второй строке мы сравнили два атома, при сравнении которых используется лексикографический порядок.

Начиная с третьей строки мы применили встроенную функцию (Built-in function, BIF) is_boolean, которая возвращает true или false в зависимости от типа аргумента.

Кортежи

Кортеж – это составной тип данных, который используется для хранения связанных элементов в виде единого набора. Кортежи создаются с использованием фигурных скобок, и их элементы разделяются запятыми. В качестве элементов кортежа могут выступать любые типы данных Erlang, например:

```
1> {1, 2}.
{1,2}
2> {1, 1.5, ok}.
{1,1.5,ok}
3> {ok, {5, 6}}.
{ok,{5,6}}
```

По соглашению, если первый элемент кортежа атом, его называют меткой, хотя это никак не отличает такой кортеж от других кортежей. С использованием таких меток можно создавать собственные типы данных, например:

```
1> {person, 'Joe', 'Armstrong'}.
{person,'Joe','Armstrong'}
2> {point, 10, 20}.
{point,10,20}
```

Такие метки упрощают извлечение информации из кортежа с использованием операции сравнения с шаблоном:

```
1> {point, X, Y} = {point, 10, 20}.
{point,10,20}
2> X.
10
```

Что такое OTP?

На Erlang часто ссылаются как на Erlang/OTP. Здесь OTP расшифровывается как Open Telecom Platform (открытая телекоммуникационная платформа) и представляет из себя набор библиотечных модулей, поставляемых с Erlang, и подходы к разработке приложений. Подавляющее большинство приложений с открытым исходным кодом, использующих Erlang, таких как ejabberd, CouchDB и MochiWeb, используют OTP.

```
3> Y.
20
4> {point, X, _, _} = {point, 10, 20, 30}.
{point,10,20,30}
5> X.
10
6> {person, Name} = {point, 20, 30}.
** exception error: no match of right hand side value
{point,20,30}
```

Здесь {point, X, Y} – это более сложный шаблон, чем тот, что мы использовали выше, присваивающий переменным X и Y значения 10 и 20 соответственно. В строке 4 мы использовали анонимную переменную (_), которой не присваивается значение и ее можно несколько раз использовать в шаблоне. В строке 6, при попытке использования шаблона {person, Name}, мы получили ошибку, так как шаблон не совпадает с кортежем {point, 20, 30} в правой части выражения. Кроме этого, с использованием встроенных функций есть возможность работать с отдельными элементами кортежей, например, получать элементы по индексу (начиная с 1):

```
1> element(2, {100, {1, 2, 3}, ok}).
{1,2,3}
```

Списки

Списки как и кортежи – это составной тип данных, который может содержать любые типы данных Erlang, но в отличие от кортежей списки обрабатываются совсем другим способом и служат для хранения данных, количество которых изменяется.

Списки создаются с использованием квадратных скобок, и их элементы разделяются запятыми, например:

```
1> [1, 2.5, ok, {point, 20, 30}, [1, 2, 3]].
[1,2.5,ok,{point,20,30},[1,2,3]]
```

Первый элемент списка (в нашем примере – это 1) называется вершиной списка, а оставшиеся элементы – хвостом списка. При обработке списков наиболее эффективная операция – это работа с вершиной списка, которая поддерживается в Erlang следующей конструкцией: [вершина | хвост]. Здесь вершина – это элемент, или набор элементов для добавления, или удаления из списка, а хвост – список для добавления элементов, или список после удаления вершины. Рассмотрим это на примерах:

```
1> List = [3, 4, 5].
[3,4,5]
2> Range = [1, 2 | List].
[1,2,3,4,5]
3> [Head | Tail] = Range.
[1,2,3,4,5]
4> Head.
1
5> Tail.
[2,3,4,5]
```

Здесь мы создали список List, затем добавили в качестве его вершины два элемента, сформировав новый список Range. После этого мы отделили один элемент из вершины списка, сохранив его как Head.

Строки

Строго говоря, в Erlang нет отдельного типа данных для строк, строки реализованы просто как списки целых чисел. Для более удобной работы со строками их можно создавать с помощью двойных кавычек, как в этом примере:

```
1> "Hello, World!".
"Hello, World!"
```

Из следующих примеров можно увидеть, что строки и списки целых – это одно и тоже:

```
1> [$h, $e, $l, $l, $o] =:= "hello".
true
2> [$h, $e, $l, $l, $o].
"hello"
```

Здесь знак «=:=» служит для точного сравнения двух элементов.

Бинарные данные

Для эффективного хранения бинарных данных рекомендуется использовать бинарный тип данных. Он состоит из набора целых чисел в диапазоне от 0 до 255 (или соответствующих символов) и представляется с помощью двух угловых скобок:

```
1> <<104,101,108,108,111>>.
<<"hello">>
2> <<"hello">>.
<<"hello">>
```

***

Итак, были кратко рассмотрены основные особенности и базовые понятия языка программирования Erlang. Более детальную информацию по языку вы можете найти в документации, находящейся на официальном сайте и других сайтах, описывающих Erlang. Вот некоторые из полезных сайтов:

http://erlang.org – основной сайт языка, где всегда можно скачать последнюю версию дистрибутива, прочитать новости и документацию;

http://www.planeterlang.org – агрегатор блогов по Erlang;

http://trapexit.org – сборник статей, новостей и блогов по Erlang;

http://erlang.dmitriid.com – русскоязычный сайт с новостями и форумом по Erlang. EOF

Сергей Яремчук:
«Сисадмин» — это мой формат»

Так утверждает наш многолетний автор и читатель. Он считает, что у него «нет больших амбиций, но есть большие требования к себе». По просьбе «СА» Сергей приоткрыл завесу над своей жизнью

Уже не могу не учиться

Я родился в Полтаве, где прожил 21 год своей жизни. Хотя сейчас живу в Ровно, считаю себя полтавчанином. С детства люблю читать.В основном люблю приключенческие и исторические книги, чуть меньше увлекаюсь фантастикой. Учился в первых классах не очень, однако 10-й класс окончил с одной тройкой, по русскому языку, доставшейся еще с 8-го класса. В школе ознакомился с первым компьютером. Моим первым языком программирования был PL-1 – сложный язык для инженерных расчетов, требовавший внимательности и не очень прощавший ошибок.

В школе активно занимался борьбой, легкой атлетикой и военно-прикладным многоборьем. Следующий этап – Полтавское высшее военное командное училище связи. Окончил его с красным дипломом, распределился в одну из частей города Ровно. Можно сказать, повезло – всю службу занимался техникой связи и компьютерами.

Теперь уже не могу не учиться, люблю во все вникать и понимать процесс. Дома компьютер появился в 1998 году. Это был Celeron 300A с 32 Мб ОЗУ, с диском на 3,2 Гб, на котором стоял Windows 95. Когда в Ровно наконец появился Интернет, то стал частым гостем в первых интернет-кафе, затем подключился и с домашнего ПК.

Так как был уже некоторый опыт прикладного программирования, писал программы на Ассемблере, Pascal, Бейсике, Delphi. В 2000 году заинтересовался языками высокого уровня, применявшимися в веб-разработке. Долгое время писал на Perl, затем на PHP и Python. Так как Windows 98 был не очень удобным, понадобилась другая платформа – так на домашнем ПК появился Linux. Первый дистрибутив был RedHat 5.1, затем RedHat 6.2 По ходу учился настраивать различные сервисы, понимать их суть. Когда компьютеры стали массовым явлением, подрабатывал эникейщиком, настраивал сервера и сети, писал программы.

Сын и дочь — это часть моей жизни и стимул для того, чтобы быть всегда чуть впереди

В 1999 году родился сын, в 2004 году – дочь. Свободное время стараюсь проводить с семьей. В хорошую погоду любим гулять в лесу, собирать ягоды, да и просто готовить шашлыки. Еще люблю водить машину. Всегда, если есть возможность, выезжаю куда-нибудь.

Я написал ее во сне

Друг принес кучу дисков, в которых все файлы были пронумерованы: 1.mp3, 2.mp3 и так далее. Нужно было извлечь информацию с ID3-тегов и переименовать файлы. Попутно подбирал модуль Perl для решения какой-то другой задачи. Уже выключая компьютер, случайно вышел на mp3_info, который умеет работать с информацией в mp3-файлах. С утра в голове был уже готовый скрипт, которым хотелось с кем-то поделиться. Так и получилась первая статья в журнале «Мой компьютер».

Примерно тогда же написал статью в журнал «Системный администратор». Так до сих пор и пишу в «СА» и читаю с первых номеров. Журнал нравится тем, что в нем публикуются практики. Читаю или просматриваю абсолютно все материалы. Бывали, кстати, и курьезы. Получил как-то журнал, но занимался решением одной проблемы и отложил его чтение на потом. Затем открываю, а там нужная статья. Если бы открыл «СА» раньше, потратил бы на порядок меньше времени. EOF

Визитка

СТАНИСЛАВ ШПАК, более 5 лет занимается сопровождением Active Directory и Windows-серверов. Имеет сертификаты MCSE по Windows Server 2000/2003

Игра

Очередная вспышка молнии осветила округу, и Эрик увидел, что до замка осталось совсем чуть-чуть. Сильные порывы ветра трепали полог повозки, порой даже грозя опрокинуть ее. Оставалось только удивляться, как еще лошадь не понесла, испугавшись близкого раската грома.

Весь день в воздухе ощущалась наступающая гроза, однако путники решили не останавливаться в деревне у подножия холма, надеясь успеть в замок до того, как непогода разбушуется. Хорошо в деревне, там даже ветер всего лишь треплет верхушки деревьев, да молнии пугают крестьян, а тут, на подступах к замку, ощущаешь себя в самом центре стихии. Нет, ну кто придумал строить замки на возвышенности? Эрик вспомнил занятия по истории – в смутные времена такое расположение было дополнительной защитой. Но теперь-то неужели барону не хочется перебраться в более веселое место, чем жить в мрачном замке на голой верхушке холма, где из растительности, поди, один кустарник в парке за стенами. «Надо будет спросить у наставника», – подумал Эрик и покосился на своего попутчика, который спокойно правил лошадью так, будто и не было вокруг разбушевавшейся непогоды.

Спустя короткое время они наконец въехали под защиту сводов толстых крепостных стен и гулко постучали в ворота. Лихие люди находятся во все времена, и ворота всегда охранялись. Однако в этом замке их ждали, поэтому, оставив лошадь и повозку конюху, подхватив сумы с необходимыми в их работе вещами, путники наконец-то вошли в парадную замковую залу. Не успел еще служка забрать для просушки мокрые вещи гостей, как на балюстраде второго этажа появился лично барон, и, суетливо оправляя одежду, кинулся им навстречу.

– О, как рад, как рад я, что вы наконец-то приехали, Братья! – радостно рассыпался в приветствиях барон, ведя их в соседнюю залу. – Пожалуйста, проходите! Вы, должно быть голодны с дороги, вот, располагайтесь у огня, сейчас вам принесут еду, и вы сможете утолить голод и жажду. Вино моих погребов считается лучшим в округе!

– Спасибо, барон! – сказал наставник. – Мы тоже весьма рады, что наш долгий путь наконец-то закончен, и даже гроза не помешала нам попасть под благословенные своды вашего замка. Мы не откажемся принять трапезу, но вот вместо вина предпочтем воду. Члены нашего Братства не могут употреблять вино, пока работа не сделана.

– О, разумеется, – продолжал суетиться барон. – Работа, конечно же, прежде всего! Да и я уже заждался вас, хотя и признаюсь, что приехали вы достаточно быстро, несмотря на дальнюю дорогу. Обычно визита Братьев из магической поддержки приходиться ждать куда дольше…

На этих словах барон осекся. Ходило много историй про нерасторопность магподдержки, но очень опрометчиво было говорить это Братьям в лицо. Однако наставник сделал вид, что не заметил упущения барона, тем более что в зале аппетитно запахло жареным мясом.

После трапезы барон возжелал показать им тронную залу и даже попытался начать объяснять, в чем состояла суть проблемы, но наставник остановил его и сказал, что они устали с дороги, хотят отдохнуть и набраться сил перед предстоящей работой, которой они намерены заниматься завтра с утра. Барон несколько приуныл, но ему хватило сообразительности не настаивать и, велев прислуге показать Братьям их комнату, пожелал мирного сна и удалился в свои покои. Засыпая, Эрик думал о том, как во многих вещах в мире еще живет смутное прошлое – во времена, когда не редкостью было проснуться от нападения на замок, пожелание «мирного сна» бывало как нельзя кстати.

Утро выдалось ярким и солнечным. После завтрака барон проводил их в тронную комнату. Раньше, говорят, тронные залы были самыми большими и в них проводили приемы вассалов и вершили всякие дела. Сейчас же здесь находилась святая святых любого замка – зеркало для Игры. У барона было хорошее зеркало – с диагональю в десяток пядей и, главное, неразбитое. Второй по значимости вещью был кристальный блок. Именно он заставлял зеркало показывать Игру. Эрик принадлежал к Братству Кристаллов и Магической Поддержки, которое заставляло кристаллы работать. Знание природы кристаллов и магия – вот то, что передавалось внутри Братства из уст в уста, и только его члены знали, что нужно, чтобы кристаллы заработали как надо. Но это была ох какая непростая работа! Трон же теперь оказался тем, чем он, по сути, и был всегда – подставкой для седалища. По старой привычке аристократы все еще пользовались вычурными, богато убранными, но не очень удобными тронами, но Эрик подозревал, что со временем это изменится, ведь игрок иногда проводит на нем чуть ли не половину суток. На троне лежала железная перчатка от рыцарских доспехов, на внешней стороне которой мерцал голубой кристалл. Ну что ж, перчатка и зер-

кало, пожалуй, были рабочими. Чего нельзя было сказать о кристальном блоке. Да, работенка им предстояла немаленькая – блок лежал на полу и кристаллы были рассыпаны вокруг. Некоторые были разбиты, некоторые казались целыми, но Эрик знал, что достаточно одной трещинки для того, чтобы кристалл пришел в негодность. Наставник тоже обвел открывшуюся картину взглядом, который затем остановил на как будто бы съежившемся от этого бароне.

– Я ничего не делал, все было как обычно, а потом блок перевернулся, и вот…

Барон замолчал под тяжелым взглядом наставника. Повисла гробовая тишина, которая так не вязалась с щебечущими за окном птицами.

– В Игре у меня был неудачный рейд, – наконец промямлил барон. – Знаете, всегда обидно проигрывать, когда победа кажется такой близкой. Ну и когда все пошло не так и мне пришлось бежать с поля боя, я не выдержал и… запустил в блок перчаткой… Я был в гневе, но я не думал, что блок опрокинется… Кристаллы… Я сначала хотел их собрать сам, но потом увидел, что некоторые разбились. Вы мне поможете? Вы сможете сделать, чтобы все снова работало? Пожалуйста, умоляю вас, Братья! Я обещаю, что больше такого не повторится, только помогите мне. Жизнь без игры так скучна. Пока я ждал вас, я пытался найти себе какое-нибудь занятие, но чтобы я ни придумал – охота ли, конные прогулки, без Игры это все не то.

Барон наконец замолчал, с мольбой глядя на наставника.

– Оставьте нас, – промолвил наставник. – Пусть кто-то из слуг дежурит за дверью на случай, если нам что-то понадобится. Но упаси его господь, если он решится подсматривать. Нас не беспокойте.

Барон мелко-мелко закивал и тут же засеменил к выходу, по дороге рассыпаясь в благодарностях. Когда дверь за ним закрылась, наставник обратился к Эрику:

– Итак, Эрик, что ты обо всем этом думаешь?

Эрик ожидал этого вопроса и с готовностью ответил:

– Зеркальная поверхность цела, думаю, тут проблем не будет. Повторно можно будет использовать перчатку, хотя, возможно, придется сменить на ней голубой кристалл. А вот блок восстановлению не подлежит. Кристаллы уже не собрать, многие разбиты, остальные наверняка наколоты. Придется сказать барону, что потребуется новый блок, так как вряд ли у нас с собой найдется необходимое количество комплектующих кристаллов для самостоятельной сборки.

– Ну что ж, пожалуй, ты прав, – сказал наставник, зачем-то усаживаясь на троне. – Проще всего было бы сказать барону, что требуется заказать новый блок. И пусть ждет, пока ему доставят его из обители Братства. Однако мы уже здесь. И у нас есть с собой немного кристаллов. Вот уже несколько сезонов после окончания своего обучения ты сопровождал меня, исправно мне помогал в работе, и я тобой доволен. Теперь я хочу, чтобы ты приложил все свои знания и умения и постарался собрать блок здесь и сейчас. Сегодня ты будешь делать все сам, а я – наблюдать. Конечно, я помогу тебе, если будет необходимость. Если у тебя получится, я порекомендую тебя хранителям обители как закончившего обучение.

Эрик немного опешил. Нет, конечно, в обители Братства он, как и другие послушники, собирал кристальные блоки на занятиях. Но одно дело собрать кристальный блок из огромного количества имеющихся в распоряжении кристаллов в спокойной обстановке, и совсем другое – собрать блок из того, что было привезено с собой! Кристаллы были весьма ценной вещью, и хотя любой феодал без раздумья казнит человека, который осмелится похитить кристалл у Братьев, безрассудные люди все же находились. Поэтому много кристаллов с собой никогда не перевозилось, и уж тем более из этого количества нельзя было собрать блок. Значит, придется перебирать имеющиеся неразбившиеся кристаллы барона, которые очень пристально придется проверять перед использованием. Если задача сопряжения кристаллов становилась тем легче, чем больше кристаллов имелось в наличии для подбора, то проверка кристалла требовала внимания и опыта. Опыта, которого у Эрика было пока очень мало. Однако ему очень хотелось закончить обучение и стать самостоятельным полноправным членом Братства.

«Знание природы кристаллов и магия — вот то, что передавалось внутри Братства из уст в уста, и только его члены знали, что нужно, чтобы кристаллы заработали как надо»

Итак, первым делом Эрик разобрал старые кристаллы,

которые уцелели и не разбились, визуально осмотрел их и выкинул те, на которых были заметны трещины. Остальные нуждались в более тщательной проверке. Эрик знал ряд специально предназначенных для этого заклинаний, запомнить их было несложно, сложность была в том, как интерпретировать реакцию кристалла на заклинания. Но он справился. Лишь в одном месте наставник вмешался – взяв один из признанных Эриком годных кристаллов, он произнес над ним заклинание преломления света, затем поместил его в солнечный луч, который рассыпался по комнате тысячей разноцветных солнечных зайчиков. Эрик знал, что правильный кристалл должен давать равномерное распределение цветов, в этом же кристалле преобладали красные отблески.

В конце концов осталось несколько кристаллов, которые оказались неповрежденными. Наставник из своей сумы извлек еще немного аккуратно завернутых кристаллов и положил их рядом. Эрик прикинул, что собрать из этого количества блок будет сложно, но попробовать стоило.

Любой кристалл мог выполнять любую функцию в блоке. Но при этом он мог и не «захотеть» работать с другими кристаллами – в этом случае заклинание сопряжения кристаллов просто не срабатывало. Эрик пыхтел, вспоминал различные виды заклинаний, по-разному вертел кристаллы, и спустя какое-то время уже начало что-то получаться. Несущий кристалл являлся основой всей конструкции – сам по себе никаких функций не выполнял, но помогал остальным кристаллам работать вместе. С ним Эрику повезло – заклинание легло на него так легко, будто он для этого и был предназначен. Если же заклинание кристаллу не подходило, тот мог начать «привередничать» и не принимал его. Либо же принимал, но нехотя и потом не работал с соседями. Выбрать для кристалла наиболее подходящую ему функцию было настоящим искусством.

«…Игра, в которую люди выплескивают воинственный пыл и человеческую злость, и становятся мирными крестьянские будни, созревают незагубленные урожаи, все так. Но…»

Базовый кристалл, кристалл памяти, кристалл обработки, кристалл времени, колебательный кристалл для создания звука, кристалл связи с другими игроками, особый синий кристалл для сопряжения с перчаткой-манипулятором – «синий зуб», несколько дополнительных кристаллов, призванных сбалансировать всю систему, – почти все Эрику удалось сделать. А вот кристалл вывода картинки на зеркало никак не удавалось правильно заговорить. И всему виной было нестандартное десятипядевое зеркало барона – кристалл никак не хотел попадать картинкой в рамки зеркала. Как это ни было прискорбно, пришлось Эрику обращаться за помощью к наставнику. Втайне он, конечно, надеялся, что наставник тоже не сможет заставить противный кристалл работать как надо.

Наставник подошел к своей суме, и Эрик уж было подумал, что сейчас оттуда будет извлечен еще один кристалл, и даже хотел обидиться на нечестное поведение, но тот достал нечто круглое. У Эрика перехватило дыхание – неужели это… Да, бережно развернув сверток, наставник достал самый настоящий бубен. Среди послушников ходили байки о том, что самые опытные наставники имеют специальный бубен и знают магические заговоры, которые не работают иначе как с бубном. Но это очень тонкий инструмент, им можно как настроить кристалл, так и полностью разрушить его. Эрик тихонько замер на краешке трона, пока наставник начал нараспев читать какое-то незнакомое заклинание, ходя вокруг почти собранного Эриком кристального блока и потряхивая бубном. Спустя какое-то время монотонность происходящего и напряжение предыдущих часов работы дали о себе знать, и Эрик незаметно заснул.

Проснулся он от наступившей тишины. За окном уже темнело, и скоро нужно будет зажигать факелы. Если не заработает зеркало, конечно. Кому нужны факелы, когда света от зеркала и так достаточно! Однако как нехорошо получилось – впервые в жизни увидел живую легенду, наставника с бубном, и заснул! Эрик от обиды закусил губу – и посвящения в Мастера ему тоже не видать, придется так и продолжать ходить в послушниках. Зеркало отображало тестовую картинку, идеально входящую в размеры рамы. У наставника все же получилось!

– Ну что, включай блок, посмотрим, что у нас вышло, – сказал наставник.

Эрик произнес простенькое заклинание активации блока, и зеркало засветилось обычным рабочим светом. Мелькнули строчки самотестирования – это кристаллы подключались друг к другу. Эрик было обрадовался, но в самый последний момент, когда он уже ожидал появления игровой заставки, зеркало мигнуло и высветило набор непонятных белых символов на синем фоне. «Синяя нежить»! Эрик знал, что можно часами копаться в кристальном блоке, менять кристаллы и заклинания, пока не обнаружится, что или угол поворота кристалла не тот или заклинание сопряжения недостаточно сильное в каком-то месте, да мало ли причин появления «синей нежити»! Мысль о том, что почти законченную работу нужно будет снова переделывать, повергла Эрика в уныние. Пробормотав короткое «резет», заклина-

ние деактивации кристаллов, он грустно посмотрел на наставника. И тут Эрик еще раз убедился в силе бубна. Наставник, встряхивая бубном все сильнее и сильнее, трижды произнес над блоком заклинание сопряжения. И чудо случилось! После повторной активации кристаллов зеркало все-таки показало картинку игрового входа.

– Можешь звать барона, а я пока соберу вещи, – улыбнулся наставник, аккуратно заворачивая бубен.

Эрик подбежал к двери, распахнул ее и обнаружил в соседней комнате мирно дремавшего слугу.

– Зови своего господина, мы закончили, – гордо и спокойно проговорил Эрик, после чего вернулся в комнату.

Барон появился спустя пару минут, слегка запыхавшись от подъема по лестнице.

– Ну как, ну как, у вас получилось? – начал он скороговоркой, и тут взгляд его упал на зеркало. – О, Братья, спасибо вам! Я снова попаду в Игру! Я оставил распоряжение своему управляющему выдать вам ту плату, которую вы пожелаете. А сейчас, если вы не против, я вернусь к Игре.

Барон устроился на троне, повернул на пальце перстень с маленьким кристаллом логина и надел перчатку. Пользователь «Барон фон Ингер» вошел в Игру…

Факелы, горевшие вдоль стен, были единственным источником освещения большой залы без окон, в которой проходил совет хранителей обители Братства. Наставник все-таки порекомендовал Эрика как закончившего обучение, и теперь он стоял перед двенадцатью сильнейшими магами, некоторые из которых, по слухам, и основали несколько поколений назад Братство. Несмотря на ответственность момента, один вопрос не выходил из головы Эрика: «Откуда появилась Игра?» И когда все закончилось и он был назван Мастером, ему разрешили задать этот вопрос.

Один из магов рассмеялся:

«Смотрите, Братья, когда мы основывали Братство, пытливыми умами человечества владела мысль: «Кто сотворил мир», а теперь: «Кто сотворил Игру!» Однако на этот вопрос ответить проще, чем на первый. До основания Братства мир был совсем не тот, что сейчас. Междоусобные войны раздирали наши земли, крестьянские деревни разорялись, голод и болезни были повсюду. Мы, маги, пытались использовать наши знания для того, чтобы изменить ситуацию, но у нас мало что получалось. Пока однажды один из нас, брат Хьюго, не сотворил заклинание перехода, открыв дверь в иной мир. Мир, где люди живут в огромных городах и не голодают, где они летают по воздуху и ездят под землей, где свой досуг они проводят перед светящимися зеркалами, которые они называют телевизор или монитор. И брату Хьюго довелось пообщаться с его обитателем».

Маг на секунду запнулся, так как было не принято говорить о том, что брат Хьюго так испугался, вывалившись из своей пещеры в комнату к Олегу – админу одного из серверов популярной онлайн-игры, что не смог сразу сплести заклинание обратного перехода. Но ему повезло – Олег раньше увлекался фэнтези, свято верил в НЛО и параллельные миры, и появлению мага в своей комнате практически не удивился. Брат Хьюго вел себя примерно так же, как царь Иван Грозный из известного кинофильма, попавший в современную Москву. Его весьма заинтересовал компьютер, а Олег, обретя благодарного слушателя, с удовольствием объяснял, что это за штуки, отчего экран светится и что означают эти бегающие фигурки. Все это маг решил не рассказывать и продолжил:

«Обитатель того мира рассказал, что у них есть Игра – место, где реальные люди управляют вымышленными войсками, осаждают замки, вступают в союзы и совершают предательства. И это все происходит в Игре, а в настоящей жизни люди не воюют, а мирно трудятся. Когда брат Хьюго понаблюдал за Игрой, он увидел много общего с нашим тогдашним миром. И решил, что если бы такая Игра была у нас, то не было бы междоусобиц и войн. Вот тогда брат Хьюго и решил, что наш мир тоже должен иметь Игру. Еще несколько раз он переходил из мира в мир и общался с жителем другого мира, который рассказывал ему все, что тот хотел знать, пока параллели наших миров вновь не разошлись и силы заклинания перехода перестало хватать, чтобы открыть проход. Но к этому моменту у нас уже была Игра».

Будь тут сам брат Хьюго, он, возможно, еще мог бы добавить, как Олег рассказывал ему про устройство компьютера, про «открытую архитектуру», про комплектующие, про сети, про системных администраторов, про специалистов технической поддержки и много чего еще. В своих рассказах Олег часто перепрыгивал с одного на другое, не всегда замечая, что некоторые вещи маг понимает по-своему. Но его здесь не было, и маг закончил свой рассказ:

«Житель того мира сказал, что Игра работает благодаря кристаллам кремния и особой магии под названием «электричество». И хотя в нашем мире нет кремния и электричества, но у нас есть другие кристаллы и собственная магия, а брат Хьюго умел смотреть в суть вещей. Поэтому он придумал свои заклинания и создал первый в нашем мире кристальный блок. Затем он созвал совет магов и рассказал нам об Игре. Мы основали Братство Кристаллов и Магической Поддержки и стали нести Игру аристократам. О да, она им понравилась. Постепенно войны были заброшены, амбиции были перенесены в Игру, крестьяне смогли работать и выращивать урожай, и мир стал становиться таким, каким ты его теперь знаешь».

Казалось, Эрик должен был удовлетвориться этим рассказом. Но позже, стоя на крепостной стене обители, он задумался. Ведь как вроде бы хорошо и складно звучит история – Игра, принесенная из развитого мира в их мир знати и крестьян, Игра, в которую люди выплескивают воинственный пыл и человеческую злость, и становятся мирными крестьянские будни, созревают незагубленные урожаи, все так. Но… Эрик чувствовал, но не мог объяснить словами, что их мир теперь стал заложником Игры. Войны не будут двигать прогресс, а лучшие умы человечества будут или уходить в Братство, или придумывать ловкие игровые стратегии, развивая уже не настоящий, а игрушечный мир. Сытое, мирное время. Только вот никогда, никогда им не летать по воздуху и не ездить под землей как в том, другом, теперь уже таком далеком мире. Эрик посмотрел вокруг: чистое небо, воздух, пахнущий хвоей, леса, реки с прозрачной водой, парящая вдалеке пара драконов. Сейчас он бы с легкостью променял все это на день в другом мире! Раздался удар колокола, и новоиспеченный Мастер стал спускаться во двор – предстояла работа.

Пословицы «хорошо там, где нас нет» в их мире пока еще не существовало… EOF

Редакционнная 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 **копия заполненного и оплаченного бланка, отправленная в редакцию по факсу: (495) 628-8253, (доб. 120) или на emil: subscribe@samag.ru**

ИЗВЕЩЕНИЕ

Кассир

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 _____

КВИТАНЦИЯ

Кассир

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 _____

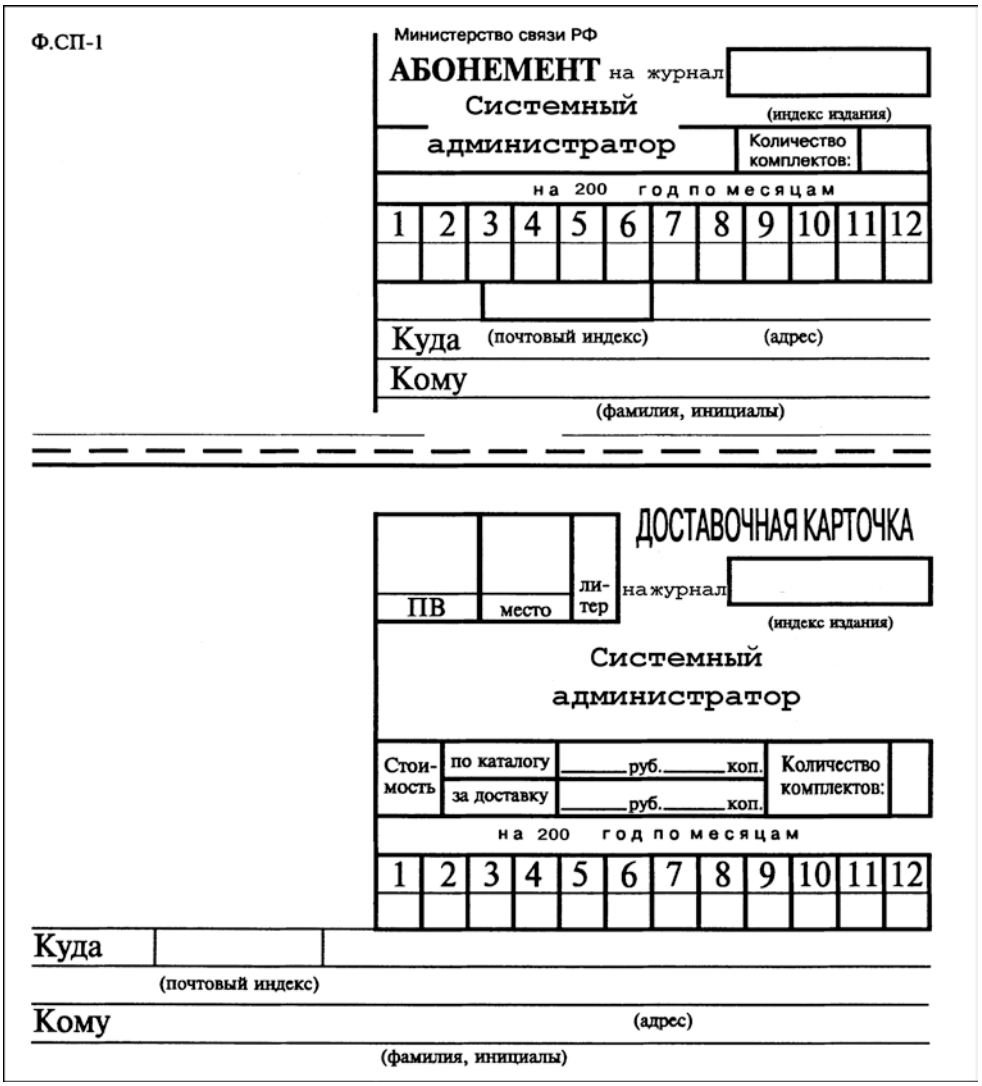
Российская Федерация

> Подписной индекс годовой – **20780**, полугодовой – **81655**
Каталог агенства **«Роспечать»**
> Подписной индекс годовой – **88099**, полугодовой – **87836**
Объединенный каталог **«Пресса России»**
Адресный каталог **«Подписка за рабочим столом»**
Адресный каталог **«Библиотечный каталог»**
> Альтернативная подписка агенства:
«Интер-Почта» (495) 500-00-60, курьерская доставка по Москве
«Вся Пресса» (495) 787-34-47
«Курьер-Прессервис»
«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 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)
> **Украина** – Киевский главпочтамт
Подписное агентство **«KSS»**, тел./факс (044)464-0220



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

УЧРЕДИТЕЛИ ИЗДАНИЯ
Частные лица

Генеральный директор
Владимир Положевец
Главный редактор
Галина Положевец
chief@samag.ru
Шеф-редактор
Наталья Хвостова
sekretar@samag.ru
Технический директор
Владимир Лукин
Главный редактор электронного приложения «Open Source»
Дмитрий Шурупов
osa@samag.ru
Дизайн-макет
Марина Рязанцева
Дмитрий Бессонов
Иллюстрации
Виктор Чумачев

Над номером работали:
Алексей Барабанов, Александр Емельянов, Андрей Бирюков, Олег Щербаков, Александр Дейтер

Рекламная и PR-служба
Дарья Зуморина, reklama@samag.ru,
Полина Гвоздь, expo@samag.ru,
тел./факс: (495) 628-82-53 (доб.120)

Распространение
Светлана Зобова
(495) 628-82-53 (доб.120)

Адрес редакции
107045, г. Москва, Ананьевский переулок, дом 4/2, стр.1,
тел./факс: (495) 628-82-53 (доб.120)
Сайт журнала: www.samag.ru

Издатель
ООО «С 13»

Отпечатано в типографии
ООО «Богородский полиграфический комбинат»
Тираж 17000 экз.
Тираж электронной версии 62000 экз.