ХАКЕР
СПЕЦ
07(68)ИЮЛЬ 2006
ЕЖЕМЕСЯЧНЫЙ
ТЕМАТИЧЕСКИЙ
КОМПЬЮТЕРНЫЙ
ЖУРНАЛ

АДМИН ВСЕЯ СЕТИ

ВСЕ ОБ АДМИНИСТРИРОВАНИИ WINDOWS И *NIX ОТ 0x00 ДО 0xFF

(game)land hi-fun media
9771609 102006 07>
publishing for enthusiasts

NT computer

AMD

СДЕЛАЙТЕ РАЗУМНЫЙ ВЫБОР

Ваш новый виртуальный дом ждет Вас!

www.nt.ru

Процессор AMD Athlon™ 64 - передовая производительность для игр, видео и музыки

AMD 64 Athlon™

www.amd.ru

Надежные компьютеры для любых задач.
Модельный ряд на все запросы и возможности. 3 года гарантии.

Компьютеры марки <NT> на базе процессора АМД Athlon ™ 64 спрашивайте в магазинах Федеральной сети компьютерных центров POLARIS.
Оптовые поставки (495) 970 1930. Сеть региональных филиалов.

intro

Если ты читаешь эти строки, значит, конец света не наступил. Один не обрушил свой молот на наш мир, мертвые не встали из могил, а пришельцы не спустились с марса в металлических цилиндрах и не стали жечь англичан своими тепловыми лучами. Ну что же, очередное пророчество не сбылось. Хотя почему я так уверен в этом? Может быть, на марсе открылся-таки портал, оттуда в наш мир действительно проникли кибердемоны, а ты, уважаемый читатель, сжимая в одной руке этот закопченный номер Спеца, а в другой — плазмаган, препятствуешь возникновению hell on Earth? Очень вероятно! Ну, ничего. Я думаю, после войны все вернется на круги своя. Помнишь, как оно было? Хорошая ведь была профессия — админ. Сидел этот человек на службе в одной конторе, по своему обыкновению ничего не делая. Жег комменты в разных блогах, знакомился по irc, получал денежки, параллельно администрируя другие конторы удаленным образом. Одновременно ухитрялся учиться в универе на бюджетной основе, заниматься фитнессом (а может, отращивать пивное брюхо — не суть важно) и ездить в Сочи пять раз в год. Красивая у админов была жизнь до войны! Как цари они жили, достойно занимая свои четырехколесные офисные троны. Так вот. Я уверен, что скоро все наладится. Красная Армия победит пришельцев, настанет эра милосердия, и воцарится мир во всем мире, и люди станут добрее друг к другу, появится порядок, а админы снова займут свое законное место под солнцем. Поэтому спрячь этот номер поглубже за бронепластины своего боевого скафандра, он тебе еще пригодится! Я думаю, немного Спецов выживет в ядерном пепле, а ведь из него ты сможешь узнать: и как сделать супер-непробиваемый хостинг и почтовый сервер, и, вообще, защитить свою корпоративную машину по полной программе. А если на развалинах городов ты найдешь хоть какое-то оборудование от CISCO — вперед, есть у нас и про это раздел!

Александр Лозовский

СПЕЦ

ЕЖЕМЕСЯЧНЫЙ
ТЕМАТИЧЕСКИЙ
КОМПЬЮТЕРНЫЙ
ЖУРНАЛ

07|68|2006

WWW.XAKEP.RU

РЕДАКЦИЯ
Главный редактор
Николай «AvaLANche» Черепанов (avalanche@real.xakep.ru)
Выпускающие редакторы
Александр «Dr.Klouniz» Лозовский (alexander@real.xakep.ru)
Андрей Каролик (andrusha@real.xakep.ru)
Редактор CD/OFFTOPIC
Иван «SkyWriter» Касатенко (sky@real.xakep.ru)
Литературный редактор
Анастасия Глухова
Арт-директор
Иван Васин (vasin@real.xakep.ru)
Дизайнер
Наталья Жукова (zhukova@real.xakep.ru)
Цветокорректор
Александр Киселев
Фотографы
Андрей Мохов
Иван Скориков

РЕКЛАМА
Директор по рекламе ИД (game)land
Игорь Пискунов (igor@gameland.ru)
Руководитель отдела рекламы цифровой группы
Ольга Басова (olga@gameland.ru)
Менеджеры отдела
Ольга Емельянцева (olgaeml@gameland.ru)
Евгения Горячева (goryacheva@gameland.ru)
Оксана Алехина (alekhina@gameland.ru)
Менеджер по работе с сетевыми РА, корпоративные продажи
Максим Григорьев (grigoriev@gameland.ru)
Трафик-менеджер
Марья Алексеева (alekseeva@gameland.ru)
тел.: (495) 935.70.34
факс: (495) 780.88.24

РАСПРОСТРАНЕНИЕ
Директор отдела дистрибуции и маркетинга
Владимир Смирнов (vladimir@gameland.ru)
Оптовое распространение
Андрей Степанов (andrey@gameland.ru)
Подписка
Алексей Попов (popov@gameland.ru)
тел.: (495) 935.70.34
факс: (495) 780.88.24

PUBLISHING
Издатель
Сергей Покровский (pokrovsky@gameland.ru)
Редакционный директор
Александр Сидоровский (sidorovsky@gameland.ru)
Учредитель
ООО «Гейм Лэнд»
Директор
Дмитрий Агарунов (dmitri@gameland.ru)
Финансовый директор
Елена Дианова (dianova@gameland.ru)

ГОРЯЧАЯ ЛИНИЯ ПО ПОДПИСКЕ
тел.: 8 (800) 200.3.999 (бесплатно для звонящих из России)
ДЛЯ ПИСЕМ
101000, Москва, Главпочтамт, а/я 652, Хакер Спец
spec@real.xakep.ru
http://www.xakep.ru

Отпечатано в типографии «ScanWeb», Финляндия
Зарегистрировано в Министерстве Российской Федерации
по делам печати, телерадиовещанию
и средствам массовых коммуникаций
ПИ № 77-12014 от 4 марта 2002 г.
Тираж 42 000 экземпляров.
Цена договорная.

ОКОННЫЙ МЕНЕДЖМЕНТ

*NIX ДЛЯ ПОВЕЛИТЕЛЯ

КОНТРОЛЬ ЖЕЛЕЗА

SPECIAL DELIVERY

ЯКОВ ХАРОН (JH@STYX.CABEL.NET)

ВПЕРВЫЕ УВИДЕЛ КОМПЬЮТЕР В 5 ЛЕТ (ЭЛЕКТРОНИКА 85), И КАК-ТО ЗАТЯНУЛО... И НЕ ОТПУСКАЛО ПОЧТИ 20 ЛЕТ. ПЕРВЫЙ СОБСТВЕННЫЙ КОМПЬЮТЕР — ATARI 800. ДАЛЬШЕ — БОЛЬШЕ. ДО СИХ ПОР ДОМА КОМПЬЮТЕРОВ БОЛЬШЕ, ЧЕМ ЛЮДЕЙ. ЗАНИМАЛСЯ ВСЕМ: ОТ СИСТЕМНОГО ПРОГРАММИРОВАНИЯ, С РАЗРАБОТКАМИ МАТЕМАТИЧЕСКИХ АЛГОРИТМОВ, ДО АДМИНИСТРИРОВАНИЯ СЕТЕЙ И ПРОЕКТИРОВАНИЯ БАЗ ДАННЫХ. ПОТОМ ПОНЯЛ: IT КУДА ИНТЕРЕСНЕЕ, КОГДА ЭТО ХОББИ — И УШЕЛ В КОММЕРЦИЮ. НО ЦЕННЫЙ СОВЕТ МОЖЕТ ДАТЬ ДО СИХ ПОР...

offtopic

HARD

SOFT

CREW

STORY

cd:

КАК ХОРОШО НАКОНЕЦ-ТО СДАТЬ ВСЕ НАКОПИВШЕЕСЯ ЗА ОСЕННЕ-ЗИМНЕ-ВЕСЕННИЙ ПЕРИОД И С ГОЛОВОЙ ОКУНУТЬСЯ В РАБОТУ. ОСОБЕННО, ЕСЛИ ТЫ АДМИН — ЭТО ВООБЩЕ ДЛЯ ТЕБЯ ЗОЛОТОЕ ВРЕМЯ, КОГДА ВСЕ БЕСТОЛКОВЫЕ ЮЗЕРЫ УХОДЯТ В ОТПУСК, И ТЫ МОЖЕШЬ СПОКОЙНО СТАВИТЬ СВОИ НЕЧЕЛОВЕСЕСКИЕ ЭКСПЕРИМЕНТЫ НАД СЕТЬЮ НА ПУТИ К БЕСКОНЕЧНОМУ САМОСОВЕРШЕНСТВОВАНИЮ!

VMWARE

- Server 1.0.0
- Server 1.0.0 (для Linux)
- Win32 Client для Server'a 1.0.0

БАБУШКИН СУНДУК

- 3proxy от 3APA3A
- AWStats
- FirefoxADM 0.4
- Mozilla Firefox 1.5.0.4
- NetOp Desktop Firewall
- Pure-FTPD 1.0.21
- WinInstall LE
- phpMyAdmin 2.8.1

УДАЛЕННОЕ УПРАВЛЕНИЕ

- DameWare Remote Control 5.1.3.0
- NetOp Remote Control
- RAdmin 2.2
- RealVNC 4.2.5
- Symantec pcAnywhere 12

СОФТ ОТ NONAME

- Audio Editor Gold 8.4.5
- AutoRun Pro Enterprise 8.0.0.71
- CloneDVD 2.8.9.9
- Magic DVD Ripper v4.1
- Portable Burning AIO by Friction Baby
- Remote Installer v1.3.76
- Virtual CloneDrive 5.1.4.5
- WinRAR v3.60 beta 5
- WinTools.NET Professional 7.4.1
- Winamp v5.22
- XoftSpySE 4.26.182
- Xplorer2 v.1.5.0.1
- Zend Studio Enterprise Edition 5.2.0


Хулиган
ЖУРНАЛ УЖЕ
В ПРОДАЖЕ
Хулиган
ЛУЧШИЕ
ФРИКИ
POSSMI

timeline

АНДРЕЙ КАРОЛИК
{andrusha@real.xakep.ru}

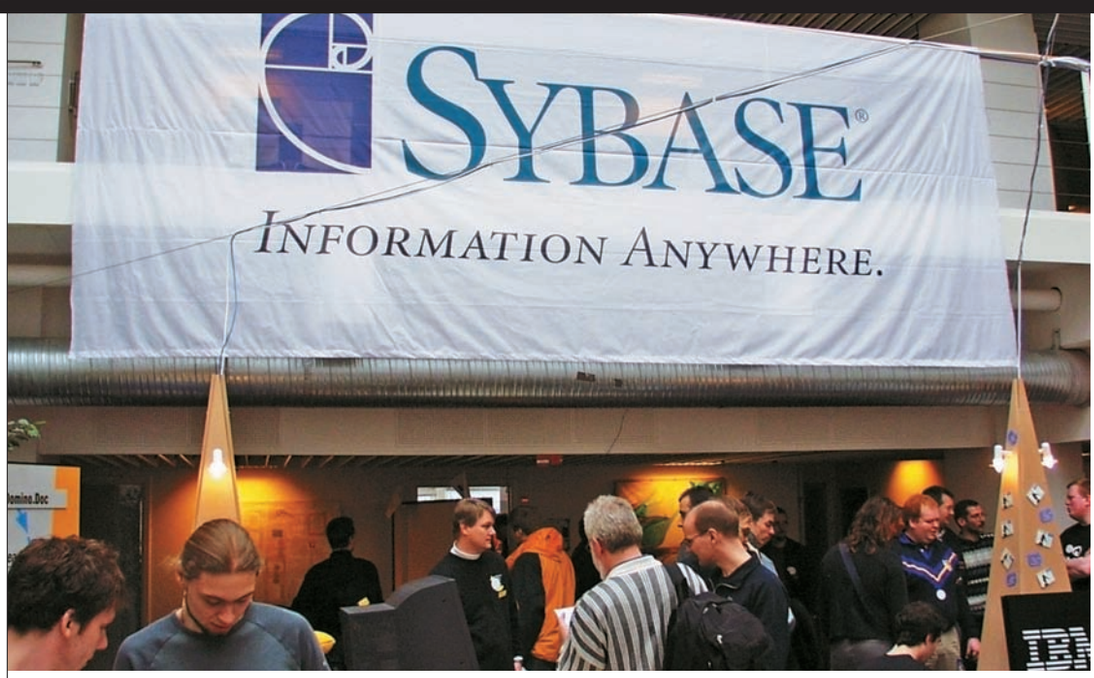
1976

Термин «Ethernet» впервые был введен Робертом Меткалфом в статье «Ethernet: технология распределенной коммутации пакетов для локальных вычислительных сетей». Этому предшествовали многочисленные эксперименты в исследовательском центре Xerox в Пало Альто, где была построена экспериментальная сеть со скоростью передачи 2,94 Мбит/с — прообраз Ethernet.

1986

Первый модульный многопротокольный маршрутизатор Cisco Advanced Gateway Server (AGS) позволил соединить устройства с различными интерфейсами с помощью протокола IP. Устройство содержало оперативную память емкостью 1 Мбайт, могло обрабатывать 200 пакетов в секунду, поддерживало соединения Ethernet, последовательные линии и ARPANET. Тогда же Cisco создает ОС, позднее названную Cisco IOS.

1988



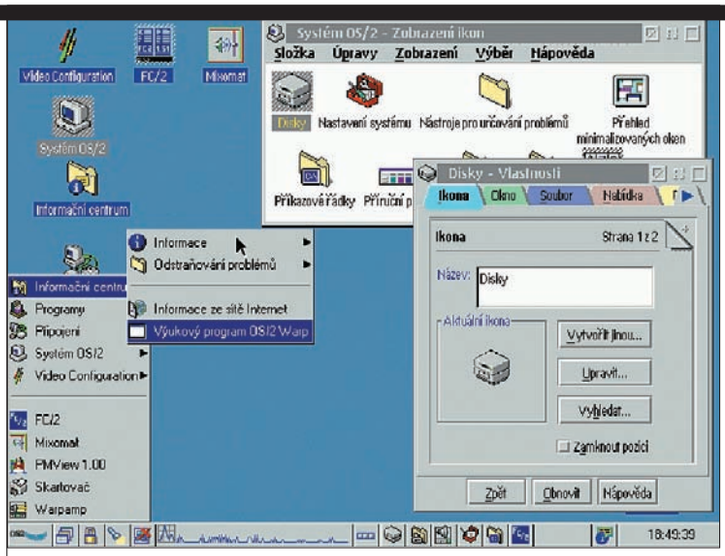
Совместно Microsoft и Sybase разработали первую версию СУБД MS SQL Server для платформы OS/2. В начале 90-х Microsoft разработала новую версию продукта, но уже для платформы Windows NT. В 1992 году были выпущены Windows NT 3.1 и SQL Server 4.2 для NT, а в 1994 году партнерство Microsoft и Sybase было формально прекращено. В 1995 году была выпущена следующая версия 6.0, однако, начиная с версии 4.2, продукт работает исключительно на платформе Windows.

1991

Операционная система Linux была разработана любителем Линусом Торвальдсом, он написал ее в качестве дипломного проекта. В 1994 году она уже была выпущена официально. С тех пор она поддерживается, развивается и дополняется сотнями тысяч таких же энтузиастов из разных стран мира. Трудно представить себе начинающего пользователя, который выбрал бы именно Linux для своей персоналки. Но если ты собираешься работать администратором локальной сети, то знакомство с Linux обеспечено тебе в любом случае.

1995

Майкрософт представила первую версию IIS (Internet Information Server) в составе Windows NT 3.51, — набор серверов для сетевых служб. Основной компонент IIS — веб-сервер, поддерживающий протоколы HTTP и HTTPS. Кроме того, IIS содержит службы, необходимые для доступа к файлам по протоколу FTP, для отправки электронной почты по протоколу SMTP, а также для предоставления доступа к группам новостей по протоколу NNTP.



1996

Вышедшая OS/2 Merlin 4.0 стала последней... IBM и Microsoft разошлись в разные стороны. Microsoft быстро переделала свою версию OS/2 в Windows NT, а сама OS/2 осталась на попечении IBM, которая, к сожалению, не уделила этой ОС должного внимания. Хотя задумка была в том, чтобы параллельно с совершенствованием Windows вести активную работу по созданию более совершенной и защищенной системы. Тем более, что нестабильность Windows не была секретом ни для кого, в том числе и для разработчиков Microsoft.

2003

В последней версии IIS 6.0 (доступной в составе систем Windows Server 2003) служба WWW претерпела серьезные изменения. Был добавлен новый режим обработки запросов, называемый режимом изоляции рабочих процессов (worker process isolation mode). В этом режиме все веб-приложения, обслуживаемые сервером, работают в разных процессах, что повышает стабильность и безопасность системы. Кроме того, для приема запросов HTTP был создан новый драйвер http.sys, который работает в режиме ядра, что ускоряет обработку каждого запроса.

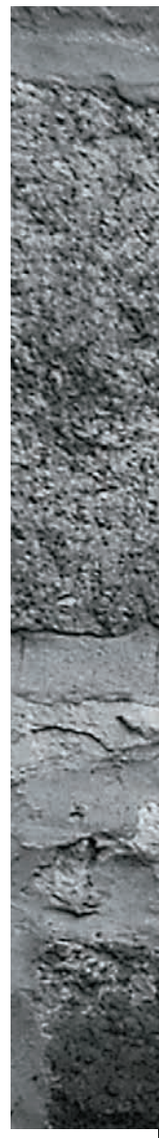
2005

Microsoft выпустила новую версию корпоративной СУБД — SQL Server 2005, под кодовым названием Yukon. Выход системы задерживался несколько раз из-за недоработок в системе безопасности. Вместе с SQL Server Microsoft выпустила среду разработки Visual Studio 2005.

8

WIN

в разделе:



фельдъегерская служба

ИНТИМНЫЕ ПОДРОБНОСТИ ИЗ ЖИЗНИ MS EXCHANGE

ИНТЕРЕСНО, КОМУ НЕ НУЖЕН ДОСТУП ИЗВНЕ К КОРПОРАТИВНОЙ ПОЧТЕ? ДУМАЮ, ТОЛЬКО ТЕМ, КТО НИКОГДА НЕ БОЛЕЕТ, НИКОГДА НЕ БЫВАЕТ В КОМАНДИРОВКАХ И ПРИ ЭТОМ ЛЮБИТ СВОЮ РАБОТУ ТАК, ЧТО НЕ ПОЗВОЛЯЕТ СЕБЕ ДАЖЕ ИЗРЕДКА ВЗЯТЬ ОТГУЛ НА ДЕНЕК. ПОСЛЕДНИЕ ИССЛЕДОВАНИЯ ПОКАЗЫВАЮТ, ЧТО СРЕДНЕСТАТИСТИЧЕСКИЙ РАБОТНИК КОМПАНИИ ТРАТИТ ДО 80% РАБОЧЕГО ВРЕМЕНИ НА КОММУНИКАЦИИ, ЛЬВИНАЯ ДОЛЯ ИЗ КОТОРОГО ПРИХОДИТСЯ НА ОБЩЕНИЕ ПО ЭЛЕКТРОННОЙ ПОЧТЕ

АНДРЕЙ СЕМЕНЮЧЕНКО
{semuha@rbcmail.ru}

Почтовый сервер Exchange является стандартом де-факто среди почтовиков, работающих на платформе Windows. Поэтому мы постараемся подробно рассмотреть организацию безопасного удаленного доступа пользователей к почтовой базе Exchange-сервера.

➜ **технологии удаленного доступа.** Существует несколько способов организации удаленного доступа к данным Exchange. Мы рассмотрим два из них. Многие знают о способе, именуемом OWA (Outlook Web Access). Для этого на стороне клиента необходимо иметь лишь веб-браузер. Но не все знают, что с появлением Microsoft Outlook 2003 и Microsoft Exchange 2003 появилась новая возможность удаленного доступа к корпоративной почте. При данном подходе Outlook оборачивает вызов удаленных процедур RPC в пакеты транспорта HTTP и передает данные в виде веб-трафика Exchange-серверу. У обоих способов есть свои преимущества, как, впрочем, и недостатки.

➜ **OWA vs. RPC через http.** Microsoft Outlook Web Access (OWA) — это плотно интегрированный компонент Exchange-сервера. Архитектура OWA сильно изменилась с первого появления этой технологии удаленного доступа в MS Exchange 5.0. Раньше OWA был фактически частью веб-сервера Microsoft IIS. Поскольку для взаимодействия с Exchange OWA версии 5.x должен был использо-


POSTBRIEFKASTEN
Leerungszeiten
täglich
außer Sonntag

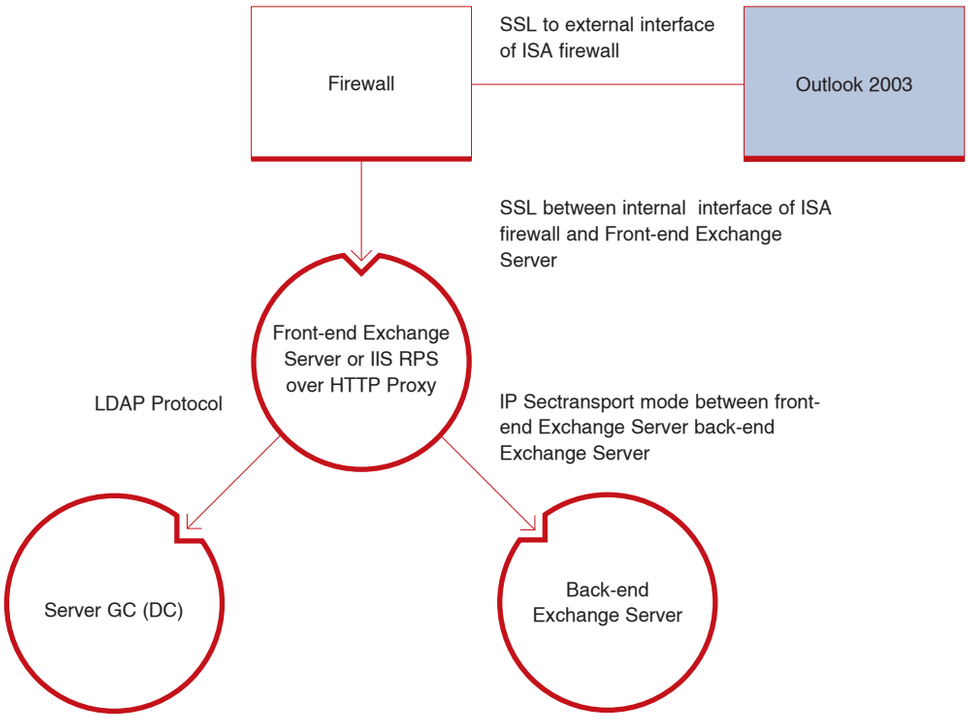


Схема взаимодействия внешнего клиента с корпоративными серверами

вать Active Server Pages (ASP) и внутри них запускать сессии MAPI. С появлением Exchange 2000 для OWA больше нет необходимости взаимодействовать через ASP и MAPI. Вместо этого клиент по-прежнему использует HTTP; однако теперь OWA встроен в систему Microsoft Web Storage и использует IIS только для получения запросов и передачи их системе Web Storage. Таким образом, IIS-сервер обрабатывает входящие от веб-браузеров http-запросы и отправляет http-ответы от Exchange 2000 или OWA. Если сервер локально содержит базу данных Exchange 2000, OWA непосредственно обращается к почтовому хранилищу. Если сервер является внешним front-end сервером (при использовании архитектуры с front-end и back-end серверами), Outlook Web Access перенаправляет запрос внутреннему back-end серверу, также используя HTTP.

Данный метод доступа давно используется многими организациями, поскольку технология стала доступна еще с появлением Microsoft Exchange 2000. Она довольно легко реализуется на корпоративном уровне и не требует установки Outlook на стороне клиента. Основной минус данного подхода — ограничение функциональности по сравнению с полноценным Outlook-клиентом.

➔ **RPC через http.** Данный способ наконец-то позволяет использовать все вкусности Outlook — от настройки правил до проверки орфографии, но при этом требует больших временных и административных ресурсов для развертывания нужной архитектуры. Также существует строгое ограничение на используемое программное обеспечение. Итак, необходима обязательная установка:

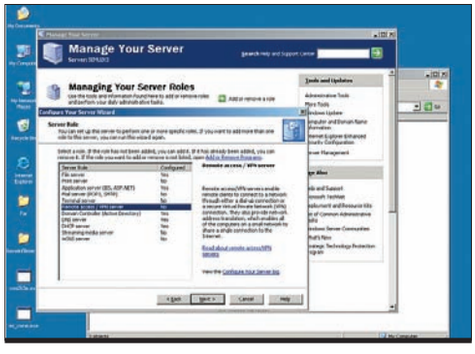
— MICROSOFT WINDOWS XP SP1 НА СТОРОНЕ КЛИЕНТА;

— MICROSOFT OUTLOOK 2003 НА СТОРОНЕ КЛИЕНТА;

— MICROSOFT WINDOWS 2003 НА ВНУТРЕННИХ И ВНЕШНИХ (FRONT-END, BACK-END) СЕРВЕРАХ, А ТАКЖЕ НА КОНТРОЛЛЕРЕ ДОМЕНА, ИМЕЮЩЕГО СТАТУС СЕРВЕРА ГЛОБАЛЬНОГО КАТАЛОГА;

— MICROSOFT EXCHANGE 2003 В КАЧЕСТВЕ ПОЧТОВОГО СЕРВЕРА;

— MICROSOFT IIS 6.0, РАБОТАЮЩЕГО В РЕЖИМЕ WORKER PROCESS ISOLATION MODE НА FRONT-END СЕРВЕРЕ.



Определение роли сервера

➔ **front-end и back-end.** Для организации удаленного доступа к Exchange-серверу через веб-браузер обычно устанавливаются и настраиваются дополнительные Exchange-серверы, называемые внешними или front-end серверами. Их отличием от внутренних (back-end) серверов является полное отсутствие почтовых ящиков пользователей. Front-end серверы используются для упрощения доступа пользователей к своей почте. При этом обеспечивается не только единообразный вид вводимого пользователями URL, но и независимость от внутренних манипуляций почтового администратора. Так, например, при переносе части почтовых ящиков с одного почтового сервера на другой, для конечных пользователей ничего не изменится, поскольку запрос пользователя сперва попадает на внешний сервер. Далее front-end сервер перенаправляет запрос серверу глобального каталога для выяснения, на каком из внутренних Exchange-серверов расположены почтовые ящики требуемых пользователей. И лишь после этого внешний сервер устанавливает HTTP-DAV соединение для нужного почтового сервера. Таким образом, все взаимодействия между клиентом и конечным сервером осуществляются через front-end сервер. На рисунке изображена схема взаимодействия пользователей с корпоративными почтовыми серверами при использовании технологии OWA.

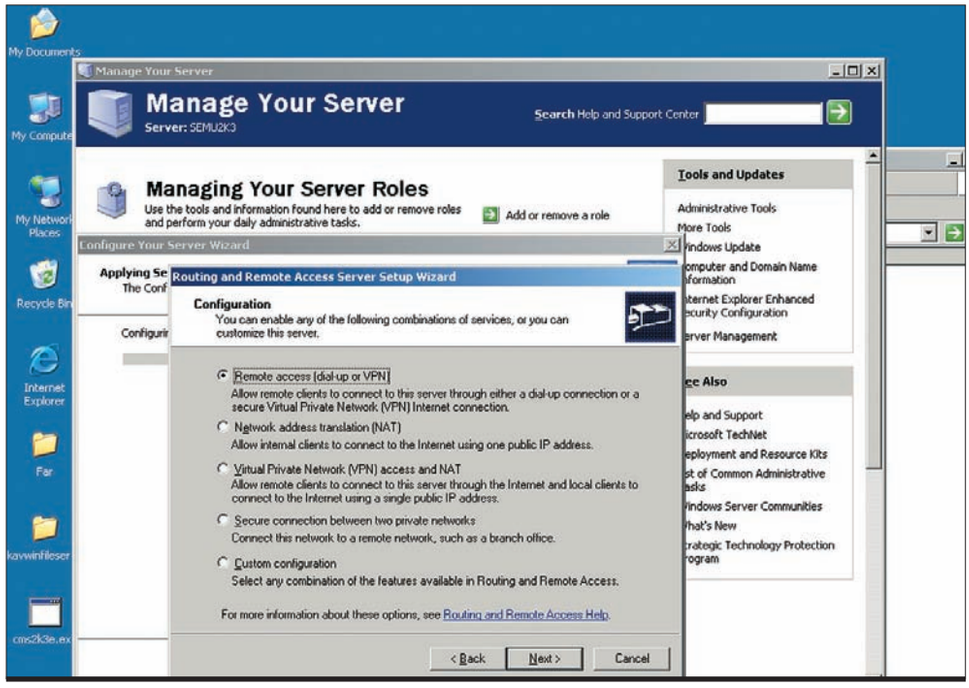
Кроме того, внешние серверы могут использоваться для выравнивания нагрузки, что бывает очень актуально при большом числе одновременно подключающихся пользователей. Правда при этом возникает проблема распределения клиентских запросов по разным front-end серверам. Решить ее можно путем настройки на DNS-сервере технологии Round Robin или же, что тоже эффективно, включением службы балансировки Windows (Load Balancing Service, WLBS).

Организовать front-end сервер довольно просто. Для этого лишь нужно запустить консоль управления (MMC) и открыть оснастку Exchange System Manager, где в свойствах выбранного Exchange-сервера нужно указать использование данного сервера в качестве внешнего (This is front-end server).

➔ **аутентификация и шифрование трафика в OWA.** По умолчанию Outlook Web Access сконфигурирован на разрешение доступа к почтовым ящикам пользователей. Однако можно перенастроить сервер таким образом, чтобы он предоставлял опре-

деленный доступ для HTTP/WebDAV-клиентов. Можно определить следующие опции:

- КАКИМ ПОЛЬЗОВАТЕЛЯМ РАЗРЕШЕН ДОСТУП К СЕРВЕРУ ЧЕРЕЗ ВЕБ-БРАУЗЕР;
- КАКИЕ МЕТОДЫ АУТЕНТИФИКАЦИИ РАЗРЕШИТЬ;
- КАКИЕ ОБЩИЕ ПАПКИ БУДУТ ДОСТУПНЫ ПОЛЬЗОВАТЕЛЯМ;
- НАСТРАИВАЕТСЯ ЭТО ДОВОЛЬНО ПРОСТО — В EXCHANGE SYSTEM MANAGER, КОТОРЫЙ ЗАПУСКАЕТСЯ ИЗ КОНСОЛИ АДМИНИСТРИРОВАНИЯ (MMC).



Настройка VPN с помощью RRAS Setup Wizard

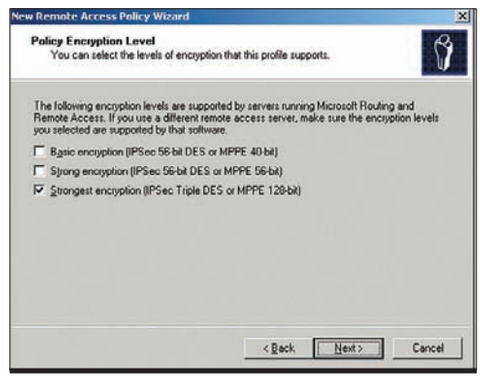
Со стороны пользователей OWA различают два вида аутентификации: явную и сквозную. Как следует из названия, явная аутентификация требует ввода учетной записи пользователя и имя нужного Exchange-сервера в строке запроса веб-браузера. Таким образом, URL может выглядеть следующим образом: **https://mycorp.com/exchange2/VasyaPupkin/**. Косвенная аутентификация более удобна для пользователей, поскольку не требует ни ввода учетных данных, ни даже имени сервера, ведь запрос сначала попадает на внешний сервер, и тот уже заботится о попадании заявки в нужные инстанции. Но при этом нужно учитывать возможность снижения производительности из-за дополнительной аутентификации на внешнем сервере.

С точки зрения внутренней корпоративной IT-инфраструктуры различают сквозную и двойную аутентификации. В первом случае внешний сервер просто пересылает запрос внутреннему серверу для аутентификации. Во втором — опознание пользователя производится как на внешнем, так и на внутреннем серверах. Этот способ более надежен.

Таким образом, при сочетании сквозной аутентификации пользователей с двойной внутренней аутентификацией достигается максимальная надежность и простота вводимого запроса.

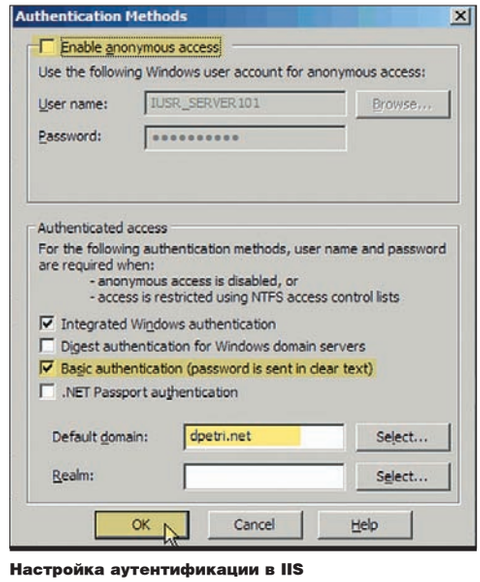
→ **организуем VPN.** Для обеспечения еще большей надежности и шифрования передаваемого трафика часто применяется туннелирование. В этом случае сначала устанавливается защищенное соединение с конечным сервером предприятия, а уже после этого пользователь может вводить URL почтового сервера в окно браузера. Самым безопасным способом является вариант с использованием сертификатов, размещенных на смарт-картах, когда клиенту даже нет необходимости вводить пароль к его учетной записи. Создание туннеля обеспечивается штатными средствами Windows Server с использованием протоколов PPTP/L2TP.

Для настройки VPN-сервера сперва необходимо поднять Routing And Remote Access-сервис. В Windows Server 2003 это делается с помощью утилиты Manage Your Server путем присвоения соответствующей роли серверу: выбираем пункт Add or Remove Role, затем выбираем Remote Access/VPN Server, жмем Next, опять отмечаем галкой VPN Server и, снова нажав Next, проходим до конца. Далее нужно выбрать протоколы аутентификации/шифрования данных. Это можно сделать при настройке политики удаленного доступа, запустив New Remote Access Policy. По умолчанию в качестве протокола аутентификации используется MS-CHAP v.2, но его можно изменить и при желании использовать, например, EAP-TLS для аутентификации, основанной на сертификатах. При использовании шифрования передаваемых данных на протоколах L2TP поверх IPSec в соединениях VPN, на VPN-сервере, также как и на клиентском компьютере, должен быть установлен цифровой сертификат.

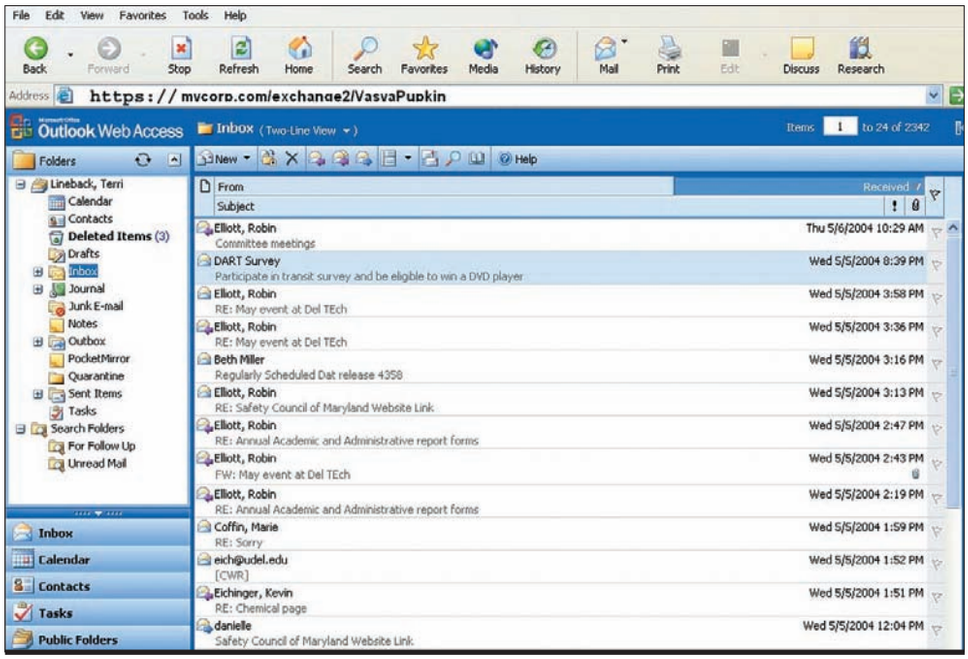


Выбор уровня шифрования

Для выписки сертификата можно воспользоваться либо платной услугой сторонних сертификационных центров, либо установить собственный центр сертификатов CA (Certificate Authority). После соответствующей настройки CA-сертификат можно выписать с помощью процедуры авторегистрации сертификатов. Для этого запускаем Administrative Tools и кликаем по ярлыку Active Directory Users and Computers. Затем раскрываем свойства домена и выбираем вкладку групповой политики Group Policy tab, выбираем Default Domain Policy, а затем нажимаем Edit. В консоли групповой политики раскрываем объект Computer Configuration, затем Windows Settings, затем Security Settings, и, наконец, Public Key Policies. Щелкаем правой кнопкой по пункту Automatic Certificate Request Settings, выбираем New, а затем Automatic Certificate Request. Если мы все сделали правильно,



Настройка аутентификации в IIS



Так выглядит Outlook Web Access в окне IE

должен запуститься мастер Automatic Certificate Request Setup Wizard. Выполняем простые шаги по запросу сертификата от сертификационного центра и заканчиваем работу мастера. После этого можно закрыть консоль групповой политики. Для немедленного применения групповой политики следует выполнить следующую команду: secedit /refreshpolicy machine_policy.

➔ **новая технология RPC через HTTP.** В принципе, в Outlook'е всегда существовала возможность использования удаленных процедур RPC для обработки вызовов MAPI и удаленного доступа к Exchange. Но, из-за огромного количества обнаруженных ранее дыр в безопасности RPC, сейчас практически невозможно подключиться к серверу с использованием данной службы. Это обусловлено тем, что администраторы просто блокируют стандартные порты RPC (135, 137, 139, 445) правилами брэндмауэров.

На помощь пришла новая технология Microsoft — RPC через HTTP. Вызовы RPC оборачиваются в пакеты http и отправляются почтовому серверу. На самом деле, архитектура RPC over http напоминает технологию OWA при использовании схемы с front-end и back-end серверами. Поэтому процедура соединения вторит рассмотренной ранее для OWA: proxy-сервер, принимая запрос от клиентского приложения, отправляет LDAP-запрос серверу GC и, получив информацию о местонахождении почтового ящика клиента, осуществляет роль посредника между конечным сервером и клиентом.

➔ **настройка серверов на работу с RPC через HTTP.** Таким образом, пакеты сперва попадают внешнему серверу, называемому внешним proxy-сервером. Причем нет никакой необходимости устанавливать на этом proxy-сервере Exchange-сервер: достаточно лишь задействовать фильтр ISAPI в IIS 6.0, который входит в состав дистрибутива Windows 2003 Server. Не забудем также установить службу RPC over HTTP. Для этого идем в Add/Remove Programs, затем Add/Remove Windows Components и раскрываем детали Network Services. В появившемся окне отмечаем для установки службу RPC over HTTP.

Следующим шагом конфигурирования является настройка виртуального каталога и определение методов аутентификации пользователей. Для этого запускаем менеджер IIS из консоли MMC. Раскрываем нужный нам сервер, которым является локальный компьютер, и находим виртуальную директорию RPC (RPC Virtual Directory). Открываем свойства объекта. На вкладке Directory Security выбираем нужный режим аутентификации: либо Windows Authentication, либо Basic Authentication, если используется SSL. Не забываем отключить anonymous login. К сожалению, RPC через HTTP в качестве Windows-аутентификации пока поддерживает только NTLM и не поддерживает Kerberos. Будем надеяться, что Microsoft добавит эту функциональность в следующих версиях задействованного ПО.

Кстати, замечание: если между Outlook-клиентом и RPC-прокси установлен файрвол или http-прокси, NTLM аутентификация работать не будет. Единственным выходом в этой ситуации остается использование basic-метода.

➔ **разрешение портов.** Теперь, для сообщения нашему прокси-серверу нового статуса, нужно внести некоторые изменения в системный реестр. Дело в том, что прокси-сервер RPC должен использовать определенные порты для обмена данными со службой каталога Active Directory и с информационным хранилищем на сервере Exchange. Exchange-сервер по умолчанию использует порты 6001, 6002 и 6004 для доступа к своему хранилищу. Поэтому на прокси-сервере с установленным IIS нужно разрешить использование этих портов. Для этого запускаем regedit.exe и создаем параметр ValidPorts типа REG_SZ и значением ServerNETBIOSName:6001-6002;ServerFQDN:6001-6002;ServerNetBIOSName:6004;ServerFQDN:6004 в разделе HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Rpc\RpcProxy. Где ServerNetBIOSName — имя используемого NetBIOS-сервера, ServerFQDN — имя используемого сервера.

На серверах глобального каталога нужно также изменить значение реестра и разрешить использование порта 6004 для обращения к службе каталогов. Для этого открываем реестр, находим подраздел HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Parameters и создаем параметр типа Multi-string с именем «NSPI interface protocol sequences» (без кавычек) и значением ncacn_http:6004. Нажимаем OK и на этом заканчиваем серверную настройку.

➔ **конфигурирование клиента.** При использовании подхода Outlook Web Access настраивать на стороне клиента ничего не нужно. Достаточно лишь запустить любимый веб-браузер и ввести необходимый URL доступа к почтовому или front-end серверу в строке запроса. В случае VPN предварительно нужно будет вставить смарт-карту, содержащую нужный сертификат (это может быть usb-свисток e-token, напоминающий флешку или что-то еще), затем ввести пин-код к карте и активизировать VPN-соединение.

При работе с MS Outlook 2003 и использовании запросов RPC через HTTP возникает необходимость правильно настроить почтовый клиент. Единственное, что нам нужно знать при настройке — это URL внешнего прокси-сервера, настроенного на работу с RPC через HTTP. Итак, для настройки Outlook запускаем Custom Installation Wizard на странице Specify Exchange Settings. Затем выбираем опцию с длинным названием Configure settings for a new Exchange Server connection or replace the settings in an existing Exchange Server connection. Если нужно ввести имя нового Exchange-сервера, вводим имя нужного почтовика. Далее кликаем на кнопку More Settings и выбираем чек-бокс с именем Connect to Exchange Mailbox using HTTP. Вот здесь то и нужно ввести URL для прокси-сервера RPC over HTTP. Кстати, вводить префикс http:// (или https:// при использовании SSL) в начале URL не нужно. Нужное значение будет подставлено автоматически в зависимости от настроек аутентификации. Поэтому далее выбираем метод аутентификации пользователя. По умолчанию используется NTLM-метод, но можно также выбрать basic-метод. При втором способе настоятельно рекомендую включить SSL, иначе login и пароль будут передаваться в открытом виде.

➔ **в завершение.** Получается, мы легко справились с задачей получения доступа к внутренним почтовым ящикам извне, при этом надежно

обезопасив себя от хакеров и прочих незаконопослушных граждан. Правда, в реальных условиях, возможно, еще придется поковыряться в таких службах как RRAS, DHCP, DNS, IIS, имеющих как прямое, так и косвенное отношение к работе почтовых приложений **C**

УСТАНОВКА И НАСТРОЙКА BACK-END СЕРВЕРА

Установка back-end сервера сводится к установке обычного Exchange-сервера. Сначала нужно выполнить этапы подготовки Active Direcory, а именно — расширить схему службы каталогов. Для этого нужно выполнить последовательно команды, предварительно вставив компакт с Exchange в CD-ROM: Setup /ForestPrep; Setup /DomainPrep. Перед выполнением очередной команды нужно выждать время для того, чтобы данные об обновлении схемы успели реплицироваться по всему лесу. По умолчанию интервал внутрисайтовой репликации составляет 5 минут, межсайтовой — 15 минут.

Поскольку Exchange плотно использует службу имен перед установкой сервера, необходимо также проверить правильность интеграции DNS и службы AD. Для этого можно воспользоваться встроенной утилитой NLTEST с ключом /DSGETSITE. Если сервер сможет обнаружить собственное имя сайта Active Directory, будут выданы строки вида:

```
Default-First-Site-Name
The command completed
successfully
```

В случае вывода на экран чего-то подобного считай, что нам повезло.

1. Далее начинается сам процесс установки Exchange-сервера. Вот основные шаги по установке: запускаем <CD-ROM>\setup\i386\setup.exe
2. При помощи нажатия кнопки Custom можно сделать выбор тех компонентов, которые тебе требуется установить.
3. Идем дальше и выбираем наш тип лицензии. Нажимаем OK. Далее помечаем галочкой «I agree» и снова жмем OK.
4. Если это первый сервер Exchange, нажимаем «Create new site» и указываем название организации и имя узла. Затем нажимаем OK.
5. Нужно выбрать учетную запись администратора Exchange. Но имеет смысл создать отдельную учетную запись для администрирования. Новая учетная запись должна располагать правами «Log on as a service» и «Restore files and directories». Теперь вводим пароль для выбранной учетной записи и нажимаем OK. На этом процесс установки Exchange-сервера заканчивается.

При использовании технологии RPC через HTTP, для правильной коммуникации Exchange-сервера с внешними front-end серверами нужно внести изменения в системный реестр сервера. Во-первых, необходимо определить порт, через который внутренний сервер устанавливает соединения RPC через HTTP с хранилищем Exchange Store. Для этого присваиваем параметру реестра HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\ Services\MSExchangeIS\ParametersSystem\RPC/HTTP Port значение 6001 типа REG_DWORD.

Затем следует настроить внутренний сервер для перенаправления Directory Service (DS) Referral, присвоив параметру реестра HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\ Services\MSExchangeSA\Parameters\HTTP Port значение 6002 типа REG_DWORD. Затем внутренний сервер настраивается для доступа DS Proxy. Для этого параметру HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSExchangeIS\ParametersSystem\RPC/HTTP NSPI Port присваивается значение 6003 типа REG_DWORD. Подобные изменения должны быть внесены на все внутренние сервера Exchange, которые могут взаимодействовать с внешними RPC прокси-серверами.

королевская рать

ISA SERVER 24X7

ЧАСТО ВОЗНИКАЕТ ВОПРОС ОБЕСПЕЧЕНИЯ ВЫСОКОЙ ПРОПУСКНОЙ СПОСОБНОСТИ И ОТКАЗОУСТОЙЧИВОСТИ ОСНОВЫ ЗАЩИЩЕННОЙ СЕТЕВОЙ ИНФРАСТРУКТУРЫ — МЕЖСЕТЕВОГО ЭКРАНА (АКА БРАНДМАУЭР, АКА FIREWALL). ПРИ ПОСТРОЕНИИ РЕШЕНИЯ С ВЫСОКИМИ ТРЕБОВАНИЯМИ К ДОСТУПНОСТИ НЕОБХОДИМО РЕШИТЬ ДВЕ ЗАДАЧИ: ЦЕНТРАЛИЗОВАННОГО ХРАНЕНИЯ ИЛИ РЕПЛИКАЦИИ ДАННЫХ И БАЛАНСИРОВКИ НАГРУЗКИ

JEDI-HOCKER
{no e-mail}

➜ **построение вертикали.** Для централизованного хранения настроек массивы ISA Server используют специально обученные Configuration Storage Servers, на которых работает служба Active Directory in Application Mode (ADAM). В ISA 2000 настройки сохранялись в Active Directory, и при установке ISA требовалось проводить расширение схемы AD. А эта операция необратимая (ну, по крайней мере, техническая поддержка Microsoft будет на этом настаивать, даже если ты по шагам распишешь, с какими параметрами запускать LDIF) и распространяется на все домены леса Active Directory. Учитывая, что леса AD легко пересекают океаны и могут содержать информацию подразделений компании, раскиданных по всему свету, необходимость расширения схемы может стать серьезной проблемой. Представь себе, что ты — главный администратор леса Active Directory транснациональной корпорации с центром во Владивостоке. И в один прекрасный день к тебе приходит запрос из всеми забытого отделения в штате Калифорния на расширение схемы в связи с необходимостью внедрения в качестве корпоративного межсетевого экрана ISA Server. Необходимость использования именно ISA обусловлена пактом Билла-Шварца, имеющего статус закона штата. И без массива не обойтись — в этом мелком подразделении работает пять тысяч пользователей, так что необходима балансировка нагрузки и повышенная отказоустойчивость. Что делать? Вводить необратимые изменения в структуру AD из-за странных местных законов?

Служба ADAM хранит в себе дополнительные свойства и объекты AD. Серверы общаются с ней через привычный LDAP. В одной сети, да и на одной машине, может существовать множество служб ADAM, реализующих расширения для разных приложений, например ISA и Exchange, которые живут в рамках конкретного экземпляра ADAM, не затрагивая «большую» AD. Но не беспокойся, тебе не придется заводить для каждого сервера ISA в массиве отдельный сервер хранения настроек. Можно обойтись только одним сервером Configuration Storage для массива (что не рекомендуется, поскольку возникает единая точка отказа) либо установить экземпляры ADAM на контроллеры домена или сами серверы ISA.

В случае если Configuration Storage Servers устанавливается на ISA Server, перед установкой других серверов в массиве необходимо разрешить им доступ к службе LDAP, что можно сделать путем редактирования системной политики.

После установки дополнительных серверов массива желательно проверить корректность работы серверов массива через закладку Monitoring.

➜ **круговая порука.** Самый простой метод распределения нагрузки между несколькими серве-

рами, выполняющими одинаковые функции, — DNS Round Robin. Суть этого метода крайне проста.

На DNS сервере создаются две или более записи типа A, указывающие на одно и тоже имя. Клиенты, посылающие запрос на разрешение имени, будут получать все адреса, однако порядок их следования в ответе будет меняться. В результате, при обращении к одному FQDN, разные клиенты (или один клиент в различные моменты времени) будут использовать различные IP-адреса. То есть фактически подключаться к разным серверам.

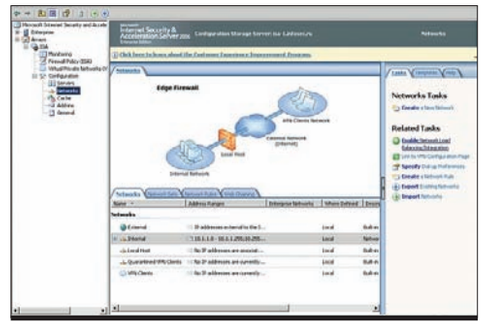
Огромным преимуществом DNS Round Robin является простота развертывания и использования. Недостатком же является отсутствие механизмов определения отказа узла. То есть в случае выхода из строя одного из серверов, клиенты все равно будут пытаться соединиться с ним до истечения времени жизни записи в кэше клиента DNS. И только вмешательство администратора, удалившего запись с адресом отказавшего узла из зоны DNS, может спасти ситуацию. Конечно, этот процесс можно автоматизировать путем проверки доступности узла и автоматического удаления его из DNS при недоступности, однако в этой ситуации возникает вопрос доступности той машины, на которой запущена контролирующая программа.

Пример простого сценария, проверяющего доступность указанного сервера, и, в случае отсутствия отклика, удаляющего его из зоны DNS-сервера:

```
CheckServer "isa.example.com",
"192.168.0.10"
Function CheckServer(strHostName, strIP)
 If Ping(strIP)<>1 Then
  DeleteRecord strHostName, strIP
 End If
End Function
Function DeleteRecord(strHostName, strIP)
 set objDNS = GetObject("winMgmts:root\
MicrosoftDNS")
 set objDNSServer = objDNS.Get("Micro-
softDNS_Server.Name='.'")
 set objRRs = objDNS.ExecQuery
(" select * " & _
      " from MicrosoftDNS_ResourceRecord
" & _
   " where OwnerName = '" & strHostName
& "'" & _
   " Or RecordData = '" & strHostName
& "'")
 if objRRs.Count < 1 then
  WScript.Echo "No such
server " & strHostName
 else
 for each objRR in objRRs
  If InStr(objRR.TextRepresentation,
strIP) Then
   objRR.Delete_
  WScript.Echo "Server down,
record deleted: " & _
   objRR.TextRepresentation
  End If
 next
 end if
End Function
Function Ping(address)
 WMI = "winmgmts:{impersonationLe-
vel=impersonate}"
 wqlQuery = "SELECT StatusCode FROM
Win32_PingStatus WHERE Address" & _
  " = '" & address & "'"
 set PingResult = GetObject(WMI).ExecQu-
ery(wqlQuery, "WQL", 48)
 For Each result in PingResult
  if result.StatusCode=0 then
   ping=1
  else
   ping=0
  end if
 Next
End Function
```

Сценарий может запускаться как на сервере DNS, так и на других машинах, но в этом случае необходимо указать имя сервера в параметре MicrosoftDNS_Server.Name. Ну и, естественно, учетная запись, по которой работает сценарий, должна иметь права на управление сервером DNS (по умолчанию — Administrators).

По умолчанию поддержка Round Robin включена в Microsoft DNS Server, но может быть отключена путем модификации параметров реестра HKLM\System\CurrentControlSet\Services\DNS\Parameters\ RoundRobin и HKLM\System\CurrentControlSet\Services\DNS\Parameters\ DoNotRoundRobinTypes. Первый из них включает или отключает поддержку технологии для всего сервера, а второй позволяет отключить балансировку для некоторых типов записей, например SRV, чтобы Round Robin не мешал серверу DNS выдавать клиентам адрес

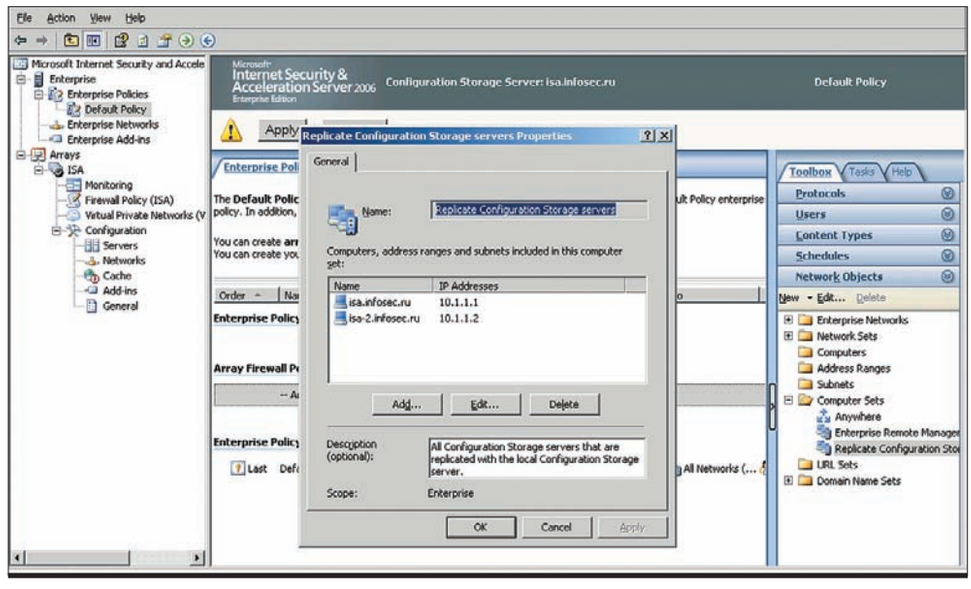


Настройка NLB в ISA

«ближайшего» к ним котроллера домена. Технология Round Robin может с одинаковым успехом использоваться как для распределения обращений внутренних пользователей к межсетевому экрану, так и для балансировки нагрузки внешних запросов или подключений через VPN.

➔ **балансировка сетевой нагрузки.** Служба, реализующая технологию Network Load Balancing (NLB), входит в стандартную поставку Windows Server и используется для повышения доступности и производительности группы серверов. По идее технология чем-то напоминает объединение жестких дисков в массивы RAID, но вместо винчестеров здесь используются несколько серверов, выполняющих одинаковые функции или содержащие одну и ту же информацию. Часто NLB используется при построении web-порталов, но может применятся и при внедрении ISA. В этом случае NLB может повысить уровень обработки запросов внутренних и внешних клиентов и уровень доступности VPN.

В отличие от «настоящего» кластера, где для хранения данных приложения используется выделенная дисковая стойка, в NLB каждый из серверов содержит свою копию данных и настроек, и задача их синхронизации ложится на плечи администратора. При использовании ISA Server Enterprise Edition эта проблема уже решена,



Разрешение доступа к службе LDAP

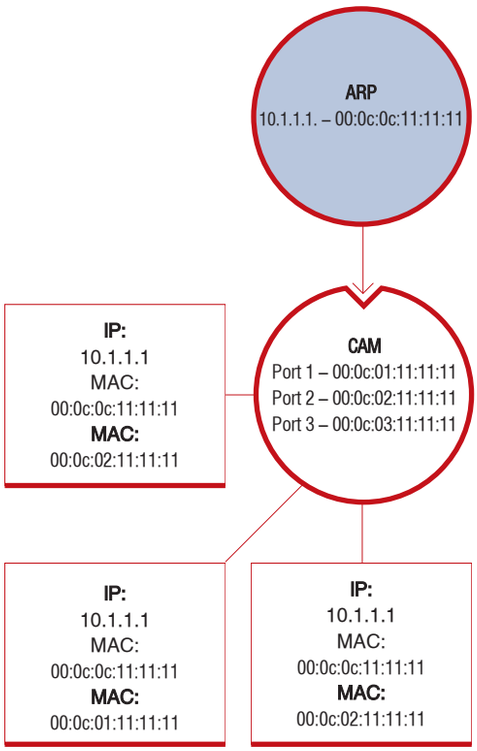


Схема работы NLB

поскольку все настройки серверов загружаются с Configuration Storage Server.

В принципе, можно реализовывать балансировку нагрузки и на ISA Server Standard Edition, но при этом надо будет самому позаботиться о синхронизации настроек (например, через функции импорта и экспорта конфигурации). Кроме того, в этом случае кластер NLB не будет отслеживать корректность работы служб ISA Server, а только сетевую доступность узла.

С точки зрения клиента, NLB представляет собой сетевой узел с одним IP-адресом (хотя у кластера может быть и несколько разных адресов в разных сетях или используемых для разных служб). Все пакеты, отправленные клиентами, доставляются каждому узлу кластера NLB, которые самостоятельно принимают решение, кто из них будет обрабатывать то или иное соединение.

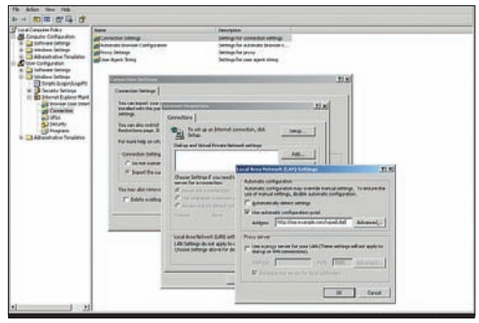
Все серверы в кластере раз в секунду обмениваются контрольными heartbeat-сообщениями, передаваемыми как Ethernet-фреймы с типом LLC 0x886F. Этот обмен позволяет обнаруживать отключение серверов или добавление нового узла в кластер. Кроме того, обмен сообщениями позволяет синхронизировать значения приоритета каждого из узлов, указываемых администратором. Механизм NLB не поддерживает контроль соединения, и в случае выхода из строя одного из серверов кластера, все установленные с ним соединения будут потеряны. Время «схождения» системы при добавлении нового члена или удалении сервера из кластера — несколько секунд.

К сожалению, механизм балансировки нагрузки не учитывает текущую загрузку процесса узлов кластера. Соответственно, если в кластер входят узлы с различной аппаратной конфигурацией, более мощные должны иметь более высокий приоритет. Могу порекомендовать выделять для обмена управляющими соединениями отдельный сетевой адаптер, подключенный к специально выделенному для этих задач коммутатору.

Распределение нагрузки происходит на основе количества запросов в единицу времени. Используя адрес отправителя и номер порта в качестве идентификатора, узлы кластера определяют узел, который будет обрабатывать тот или иной запрос. В принципе, разные запросы одного клиента могут обрабатываться разными узлами кластера, что может привести к нежелательным последствиям. Чтобы избежать этой ситуации, есть возможность сконфигурировать правила обработки запросов от клиентов, так называемые Affinity. Если значение этого параметра равно Single Affinity, то все запросы с одного IP-адреса будут обрабатываться одним и тем же узлом кластера. Это позволит избежать проблем с протоколами, устанавливающими несколько соединений (например, PPTP, который передает управляющую информацию по TCP, а непосредственно данные — с использованием GRE). Еще один вариант распределения нагрузки — Class C Affinity, когда одним узлом кластера обслуживаются запросы группы узлов, чьи адреса принадлежат одной сети с маской 255.255.255.0.

Рассмотрим подробнее механизм балансировки нагрузки. Как уже говорилось, все узлы NLB-кластера используют один и тот же виртуальный IP-адрес, по которому происходят обращения клиентов. Логично предположить, что все эти машины должны быть расположены в одном сегменте. Соответственно, когда приходит первый пакет от клиента на виртуальный адрес кластера, маршрутизатор просматривает свою таблицу ARP, и, не обнаружив в ней соответствующего MAC-адреса, посылает широковещательный ARP-запрос. На всех узлах кластера используется не только виртуальный IP-адрес, но и виртуальный MAC-адрес, который они возвращают в ARP-ответе маршрутизатору. Однако в заголовках Ethernet ARP-ответа указывается совсем другой MAC-адрес отправителя, уникальный для каждого узла кластера.

Маршрутизатор заносит MAC-адрес в таблицу ARP и передает пакет коммутатору. Коммутатор пересылает пакет на все порты, поскольку в его таблице коммутации нет соответствия между номером порта и виртуальным MAC-адресом кластера. Все узлы NLB получают пакет, и тот из них, который должен обрабатывать пакет, формирует ответ, опять-таки указывая в поле «адрес отправителя» Ethernet-заголовка свой индивидуальный MAC-адрес (не только Cain умеет делать ARP-Spoofing). Таким образом, мы держим коммутатор в неведении относительно виртуального MAC-адреса кластера, заставляя передавать входящие пакеты на все порты. Так работает Unicast-режим кластера NLB.



Настройка IE через групповые политики

Кластер может работать в режиме Multicast, когда адаптерам узлов присваивается адрес многоадресной рассылки Ethernet, соответствующий виртуальному IP-адресу. Использование Multicast-режима предпочтительнее, поскольку он позволяет узлам взаимодействовать друг с другом без добавления дополнительного сетевого интерфейса. Правда, иногда возникают проблемы с маршрутизаторами, которые не добавляют в ARP-таблицу соответствие между Multicast-адресом Ethernet и обычным IP-адресом. В этом случае запись надо добавлять вручную.

Настройка массива NLB в ISA тривиальна — через пункт Networks необходимо выбрать Enable Load Balancing Integration и указать используемые сетевые интерфейсы и их общий адрес.

Дополнительно надо проверить наличие записей DNS и Service Principle Name для каждого из узлов массива и всего массива в целом. Это необходимо для корректной работы аутентификации Kerberos между серверами ISA.

Записи SPN можно зарегистрировать с помощью утилиты SetSPN из состава ResourceKIT:

```
setspn -a ldap/isa-1.msfirewall.org ISA-1
setspn -a ldap/isa-2.msfirewall.org ISA-2
setspn -a ldap/isa.msfirewall.org ISA
setspn -a ldap/isa-1.msfirewall.org:
389 ISA-1
setspn -a ldap/isa-2.msfirewall.org:
389 ISA-2
setspn -a ldap/isa.msfirewall.org ISA
```

Для изменения свойств кластера (например, изменения режима работы на Multicast) можно воспользоваться свойствами службы балансировки нагрузки в настройках сетевого интерфейса.

➔ **экономим трафик.** Если на предприятии используются в основном клиенты HTTP-Proxy, то есть смысл задействовать механизм Cache Array Routing Protocol (CARP). Эта техника, доступная в рамках серверов одного массива, позволяет оптимизировать использование кэша серверов.

Серверы ISA не реплицируют содержимое кэша между собой, но вместо этого клиенты и ни-

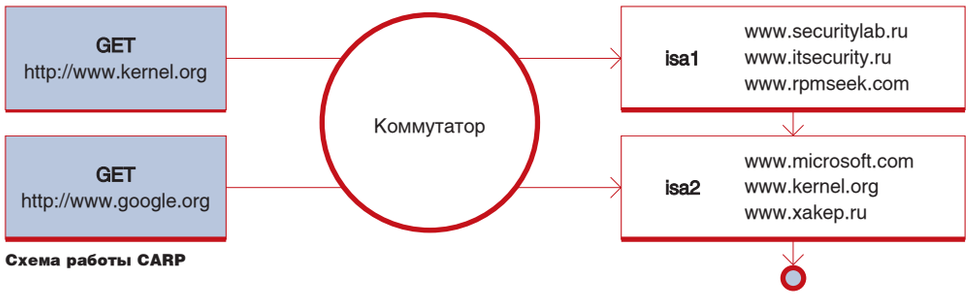


Схема работы CARP

жестоящие серверы выбирают для отправки запроса тот сервер, на котором с большей вероятностью будет присутствовать уже загруженный объект. Для этого клиенты, получив настройки массива, периодически отправляют запросы на получение текущей конфигурации массива (**http://array.example.com/array.dll?get.routing.script**). Файл содержит информацию об URL (точнее их хэши), которые известны различным серверам массива. По этой информации браузер определяет, к какому из серверов послать запрос. Если информация клиента не актуальна, и запрос пришел не на тот сервер, ISA Server перенаправит запрос на другой узел массива и вернет полученную из кэша информацию клиенту.

Таким образом, объем кэша массива будет равняться суммарному объему всех закэшированных объектов на каждом из узлов. Это позволяет значительно поднять вероятность получения объекта из кэша сервера, а не из интернета, и увеличить размер кэша.

➔ **настройка клиентов.** Текущая конфигурация массива публикуется либо на внешнем, либо на встроенном в ISA web-сервере. Во втором случае ISA следит за актуальностью информации. При использовании функции публикации средствами ISA могут возникать конфликты с установленным на этом же компьютере web-сервером, поскольку и ISA, и web-сервер будут пытаться занять один и тот же порт.

Информация о массиве представляет собой файл, написанный на языке JavaScript, содержащий инструкции для браузера, где указывается, в каких ситуациях должен использоваться тот или иной сервер ISA или прямое соединение. В файлах конфигурации браузера определены дополнительные функции и переменные, на основании которых браузер принимает решение об обращении к proxy. Основной функцией подобного сценария является FindProxyForURL(url, host), которой браузер передает имя узла, к которому обращается, и полный URL. Функция должна вернуть либо имя сервера, либо указание на прямое соединение.

Сценарий предписывает использовать proxy. example.com:8080 для соединения со всеми серверами, за исключением тех, доменные адреса которых заканчиваются на .example.com или имеющих адрес в сети 10.55.0.0/32:

```
function FindProxyForURL(url, host)
{
 if (isPlainHostName(host) ||
   dnsDomainIs(host, ".example.com") ||
   isInNet(host, "10.55.0.0",
"255.255.0.0"))
   return "DIRECT";
 else
   return "PROXY proxy.example.com:8080";
}
```

Подробнее о создании файлов автоматической настройки можно узнать из документа «Navigator Proxy Auto-Config File Format», доступного по адресу **http://wp.netscape.com/eng/mozilla/2.0/relnotes/demo/proxy-live.html**. Если задействована функция публикации настроек через ISA Server, то формированием файла занимается сервер, в зависимости от текущего состояния массива.

Настроить клиента на работу с массивом можно двумя способами. Первый: указать URL, по которому доступен сценарий автоматической конфигурации. Это можно сделать локально, либо централизовано, с помощью групповых политик. К сожалению, стандартный набор параметров групповых политик позволяет настраивать только Internet Explorer. В случае использования других браузеров можно применить альтернативные методы настройки.

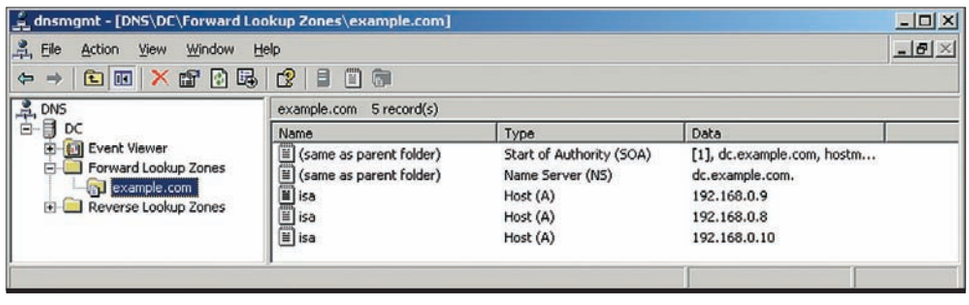
Еще один вариант централизованной настройки Firefox через групповые политики — набор сценариев FirefoxAdm (**http://prdownloads.sourceforge.net/firefoxadm/**). В набор входит административный шаблон, подключаемый к редактору групповых политик, и сценарий входа в систему (Logon Script), добавляемый в объект групповой политики пользователей. Указанные с помощью административного шаблона настройки сохраняются в ключе реестра HKCU\Software\Policies\Firefox, откуда считываются сценарием входа в систему и сохраняются в файле конфигурации FireFox. Немного сложная схема, но что делать, если FireFox сохраняет параметры настройки в файлах, а не ключах реестра!

Можно воспользоваться альтернативным дистрибутивом FrontMotion Firefox Community Edition (**www.frontmotion.com/Firefox/fmfirefox.htm**), который обучен читать настройки из реестра. Кроме того, дистрибутив оформлен в виде файла MSI, что позволяет развертывать его через групповые политики, и при установке указывает себя в качестве браузера «по умолчанию» для ОС.

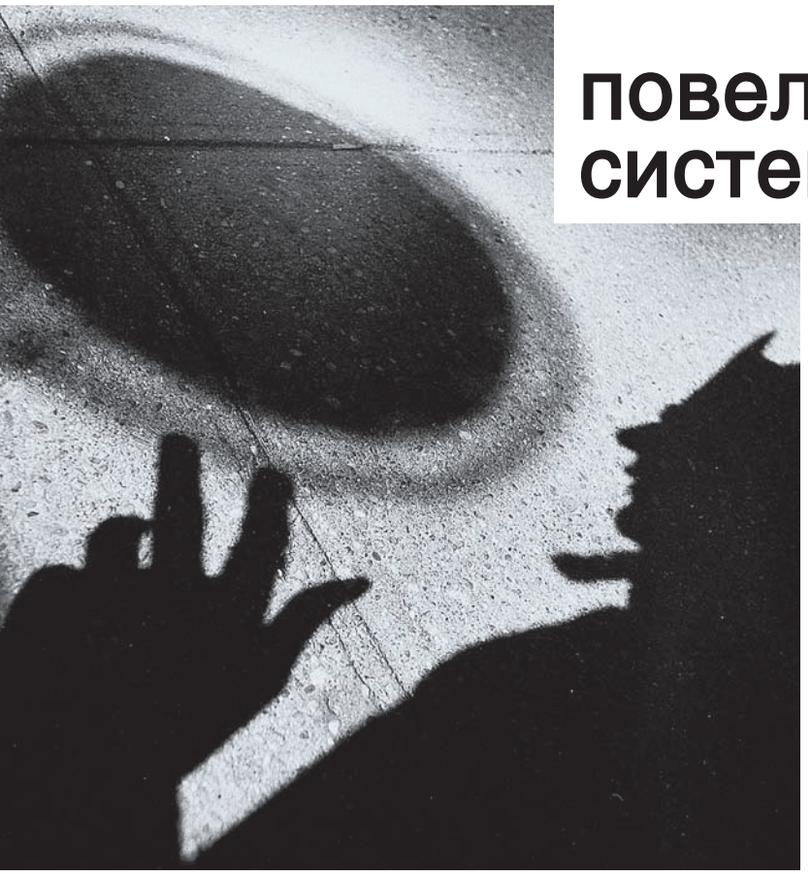
Другой метод настройки, поддерживаемый многими браузерами, — использование механизма полностью автоматической настройки Web Proxy Auto-Discovery (WPAD). Настройки WPAD могут передаваться клиентам двумя способами: через сервер DHCP, либо с помощью системы DNS. Если клиент получает IP-адрес с сервера DHCP, то на сервере можно создать дополнительную опцию WPAD--, в которой указывается URL сценария автоматической настройки. Машина пользователя вместе с настройками TCP/IP получает URL, к которому обращается браузер для настройки. Недостатком данного метода является необходимость использования DHCP и возможность применения только в рамках одного сегмента. Если есть необходимость настраивать клиентов в разных сегментах, лучше воспользоваться распространением настроек через службу DNS.

В этом случае в зоне DNS-домена, к которому принадлежат компьютеры пользователей, создается запись CNAME с именем WPAD, например WPAD.example.com. Эта запись указывает на адрес web-сервера, на котором опубликован сценарий автоматической настройки. Браузер клиента посылает DNS-запрос на разрешение имени WPAD.example.com и в ответе получает адрес (или адреса, ведь никто не мешает задействовать Round Robin) web-сервера, к которому обращается с запросом на получение файла wpad.dat. Файл представляет собой уже известный JavaScript, используемый для определения адресов proxy.

Как видишь, вариантов повышения производительности и отказоустойчивости ISA Server множество. Правильно выбирай, толково настраивай и спокойно спи ночами **C**



Настройка записей DNS



повелители систем

ОБЗОР СОФТА ДЛЯ УДАЛЕННОГО АДМИНИСТРИРОВАНИЯ

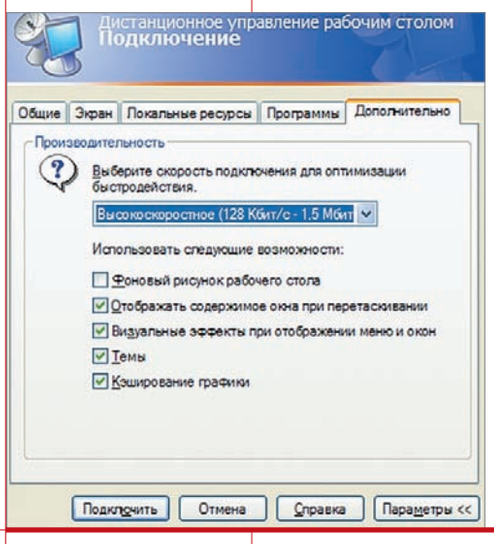
ХОРОШАЯ ВЕЩЬ — УДАЛЕННОЕ АДМИНИСТРИРОВАНИЕ! ЕСЛИ БЫ ЕГО НЕ БЫЛО, НЕ БЫЛО БЫ И АДМИНОВ, КОТОРЫЕ ТИХОНЬКО ОТРАЩИВАЮТ ПИВНОЕ ПУЗО, ОДНОВРЕМЕННО РАБОТАЯ НА ТРЕХ РАБОТАХ. ОНО ПОМОГАЕТ И ПРОСТЫМ ПОЛЬЗОВАТЕЛЯМ, КОТОРЫЕ МОГУТ ПОРАБОТАТЬ ЗА СВОИМ ДОМАШНИМ ИЛИ РАБОЧИМ КОМПЬЮТЕРОМ С ЛЮБОГО ДРУГОГО УСТРОЙСТВА, ОСНАЩЕННОГО ДОСТУПОМ В ИНТЕРНЕТ (В ТОМ ЧИСЛЕ И С МОБИЛЬНЫХ ТЕЛЕФОНОВ, КПК И Т.Д.). ОНО ПОМОГАЕТ БЫСТРО СОСТЫКОВАТЬ РАЗЛИЧНЫЕ ПЛАТФОРМЫ (НАПРИМЕР, WINDOWS И LINUX). БЛАГОДАРЯ ЕМУ МОЖНО ОПЕРАТИВНО ПЕРЕДАТЬ ФАЙЛЫ С КОМПЬЮТЕРА НА КОМПЬЮТЕР. ТАКАЯ ПРОГРАММА БУДЕТ ОТЛИЧНЫМ ПОДАРКОМ, КОТОРЫЙ МОЖНО ОСТАВИТЬ НА ВЗЛОМАННОЙ МАШИНЕ. ЕСЛИ НА АТАКУЕМОМ КОМПЬЮТЕРЕ УЖЕ УСТАНОВЛЕН НЕПРОПАТЧЕННЫЙ ИЛИ ПЛОХО НАСТРОЕННЫЙ СОФТ ДЛЯ УДАЛЕННОГО АДМИНИСТРИРОВАНИЯ, ЭТО МОЖЕТ БЫТЬ КАК НЕЛЬЗЯ КСТАТИ ДЛЯ ПРОНИКНОВЕНИЯ В СИСТЕМУ (ПРАВДА, НЕ СТОИТ ЗАБЫВАТЬ, ЧТО ТОТ ЖЕ ПРИЕМ МОГУТ ИСПОЛЬЗОВАТЬ ПРОТИВ ТЕБЯ)

ФЕДОР ГАЛКОВ
{ICQ 3266669}

REMOTE ASSISTANCE & REMOTE DESKTOP

http://www.microsoft.com
Версия: нет данных
Размер: нет данных
Статус: отдельно не распространяется

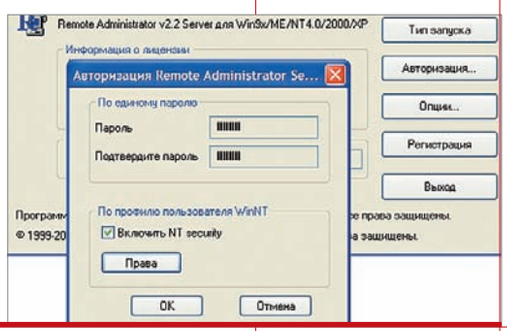
Начнем разговор о программных средствах удаленного администрирования с того, что досталось нам в комплекте с Windows XP Professional. С пары приложений — «Удаленный помощник» (Remote Assistance) и «Удаленный рабочий стол» (Remote Desktop), первый из которых служит сервером, а второй, соответственно, — клиентом. В состав дистрибутива они были включены якобы для того, чтобы более опытные товарищи могли помочь новичкам настроить систему, однако сути дела это не меняет — данные средства позволяют не только настраивать, но и полностью управлять удаленным компьютером. Для активации серверной части необходимо зайти в «Службы» («Панель управления» → «Администрирование» → «Службы») и проверить, что в статусе «Службы терминалов» значится «Работает» (по умолчанию так оно и есть). Далее надо заглянуть в «Панель управления» → «Система» → «Удаленные сеансы» и разрешить там удаленное управление, внеся нужных пользователей в доверительный список. А специальное приглашение для «опытного товарища» с просьбой погостить на компьютере и все настроить, можно отправить прямо через Windows Messenger или по почте. Теперь — про клиентскую часть. Запустить ее можно, нажав «Пуск» → «Все программы» → «Стандартные» → «Связь» → «Подключение к удаленному рабочему столу» (или «Пуск» → «Выполнить...» → «mstsc»). Правда, перед тем, как вводить IP-адрес удаленного компьютера, следует покопаться в настройках, проследовав по кнопке «Параметры». Помимо логина с паролем, будет полезным выбрать скорость подключения, отключить лишние визуальные эффекты и уменьшить цветовую палитру. Также можно настроить автоматическое подключение к принтеру, накопителям и последовательным портам нужного компа. В зависимости от твоих прав на удаленном компьютере, при подсоединении сессия текущего пользователя будет либо закрыта (если ты — администратор), либо станет недоступной (если ты в доверительном списке), либо станет недоступной, но с возможностью текстового чата с подключившимся пользователем (если ты — приглашенный специалист). В общем, встроенные средства хоть и не предлагают широких возможностей, зато есть почти у всех и полностью бесплатны.



RADMIN (REMOTE ADMINISTRATOR)

http://www.radmin.ru/download/radmin22ru.zip
Версия: 2.2
Размер: 1,8 Мб
Статус: условно-бесплатная (885 руб.)

Одной из самых известных и хорошо себя зарекомендовавших утилит является, конечно, Radmin. «Удаленный администратор» может показаться излишне примитивным, однако в данном случае первое впечатление обманчиво. Одним из основных преимуществ Radmin'а является на удивление компактный размер дистрибутива и скромные запросы к системным ресурсам и скорости соединения. Чтобы утилита без нужды не пожирала дорогой трафик, ее аппетиты легко поумерить, задав в настройках ограничение на количество цветов в палитре и предельное количество кадров в секунду. Интерфейс Radmin продуман на славу — ничего лишнего, и это при том, что все нужное всегда под рукой. Клиентский модуль предлагает на выбор пять режимов работы: «управление» (просмотр экрана, управление с помощью клавиатуры и мыши, короче, полный контроль), «просмотр» (просто наблюдаем, не вмешиваясь в работу), «телнет» (для фанатов командной строки), «обмен файлами» (ограничение — файлы не более 2 Гбайт) и «выключение».

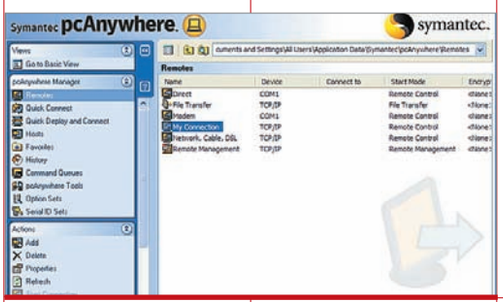


Настройки как клиентской, так и серверной частей не вызывают никаких затруднений, тем более, что их совсем немного. По умолчанию Radmin висит на порте под номером 4899, но для разнообразия можно задать и другой. Чтобы каждый раз вручную не запускать сервер, при старте системы можно включить автоматический режим, а чтобы сервер не мозолил глаза, соответствующей опцией можно отключить отображение значка в трее. Также авторы не забыли позаботиться и о безопасности. Клиент помимо стандартного пароля позволяет задать список IP-адресов, с которых (и только с них) будет разрешено удаленное администрирование, плюс для NT-систем можно разграничить права подключающихся пользователей (к примеру, запретить «полный доступ»). Тем, кому чужд английский, придется по вкусу русифицированный интерфейс и хэлп. Что можно сказать в итоге? Утилита не обременена большим количеством функций, зато работает быстро и надежно. Кстати, долгое время разработка программы буксовала, но недавно авторы наконец-таки активизировались и выпустили первую бета-версию RADMIN 3.0. Если есть желание протестировать новинку (три месяца бесплатно) — проследуйте по адресу **www.radmin.ru/ru/products/radmin30beta/**.

SYMANTEC PCANYWHERE

http://www.symantec.com/home_homeoffice/products/overview.jsp?pcid=pf&pvid=pca12
Версия: 12.0
Размер: 22,4 Мб
Статус: платная ($199.99)

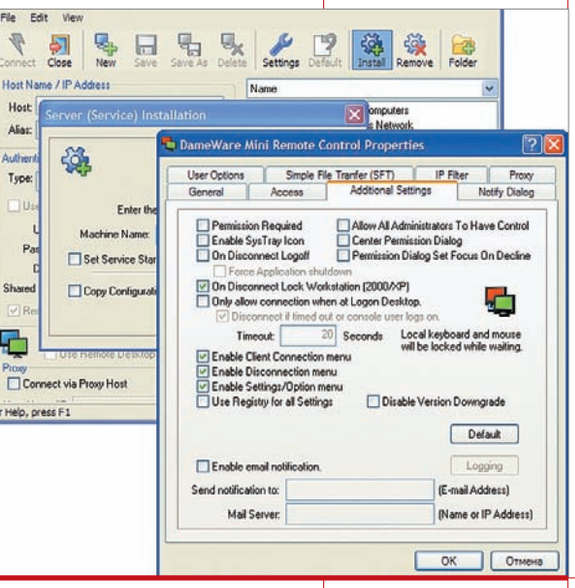
Авторы позиционируют свой продукт как лидирующий на рынке софта для удаленного администрирования, но почему-то такие заявления всегда крайне сомнительны. Первое, чем выделяется pcAnywhere на фоне Radmin'а, это существенно более широкая кросс платформенность. Серверная часть будет комфортно себя чувствовать как в среде Windows (98, Me, NT, 2000, XP), так и Linux (Red Hat, Novell, SuSE), и Mac OS X (10.3 и выше). Однако это еще скромный список, по сравнению с тем, что предлагается для клиентской части. Для начала — все те же операционные системы, плюс Windows Mobile (вообще мечта — управлять домашним компом с КПК или смартфона в любой точке земного шара, где есть сотовая связь), плюс вэб-интерфейс (нужен только Java Runtime Environment 1.4.2 или выше). Жалко только, что нет клиента под Symbian. Стандартная установка под Windows одновременно включает в себя и серверный, и клиентский модули, поэтому какая роль будет исполняться утилитой — всецело зависит от настроек. Утилита способна самостоятельно подстраиваться под скорость соединения, но если ты ей не доверяешь, то все поддается настройке вручную. Под свои нужды pcAnywhere занимает два порта (по умолчанию 5631 и 5632): один для передачи данных, другой — статусной информации. За безопасность отвечают: пароль, список IP-адресов, с которых разрешен доступ, выбранный пользователем алгоритм шифрования (вплоть до AES 256-бит) и некоторые другие. Дополнительно pcAnywhere может предложить свои услуги для передачи файлов, а также поработать в качестве шлюза (то есть связующего звена для упрощения соединения между клиентами и серверами). Кстати, любителей всяких нетрадиционных развлечений может заинтересовать то, что программа способна работать не только по TCP/IP, но и NetBIOS, SPX, плюс через нольмодемное соединение по LPT или COM-порту. К сожалению, как и многие другие утилиты от Symantec, pcAnywhere является полностью платной — никаких триальных версий не предусмотрено, поэтому с поиском дистрибутива могут возникнуть определенные проблемы.



DAMEWARE MINI REMOTE CONTROL

http://download.dameware.us/files/DWMRC5x.zip
Версия: 5.1.3.0
Размер: 10,4 Мб
Статус: условно-бесплатная ($89.95)

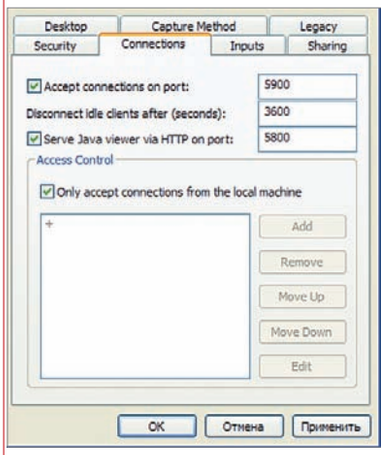
Достаточно простая и неприхотливая утилита. Может понравиться тем, кому не нужны лишние навороты. После установки не требует перезагрузки, и к тому же не занимает много места на жестком диске. Практически все функции Mini Remote Control уменьшаются внутри главного окна, однако, из-за нестандартных иконок, в поисках нужной поначалу придется перебирать все подряд. Для разнообразия программа позволяет менять темы оформления, но проку от этого не так много. Из операционных систем поддерживаются все Windows, начиная с 95, но некоторые полезные функции доступны только начиная с 2000. Установка сервера на удаленную машину организована достаточно нестандартно. Для этого придется сначала запустить «Mini Remote Control», нажать кнопку «Connect», затем, в появившемся меню — «Install», там ввести имя требуемого компьютера или его IP-адрес, потом, отметив галочку «Copy Configuration File DWRCS.INI» и кликнув по кнопке «Edit», определиться со всеми настройками, и, наконец, щелкнуть «OK». Если ты нигде не ошибся, и на подопытном компе у тебя есть администраторские права, то серверная служба должна успешно установиться. Зачем разработчикам понадобилось придумывать столь неудобный алгоритм — не совсем понятно. Впрочем, слегка подпорченное впечатление от первого знакомства меняется во время дальнейшей работы. Все стандартные функции, которые нужны для удаленного администрирования, здесь присутствуют в полном объеме. Если ничего не менять, программа займет 6129 порт, для медленных соединений предусмотрены всякие облегчающие приемы, вроде ограничения разрешения, отключения визуальных эффектов и уменьшения глубины цвета. Относительно вопросов безопасности соединения дела также обстоят неплохо (хотя в багтрек порой попадают неприятные уязвимости, вроде переполнения буфера) — пароли, шифрование, аутентификация, доступ лишь для заданных групп или пользователей — все на месте. Напоследок, Mini Remote Control готов предложить свои услуги еще и для передачи файлов.



REALVNC

http://www.realvnc.com/cgi-bin/download.cgi
Версия: 4.2.5 (Enterprise Edition)
Размер: 1,0 Мб
Статус: условно-бесплатная ($50.00)

Следующий пациент принадлежит к целому семейству так называемых VNC-систем (Virtual Network Computing), предназначенных для удаленного администрирования. В интернете, можно найти много разных реализаций VNC. Вот некоторые из них: TightVNC (**www.tightvnc.com**), VNC Scan (**www.vncscan.com**), TridiaVNC (**www.tridiavnc.com**), UltraVNC (**www.ultra-vnc.com**) и так далее. Однако остановимся на официальной программе, созданной разработчиками самой системы VNC. Утилита распространяется в трех вариантах комплектации, которые отличаются друг от друга как функциональностью, так и стоимостью (самая примитивная и вовсе бесплатна).
На сайте авторов можно скачать инсталляторы RealVNC под Windows (98-2003), Linux, HP-UX и Solaris, причем, если нужная ось в этом списке отсутствует, не стоит отчаиваться: можно попробовать поискать совместимые клиенты от других разработчиков. К сожалению, возможности RealVNC не особо впечатляют, но, если взглянуть на размер дистрибутива (установленный сервер занимает 1,4 Мб, а клиент — 0,6 Мб), многое сразу можно простить. Впрочем, для основной массы задач и имеющихся функций будет вполне достаточно. Стандартно сервер занимает

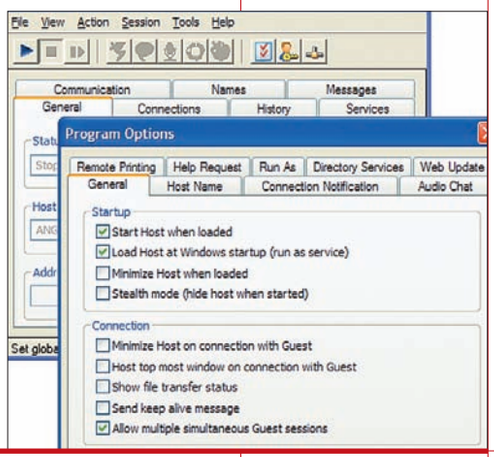


5900 порт для соединения с обычными клиентами, а на 5800 порт вешает HTTP-сервис для подключения Java-клиентов (конечно, номера портов можно переназначить или оставить только один из этих сервисов). Интерфейсы, серверы и клиенты выполнены в лучших традициях минимализма: настроек совсем не много — все интуитивно понятно. Запросы к скорости соединения также весьма скромные. К тому же, RealVNC обеспечивает достаточно неплохой уровень безопасности — распространенные виды сетевых атак автоматически отражаются, поддерживается аутентификация и шифрование трафика.
В итоге, RealVNC можно посоветовать тем, кому нужна простая и компактная кросс-платформенная замена встроенному Remote Desktop.

NETOP REMOTE CONTROL

http://www.netop.com/netop-152.htm
Версия: 8.00
Размер: 17,1 Мб
Статус: условно-бесплатная (172 евро)

Рассказывая про выдающуюся кроссплатформенность pcAnywhere, я не утверждал, что он является рекордсменом в этой области. На самом деле, по этому параметру нет равных утилите под названием NetOp Remote Control. Сервер может быть запущен под операционными системами Windows (95, 98, Me, NT, 2000, XP, 2003), Linux, Solaris, Mac OS X, OS/2 и DOS! При этом клиентский модуль приживется заодно и под Windows CE, и под Symbian OS, к тому же, на ПК можно обойтись без установки клиента (например, запускать с USB-брелка) или вовсе отказаться от дополнительных утилит, подсоединившись к хосту через браузер (только нужен ActiveX). В комплект NetOp Remote Control входит сразу шесть независимых утилит (можно установить лишь выбранные). В частности, это клиентский модуль «Guest», серверный модуль «Host», шлюз «Gateway», сервер для преобразования компьютерных имен в IP-адреса «Name Server» плюс утилиты для контроля клиентов и разграничения прав «Security Server» и «Security Manager». В каждой подпрограмме имеется гигантское количество функций и всевозможных настроек, однако, благодаря удобной сортировке по категориям, со всем можно достаточно быстро разобраться. Среди интересных возможностей можно отметить функции текстового и голосового чата между клиентами и серверами. К одному серверу могут одновременно подключаться несколько клиентов, однако, во избежание путаницы, управлять с помощью клавиатуры и мыши может только один из них — остальные только наблюдают. Огромное внимание уделено безопасности: доступны всевозможные методы аутентификации и авторизации, шифрование трафика (AES 256-бит), масса настроек по ограничению прав удаленных пользователей, защита паролем (можно задать максимальное количество неправильных попыток) и т.д. В целом, утилита оставляет впечатление продукта действительно профессионально-корпоративного уровня, поэтому для решения домашних задач удобнее выбрать нечто более простое. Кстати, чтобы попробовать условно-бесплатную версию, необходимо получить тестовые ключи — их высылают по почте после прохождения небольшой процедуры регистрации.



MICROSOFT INTERNET INFORMATION SERVICES (IIS)

http://www.microsoft.com/WindowsServer2003/iis/default.mspx
Версия: 6.0
Размер: нет данных
Статус: отдельно не распространяется

Ты, наверняка, подумал, что тут какая-то ошибка. Чего делает один из самых известных web-серверов среди программ для удаленного администрирования? Но никакой ошибки тут нет. В общем, в том, что в IIS встроены весьма продвинутые средства для удаленного управления, нет ничего удивительного, ибо в Microsoft в последнее время пытаются заботиться об удобстве использования их продуктов, или, по крайней мере, делают вид, что пытаются. Для того, чтобы заполучить в свое распоряжение IIS 6.0, необходимо и достаточно установить любую ось из семейства Windows Server 2003. Про то, как установить и настроить web-сервер, думаю, рассказывать не нужно, тем более разговор сегодня не об этом. Собственно, интересующие нас способы порулить сервером через интернет предложены аж в трех вариантах, причем это если не считать всякие приемы с самодельными скриптами. Итак, первый способ предполагает использование базового инструмента для управления сервером — IIS Manager (необходимо, чтобы он присутствовал на компьютере, с которого нужно подключиться к серверу). Второй способ также вполне стандартен — через службу терминалов, правда, это практически то же самое, что встроенное удаленное администрирование Windows XP, про которое рассказывалось в самом начале статьи. А вот про третий способ многие незаслуженно забывают, и это притом, что он куда универсальнее первых двух. Оказывается, дистанционное управление доступно и вовсе с любой платформы, и не требует каких-либо дополнительных утилит — для этого предусмотрен специальный web-интерфейс — Remote Administration (HTML). К сожалению, по умолчанию этот компонент не устанавливается, да и поддается довольно чуткой настройке контроля доступа, поэтому не стоит надеяться, что через него удастся легко забраться в недра любого сервера **C**

золотой запас данных

MS SQL SERVER 2005

XXI ВЕК ПОДАРИЛ НАМ НОВУЮ ЭПОХУ ПРОГРАММИРОВАНИЯ. СИСТЕМЫ УПРАВЛЕНИЯ БАЗАМИ ДАННЫХ НАЧАЛИ ИГРАТЬ ВАЖНУЮ РОЛЬ. ЭТО СВЯЗАННО С ВОЗРАСТАЮЩИМ ПОТОКОМ ИНФОРМАЦИИ, КОТОРУЮ НЕОБХОДИМО СИСТЕМАТИЗИРОВАТЬ, АНАЛИЗИРОВАТЬ И ПРИНИМАТЬ РЕШЕНИЯ, ОШИБКИ В КОТОРЫХ МОГУТ ДОРОГО ОБОЙТИСЬ

ВЛАДИМИР ХОПТЫНЕЦ
{начальник отдела автоматизации}

Вычислительная мощь сейчас направлена на обработку громадных массивов информации, которая лавинообразно нарастает. Разработчик БД стоит перед сложным вопросом выбора СУБД для разработки автоматизированных систем. Выбор, конечно, определяется многими факторами, но в основном — типом задачи и масштабами ее развертывания. К примеру, настольные системы не идут ни в какое сравнение с распределенными сложными автоматизированными комплексами обработки больших потоков информации. Остановимся на новом подарке от Microsoft — SQL Server 2005.

→ **краткий обзор.** SQL Server 2005, или как его еще называют — SQL Server «YUKON» — продукт не для настольных систем. Возможности, заложенные в нем, позволяют решать массу глобальных задач и строить огромные комплексные системы.

— РЕЛЯЦИОННАЯ БАЗА ДАННЫХ. ЭТО НОВОЕ ПЕРЕРАБОТАННОЕ ЯДРО, С УЛУЧШЕННОЙ ПРОИЗВОДИТЕЛЬНОСТЬЮ, С ПОДДЕРЖКОЙ ОБРАБОТКИ ДАННЫХ, ПРЕДСТАВЛЕННЫХ ЧЕРЕЗ XML.

— REPLICATION SERVICES. СЕРВИСЫ ДЛЯ ОБЕСПЕЧЕНИЯ РЕПЛИКАЦИИ ДАННЫХ ДЛЯ РАСПРЕДЕЛЕННЫХ И МОБИЛЬНЫХ СИСТЕМ. РЕАЛИЗОВАНА ИНТЕРЕСНАЯ ВОЗМОЖНОСТЬ МАСШТАБИРУЕМОГО ПАРАЛЛЕЛИЗМА С ВТОРИЧНЫМИ ХРАНИЛИЩАМИ ДАННЫХ, ПРЕДНАЗНАЧЕННЫХ ДЛЯ ОТЧЕТНЫХ РЕШЕНИЙ. КРОМЕ ТОГО, ВОЗМОЖНА ИНТЕГРАЦИЯ С РАЗНОРОДНЫМИ СИСТЕМАМИ, ТО ЕСТЬ С СИСТЕМАМИ, РАЗРАБОТАННЫМИ С ПОМОЩЬЮ ДРУГИХ СУБД.

— NOTIFICATION SERVICES. СЕРВИСЫ УВЕДОМЛЕНИЯ, ПРЕДНАЗНАЧЕННЫЕ ДЛЯ УЛУЧШЕННОЙ РАЗРАБОТКИ И ВНЕДРЕНИЯ ПРИЛОЖЕНИЙ. ОБЕСПЕЧИВАЮТ ВОЗМОЖНОСТЬ СВОЕВРЕМЕННОЙ ДОСТАВКИ ОБНОВЛЕНИЯ ИНФОРМАЦИИ БОЛЬШОМУ КОЛИЧЕСТВУ РАЗНООБРАЗНЫХ СОЕДИНЕННЫХ И МОБИЛЬНЫХ УСТРОЙСТВ.

— INTEGRATION SERVICES. ПРИМЕНЯЕТСЯ ДЛЯ ОБЕСПЕЧЕНИЯ ВОЗМОЖНОСТИ ИЗВЛЕЧЕНИЯ, ПРЕОБРАЗОВАНИЯ И ЗАГРУЗКИ ДАННЫХ В ХРАНИЛИЩА, ОБЕСПЕЧИВАЕТ ИНТЕГРАЦИЮ ДАННЫХ В МАСШТАБАХ ВСЕГО ПРЕДПРИЯТИЯ.

— ANALYSIS SERVICES. ЭТО СЕРВИСЫ ДЛЯ ОБЕСПЕЧЕНИЯ OLAP — АНАЛИТИЧЕСКОЙ ОБРАБОТКИ БОЛЬШИХ НАБОРОВ ДАННЫХ В РЕАЛЬНОМ ВРЕМЕНИ С ИСПОЛЬЗОВАНИЕМ МНОГОМЕРНОГО ХРАНИЛИЩА.

— REPORTING SERVICES. ОБЕСПЕЧИВАЕТ СОЗДАНИЕ, УПРАВЛЕНИЕ И ДОСТАВКУ ЛЮБЫХ ОТЧЕТОВ.

Новое поколение SQL Server также обладает довольно удобными инструментами управления и разработки. К первым относятся Microsoft Operations Manager и Microsoft System Management Server. Инструменты же разработки тесно интегрированы в Microsoft Visual Studio 2005.

Следует еще отметить, что SQL Server 2005 полностью поддерживает 64-битную архитектуру, и это не может не радовать.

→ **SQL Server Express**. Абсолютно бесплатный продукт от Microsoft, что радует. Некоторые могут подумать, что это клон MSDE, но это не так. У него нет никаких ограничений при работе в сети. Единственное что, работа по сети отключена по умолчанию после установки.

ограничения:

- 1 ПРОЦЕССОР;
- 1 ГБ ОПЕРАТИВНОЙ ПАМЯТИ;
- 4 ГБ БАЗА ДАННЫХ.

Server Express доступен для загрузки с официального сайта Microsoft и совместим со всеми последующими версиями продукта. Но содержит, как говорится, только базовый набор возможностей, то есть саму реляционную базу данных. А вот модули, обеспечивающие дополнительные возможности, такие как Full Text Search, Reporting Services — доступны в отдельно загружаемых Advanced Services, кстати говоря, тоже бесплатных. Кроме того, Microsoft System Management Server тоже можно скачать отдельно и спокойно установить себе на радость. На сайте Microsoft доступна для скачивания Microsoft Visual Studio 2005 Express Edition, правда, с ограничением на один язык для среды разработки, зато содержащая все необходимые инструменты для разработки баз данных.

➔ **SQL Server Workgroup.** Предназначен для работы в среде небольшой компании или офиса. Тут уже есть полный набор всех инструментов с автоматическим распределением памяти и вычислительной нагрузки. Присутствуют средства автоматического резервного копирования, ведения логов, импорта/экспорта данных. Но отсутствуют такие полезные вещи, как Database Tuning Advisor и Notification Services.

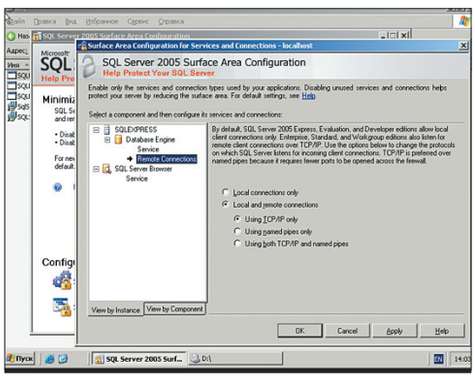
ограничения:

- 2 ПРОЦЕССОРА;
- 3 ГБ ОПЕРАТИВНОЙ ПАМЯТИ.

➔ **SQL Server Standart.** Мощная СУБД, предназначенная для работы в средних по масштабу компаниях, снаряженная почти полным боекомплектом. Тут уже присутствует зеркалирование баз данных и отказоустойчивая кластеризация, правда, только на две ноды. Но нет онлайнового индексирования и многих усовершенствований, которые, в принципе, на данном уровне масштабирования не нужны.

ограничения:

- 4 ПРОЦЕССОРА.



Настройка работы по сети

➔ **SQL Server Enterprise, SQL Server Developer, SQL Server Evaluation Edition.** Можно рассматривать вместе, так как разница у них только в лицензировании. Enterprise предназначен для работы крупного предприятия, Developer — для разработки баз данных любого масштаба, поэтому обладает полным спектром возможностей. А Evaluation предназначен для ознакомления со всеми возможностями и распространяется свободно с сайта Microsoft с периодом использования в 180 дней. Не имеет каких-либо ограничений, так что все зависит от железа.

➔ **SQL Server Mobile.** Предназначена для использования в мобильных устройствах. Очень удобна для организации распределенных баз данных, для сбора и анализа статистической информации.

➔ **установка.** Если интересуешься тем, что получше и побесплатнее, то в этом плане для небольших компаний или для собственных разработок вполне подходит SQL Server Express. На нем и остановимся более подробно. Дело в том, что здесь уже есть все, что необходимо разработчику баз данных.

Microsoft предоставила бесплатно также Visual Studio Express, правда с отдельными продуктами. Возьмем для примера C# Express, который позволяет разрабатывать любые приложения .NET с помощью мощного языка C#. Для установки надо обновить платформу .NET до 2.0, которая идет вместе с образом диска C# Express. SQL Server Express, конечно же, идет вместе с этим образом. Но прежде чем установить, обнови еще Windows Installer до версии 3.1. Иначе установка SQL Server просто не начнется — он будет жалобно просить обновить этот компонент. Тут поджидает небольшой подвох: дело в том, что даже после выкачки соответствующего патча он не установится, пока вручную не остановишь предыдущую версию службы Windows Installer. Во всяком случае, так пришлось сделать мне.

➔ **ставим на Microsoft Windows Server 2003 Standart Edition SP1.** Процесс инсталляции начинаешь с запуска самораспаковывающегося архива SQLEXPR.EXE. После распаковки проверяется версия Windows Installer и, если она соответствует требованиям, на экран выплевывается лицензионное соглашение. Его, конечно, принимаешь и жмешь Next. Далее установка захочет поставить Microsoft SQL Native Client и Microsoft SQL Server 2005 Setup Support Files. Молча со всем соглашаешься и жмешь клавишу Install. После этого фактически стартует мастер установки уже самого SQL Server. После экрана приветствия система пройдет еще один этап тестирования на совместимость, и появится экран со списком соответствий/несоответствий и разных предупреждений.

Список не маленький, но все понятно, и никаких особых сложностей с установкой возникнуть не должно. В итоге, ты попадешь на выбор устанавливаемых компонентов. В качестве базового набора предлагается установить:

в разделе Database Services:

- DATA FILES
  ПОДДЕРЖКА ФАЙЛОВ БАЗ ДАННЫХ. ФАКТИЧЕСКИ ЭТО ИМЕННО ТО, РАДИ ЧЕГО ТЫ СТАВИШЬ SQL SERVER.
- REPLICATION
  НАБОР ОБЪЕКТОВ РЕПЛИКАЦИИ, НЕОБХОДИМЫХ ДЛЯ КОПИРОВАНИЯ ДАННЫХ И ОБЪЕКТОВ БАЗ ДАННЫХ В ОДНУ ИЛИ НЕСКОЛЬКО БАЗ ДАННЫХ.
- SHARED TOOLS
  ОБЪЕКТЫ ДЛЯ ОРГАНИЗАЦИИ ОБЩЕГО ДОСТУПА.

в разделе Client Components:

- CONNECTIVITY COMPONENTS
  КОМПОНЕНТЫ ДЛЯ ВЗАИМОДЕЙСТВИЯ КЛИЕНТА С СЕРВЕРОМ, ВКЛЮЧАЯ СЕТЕВЫЕ БИБЛИОТЕКИ ДЛЯ ODBC И OLE DB.
- SOFTWARE DEVELOPMENT KIT
  НАБОР КОМПОНЕНТОВ ДЛЯ РАЗРАБОТКИ МОДЕЛЕЙ И ПРОГРАММИРОВАНИЯ.

Выбирай для установки хоть все, что перечислено, хотя Replication, Shared Tools и Software Development Kit — не обязательны.

Далее мастер запросит имя для данного экземпляра объекта службы SQL Server. Теперь нужно выбрать тех, кто будет использовать данную службу.

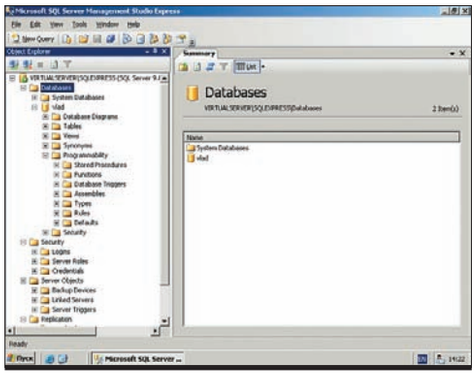
Также нужно будет указать, какая служба стартует автоматически. Отдельно о службе SQL Browser: она используется для возврата именованного канала и адреса TCP-порта клиенту. По умолчанию эта служба выключена, так как SQL Server 2005 Express Edition вначале настроен на локальное рабочее место.

Следующий шаг — режим аутентификации, используемый при подключении к службе SQL Server. Рекомендуется смешанный, так как ты можешь использовать пользователей домена для разрешения подключения к серверу, но некоторые дополнительные инструменты и скрипты могут быть настроены на подключение через авторизацию в самой службе.

После этого необходимо настроить установки сортировки для SQL Server. Все зависит от используемого в базах языка и особенностей работы на сервере, так как иногда необходимо различать прописные и строчные буквы, и т.д.

➔ **сервер установлен.** Тем не менее, он настроен еще и на работу на локальном рабочем месте. Для того чтобы разрешить работу по сети, необходимо запустить SQL Server 2005 Surface Area Configuration из меню Пуск → Программы → Microsoft SQL Server 2005 → Configuration Tools, выбрать Surface Area Configuration for Services and Connections и настроить свойство Remote Connection в группе Database Engine.

Чтобы получить возможность работать с базами данных, назначать права пользователей и проводить отладочную и административную работу, пона-



Интерфейс SQL Server Management Studio Express

добится утилита SQL Server Management Studio Express, которую совершенно бесплатно можно скачать с сайта Microsoft. Она предоставляет собой интерфейс привычного проводника и полную среду разработки баз данных, начиная с разработки схемы базы данных и заканчивая отладкой хранимых процедур. Кроме того, организован доступ к стандартным процедурам и функциям SQL Server, где можно просмотреть подробную спецификацию по каждой.

На сайте Microsoft можно еще скачать Microsoft SQL Server 2005 Express Edition with Advanced Services. Эта утилита уже включает в себя средства интегрированной разработки баз данных и средства полнотекстового поиска, которые позволяют составлять запросы простым текстом в виде предложений. Также эта утилита обладает встроенной службой Reporting Services, которая позволяет разрабатывать отчеты и использовать web-ресурсы. Для этого необходимо иметь установленным и настроенным IIS 5.0 или выше, который есть на установочном диске системы. Если перед этим ты уже установил SQL Server 2005 Express Edition, то для установки утилиты необходимо его удалить, либо удалить все данные из папки Template Data, которая по умолчанию находится в C:\Program Files\Microsoft SQL Server\MSSQL.#\MSSQL\Template Data. И настоятельно рекомендую скопировать всю информацию, прежде чем удалять...

Другая утилита — Microsoft SQL Server 2005 Express Edition Toolkit — расширяет возможности предыдущей. Содержит Business Intelligence Development Studio, с помощью которого можно быстро и просто создавать и редактировать отчеты для SQL Server 2005 Reporting Services. Работа с Development Studio напоминает, если не повторяет, работу на Visual Studio с соответствующими проектами.

И последнее — SQL Server 2005 Books Online. Полноценная помощь с примерами установки, настройки и языка Transact-SQL Microsoft SQL Server 2005. Занимает порядка 125 Мб.

НОВЫЕ ВОЗМОЖНОСТИ

Основной секрет эффективного использования программного продукта — досконального знание его возможностей. Что же нового предлагает SQL Server 2005? Для начала стоит упомянуть службу Service Broker, которая позволяет хранить очереди сообщений внутри базы данных SQL Server, и таким образом достигается новый уровень интеграции с базами данных.

❶ Новые выражения Transact-SQL позволяют разрабатывать приложения, которые способны обмениваться сообщениями. Каждое сообщение — это часть диалога, независимого коммуникационного канала между двумя приемниками. Теперь работать с SQL Server можно с помощью областей — назначение прав можно проводить областями или по схемам базы данных. Возможно онлайн-восстановление базы данных: база данных остается доступной для работы, в то время как ее часть восстанавливается. Удаление и создание новых индексов также доступны в режиме онлайн.

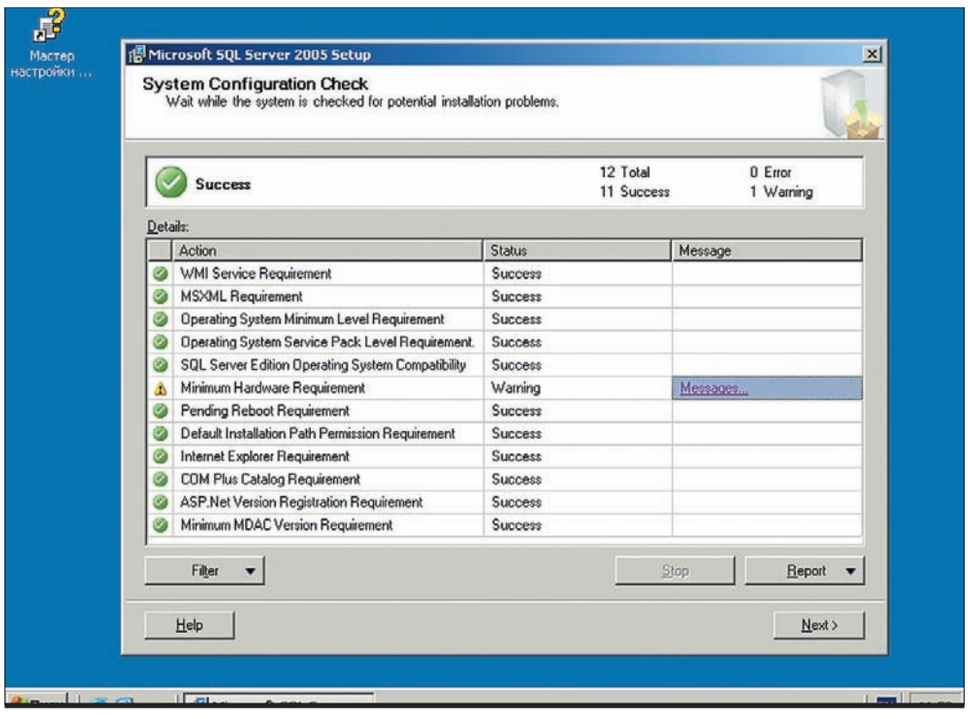
❷ Что касается самого движка базы данных, то, во-первых, следует отметить поддержку технологии .NET или так называемую CLR-интеграцию. Теперь объекты базы данных (триггеры, хранимые процедуры, типы), определяемые пользователем, могут быть написаны на одном из языков .NET Framework, например на C#. Одним из главных преимуществ управляемого кода является безопасность типов. До того, как управляемый код будет выполнен, CLR выполняет несколько проверок, известных как верификация, чтобы гарантировать безопасность выполняемого кода. Использование CLR в базе данных существенно расширяет возможности, так как программист может создать свой собственный объект, обладающий определенным поведением, и определить поля с типом этого объекта. Таким образом, поведение и данные будут инкапсулированы, и для доступа к ним будет необходимо использование программных методов.

❸ Кроме стандартных механизмов доступа к базе данных (ODBC, OLE DB) есть еще и .NET Framework Data Provider для SQL Server, называемый sqlClient'ом, который оптимизирован для доступа из программ, написанных на .NET ориентированных языках именно к SQL Server 2005.

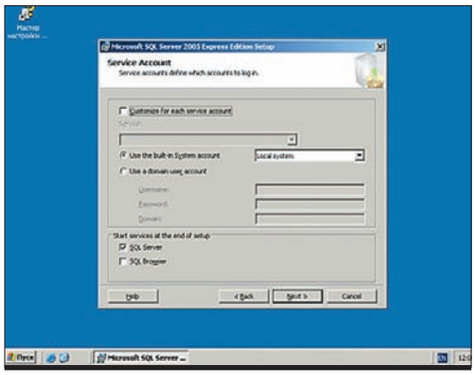
❹ Для поддержки распределенных запросов в Transact-SQL используются новые типы данных и добавлены новые события SQL Trace для улучшения отладки. Кроме того, Transact-SQL теперь позволяет разрабатывать рекурсивные запросы.

❺ Управление ядром базы данных теперь снабжено автоматическим распределением памяти и автоматическим распределением нагрузки средств ввода/вывода и процессора.

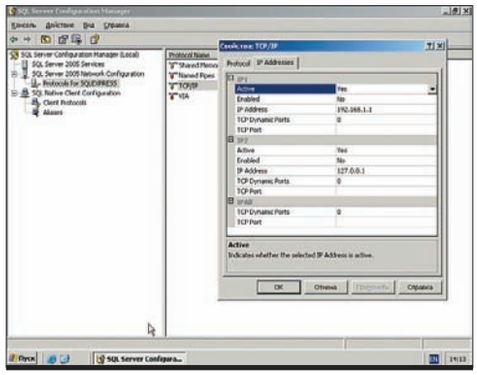
❻ Ядро поддерживает XML-типы данных для хранения XML-документов, столбцов таблиц или переменных Transact-SQL. Также есть поддержка XQuery и XML Schema definition language (XSD). В SQL Server 2005 XML-данные хранятся в виде больших двоичных объектов, которые можно анализировать и частично сжимать. SQL Server 2005 позволяет выполнять запросы к частям XML-документа, проверять документ на соответствие XML-схеме и изменять содержимое XML-документа. Также происходит объединение традиционных



Процесс установки Microsoft SQL Server 2005



Кто будет пользоваться службой



SQL Server Configuration Manager позволяет производить тонкую настройку служб, сети и портов

реляционных данных и частично структурированных и неструктурированных XML-документов. Поддержка XQuery позволяет строить запросы ко всем типам XML-данных.

❼ Улучшения коснулись и Data Mining, которая используется в Analisys Services взамен стандартного подхода к OLAP-технологиям.

❽ Многомерные базы данных (MD) позволяют производить уникальный анализ данных в онлайн режиме. Появились такие возможности, как правило ассоциации, временные ряды, регрессионные деревья, кластеризация последовательностей, нейронные сети. Кубы данных также получили новые возможности, такие как инфраструктура ключевых индикаторов производительности (KPI), сценарии MDX и т.д.

❾ Набор кубов и измерений, определенный в Analysis Services 2005, называется единообразной пространственной моделью (UDM). UDM является центральным хранилищем метаданных, определяющим бизнес сущности, бизнес-логику, вычисления и метрики, служащие источником для всех отчетов, электронных таблиц, программ просмотра OLAP, KPI и аналитических приложений.

❿ Находкой для программера будут Analysis Management Objects (AMO) — объекты управления Analysys Services. Связь с этими объектами заменит написание сценариев DDL и сценариев на ASSL.

⓫ Для обеспечения доступа клиента к базам данных Microsoft SQL Server 2005 теперь предусмотрена технология SQL Native Client, которая комбинирует SQL OLE DB провайдера с SQL ODBC-драйвером, а также их сетевые функции в одной библиотеке DLL. Эта технология позволяет разрабатывать приложения, использующие такие возможности SQL Server 2005, как множественные активные наборы данных (MARS), типы данных, определенные пользователем (UDT), и поддержка XML-типов данных.

⓬ Для web-доступа организован доступ Simple Object Access Protocol (SOAP) через HTTP. При этом ядро получает пакеты напрямую, без организации вспомогательных сервисов или IIS.

⓭ С помощью ADO.NET реализованы такие возможности, как уведомление о запросах и MARS. Уведомление о запросах — это уведомление о том, что одна и та же команда к SQL Server 2005 дала разные результаты. И сама команда, и отличия, на которые необходимо создавать уведомление, — программируемые. MARS — новая концепция, которая позволяет иметь более одного открытого результирующего набора данных на одно подключение. Множественные активные результирующие наборы устраняют существующее на данный момент ограничение, когда открытый результирующий набор по умолчанию блокирует драйвер от отправки запросов на сервер до тех пор, пока не употреблен весь результирующий набор.

⓮ Reporting Services предлагают возможности создания OLAP-отчетов и глубоко связаны с Microsoft Office System, что позволяет открывать эти отчеты в привычном Word и Excel.

⓯ Предоставлено огромное количество средств для настройки производительности базы данных: настройка использования памяти, настройка блокировок и даже настройка сетевого и дискового ввода/вывода. Для обеспечения достаточного уровня прозрачности и видимости состояния базы данных и обеспечения упреждающего мониторинга используется Dynamic Management Views.

⓰ Управлять базой данных SQL Server можно программно. Для этого существуют SQL Management Objects (SMO) — объекты управления SQL, на которых и построена Management Studio. С помощью этих объектов можно программно получать конфигурацию настроек, выполнять сценарии Transact-SQL, резервное копирование и т.д. Теперь душе программиста есть куда развернуться, и можно не быть привязанным к набору стандартных утилит, хотя они и предлагают исчерпывающий набор средств управления. Модель SMO является заменой уже устаревшей модели распределенных объектов управления (DMO). Хотя DMO и можно использовать, но дальше развиваться эта ветвь не будет.

⓱ Существует возможность зеркалирования базы данных — когда содержимое журнала транзакций основного сервера передается также и на другой, и, в случае сбоя основного сервера, все транзакции сразу же перенаправляются на другой сервер. Благодаря этому достигается высокая отказоустойчивость. Следует также упомянуть кластеры с восстановлением после отказа, количество которых в SQL Server 2005 увеличено до 8.

⓲ Очень полезное решение для восстановления баз данных — моментальный снимок базы данных. При этом нет необходимости создавать полную копию базы данных. Логика работы такова, что если основная база расходится со снимком, то она изменяется до соответствия ему, и, таким образом, можно восстанавливать базу данных после случайных изменений. Новая технология быстрого восстановления позволяет пользователям подключиться к базе данных, которая еще находится в стадии восстановления, без отката незавершенных транзакций. При оперативном восстановлении связь с базой данных не обрывается. Заблокированной становится только та часть, которая подлежит восстановлению.

⓳ Для решения проблем на сервере SQL Server 2005 предоставляет выделенное административное соединение, которое может быть доступно через утилиту командной строки SQLCMD локально или с удаленной машины. С помощью нее можно выполнять диагностические функции и операторы Transact-SQL.

⓴ Для управления большими базами данных предусмотрено секционирование таблиц и индексов, а новым в этой идее является то, что теперь секционирование таблиц возможно по файловым группам. Но такая возможность реально пригодится только при размерах базы от сотен гиг до терабайта.

㉑ Приемницей довольно популярной функции Data Transformation Services (DTS) в SQL Server 2005 является SQL Server Integration Services (SSIS), которая позволяет во много раз проще объединять и анализировать данные из нескольких разнородных источников информации, и является полностью программируемой платформой.

→ **немалый арсенал возможностей.** Возможно, многое из описанного просто не потребуется использовать, но всегда лучше иметь арсенал в запасе, чем в последний момент изобретать невесть что. А ведь так иногда и получается — из-за неверных решений, принятых в начале создания автоматизированной системы или хранилища данных, приходится потом так изворачиваться и строить подпорки, что это уже никак не оправдывает упрощенные подходы. Кроме того, давай смотреть правде в глаза: пользователи работают в основном на Windows-системах, а программисты смогут заработать на жизнь, имея стабильный контингент заказчиков, и ориентироваться нужно на среднего, а не на продвинутого пользователя. Поэтому как бы это ни было скучно, а писать приходится для них — пользователей. А грамотное использование любых программных средств чьей угодно разработки всегда дает хороший результат **C**

перстолонаследование

О РАЗМНОЖЕНИИ WINDOWS

MICROSOFT WINDOWS ЗАНИМАЕТ ЦЕЛЫХ 99% ЭКОЛОГИЧЕСКОЙ НИШИ НАСТОЛЬНЫХ ОПЕРАЦИОННЫХ СИСТЕМ В РОССИИ. ТАКИЕ ГРАНДИОЗНЫЕ УСПЕХИ БЫЛИ БЫ НЕВОЗМОЖНЫ, ЕСЛИ БЫ WINDOWS НЕ БЫЛ СПОСОБЕН К БЫСТРОМУ, ЭФФЕКТИВНОМУ И МАССОВОМУ РАЗМНОЖЕНИЮ. ОБ ЭТО ДЕЛИКАТНОМ ПРОЦЕССЕ И ПОГОВОРИМ

РОМАН ЛУКОВНИКОВ, ЗАРАЗА
{lrb@sandy.ru, 3apa3a@security.nnov.ru}

→ **1. семенное размножение** — выращивание нового экземпляра Windows из семени. Дистрибутива то есть. С этим процессом знакомы многие. Но что делать, если надо вырастить не один Windows и не два, а, например, несколько десятков. Причем ставить придется не только Windows, но еще и десяток программ, необходимых в производстве. Чтобы не свихнуться от монотонного процесса осеменения, придется применять методы автоматизации...

→ **1.1. расширение дистрибутива Windows.** Основное отличие дистрибутива Windows от яйца состоит в том, что управлять характеристиками того, что вылупится из яйца, практически невозможно. Сделать же свой дистрибутив Windows, в котором будет все, что необходимо для жизни, вполне реально.

→ **1.1.1. интеграция сервис-пака и хотфиксов.** Итак, у нас имеется некий дистрибутив Windows, но Microsoft успел выпустить новый сервис-пак и кучу хотфисов. Устанавливать их каждый раз после окончания процедуры инсталляции Windows очень не хочется. Что делать? Можно интегриро-

вать сервис-пак в имеющийся дистрибутив Windows. Для этого необходимо:

1. СКОПИРОВАТЬ ДИСТРИБУТИВ НА ЖЕСТКИЙ ДИСК, НАПРИМЕР В ПАПКУ C:\WINDIST;
2. ЕСЛИ СЕРВИС-ПАК ВЫКАЧАН ИЗ СЕТИ, А НЕ ПОЛУЧЕН НА КОМПАКТ-ДИСКЕ В РАСПАКОВАННОМ ВИДЕ, ТО НЕОБХОДИМО РАСПАКОВАТЬ СЕРВИС-ПАК. ДЛЯ ЭТОГО ЕГО СЛЕДУЕТ ЗАПУСТИТЬ С КЛЮЧИКОМ /X И УКАЗАТЬ ПУТЬ ДЛЯ РАСПАКОВКИ;
3. ЗАПУСТИТЬ UPDATE.EXE ИЗ КАТАЛОГА UPDATE СЕРВИС-ПАКА С КЛЮЧИКОМ /INTEGRATE (НАПРИМЕР, WINDOWSXP-KB######-X86-LLL.EXE /INTEGRATE:C:\WINDIST).

Пункты 2 и 3 необходимо выполнить для сервис-пака и каждого обновления.

Дистрибутив готов к использованию, но находится на жестком диске. Если мы просто запишем его на компакт-диск, то CD не будет загрузочным. Поэтому необходимо извлечь загрузочный сектор оригинального компакт-диска Windows с помощью утилиты ISO Buster или UltraISO. Либо подготовить загрузочный ISO-образ с помощью того же UltraISO или используя встроенные возможности Nero (во вкладочке Boot при создании проекта необходимо выставить число секторов не менее 4).

➔ **1.1.2. интеграция драйверов и программ через OEM-директории.** OEM-директории используются для расширения дистрибутива Windows, особенно при автоматической установке. Файлы, содержащиеся в них, в процессе установки автоматически копируются в загрузочный раздел диска или в служебные папки Windows. Это могут быть файлы дистрибутива программного продукта или драйвера к соответствующему железу. А необходимость присутствия файлов непосредственно на диске (а не на CD или сетевом ресурсе) есть, так как, к примеру, создать универсальный командный файл, который бы запускал программу установки программного обеспечения с CD, проблематично. В частности, на разных машинах может быть разная буква привода CD, либо может не быть системной переменной, указывающей на нее. А в процессе установки системы поиск необходимых драйверов может осуществляться только с локального диска.

Все, что будет находиться в директории $1, в процессе установки будет скопировано на загрузочный раздел (раздел, на котором находятся системные файлы ОС). Все, что расположено в папке $$, будет скопировано в директорию Windows (c:\winnt или c:\windows в зависимости от ОС и буквы загрузочного раздела).
$1 — корневой каталог загрузочного раздела;
$$ — директория Windows;
$Docs — Document and Settings
(присутствует в ОС выше Windows 2000);
$Progs — Program Files
(присутствует в ОС выше Windows 2000).
Буква диска — корневой каталог диска, буква которого указана (OEM\D\Distrib приведет к созданию папки D:\Distrib, если буква D назначена разделу, на котором возможна запись).

В корне OEM можно создать файл cmdline.txt, в котором указать команды, необходимые для выполнения. Команды будут выполнены на конечной стадии установки системы под системной учетной записью. Файл cmdline.txt должен начинаться со строки COMMANDS, далее в двойных кавычках идут команды, которые необходимо выполнить. Если исполняемый файл находится либо в корне каталога %OEM%, либо в каталоге, путь к которому указан в переменной PATH, то в cmdline.txt путь не пишется. А если нужно запустить файл OEM\Tools\Install.cmd, в файле прописывается путь «.\Tools\Install.cmd», где .\ означает текущий каталог.

пример файла cmdline.txt:

```
[COMMANDS]
"regedit /s formysoft.reg"
".\Tools\Install.cmd"
```

При использовании OEM-директорий с файлом ответов необходимо убедиться, что в секции [Unattended] параметр OemPreinstall имеет значение Yes. Если в папку OEM ты добавляешь драйвера и хочешь, чтобы процедура установки искала их в указанном месте, то в секции [Unattended] параметр OemPnpDriversPath должен указывать путь к ним.

если в папке OEM\1\Drivers\ у тебя есть папки NIC, VIDEO, AUDIO, CHIPSET:

```
[Unattended]
OemPreinstall = yes
OemPnpDriversPath = "Drivers\NIC;
Drivers\CHIPSET;Drivers\VIDEO;
Drivers\AUDIO"
```

Путь нужно указывать к папкам, в которых находятся inf-файлы, учитывая при этом, что в подпапках поиск не производится.

➔ **1.1.3. использование утилиты sysdiff.** Что делать, если необходимо установить программное обеспечение, которое не поддерживает автоматическую установку? Можно, например, воспользоваться утилитой sysdiff, входящей в комплект Windows Resource Kit. Она позволяет выделить изменения, происшедшие в системе, начиная с некоторой контрольной точки, сохранить их в файл, а потом применить в системе другого компьютера. Использовать sysdiff можно по алгоритму следующим образом:

1. СНАЧАЛА ДЕЛАЕТСЯ СНИМОК «ГОЛОЙ» СИСТЕМЫ С ПОМОЩЬЮ КОМАНДЫ SYSDIFF /SNAP SOMENAME.IMG, ПРИ ЭТОМ СОЗДАЕТСЯ ФАЙЛ SOMENAME.IMG, В КОТОРОМ СОДЕРЖАТСЯ СВЕДЕНИЯ О СОСТОЯНИИ СИСТЕМЫ (РЕЕСТРА И ФАЙЛОВ);
2. УСТАНАВЛИВАЕТСЯ НЕОБХОДИМОЕ ПО;
3. НАХОДЯТСЯ ИЗМЕНЕНИЯ, ПРОИСШЕДШИЕ В ХОДЕ УСТАНОВКИ ПО. ДЛЯ ЭТОГО ИСПОЛЬЗУЕТСЯ КЛЮЧИК /DIFF (SYSDIFF /DIFF SOMENAME.IMG INSTALL.DIF), ТЕПЕРЬ В ФАЙЛЕ INSTALL.DIF ЗАПИСАНЫ ТЕ ДЕЙСТВИЯ, КОТОРЫЕ ВЫПОЛНИЛ ИНСТАЛЛЯТОР ПРОГРАММЫ;
4. ВМЕСТО УСТАНОВКИ ПРОГРАММЫ МОЖНО ЗАПУСТИТЬ SYSDIFF /APPLY INSTALL.DIF, ЧТОБЫ ВОССОЗДАТЬ ФАЙЛЫ И КЛЮЧИ РЕЕСТРА, СОЗДАННЫЕ В ПРОЦЕССЕ УСТАНОВКИ ПРОГРАММЫ;
5. МОЖНО ИСПОЛЬЗОВАТЬ SYSDIFF /INF INSTALL.DIF (ПУТЬ К ПАПКЕ OEM) ДЛЯ СОЗДАНИЯ ВКЛЮЧЕНИЯ ИЗМЕНЕНИЙ, ОТЛОВЛЕННЫХ SYSDIFF, В ДИСТРИБУТИВ.

Microsoft не рекомендует использовать sysdiff под Windows XP, хотя в большинстве случаев проблем не возникает. Как альтернативу, Microsoft предлагает WinInstall LE от OnDemand Software (**www.ondemandsoftware.com**). Утилиту можно так же найти в папке Valueadd дистрибутива Microsoft Windows 2000 Server.

➔ **1.2. установка по сети.** Для установки Windows не обязательно загружаться с компакт-диска, можно подключиться к дистрибутиву Windows по сети. Для этого потребуется: дистрибутив, доступный по сети (его можно создать через тот же setupmgr.exe), загрузочная дискета с сетевым клиентом Microsoft и, для облегчения жизни, файл ответов. К сожалению, начиная с Windows 2000, Microsoft не заботится о том, чтобы предоставить возможность создания диска сетевой загрузки. Есть следующие варианты:

1. ИСПОЛЬЗОВАТЬ ФАЙЛЫ ИЗ ДИСТРИБУТИВА WINDOWS NT 4.0

важно

ПРИ СОЗДАНИИ СТРУКТУРЫ OEM-ПАПОК ДЛЯ УСТАНОВКИ ОС С CD ДИРЕКТОРИЯ OEM ДОЛЖНА БЫТЬ НА ОДНОМ УРОВНЕ С ДИРЕКТОРИЕЙ I386, А ПРИ СОЗДАНИИ АНАЛОГИЧНОЙ СТРУКТУРЫ ДЛЯ УСТАНОВКИ ПО СЕТИ ИЛИ С ЖЕСТКОГО ДИСКА ПАПКА OEM ДОЛЖНА БЫТЬ ВЛОЖЕНА В I386.

SERVER (ИЗ ПАПКИ I386 ВЗЯТЬ ФАЙЛЫ NCADMIN.CN_, NCADMIN.EX_, NCADMIN.HL_), ВЫПОЛНИТЬ ДЛЯ НИХ КОМАНДУ EXPAND И ЗАПУСТИТЬ NCADMIN.EXE.

ВОСПОЛЬЗОВАТЬСЯ АДРЕСОМ WWW.NU2.NU/BOOTDISK/NETWORK/.

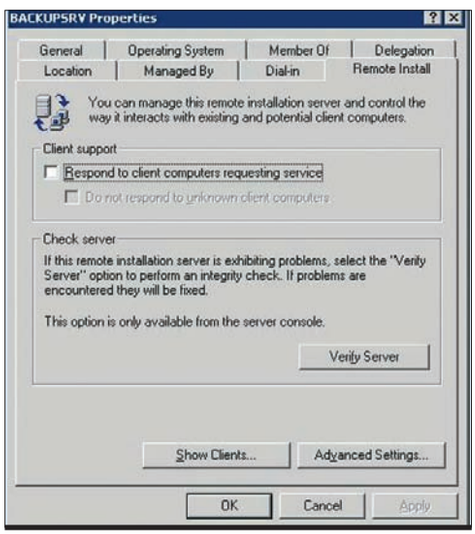
[3] ИСПОЛЬЗОВАТЬ NORTON GHOST 2003 (NORTON GHOST BOOT WIZARD).

.bat-файл для автоматического запуска процесса установки можно так же подготовить с помощью setupmgr.exe. Для сетевой установки запускается winnt.exe из папки I386 дистрибутива. Не забудь проверить наличие раздела FAT. Для оптимальной конвертации раздела в NTFS рекомендуется использовать утилиты oformat.com и cvtarea.exe из deploy.cab, которые так же можно включить в bat-файл автоматической установки.

→ **1.3. сервер удаленной установки RIS** (Remote Installation Server) — продукт компании Microsoft, предназначенный для автоматической установки операционных систем по сети. Он входит в состав серверных ОС, начиная с Windows 2000 Server. RIS можно использовать для разведения Windows в поистине фермерских масштабах, так как вся установка происходит по сети и от клиентского компьютера практически не требуется каких-либо действий. Причем установка производится прямо на «голое» железо.

Как это происходит? Используется протокол сетевой загрузки (BOOTP). Загрузка системы по сети поддерживается любым сетевым адаптером с встроенным BIOS — Pre-Boot Execution Environment (PXE). Сейчас практически все адаптеры поддерживают загрузку по сети.

Если сетевой адаптер все-таки не поддерживает загрузку по сети, то в комплект RIS входит утилита rbfg.exe (Remote Boot Floppy Generator), которая создает загрузочную дискетку с возможностью удаленной загрузки системы. RBFG поддерживает большую часть сетевых адаптеров: 3COM, Intel, SMC, AMD, Compaq, Dec, Realtek и т.д. Когда «голый» компьютер, готовый принять в себя Windows, инициализирует загрузку через сеть (как и любая загрузка, она происходит сразу после окончания инициализации BIOS), PXE сначала запрашивает сетевые параметры (IP-адрес, маску, адреса DNS) по DHCP, затем через DNS находит сервер RIS, который и «заливает» по сети установщик Windows, после чего идет обычный процесс установки системы.



Включение протокола BOOTP на сервере

При помощи RIS, входящего в состав Windows 2003 Server, можно устанавливать практически любые версии Windows 2000, XP и 2003.

Аналогичная служба из состава Windows 2000 Server не поддерживает установку серверных платформ и позволяет разворачивать ОС только одной языковой версии (той, что установлена на сервере RIS). К тому же, установка Windows XP с помощью RIS 2000 проходит сложнее и требует дополнительных настроек (Microsoft рекомендует разворачивать эту ОС с помощью RIS 2003).

→ **для успешной работы RIS** должны выполняться следующие требования:

требования к сети:

— НАЛИЧИЕ ACTIVE DIRECTORY (СОДЕРЖИТ УЧЕТНЫЕ ЗАПИСИ КЛИЕНТСКИХ КОМПЬЮТЕРОВ И RIS-СЕРВЕРА ВМЕСТЕ СО ВСЕМИ НАСТРОЙКАМИ);

— НАЛИЧИЕ DNS (ПОЗВОЛЯЕТ КЛИЕНТАМ НАЙТИ НЕОБХОДИМЫЕ СЛУЖБЫ В AD);

— НАЛИЧИЕ DHCP (ВЫДАЕТ АДРЕСА КЛИЕНТСКИМ МАШИНАМ).

требования к серверу:

— ПОД ФАЙЛЫ ОБРАЗОВ ДОЛЖЕН БЫТЬ ВЫДЕЛЕН ОТДЕЛЬНЫЙ РАЗДЕЛ (НЕ СИСТЕМНЫЙ И НЕ ЗАГРУЗОЧНЫЙ) С ФАЙЛОВОЙ СИСТЕМОЙ NTFS;

— НА ЭТОМ РАЗДЕЛЕ ДОЛЖНО БЫТЬ НЕ МЕНЕЕ 2 ГБ СВОБОДНОГО ПРОСТРАНСТВА.

требования к клиентам:

— ДОЛЖНЫ УДОВЛЕТВОРЯТЬ МИНИМАЛЬНЫМ ТРЕБОВАНИЯМ ПО АППАРАТНОМУ ОБЕСПЕЧЕНИЮ УСТАНАВЛИВАЕМОЙ ОПЕРАЦИОННОЙ СИСТЕМЫ;

— ДОЛЖНЫ ИМЕТЬ ДИСК ОБЪЕМОМ РАВНЫМ ИЛИ БОЛЬШИМ, ЧЕМ КОПИРУЕМЫЙ РАЗДЕЛ ШАБЛОННОЙ МАШИНЫ, И ДОЛЖНЫ ИМЕТЬ ТАКОЙ ЖЕ HAL (HARDWARE ABSTRACTION LAYER) (ДЛЯ КЛИЕНТОВ, НА КОТОРЫХ УСТАНАВЛИВАЕТСЯ RIPREP ОБРАЗ);

— ДОЛЖНЫ ПОДДЕРЖИВАТЬ PRE-BOOT EXECUTION ENVIRONMENT (PXE) — ТЕХНОЛОГИЮ УДАЛЕННОЙ ЗАГРУЗКИ, КОТОРАЯ ПОЗВОЛЯЕТ КЛИЕНТСКИМ КОМПЬЮТЕРАМ ПОЛУЧАТЬ ЗАГРУЗОЧНЫЙ КОД ЧЕРЕЗ СЕТЕВОЙ АДАПТЕР.

→ **образы бывают двух видов.** Одни предназначены для чистой установки и представляют собой файлы дистрибутива определенной ОС (CD-Based-образ). Другие являются копией раздела (который должен быть и системным, и загрузочным) рабочей станции, которую необходимо клонировать (RIPrep-образ). Процесс создания CD-Based-образа запускается на сервере RIS, а создание RIPRep образа — на клиентской машине, причем на сервере необходим CD-Based-образ той операционной системы, RIPRep-образ которой создается. При установке RIS создается один CD-Based-образ. После установки можно добавить тот или иной тип образов.

процедура установки RIS-сервера:

[1] УСТАНАВЛИВАЕШЬ КОМПОНЕНТ REMOTE INSTALLATION SERVICES ЧЕРЕЗ ВЫБОР КОМПОНЕНТА СИСТЕМЫ.

[2] ЗАПУСКАЕШЬ REMOTE INSTALLATION SERVICES SETUP ИЗ МЕНЮ ADMINISTRATIVE TOOLS.

[3] ОТВЕЧАЕШЬ НА ВОПРОСЫ МАСТЕРА, УКАЗЫВАЯ:

— РАЗДЕЛ ДЛЯ СОЗДАВАЕМЫХ ОБРАЗОВ (ПУСТОЙ NTFS-РАЗДЕЛ НЕОБХОДИМО ПОДГОТОВИТЬ ЗАРАНЕЕ);

— ОТВЕЧАТЬ ЛИ НА КЛИЕНТСКИЕ ЗАПРОСЫ СРАЗУ ПОСЛЕ УСТАНОВКИ ИЛИ НЕТ (ДО ПОЛНОЙ НАСТРОЙКИ RIS РЕКОМЕНДУЕТСЯ ЭТОГО НЕ ДЕЛАТЬ);

— ПУТЬ К УСТАНОВОЧНЫМ ФАЙЛАМ ОПЕРАЦИОННОЙ СИСТЕМЫ, ОБРАЗ КОТОРОЙ ХОЧЕШЬ СОЗДАТЬ НА СЕРВЕРЕ (НЕОБХОДИМО УКАЗАТЬ ПУТЬ К ПАПКЕ I386);

— НАЗВАНИЕ ПАПКИ, В КОТОРУЮ БУДУТ ЗАПИСАНЫ УСТАНОВОЧНЫЕ ФАЙЛЫ ДЛЯ ДАННОГО CD-BASED ОБРАЗА;

— ОПИСАНИЕ ОБРАЗА ОС И ТЕКСТ ПОДСКАЗКИ, КОТОРЫЙ БУДЕТ ВИДЕН КЛИЕНТАМ PXE.

Мастер выполняет необходимые действия и завершает процесс установки.

После этого из оснастки Active Directory Users and Computers можно произвести дальнейшую настройку RIS:

[1] НАСТРОИТЬ ИМЕНА, КОТОРЫЕ БУДУТ ДАВАТЬСЯ КЛИЕНТСКИМ МАШИНАМ, И УКАЗАТЬ, В КАКОЙ КОНТЕЙНЕР ACTIVE DIRECTORY БУДУТ ДОБАВЛЯТЬСЯ ИХ УЧЕТНЫЕ ЗАПИСИ:

- ОТКРЫТЬ ОСНАСТКУ ACTIVE DIRECTORY USERS AND COMPUTERS И ВЫБРАТЬ ЗАКЛАДКУ REMOTE INSTALL В ОКНЕ СВОЙСТВ УЧЕТНОЙ ЗАПИСИ КОМПЬЮТЕРА, НА КОТОРОМ УСТАНОВЛЕНА СЛУЖБА RIS;
- НА ЗАКЛАДКЕ REMOTE INSTALL ВЫБРАТЬ ADVANCED SETTINGS, ДАЛЕЕ ЗАКЛАДКА NEW CLIENTS;
- ДАЛЕЕ МОЖНО ВЫБРАТЬ СПОСОБ ИМЕНОВАНИЯ КОМПЬЮТЕРОВ И УКАЗАТЬ РАЗМЕЩЕНИЕ УЧЕТНЫХ ЗАПИСЕЙ, ДОБАВЛЯЕМЫХ В ДОМЕН КОМПЬЮТЕРОВ.

[2] СОЗДАТЬ ДОПОЛНИТЕЛЬНЫЕ CD-BASED-ОБРАЗЫ И СВЯЗАТЬ НОВЫЕ ФАЙЛЫ ОТВЕТОВ С СУЩЕСТВУЮЩИМИ ОБРАЗАМИ:

- ВЫБРАТЬ ЗАКЛАДКУ IMAGES И КНОПКОЙ ADD ЗАПУСТИТЬ МАСТЕР;
- ВЫБРАТЬ МЕЖДУ СВЯЗЫВАНИЕМ НОВОГО ФАЙЛА ОТВЕТОВ С СУЩЕСТВУЮЩИМ ОБРАЗОМ И ДОБАВЛЕНИЕМ НОВОГО CD-BASED-ОБРАЗА.

При создании любого образа создается файл ответов, в котором находятся параметры, необходимые для установки. Можно либо создать свой файл ответов (с помощью утилиты setupmgr.exe, которую можно извлечь из архива deploy.cab, расположенного на установочном диске) и связать его с соответствующим образом, либо изменить существующий файл (например, добавить в секцию [UserData] строку ProductID = "" с лицензионным ключом), который располагается в соответствующей образу папке в каталоге Templates с расширением sif. Подробную информацию о структуре и параметрах файла ответов можно посмотреть в файле unattend.doc, который находится в архиве \SUPPORT\TOOLS\DEPLOY.CAB на установочных дисках ОС семейства Windows 2000.

Теперь осталось настроить на клиентском компьютере либо загрузку через сеть (если это PXE-enabled компьютер), либо загрузку с флоппи (если PXE эмулируется загрузочной дискеткой), авторизоваться с помощью доменной учетной записи и выбрать из списка доступных необходимый образ.

Не спеши радоваться, если компьютер удачно прошел этап получения IP-адреса, обнаружения сервера RIS, закачки программы авторизации в домене и выбора необходимого дистрибутива. Уже после того, как все это прошло, на первом этапе установки Windows (при начале копирования файлов образа) может появиться сообщение типа: «Выбранный образ операционной системы не содержит необходимых драйверов для имеющегося адаптера сети. Попробуйте выбрать другой образ операционной системы. Если это не поможет, обратитесь к системному администратору. Продолжение установки невозможно. Для выхода нажмите любую клавишу».

Можно попробовать решить проблему, скопировав в папку i386 файлы *.inf и *.sys сетевой карты. Если это не поможет, создать в i386 папку OEM\$1\Drivers\Nic, записать туда файлы драйвера сетевой карты и в файл ответов добавить строчки:

```
[Unattended]
OemPreinstall = yes
OemPnpDriversPath = Drivers\NIC
DriverSigningPolicy=Ignore
```

К сожалению, и это может не помочь. Поэтому, если у тебя стоит задача распространить ОС на десятки новых машин, которые еще не закуплены, договорись с поставщиком и возьми на тестирование одну машину, чтобы убедиться, что установка через RIS проходит без проблем от начала до конца. Только это может дать полную гарантию, что RIS дружит с подобным железом.

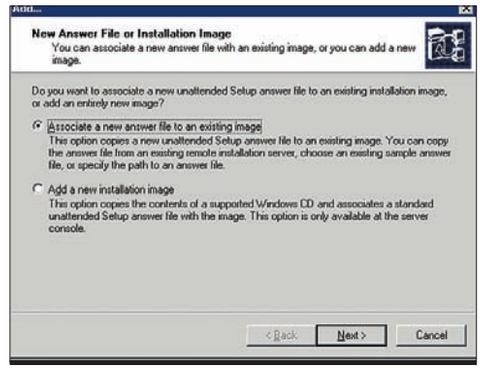
По умолчанию любой пользователь может добавить в домен 10 компьютеров. Как увеличить это число, смотри в статье «Default Limit to Number of Workstations a User Can Join to the Domain» на сайте Microsoft.

Ограничить пользователя в установке определенных образов можно NTFS-разрешениями:

- НА ЗАКЛАДКЕ IMAGES ВЫБЕРИ НУЖНЫЙ ОБРАЗ, ДАЛЕЕ PROPERTIES;
- ДАЛЕЕ PERMISSIONS...;
- НА ЗАКЛАДКЕ SECURITY ЛИБО РАЗРЕШАЕШЬ (ЧТО ПРАВИЛЬНЕЕ), ЛИБО ЗАПРЕЩАЕШЬ ОПРЕДЕЛЕННЫМ ГРУППАМ ЧТЕНИЕ И ВЫПОЛНЕНИЕ.

Если ты выбрал для установки CD-Based-образ, то файлы дистрибутива сначала копируются на клиентскую машину, а затем начнется обычный процесс установки Windows со всеми этапами, с той лишь разницей, что параметры, запрашиваемые во время установки, берутся из файла ответов, расположенном на сервере RIS. Если какие-то параметры там не указаны или указаны некорректно, то мастер будет запрашивать их у пользователя.

Если устанавливается RIPrep-образ, то после копирования файлов образа на клиентскую машину и рестарта запускается программа мини-установки, во время которой запрашивается уникальная информация, которая опять же берется из файла ответов с сервера RIS.



Добавление файла ответов к образу

➔ **1.4. автоматизация процесса установки — файл ответов.** В некоторых случаях для автоматизации процесса установки используются файлы ответов, которые содержат информацию, обычно запрашиваемую у пользователя с экрана. Файл ответов может применяться для автоматизации процесса установки с компакт-диска или по сети.

Фактически, это текстовый файл, который можно создать в примитивном текстовом редакторе или с помощью утилиты setupmgr.exe, которую можно извлечь из архива SUPPORT\TOOLS\DEPLOY.CAB, расположенного на диске с дистрибутивом Windows.

Кроме файла ответов обычно создается база данных уникальных параметров (UDF) — текстовый файл, в котором хранятся индивидуальные настройки для каждого компьютера (имя компьютера, IP-адрес и так далее).

Подробную информацию о структуре и параметрах файла ответов и UDF можно посмотреть в файле unattend.doc, который находится в архиве \SUPPORT\TOOLS\DEPLOY.CAB на установочных дисках ОС семейства Windows 2000 или в файле помощи ref.chm, расположенном в том же архиве в дистрибутиве Windows XP. При установке в параметрах winnt.exe или winnt32.exe можно указать путь к файлу автоматической установки, путь к файлу UDF и идентификатор компьютера, который будет использован для поиска уникальных параметров в UDF-файле.

Теперь установка Windows, драйверов и приложений сводится к загрузке с компакт-диска или дискеты.

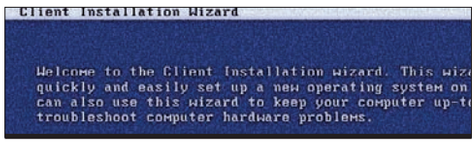
➔ **2. размножение почкованием.** А если не хочется устанавливать новую копию Windows из дистрибутива, а хочется клонировать уже имеющуюся копию? Такое тоже возможно.

➔ **2.1. общие принципы — sysprep.** Если ты каким-либо образом изготовишь полный клон системы и попытаешься использовать его в сети, то получишь много нехороших граблей — клонированная система будет иметь то же имя компьютера и тот же уникальный идентификатор учетной записи компьютера в домене. Кроме того, установка клонированной системы на другой компьютер может не пройти из-за различий в оборудовании. Для устранения этих проблем предназначена утилита sysprep.exe из deploy.cab. Она сносит из системы

www.ondemandsoftware.com — альтернатива утилите sysdiff
www.vmware.com — виртуальная машина vmware server

sysperp

SYSPREP НИКАК НЕ МЕНЯЕТ НАСТРОЙКИ ПРОТОКОЛА TCP/IP, И ЕСЛИ ОБРАЗ СДЕЛАН С МАШИНЫ СО СТАТИЧЕСКИМ IP-АДРЕСОМ, КОНФЛИКТОВ IP-АДРЕСОВ В СЕТИ ПОСЛЕ УСТАНОВКИ ОБРАЗОВ НА ДРУГИЕ МАШИНЫ НЕ ИЗБЕЖАТЬ. ПОЭТОМУ ЛУЧШЕ ПЕРЕД КЛОНИРОВАНИЕМ УСТАНОВИТЬ НА МАШИНЕ АВТОМАТИЧЕСКОЕ НАЗНАЧЕНИЕ АДРЕСОВ.



Запуск мастера инсталляции клиента по сети

уникальную информацию и конфигурирует систему таким образом, что при следующей загрузке будет запущена программа генерации новых уникальных параметров и программа мини-установки, которая их донастроит. Как и программой полной установки, программой мини-установки можно управлять через файлы ответов.

Sysprep следует запускать перед любым клонированием системы, чтобы избежать накладок.

➔ **2.2. клонирование с помощью RIS — RIPrep.** RIS поддерживает как CD-образы, так и клонированные (RIPRep) образы. Чтобы создать RIPrep-образы, нужно с компьютера, образ ОС которого создается, запустить файл riprep.exe, расположенный на сервере с RIS, и следовать инструкциям мастера создания образа.

Перед тем, как копировать файлы образа на сервер, на клиентской машине запускается sysprep.

➔ **2.3. ntbackup и набор аварийного восстановления.** В Windows XP и 2003 можно полностью сохранить состояние системы с помощью утилиты ntbackup. Для этого необходимо запустить ntbackup.exe, переключиться в расширенный вид и выбрать Сервис/Мастер аварийного восстановления. Система подготовит архив со слепком системы и служебную дискету (диск аварийного восстановления). Для «восстановления» системы на другом компьютере необходимо запустить процесс установки Windows, но вместо установки выбрать аварийное восстановление и использовать дискету аварийного восстановления.

На Windows 2000 такой фокус не пройдет. Придется сделать полный ntbackup всех файлов и состояния системы, затем установить Windows и только после этого произвести аварийное восстановление.

➔ **2.4. клонирование дисков.** Рассмотрим ситуацию, когда диск, с которого клонируется ОС, и диск, на который она клонируется, подключены к одному компьютеру. Конечно, сама по себе такая ситуация не встретится. Для этого надо самому подключать диск к клонируемой машине, что займет много времени (нужно отключить диск от одной машины и вставить в другую, затем вернуть на место) и, вообще, не всегда возможно (например, если с машин нельзя срывать пломбы, олицетворяющие гарантию). Но предположим, что по тем или иным причинам другие способы невозможны или неудобны (мало машин, не выполняются необходимые условия для установки через RIS или просто не хочется заморачиваться с сетевым вариантом).

Можно, работая в операционной системе, клонировать ее саму (воспользовавшись для этого ее ресурсами) или создать загрузочный диск и запустить стороннюю программу для клонирования.

Как скопировать содержимое системного и загрузочного раздела на другой раздел? Через Windows Explorer не получится. Во-первых, не скопируются файлы, используемые системой (например, пользовательская ветка реестра, находящаяся в файле NTUSER.DAT в профиле пользователя), во-вторых, не перенесутся NTFS разрешения (или кто-то держит систему на FAT-разделе?). Вторую проблему можно решить с помощью утилиты копирования xcopy, в которой с помощью ключа /O сохраняются NTFS-разрешения. Но первую проблему это не решит...

➔ **2.4.2. пишем утилиту клонирования дисков сами.** Не беда. Раз никто не догадался написать утилиту клонирования дисков прямо из-под Windows — сделаем это сами! Конечно, не будем сильно напрягаться. Наша утилита сможет копировать данные только между абсолютно идентичными жесткими дисками. Зато одним из этих дисков может быть диск, на котором установлена копия Windows, в которой мы работаем прямо сейчас. При запуске без параметров утилита выдаст подсказку с примерами использования.

самописная утилита клонирования дисков из-под работающей Windows:

```
#define _CRT_SECURE_NO_DEPRECATE
#define _CRT_SECURE_CPP_OVERLOAD_STANDARD_NAMES 1
#define _CRT_SECURE_CPP_OVERLOAD_SECURE_NAMES 1
#include <stdio.h>
#include <windows.h>
#define NPAGES 4
#define PAGESIZE (4*1048576)
/* Синхронизация между потоками */
CRITICAL_SECTION cs;
/* Страницы буфера чтения данных */
char * cPages;
/* Текущая записываемая страница */
int iCurpage=0;
/* Страниц считано */
int iPagesRed=0;
/* Чтение закончено */
int iStop=0;
/* Число байт в последней странице */
int iInLastPage=0;
/* Поток чтения из файла */
DWORD WINAPI ReadFileInBuf(LPVOID arg){
 int iPageToFill;
 DWORD dwBytesRed;
 while(1){
  /* Если нет свободных страниц — спим */
  while(iPagesRed==NPAGES)Sleep(10);
  /* Синхронизуемся перед использованием переменных */
  EnterCriticalSection(&cs);
  /* Номер страницы, на которую считываются данные */
  iPageToFill = ((iCurpage + iPagesRed)%NPAGES);
  iInLastPage = 0;
  LeaveCriticalSection(&cs);
  /* Заполняем страницу */
  if(ReadFile((HANDLE)arg,
   cPages + iPageToFill*PAGESIZE,
  PAGESIZE, &dwBytesRed, NULL))
   iInLastPage += dwBytesRed;
  EnterCriticalSection(&cs);
  /* Страница считана */
  iPagesRed += 1;
  if(iInLastPage != PAGESIZE){
   /* Дошли до конца файла или ошибка */
   iStop = 1;
   break;
 }
 LeaveCriticalSection(&cs);
// printf("+");
// fflush(stdout);
 }
 LeaveCriticalSection(&cs);
 return 0;
}

int main(int argc, char *argv[]){
 DWORD n, dwBytesToWrite, dwBytesWritten;
 char * cDrive;
 char buf[256];
 int c;
 HANDLE hFrom, hTo, hThread;
 LONGLONG llFileLength=0;
 int iSmallPageSize;
 SYSTEM_INFO si;
 GetSystemInfo(&si);
 iSmallPageSize = si.dwPageSize;
 if(argc!=3){
  fprintf(stderr,
   "Windows NT/2K/XP Hard Drive copy\n"
   "Usage: %s <from_path> <to_path>\n"
   " # — Disk number (0 means first hard drive) of path\n"
   " Examples:\n"
   " %s 0 1\n"
   "\tcopies disk 0 to disk 1\n"
```

```
    " %s 0 file.img\n"
    "\tcopies disk 0 to file.img\n"
    " %s file.img 1\n"
    "\tcopies file.img to disk 1\n"
    "(c) 2006 by Vladimir Dubrovin\n"
    , argv[0], argv[0], argv[0], argv[0]);
  return 1;
 }
 /* Открываем файл, из которого копировать */
 if(*argv[1]>='0' && *argv[1]<='9' &&
!argv[1][1]){
  sprintf(buf, "\\\\.\\PhysicalDri-
ve%d", atoi(argv[1]));
  cDrive = buf;
 }
 else cDrive = argv[1];
 printf("From: %s\n", cDrive);
 hFrom=CreateFile(cDrive, GENERIC_READ,
  FILE_SHARE_READ | FILE_SHARE_WRITE, NULL,
  OPEN_EXISTING,
  FILE_FLAG_NO_BUFFERING|FI-
LE_FLAG_SEQUENTIAL_SCAN,
  NULL);
 if(hFrom == INVALID_HANDLE_VALUE){
  fprintf(stderr, "Unable to access
device\n");
  return 2;
 }
 /* Открываем файл, в который копировать */
 if(*argv[2]>='0' && *argv[2]<='9' &&
!argv[2][1]){
  sprintf(buf, "\\\\.\\PhysicalDri-
ve%d", atoi(argv[2]));
  cDrive = buf;
 }
 else cDrive = argv[2];
 printf("To: %s, are you sure (y/n)?",
cDrive);
 if((c = getchar()) != 'y' && c != 'Y')
return 10;
 hTo=CreateFile(cDrive,
  GENERIC_WRITE, FILE_SHARE_READ |
FILE_SHARE_WRITE,
  NULL, OPEN_ALWAYS,
  FILE_FLAG_NO_BUFFERING|
FILE_FLAG_SEQUENTIAL_SCAN,
  NULL);
 if(hTo == INVALID_HANDLE_VALUE){
  fprintf(stderr, "Unable to access
device\n");
  return 3;
 }
 fflush(stdout);
 if(!(cPages = VirtualAlloc(NULL,
  PAGESIZE*NPAGES, MEM_COMMIT,
PAGE_READWRITE))){
  fprintf(stderr, "VirtualAlloc failed\n");
  return 4;
 }
 /* запускаем поток считывания из файла */
 InitializeCriticalSection(&cs);
 hThread = CreateThread(NULL, 0,
ReadFileInBuf,
  (LPVOID)hFrom, 0, &n);
 if(hThread == NULL){
  fprintf(stderr, "Failed to create
thread \n");
  return 5;
 }
 CloseHandle(hThread);
 /* начинаем запись файла */
 while(1){
  /* ждем, пока не появятся страницы
для записи */
  while(!iStop && !iPagesRed)Sleep(1);
  /* синхронизуем потоки */
  EnterCriticalSection(&cs);
  if(iStop && !iPagesRed) break;
/* кончился файл */
/* Если дошли до конца — то писать
страницу, округленную до размера
системной страницы */
  dwBytesToWrite = (iStop && iPagesRed
== 1)?
   ((iInLastPage + iSmallPageSize - 1) /
    iSmallPageSize) * iSmallPageSize
   : PAGESIZE;
  LeaveCriticalSection(&cs);
  /* Пишем файл */
  dwBytesWritten = 0;
  if(WriteFile(hTo,
   cPages + iCurpage*PAGESIZE,
   dwBytesToWrite, &n, NULL))
   dwBytesWritten += n;
  if(dwBytesWritten!=PAGESIZE) break;
  /* Помечаем страницу как записанную */
  EnterCriticalSection(&cs);
  iCurpage = ((iCurpage + 1) % NPAGES);
  iPagesRed--;
  if(dwBytesWritten!=PAGESIZE)break;
  LeaveCriticalSection(&cs);
// printf("-");
// fflush(stdout);
 }
 LeaveCriticalSection(&cs);
 CloseHandle(hFrom);
 CloseHandle(hTo);
}
```

➔ **2.4.3. клонирование для бедных.** Как немного экзотический вариант можно рассмотреть клонирование с помощью зеркалирования. Это возможно только на серверных платформах и с динамическими дисками. Создаешь зеркало, дожидаешься окончания синхронизации, извлекаешь диск–приемник и разрываешь зеркало.

➔ **2.4.4. специальные утилиты.** Для клонирования из-под DOS можно воспользоваться программой Norton GHOST от Symantec, в которой есть мастер создания загрузочной дискетки, содержащей 16-разрядную версию этой программы. С помощью GHOST можно:

1. СКОПИРОВАТЬ ДИСК НА ДИСК;
2. СКОПИРОВАТЬ РАЗДЕЛ В РАЗДЕЛ (ИЗМЕНЯЯ РАЗМЕР РАЗДЕЛА-ПРИЕМНИКА);
3. СКОПИРОВАТЬ В РАЗДЕЛ ПРЕДВАРИТЕЛЬНО СОЗДАННЫЙ GHOST-ОБРАЗ.

У GHOST есть и сетевой вариант, при котором создается загрузочная дискетка с поддержкой сети. После этого с дискетки загружаются и машина-источник, и машина-приемник. Они указываются друг другу (по IP-адресу, который можно либо прописать руками, либо назначить автоматически через DHCP), и запускается процедура клонирования, при которой через сеть заливается образ на машину-приемник. У одной машины-источника одновременно может быть только одна машина-приемник.

➔ **3. виртуальный секс.** Сделать разное железо одинаковым можно с помощью программной прослойки, называемой виртуальной машиной. То есть ставишь операционную систему, на нее программу виртуальной машины, которая сама работает через драйверы «настоящей» (хостовой) операционной системы, а для пользователя виртуализирует другое железо, драйверы к которому входят в состав программного продукта. В эту виртуальную машину и устанавливается новая (гостевая) операционная система. Таким образом, можно сделать образ виртуальной машины (а можно и не один) и скопировать его средствами хостовой операционной системы на все машины.

Пользователь загружает хостовую систему, запускает ПО виртуальной машины, выбирает среди них нужный и работает. Если при этом раскрыть приложение виртуальной машины на полный экран, у пользователя будет полная иллюзия, что операционная система, в которой он работает, — единственная на машине :). Причем виртуализация позволяет запускать гостевую систему Windows поверх Linux или FreeBSD поверх Windows. В любых сочетаниях. Количество одновременно работающих гостевых систем определяется возможностями компьютера.

При этом на хостовой машине пользователю достаточно прав гостя, чтобы запустить виртуальную, в которой его можно сделать хоть админом. Этот способ подходит для ситуаций, когда достаточно мощные машины (ведь ресурсы тратятся и на реальную, и на виртуальную ОС) с разным железом используются для работы разных пользователей, и, по определенным причинам, ОС необходимо часто менять (ситуация учебных курсов, когда одна группа занимается на одних виртуальных машинах, другая — на других, и если что-то поломалось быстренько заливается необходимый образ).

Наиболее распространенные виртуальные машины: VMWare и Virtual PC (последняя от Microsoft). VMWare Server можно получить бесплатно на официальном сайте (**www.vmware.com**) C

европейский политикъ

ГЛАВНОЕ О ГРУППОВЫХ ПОЛИТИКАХ БЕЗОПАСНОСТИ

ЭФФЕКТИВНО СПЛАНИРОВАННАЯ ГРУППОВАЯ ПОЛИТИКА В СОЧЕТАНИИ С УМЕНИЕМ ЕЕ ПРИМЕНЕНИЯ — ПРЕКРАСНЫЙ И ПРАКТИЧЕСКИ НЕЗАМЕНИМЫЙ ИНСТРУМЕНТ УПРАВЛЕНИЯ. НО ДАЛЕКО НЕ КАЖДЫЙ ИСПОЛЬЗУЕТ GP НА СТОЛЬКО, НАСКОЛЬКО ЭТО ВОЗМОЖНО. НЕ СОВСЕМ ВЕРНОЕ ПОНИМАНИЕ ПРИНЦИПОВ И МЕТОДОВ РАБОТЫ МЕШАЮТ ДОСТИГНУТЬ БОЛЬШЕЙ ЭФФЕКТИВНОСТИ. НА САМОМ ДЕЛЕ РАЗОБРАТЬСЯ И ПОНЯТЬ GROUP POLICY НЕ ТРУДНО. ГЛАВНОЕ — СТРЕМИТЬСЯ ПОНЯТЬ СУТЬ МЕХАНИЗМА И ИМЕТЬ ХОТЯ БЫ БАЙТ ФАНТАЗИИ...

НАУМОВ ЮРИЙ AKA CRAZY_SCRIPT
{crazy_script@vr-online.ru}

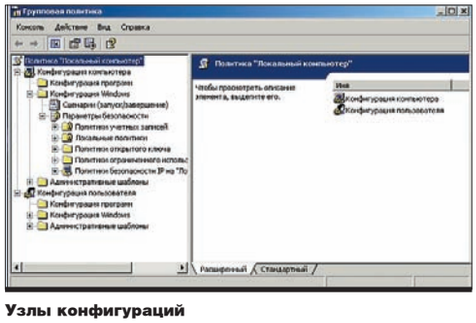
→ **active directory.** Для организации домена необходимо иметь хотя бы базовые понятия служб каталогов, в частности Active Directory. Одним из достоинств AD является расширение числа объектов. Теперь их может быть до нескольких миллионов. Служба каталогов управляется с помощью консоли Microsoft Managment Console (Пуск → Выполнить → mmc).

Одной из ключевых фигур AD является домен — элемент каталога, с собственным пространством имен и правилами безопасности, не распространяющимися за его пределы. Между доменами устанавливаются транзитивные отношения доверия. Например: домен A доверяет домену B, а B, в свою очередь, доверяет домену C. Исходя из этих доверий, домен A будет доверять домену C, их отношения будут называться транзитивными. Домены объединяются в деревья: первый домен называется «корнем дерева», остальные — дочерние, использующие пространство имен от первого домена. Деревья, объединяются в леса. Первый домен в первом дереве леса называется корнем леса. Каждое дерево наследует имя корня, а лес — имя корневого домена.

Леса характеризуются разным пространством имен и не имеют транзитивных отношений доверия. Для управления пользователями и доменами в Active Directory используют две очень важные оснастки — «Domains and Trusts» и «Users and Computers». Причем вторая, предназначенная для управления пользователями и группами, не работает и будет работать только если компьютер изолирован (на рабочих станциях и изолированных серверах). Ну а первая осуществляет работу с доменами: просмотр лесов, настройка режима работы. Под властью этой оснастки находится очень важная функция настройки доверительных отношений, о которых мы упомянули выше. Но это все теория...

→ **GPO и Group Policy.** Правила настройки различных компонентов программного обеспечения в совокупности представляют собой групповые политики (group policy) — по сути, основной инструмент для централизованного управления практически всеми подсистемами и компонентами Windows. Политики могут применяться как к компьютеру (во время загрузки ОС), так и к пользователю (во время его входа в систему). Групповая политика позволяет настраивать огромное количество разнообразных параметров операционных систем Windows, от внешнего вида рабочего стола пользователя до конфигурации сетевых протоколов. С помощью этой технологии можно производить централизованное развертывание программного обеспечения, что сэкономит время и силы.

Фактически, GP не только используют преимущества AD, но и расширяют их. Настройки находятся в объектах групповой политики (GPO —



Узлы конфигураций

установка оснасток

ВООБЩЕ ОСНАСТКА — ЭТО САМЫЙ ОСНОВНОЙ КОМПОНЕНТ КОНСОЛИ MMC. РАЗНОВИДНОСТЕЙ ОСНАСТОК ВСЕГО ДВЕ: ИЗОЛИРОВАННЫЕ ОСНАСТКИ (В ОСНОВНОМ ТЕРМИН УРЕЗАЮТ ДО «ОСНАСТКИ») И РАСШИРЕНИЯ. ОТЛИЧИЕ В ТОМ, ЧТО ОСНАСТКИ ПОСЛЕ ДОБАВЛЕНИЯ ПРИКРЕПЛЯЮТСЯ К ДЕРЕВУ КОНСОЛИ. РАСШИРЕНИЯ ЖЕ УСТАНАВЛИВАЮТСЯ К СУЩЕСТВУЮЩЕЙ ОСНАСТКЕ И МОГУТ РАБОТАТЬ С ЕЕ ОБЪЕКТАМИ. УСТАНОВКА ПРОИСХОДИТ ПУТЕМ «КОНСОЛЬ → ДОБАВИТЬ/УДАЛИТЬ ОСНАСТКУ...», В ПОЯВИВШЕМСЯ ОКНЕ ВЫБИРАЕМ, ЧТО НУЖНО И ЖМЕМ «ДОБАВИТЬ». ИЛИ ЧЕРЕЗ КОМАНДНУЮ СТРОКУ «MMC %SYSTEMROOT%\SYSTEM32\NAME.MSC».

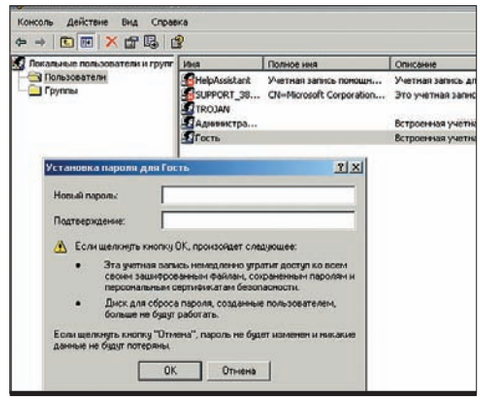
В ОДНУ КОНСОЛЬ МОЖНО УСТАНАВЛИВАТЬ СРАЗУ НЕСКОЛЬКО ОСНАСТОК И ДАЖЕ НЕСКОЛЬКО КОПИЙ ОДНОЙ (В ОПРЕДЕЛЕННЫХ СЛУЧАЯХ ЭТО ВЫРУЧАЕТ). ЕСЛИ КОМПЬЮТЕР ЯВЛЯЕТСЯ ЧАСТЬЮ ДОМЕНА, MMC ДАЕТ ВОЗМОЖНОСТЬ ЗАГРУЗКИ ОСНАСТОК, КОТОРЫЕ УСТАНОВЛЕНЫ ЛОКАЛЬНО, НО ДОСТУПНЫ ИЗ AD.

Group Policy Object), которые в свою очередь могут ссылаться на сайты/домены/подразделения. Редактирование GPO осуществляется с помощью оснастки «Редактор групповых политик» (gpedit.msc). Объекты GP — локальный объект групповой политики и объект групповой политики домена. Сами GPO хранят свои настройки в контейнере GPC (Group Policy Container) и шаблоне GRT (Group Policy Template). Первый является объектом AD, второй представляет собой папку с настройками, управляемую с помощью одного из расширений GP — административных шаблонов.

➜ **узлы и расширения GP.** При запуске Group Policy загружает корневой узел — GPO, привязанный к определенному контейнеру. Узел получает имя: Политика Имя_GPO[.Имя_домена.com]

Далее идет разделение пространства имен на 2 уровня, с помощью которых собственно и производится настройка групповых политик.

❶ Узел «Конфигурация компьютера». Здесь содержатся параметры тех политик, которые отвечают за работу компьютера. Политики следят за работой ОС, задают параметры приложений, определяют работу системы безопасности.



Установка пароля пользователя

❷ Узел «Конфигурация пользователя». Включает в себя политики, отвечающие за работу пользователя. Слежение идет все за теми же параметрами приложений и системой безопасности, а так же за пользовательскими сценариями входа/выхода.

Ниже находятся дочерние узлы, расширяющие узлы конфигурации индивидуально для каждого. Индивидуальность проявляется в следствие различия параметров каждого из узлов конфигурации. Group Policy имеет следующие расширения:

— АДМИНИСТРАТИВНЫЕ ШАБЛОНЫ (ADMINISTRATIVE TEMPLATES) ПОЛИТИКИ, БАЗИРУЮЩИЕСЯ НА РЕЕСТРЕ ОС. БЕЗ ТОГО ШИРОКАЯ ФУНКЦИОНАЛЬНОСТЬ GP МОЖЕТ ПРИМЕНЯТЬСЯ НЕ ТОЛЬКО К СТАНДАРТНЫМ ПАРАМЕТРАМ, СВЯЗАННЫМ С ОС, НО И К ДРУГИМ ОБЪЕКТАМ.

— ПАРАМЕТРЫ БЕЗОПАСНОСТИ (SECURITY SETTINGS) КАК НИ СТРАННО, СЛУЖАТ ДЛЯ НАСТРОЙКИ ПАРАМЕТРОВ БЕЗОПАСНОСТИ КОМПЬЮТЕРА/ДОМЕНА/СЕТИ.

— УСТАНОВКА ПРОГРАММ (SOFTWARE INSTALLATION) НАЗНАЧАЕТ И ПУБЛИКУЕТ ПРОГРАММЫ ДЛЯ ПОЛЬЗОВАТЕЛЕЙ.

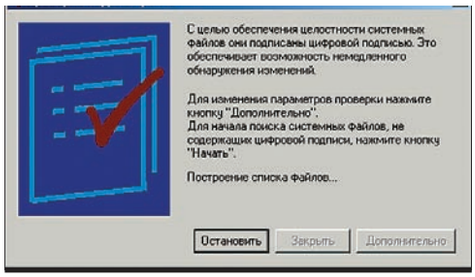
— СЦЕНАРИИ (SCRIPTS) ОПРЕДЕЛЯЮТ ПРОЦЕДУРЫ START/STOP КОМПЬЮТЕРА, LOGIN/LOGOUT ПОЛЬЗОВАТЕЛЯ. СЦЕНАРИИ ПОЛНОСТЬЮ СОВМЕСТИМЫ С ЯЗЫКОМ WINDOWS SCRIPT HOST.

— ПЕРЕНАПРАВЛЕНИЕ ПАПОК (FOLDER REDIRECTION) ПЕРЕНАПРАВЛЯЕТ ОБРАЩЕНИЕ К СПЕЦИАЛЬНЫМ ПАПКАМ WINDOWS (DESKTOP, APPLICATION DATA, MY DOCUMENTS) В СЕТЬ.

Различие в создании системных политик

Задача	Средство Windows NT 4.0	Средство Windows XP
Установка политик для пользователей и компьютеров сайта	Не применяется	Групповая политика, доступна посредством оснастки Active Directory — сайты и службы
Установка политик для пользователей и компьютеров домена	Редактор системной политики (poledit.exe)	Групповая политика, доступная с помощью оснастки Active Directory — пользователи и компьютеры
Установка политик для пользователей и компьютеров подразделения	Не применяется	Редактирование записи разрешений для действия «Применение групповой политики» на вкладке «Безопасность» диалогового окна свойств объекта групповой политики.
Управление программным обеспечением	Для администраторов — сервер Systems Management Server. Для пользователей — компонентпанели управления «Установка и удаление программ»	Сервер Systems Management Server и три компонента установки и сопровождения программ: • Установка программного обеспечения, расширение «Групповая политика» оснастки. • Установщик Windows. • Компонент панели управления. «Установка и удаление программ».
Создание безопасного пользовательского интерфейса для редактирования реестра	Административные шаблоны в формате Windows NT 4.0 для редактора системной политики	Административные шаблоны в формате Windows XP для групповой политики
Выполнение основных административных задач	Мастер администрирования, диспетчер пользователей и диспетчер серверов	Оснастки консоли управления MMC, в частности, Active Directory — пользователи и компьютеры, Active Directory — сайты и службы и «Групповая политика», а также их расширения

www.vr-online.ru/cscript/docs/ad4win2003.rar — ad на платформе win2003
www.networkdoc.ru/files/insop/ad/adtechs.doc — техническое описание ad
www.n-admin.com, www.hub.ru — портал для сисадминов
www.sysadmins.ru — несомненно, лучший форум сисадминов



Проверка цифровой подписи

➔ **политики учетных записей.** Практически все управление юзерами и группами осуществляется с помощью этой оснастки. Пользователь или группа представляют собой учетную запись, которой можно дать различные права и разрешения, определяя таким образом их взаимодействие с доменом. Политика учетных записей (lusrmgr.msc) включает в себя политики паролей, блокирования учетных записей и др.

Оснастка дает возможность полностью сконфигурировать требования для групп и пользователей: max/min длину пароля, срок его действия, требования к сложности. Но тут нужно обратить внимание на то, что все перечисленные настройки в ветке «Политика паролей» относятся не к одному, а сразу ко всем пользователям. После настройки длины пароля и срока его действия следует обратить внимание на хранение паролей. То есть когда у пользователя истекает срок действия пароля, ему предлагается его сменить. А что будет вводить юзер? Конечно, старый пароль. Для предотвращения таких ситуаций нужно включить сохранение паролей: политика будет записывать все используемые юзером пароли и фиксировать их смену. Но здесь есть одно большое НО: хранение осуществляется с использованием обратимого шифрования, а практически это означает, что вообще без шифрования. Поэтому здесь стоит выбирать: либо важнее приложение, либо защита пароля пользователя.

➔ **локальные политики.** Как мы уже говорили, существует два вида GPO. Локальные объекты групповой политики (Local Group Policy Object, LGPO) создаются сразу при установке ОС и существуют независимо от того, является ли компьютер частью домена или нет. Когда производится подключение, компьютер автоматически попадает под влияние GPO, определенных в домене. В следствие этого локальные параметры могут измениться. Рассмотрим по порядку состав локальной политики:

— ПОЛИТИКА АУДИТА. ОПРЕДЕЛЯЕТ, КАКИЕ СОБЫТИЯ БЕЗОПАСНОСТИ ЗАНОСЯТСЯ В ЖУРНАЛ КОМПЬЮТЕРА. САМ ЖУРНАЛ ПРОСМАТРИВАЕТСЯ С ПОМОЩЬЮ ОСНАСТКИ «ПРОСМОТР СОБЫТИЙ» (EVENTVWR.MSC). ЭТА ПОЛИТИКА МОЖЕТ БЫТЬ КАК ДЛЯ ЛОКАЛЬНОГО КОМПЬЮТЕРА, ТАК И ДЛЯ КОНТРОЛЛЕРА ДОМЕНА.

— НАЗНАЧЕНИЕ ПРАВ ПОЛЬЗОВАТЕЛЯ. ОПРЕДЕЛЯЕТ, КАКИЕ ПОЛЬЗОВАТЕЛИ (ГРУППЫ) ОБЛАДАЮТ ПРАВАМИ НА ЛОКАЛЬНЫЙ ВХОД В СИСТЕМУ И НА ДОСТУП КОМПЬЮТЕРА ИЗ СЕТИ.

Не стоит забывать о том, что применение нескольких политик может повлечь за собой конфликт между параметрами безопасности. Поэтому запомни приоритет расположения объектов: подразделение; домен; локальный компьютер.

➔ **политики открытого ключа.** Шифрование информации в политиках безопасности Windows осуществляется с открытым ключом (асимметричное шифрование). Суть его в том, что данные шифруются одним ключом, а расшифровываются другим, связанным с ним, но не совпадающим. У пользователя есть открытый (public key) и закрытый ключ (private key). Первый распространяется свободно и дает возможность шифровать для тебя данные любому. Применение и распространение этих двух ключей повлекло за собой возникновение новых технологий. Цифровые подписи — наиболее яркий пример использования шифрования с открытым ключом. Положения технологии следующие:

1 ВОЗМОЖНОСТЬ СОЗДАНИЯ ЦИФРОВОЙ ПОДПИСИ ИМЕЕТ ТОЛЬКО ВЛАДЕЛЕЦ СЕКРЕТНОГО КЛЮЧА.

2 ИСТИННОСТЬ ЦИФРОВОЙ ПОДПИСИ МОЖЕТ ПРОВЕРИТЬ ЛЮБОЙ ПОЛЬЗОВАТЕЛЬ, У КОТОРОГО ИМЕЕТСЯ СООТВЕТСТВУЮЩИЙ ОТКРЫТЫЙ КЛЮЧ (SIGVERIF.EXE).

3 ЦИФРОВАЯ ПОДПИСЬ СТАНОВИТСЯ НЕВЕРНОЙ ПРИ ИЗМЕНЕНИИ ДАЖЕ ОДНОГО БИТА ПОДПИСАННЫХ ДАННЫХ.

Цифровая подпись либо связана с данными, либо вообще передается отдельно. При этом подписи никак не влияют на содержание данных. Самое главное и важное в цифровой подписи при распространении данных открытым текстом состоит в том, что получатель может проверить и удостовериться, что изменений в данных не было. Для этого существует служба распределенной аутентификации, гарантирующая, что данные пришли от того, от кого надо. Но этих гарантий мало. Нужно полностью удостовериться в том, что между открытым ключом и передавшим его человеком существует достоверная связь. Если это не так, может произойти подмена открытого ключа и получение доступа к данным. Применение так называемых сертификатов позволяет установить связь между открытым ключом и передавшим его лицом. Сертификат — это набор зашифрованных цифровой подписью данных, содержащих подтверждение неизменности. Для управления ими используется специальная оснастка (certmgr.msc), позволяющая просматривать содержимое хранилищ для поиска своих сертификатов, а так же сертификатов служб или компьютеров. В сертификате содержится следующая информация:

1 КРИПТОГРАФИЧЕСКАЯ ПОДПИСЬ, ИДЕНТИФИЦИРУЮЩАЯ СОЗДАТЕЛЯ СЕРТИФИКАТА.

2 ПОДТВЕРЖДЕНИЕ СВЯЗИ ОТКРЫТОГО КЛЮЧА С ЛИЦОМ, ПЕРЕДАВШИМ ДАННЫЕ.

3 СОЗДАНИЕ СЕРТИФИКАТА ТЕМ ЦЕНТРОМ СЕРТИФИКАТОВ, КОТОРОМУ ДОВЕРЯЕТ ЛИЦО, ПРИНИМАЮЩЕЕ ДАННЫЕ.

Некоторые контейнеры групповой политики

Контейнер	Описание
Сценарии (запуск/завершение)	Содержит параметры «Автозагрузка» и «Завершение работы», предназначенные для указания файлов сценариев, которые выполняются при загрузке и выключении компьютера
Политика паролей	Содержит параметры, задающие ограничения и правила использования паролей, такие как минимальная длина пароля и срок действия пароля
Политика блокировки учетной записи	Содержит параметры, определяющие правила автоматической блокировки учетных записей при вводе неправильных паролей
Параметры безопасности	Содержит параметры, определяющие поведение системы безопасности, как при локальной работе пользователя, так и при взаимодействии компьютеров в сети
Вход/выход из системы	Содержит параметры, определяющие поведение операционной системы при загрузке компьютера и регистрации пользователя, а также ограничивающие возможности пользователя при выполнении некоторых операций

device lock

КОМПАНИЯ «СМАРТ ЛАЙН ИНК» РАЗРАБАТЫВАЕТ ПРОДУКТ DEVICELOCK — СРЕДСТВО ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА. ПРОГРАММА РАБОТАЕТ С ГРУППОВОЙ ПОЛИТИКОЙ WINDOWS И ПОЗВОЛЯЕТ ОСУЩЕСТВЛЯТЬ АУДИТ ДЕЙСТВИЙ ПОЛЬЗОВАТЕЛЕЙ СО СМЕННЫМИ НОСИТЕЛЯМИ. DEVICELOCK ВКЛЮЧАЕТ В СЕБЯ ТАКИЕ ВАЖНЫЕ ДОПОЛНИТЕЛЬНЫЕ ФУНКЦИИ, КАК:

- ФУНКЦИЯ АУДИТА, КОТОРАЯ ИНФОРМИРУЕТ СИСТЕМНОГО АДМИНИСТРАТОРА О ТОМ, КТО И КОГДА ИМЕЛ ДОСТУП К СМЕННЫМ НОСИТЕЛЯМ НА КОМПЬЮТЕРЕ.
- ИНТЕГРАЦИЯ С ACTIVE DIRECTORY, КОТОРАЯ ПОЗВОЛЯЕТ СИСТЕМНЫМ АДМИНИСТРАТОРАМ УПРАВЛЯТЬ НАСТРОЙКАМИ DL ЧЕРЕЗ ГРУППОВЫЕ ПОЛИТИКИ. АДМИНИСТРАТОРЫ МОГУТ УСТАНАВЛИВАТЬ DEVICELOCK И ЕГО НАСТРОЙКИ НА ВСЮ СЕТЬ, ИСПОЛЬЗУЯ СТАНДАРТНЫЕ ИНСТРУМЕНТЫ УПРАВЛЕНИЯ.
- УСТАНОВКА ПРАВ ДОСТУПА, КАК ДЛЯ ИНДИВИДУАЛЬНЫХ ПОЛЬЗОВАТЕЛЕЙ, ТАК И ДЛЯ ГРУПП ПОЛЬЗОВАТЕЛЕЙ.
- НАЗНАЧЕНИЕ ПРИВИЛЕГИЙ ДОСТУПА ПО КЛАССУ.
- ВОЗМОЖНОСТЬ УСТАНОВКИ РЕЖИМА «ТОЛЬКО ДЛЯ ЧТЕНИЯ»

И ЕЩЕ МНОГОЕ ДРУГОЕ.

И все же, в открытом ключе есть один недостаток. Дело в том, что алгоритмы шифрования с открытым ключом, в отличие от секретного, требуют много ресурсов. Выход из этой ситуации разработчики нашли в комбинации двух алгоритмов: данные шифруются с помощью секретного ключа, не отнимая лишнего времени, а секретный ключ, в свою очередь, шифруется открытым ключом и посылается вместе с зашифрованными данными. Получатель сначала расшифровывает секретный ключ, а затем с его помощью данные.

В результате всех этих положений и правил возникает цепочка сертификатов, берущая свое начало с сертификата открытого ключа. Обо всех сертификатах, идентификаторах связи и о модели в рамках статьи написать нереально. Кому интересно, вполне может найти информацию самостоятельно.

Стандартом сертификатов, наиболее распространенным сегодня, является ITU-T X.509. О нем и других протоколах сетевого взаимодействия, в частности, о инфраструктуре открытого ключа, можно узнать из соответствующего курса.

➔ **политики безопасности IP.** Несомненно, админу просто жизненно необходима уверенность в безопасной передаче данных по сети. Трафик обязан быть защищенным от доступа лиц, не имеющих на это прав, от просмотра передаваемых данных, от копирования и модификации. Реализация безопасности IP в Windows основана на стандартах RFC, разработанных консорциумом Internet Engineering Task Force (IETF), рабочей группой IP Security (IPSEC). Политика безопасности сначала требует аутентифицировать любой подключаемый компьютер, используя заранее переданный секретный ключ, а затем шифрует трафик. Исключение составляют лишь http(80) и https(443). По этим протоколам web-сервер должен принимать соединения от любых узлов. В Windows безопасность IPSec реализована в виде средства управления политик безопасности для сетевого трафика. Она представляет собой набор фильтров, действие которых определяется исходя из требований безопасности.

Неотъемлемой частью работы IPSec является протокол, с помощью которого устанавливаются доверительные отношения, согласование параметров безопасности и создается общий секретный ключ. Согласования, связанные с ключом, принято называть сопоставлением безопасности или SA (Security Association) и разделять на два типа:

[1] SA ОСНОВНОГО РЕЖИМА ОБЕСПЕЧИВАЕТ ЗАЩИТУ САМОГО СОГЛАСОВАНИЯ IKE.

[2] SA БЫСТРОГО РЕЖИМА ОБЕСПЕЧИВАЕТ ЗАЩИТУ ТРАФИКА ПРИЛОЖЕНИЯ.

Настройка требований безопасности производится при помощи достаточно гибкой настройки действия фильтра как в основном, так и в быстром режиме. Подытожить все вышесказанное можно схемой этапов работы IPSec.

[1] ДАННЫЕ В ПРИЛОЖЕНИИ ПЕРЕДАЮТСЯ ФУНКЦИИ АУТЕНТИФИКАЦИИ И ОБЕСПЕЧЕНИЯ ЦЕЛОСТНОСТИ ПЛЮС ПОДДЕРЖКИ ЦИФРОВОЙ ПОДПИСИ;

[2] ШИФРОВАНИЕ ДАННЫХ ОТКРЫТЫМ КЛЮЧОМ;

[3] ДАННЫЕ ПЕРЕСЫЛАЮТСЯ ПО СЕТИ ЗАШИФРОВАННЫМИ ПАКЕТАМИ В ЗАЩИЩЕННОМ ТУННЕЛЕ;

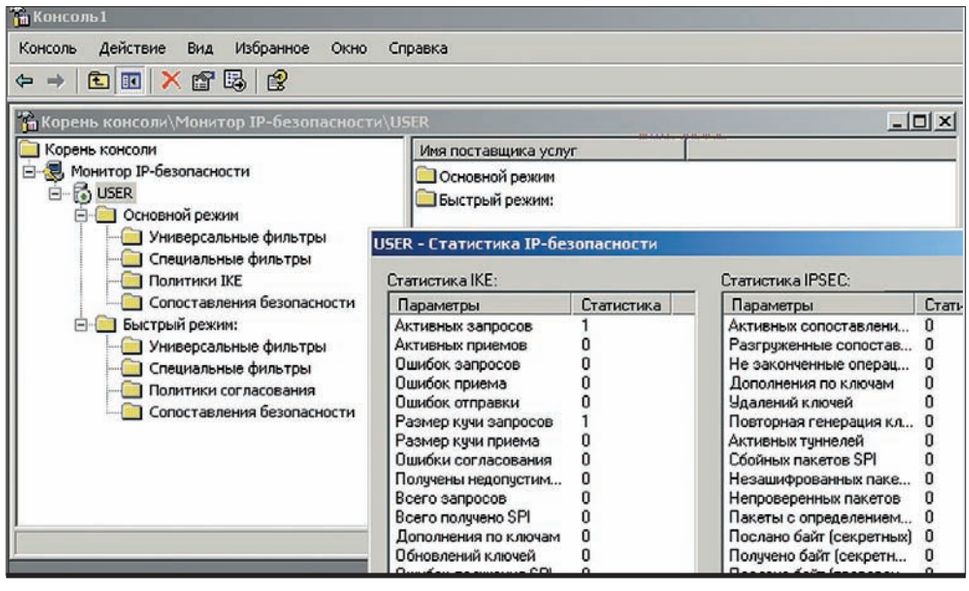
[4] В ТУННЕЛЕ СНОВА ПРОИСХОДИТ ШИФРОВАНИЕ. НА ЭТОТ РАЗ ИСПОЛЬЗУЕТСЯ ТАК НАЗЫВАЕМЫЙ «КЛЮЧ СЕАНСА»;

[5] В КОНЦЕ ТУННЕЛЯ ИДЕТ ДЕШИФРОВКА С ПОМОЩЬЮ ЛИЧНОГО КЛЮЧА;

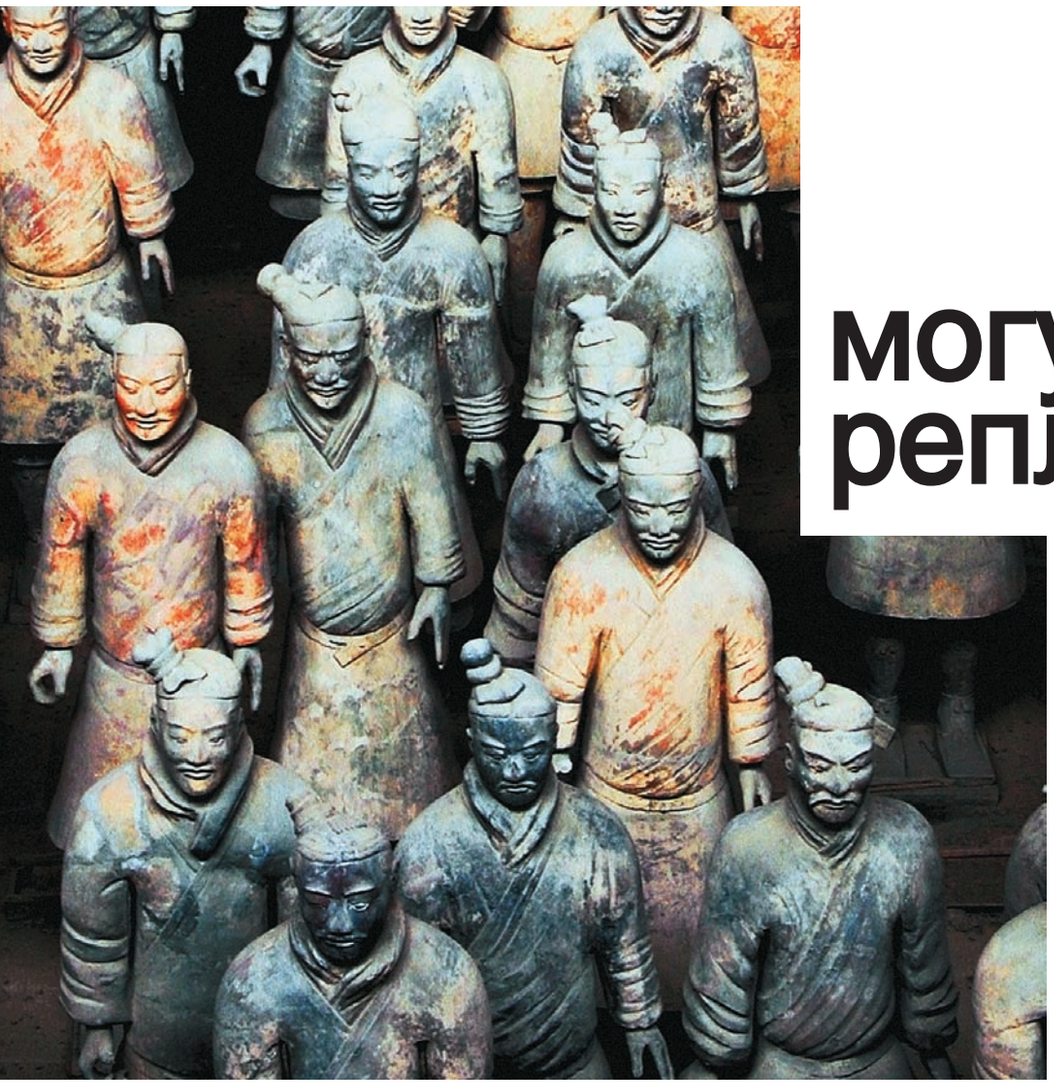
[6] ДАННЫЕ ДОБИРАЮТСЯ ДО КОМПЬЮТЕРА, И ПРОВЕРЯЕТСЯ ПОДЛИННОСТЬ ОТПРАВИТЕЛЯ;

[7] ПОЛЬЗОВАТЕЛЬ ПОЛУЧАЕТ СООБЩЕНИЕ.

➔ **правильная политика.** Конечно же, на эту тему можно писать (и, как не странно, пишут) толстенные книги без картинок и читать скучнейшие лекции. Но основная цель статьи — не разбор служб каталогов, не ознакомление с параметрами и установками, а разъяснение сути. Остальное каждый может без труда изучить самостоятельно. Ну а если возникнут вопросы — помогу, чем смогу. Удачи! C



Средство управления политикой безопасности ip



могучая репликация

СЕКРЕТЫ РЕПЛИКАЦИИ БАЗ ДАННЫХ

РЕПЛИКАЦИЯ — ЭТО НЕ ПРОСТО НОВОМОДНОЕ СЛОВО: В ПРАВИЛЬНО ОТШЛИФОВАННЫХ РУКАХ ЭТО УДОБНЫЙ И МОЩНЫЙ ИНСТРУМЕНТ. НЕКОТОРЫЕ СЧИТАЮТ, ЧТО РЕПЛИКАЦИЯ — ЭТО СИНОНИМ СИНХРОНИЗАЦИИ. ЕСЛИ ЗАГЛЯНУТЬ В ABBYY LINGVO, ТО СРЕДИ ВОЗМОЖНЫХ ПЕРЕВОДОВ СЛОВА REPLICATION ТЫ НЕ УВИДИШЬ СИНХРОНИЗАЦИИ, ЗАТО БУДУТ ТАКИЕ СЛОВА КАК: ЭХО, ОТРАЖЕНИЕ, ДУБЛИРОВАНИЕ, ПОВТОРЕНИЕ, РАЗМНОЖЕНИЕ... ЭТИ СЛОВА ХОРОШО ОТРАЖАЮТ ДАННУЮ ТЕХНОЛОГИЮ И ТО, ЧТО МЫ БУДЕМ РАССМАТРИВАТЬ СЕГОДНЯ

ФЛЕНОВ МИХАИЛ
{http://www.vr-online.ru}

➜ **издатель-дистрибьютор-подписчик.** Чаще всего репликацию связывают с базами данных. Причем не только с классическими базами, но и с такими специализированными, как Active Directory. Но на этом мир не перевернулся: репликацию можно удачно использовать и для простых файлов, главное — правильный подход.

Репликация базируется на трех понятиях — издатель, дистрибьютор и подписчик. Чтобы понять, что это означает, достаточно обратиться к нашей реальной жизни, где издатель выдает какую-то информацию дистрибьютору, а тот рассылает ее подписчикам. Точно также и в компьютерной жизни. Но обо всем по порядку.

Издатель — хранит источник базы данных, делая опубликованные материалы из таблиц базы данных доступными для репликации; находит и отправляет изменения дистрибьютору.

Дистрибьютор — это сервер, который содержит распределенную базу данных и хранит метаданные, историю данных и транзакции. Роль дистрибьютора может быть разной и зависит от типа развернутой репликации.

Дистрибьютор и издатель могут находиться на одном компьютере. Чаще всего нет смысла выделять для каждого из них отдельный сервер, но для большой базы данных и наиболее активных сайтов для оптимизации производительности можно расположить дистрибьютора на собственном сервере.

Подписчик — владеет копией данных и получает изменения, произведенные издателем. В зависимости от настроек репликации, подписчик может иметь право изменять данные и реплицировать их обратно издателю для репликации другим подписчикам. Такой подписчик называется обновляющим.

➜ **фильтруй базар.** Возможно, для публикации нам понадобится поднабор таблицы как отдельной статьи. Это называется фильтрацией данных. Фильтрация данных позволяет избавиться от конфликтов репликации, когда право обновлять данные имеют несколько сайтов. Ты можешь фильтровать таблицы вертикально, горизонтально или смешанно для создания отфильтрованной порции данных.

Вертикальный фильтр содержит поднабор колонок таблицы. Только реплицированные колонки отображаются подписчику. Для примера: вертикальный фильтр можно использовать для публикации всех колонок, кроме «Заработная плата» в таблице «Работники».

Горизонтальный фильтр содержит поднабор строк таблицы. Подписчик получает только этот поднабор строк. Если информацию о левых доходах не нужно реплицировать, то ее можно отфильтровать запросом.

Возможно подписание на публикацию с помощью Push или Pop метода. Метод Push обычно используется в приложениях, которые должны отправлять изменения подписчику как можно быстрее. Этот метод более предпочтителен для публикаций, требующих высокой степени защищенности, где высокая загрузка процессора у дистрибьютора не влияет на производительность.

Метод Pop более подходит для публикаций с меньшей степенью защищенности и может поддерживать большое количество подписчиков, — например подписчиков Internet.

➜ **типы репликации.** Существует три основных типа репликации: снимок, журнальный тип и смешение. Тип репликации назначается для каждой публикации. Таким образом, возможно исполь-

зование нескольких типов репликации в одной базе данных.

Репликация снимка распределяет данные напрямую как отображение на определенный момент времени, без мониторинга изменений. Это самый простой тип, при котором происходит банальное копирование снимка всех или только отфильтрованных данных. Этот тип можно использовать в следующих случаях:

- ДАННЫЕ ИЗМЕНЯЮТСЯ СУЩЕСТВЕННО, НО РЕДКО;
- ПОДПИСЧИКУ ТРЕБУЮТСЯ ДАННЫЕ ТОЛЬКО ДЛЯ ЧТЕНИЯ;
- ВОЗМОЖНА БОЛЬШАЯ ЗАДЕРЖКА, ПОТОМУ ЧТО ОБЫЧНО ДАННЫЕ ОБНОВЛЯЮТСЯ ТОЛЬКО ПЕРИОДИЧЕСКИ;
- ПОДПИСЧИКУ ТРЕБУЕТСЯ АВТОНОМНОСТЬ.

При репликации транзакций от источника к приемнику поступают только изменения. Агент мониторит изменения в журнале транзакций на замену реплицированных данных и переносит необходимые записи дистрибьютору. Агент дистрибьютора отправляет изменения подписчику. Прежде чем этот тип начнет работать, подписчику отправляется полный снимок реплицированных таблиц, а затем он получает только изменения.

Репликация транзакций может использоваться там, где необходимо, чтобы подписчик получал изменения с минимальной задержкой. Тип смешения позволяет сайтам автономно изменять реплицированные данные. Позже изменения с сайтов сливаются в одно целое. Этот тип не обещает целостности транзакций, но он гарантирует, что все сайты сливаются в один результирующий набор.

➔ **репликация MS SQL Server.** Очень удачно дана возможность репликации в MS SQL Server. Настройка проста, как три копейки, потому что ее легко сделать с помощью двух мастеров. Но есть подводные камни, о которых мастер не может рассказать, а мануалы просто умалчивают. Итак, давайте бегло пройдемся по процессу настройки репликации и сделаем упор на подводные булыжники, о которых все молчат как рыбы.

Для начала необходимо создать издателя и дистрибьютора. Для этого на одном из серверов выбираем меню Tools → Replication → Create and Manage Publication. Для издателя я бы порекомендовал использовать машину помощнее. Первое, что у нас попросит мастер — выбрать базу данных. Выбираем, жмем Create Publication, и на следующем этапе сервер предложит создать дистрибьютора. По умолчанию дистрибьютором предлагается сделать ту же машину.

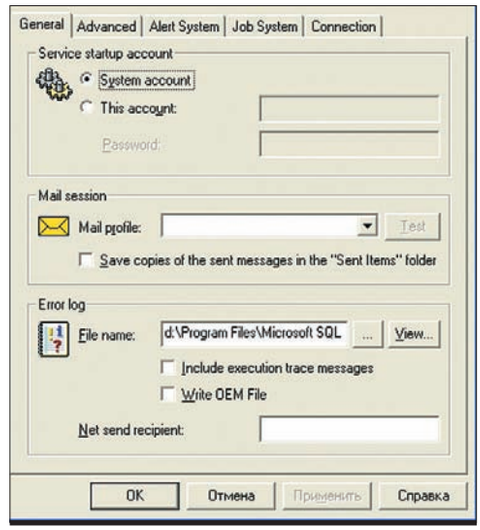
Тут появляется первый подводный камень: если дистрибьютор будет установлен удаленно от издателя (на другой машине), то SQL Server Agent не может работать от имени системного аккаунта. Почему? Агент должен иметь возможность авторизоваться на машине дистрибьютора и передать изменения, а для этого используется учетная запись, под которой работает агент. Под Local Account авторизоваться нигде не удастся, поэтому изменения никуда не пойдут.

После этого нам предложат сконфигурировать самого агента вручную или автоматически. Если выбрать ручной режим, то количество шагов мастера резко возрастает, но они просты, и с минимальными знаниями английского ты в них разберешься. Если выбрать автомат, то остается только указать мастеру требуемый тип репликации — снимок (Snapshot publication), транзакции (Transaction publication) или смешение (Merge publication) — и указать необходимые таблицы. Да, в репликации участвует не вся база, а указанные таблицы. Системные таблицы реплицировать незачем.

После создания издателя необходимо создать подписчика, и настройку можно считать завершенной. Во время создания подписчика ты сможешь настроить план выполнения, указать дни, время или промежутки, через которые нужно выполнять репликацию.

Если ты настроил репликацию и решил перенести базу данных на другой сервер, то можешь забыть про перенос через резервное копирование и восстановление. Дело в том, что в резервную копию не попадает информация о репликации. Тут приходится отключать базу Detach, копировать файлы на другой компьютер и подключать их заново Attach.

➔ **золотой ключик.** Следующая проблема, с которой есть вероятность столкнуться — репликация ключевых полей. Если у нас они имеют тип Guid, то никаких проблем тут не будет, но если — Identity, то предстоят серьезные проблемы. Дело в том, что автоматически увеличиваемые поля не могут корректно реплицироваться с настройками по



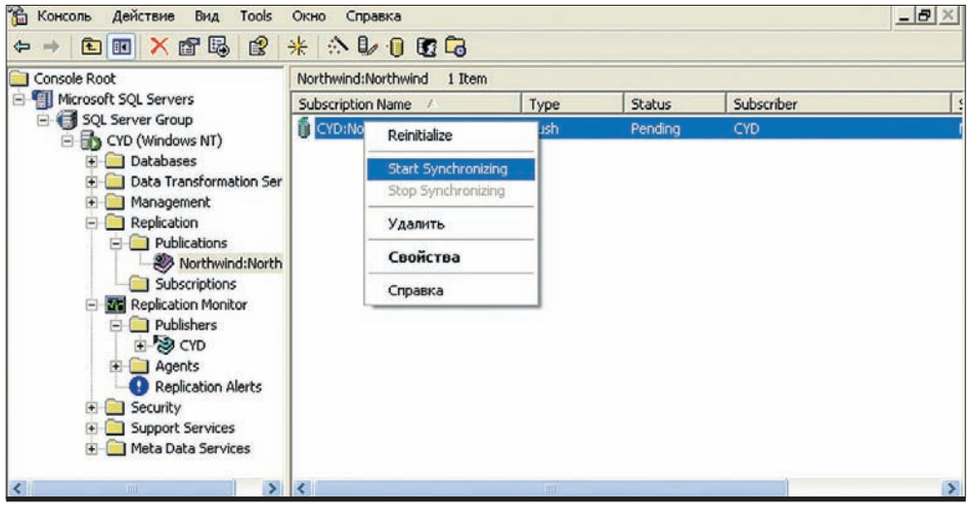
Настройка учетной записи MS SQL Server Agent

умолчанию, особенно при смешении, когда подписчик может изменять данные и должен уметь возвращать их издателю.

Допустим, что на двух компьютерах были созданы две разные записи с одинаковыми идентификаторами. Что делать серверу? Какую из записей выбирать? По идее, в результирующую таблицу должно попасть обе записи, но изменять ID нельзя, особенно если таблица связанная, а две записи с одинаковым ключом невозможны.

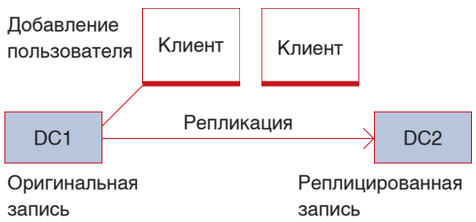
Проблема решается достаточно просто, нужно только выполнить следующие шаги:

1. СОЗДАЕМ КОПИЮ БАЗЫ ДАННЫХ ИЗДАТЕЛЯ НА КОМПЬЮТЕРЕ ПОДПИСЧИКА.
2. ОТКРЫВАЕМ ОКНО РЕДАКТИРОВАНИЯ ТАБЛИЦЫ ИЛИ С ПОМОЩЬЮ SQL ЗАПРОСА УСТАНАВЛИВАЕМ НА ИЗДАТЕЛЕ ДЛЯ КЛЮЧА НАЧАЛЬНОЕ ЗНАЧЕНИЕ 1, А ДЛЯ ПОДПИСЧИКА 1 000000.



Ручной запуск репликации

Схема разрешения конфликтов



Репликация пользователя между двумя контроллерами доменов (DC1 и DC2)

Все просто и красиво. Теперь при добавлении записи на издателе новые записи будут нумероваться 1, 2, 3, 4..., а на подписчике 1000001, 1000002, 1000003... Таким образом, записи пересекутся не скоро, и конфликты могут никогда не появиться, особенно если записи добавляются в таблицу не слишком интенсивно. Если же они добавляются интенсивно, то откажемся от автоувеличения и используем GUID-поля в качестве ключа.

Но и это еще не все. При создании подписчика нам предложат перенести всю схему с издателя. Это удобно, если структура таблиц разная и их необходимо синхронизировать, но в нашем случае неприемлемо. Если ты поведешься на это предложение и ответишь «Yes», то схема издателя будет скопирована подписчику, и у обоих начальное значение ключа станет единицей, и все наши старания пойдут прахом, т.е. затрутся. Чтобы этого не произошло, жми «No» и наслаждайся. Главное, чтобы на подписчике структура таблиц была такой же, как и у издателя.

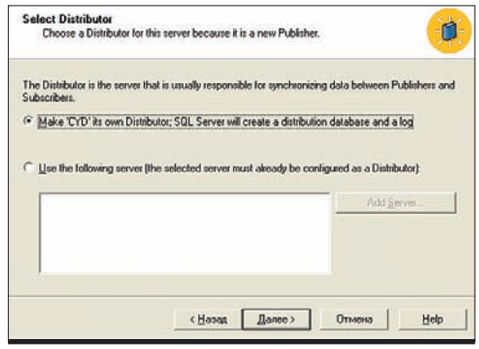
➔ **типы репликации.** Active Directory, которая активно используется серверами Windows — это тоже база данных. Она может быть распределенной, когда в работе участвуют несколько серверов, и при этом пользователь должен иметь возможность войти на любой из них с одним и тем же паролем. Каким образом это сделать? Зарегистрироваться на каждом сервере в отдельности? Глупо и бессмысленно. И тут на помощь приходит репликация. Достаточно зарегистрироваться на одном сервере и прописать необходимые права доступа, — и вся информация будет реплицирована куда надо.

Репликация в AD происходит автоматически и чаще всего особого вмешательства не требует, но требует хорошего понимания основной идеи. Если бы с Active Directory все было так просто, я бы не рассматривал эту технологию отдельно. Для начала нужно понимать, что для аутентификации используется протокол Kerberos, и ответственность за подлинность берет на себя контроллер домена. Когда ты заходишь на сервер, то имя и пароль направляются серверу, который, в свою очередь, проверяет эти данные и, в случае удачи, выдает белый билет. Если что-то не так, билет конечно не белый, но на его основе пользователь получает те или иные права. Если есть желание, но не хватает знаний, то советую поближе познакомиться с Active Directory и Kerberos, но не забывай, что наша задача — репликация.

Если до Windows 2000 в сети мог быть только один контроллер домена, который хранил все самое важное и управлял репликацией (тогда не было и Kerberos), то в нынешних версиях контроллеров может быть несколько. При этом все они будут равноправными. Это усложняет задачу по управлению процессом репликации и разрешения возможных конфликтов, но «окна» нашли выход. Контроллеры домена наблюдают друг за другом, определяя, какой из них в данный момент будет дистрибьютором, т.е. одарит других изменениями.

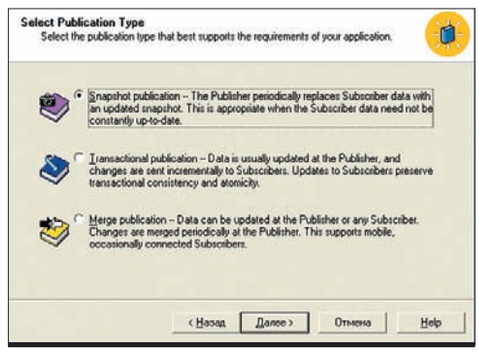
Настраивать вручную соединения между контроллерами доменов в сети нет необходимости, хотя и есть такая возможность. Серверы сами, через определенные промежутки времени, отслеживают доступные контроллеры и хранят в памяти всю необходимую информацию.

По умолчанию репликация происходит каждые пятнадцать минут. Через эти промежутки времени сервер направляет контроллерам домена сообщения о том, что есть изменения и, конечно же, становится дистрибьютором. Остальные участники репликации, получив подобное сообщение, подключаются к серверу и вытягивают данные. Сам дистрибьютор без запроса свои изменения в сеть не выплюнет, чтобы злые хакеры перехватили подобный пакет. Просто нет смысла без надобности кидать в сеть такие важные данные — вдруг остальные контроллеры домена упали.

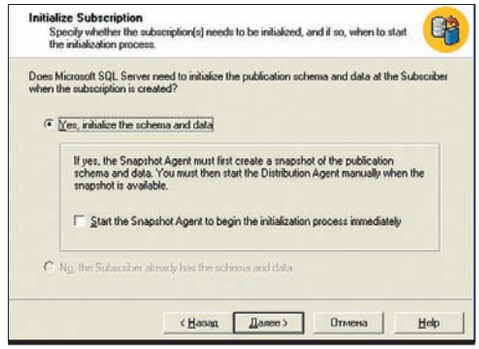


Мастер запрашивает создание дистрибьютора

➔ **конфликты в Active Directory.** Благодаря тому, что репликация выполняется с задержкой, сервер реплицирует обновления пачками. Все изменения в Active Directory накапливаются и в определенный момент рассылаются всем контроллерам домена. Это хорошо, но за счет задержки возможны и проблемы. Допустим, что в определенный



Выбор типа репликации



Запрос на копирование схемы

промежуток времени, одновременно произошло изменение на двух контроллерах домена. Чьи изменения будут реплицированы? Давай попробуем разобраться.

Все объекты Active Directory имеют определенную версию, которая при создании получает значение единицы. После каждого редактирования объекта версия увеличивается, поэтому если приходит просьба реплицировать запись с меньшим номером версии, чем текущая, такие изменения откатываются.

А что если серверу придет одновременно два предложения на репликацию от разных контроллеров, и при этом версии объектов будут одинаковыми, но сами объекты разными? Такое может случиться, когда один и тот же объект с идентичной версией изменяется на разных контроллерах. Оба контроллера увеличат версию, и она снова будет одинаковой. В этом случае побеждает тот сервер и соответствующее изменение, которое было сделано последним.

Самый крайний случай — когда версии одинаковы, и даже время изменения идентично. Конечно, вероятность этого слишком мала, но она есть, поэтому разработчики Active Directory в данном случае предпочли выбирать то изменение, которое пришло с сервера с большим глобальным идентификатором GUID. Конечно, этот глупый выбор может оказаться далеко не точным, но он хоть как-то решает конфликт.

Каждый контроллер, получив изменения, пытается втулить их другим контроллерам нашей сети. Тут тоже есть проблема. Представим, что у нас три контроллера домена. Редактируем объект на первом, и он, конечно же, должен уведомить об изменениях другие контроллеры. Они забрали эти изменения, и тут же второй контроллер пытается эти же изменения впихнуть обратно нам, или на третий домен, который уже забрал изменения. Что делать в этом случае? Все очень просто — у нас же есть версия изменений, и по ней можно узнать, нужно забирать запись или она уже реплицирована.

Эта проблема частично решается и тем, что репликация может пройти не дальше трех контроллеров. Если сервер получил изменения третьим, то дальше он уже никому его передавать не будет. Передача репликации по цепочке происходит, только если контроллер получил новую версию объекта первым или вторым.

➔ **репликация AD через 56к.** Реплицировать данные каждые 15 минут удобно и приятно, но только в том случае, если все контроллеры домена связаны между собой высокоскоростным соединением. А что если два контроллера находятся в другом районе или деревне, где они могут быть подключены к общей сети только по DialUp? В этом случае трафик репликации может отнять слишком много ресурсов, и полосы пропускания не хватит на решение других задач.

Чтобы этого избежать, можно, и даже нужно разделить эти серверы на отдельные сайты. Все контроллеры, подключенные по высокоскоростной связи, поместить в один сайт, а два удаленных — в другой сайт. Внутри сайтов репликация может происходить по правилам, установленным по умолчанию, а вот между сайтами можно настроить обмен так, чтобы не перегрузить полосу и оставить ее для передачи более важных данных. Такое распределение ты без проблем сможешь настроить с помощью такой оснастки как AD Sites and Services.

В качестве возможных вариантов сохранения трафика в technet от MS предлагаются несколько вариантов:

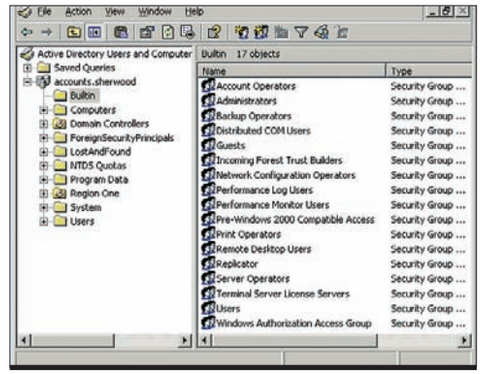
— РЕПЛИКАЦИИ ДАННЫХ ПО НОЧАМ;

— РЕПЛИКАЦИИ В ОБЕДЕННЫЕ ПЕРЕРЫВЫ;

— РЕПЛИКАЦИИ С БОЛЬШИМИ ПРОМЕЖУТКАМИ ВРЕМЕНИ.

Мне импонируют первые два варианта, особенно, если сайты находятся в одной временной зоне.

➔ **еще о репликации AD.** Если хочешь узнать больше о репликации в Acive Directory, и нет проблем с английским, то рекомендую скачать материал по следующей ссылке: **www.certmag.com/bookshelf/C0617953.pdf**. Это 92 страницы полезного и халявного чтива. Если и этого мало, то бегом на technet от Microsoft. Там информация изложена не так удобно и последовательно, но хороших рекомендаций очень много.

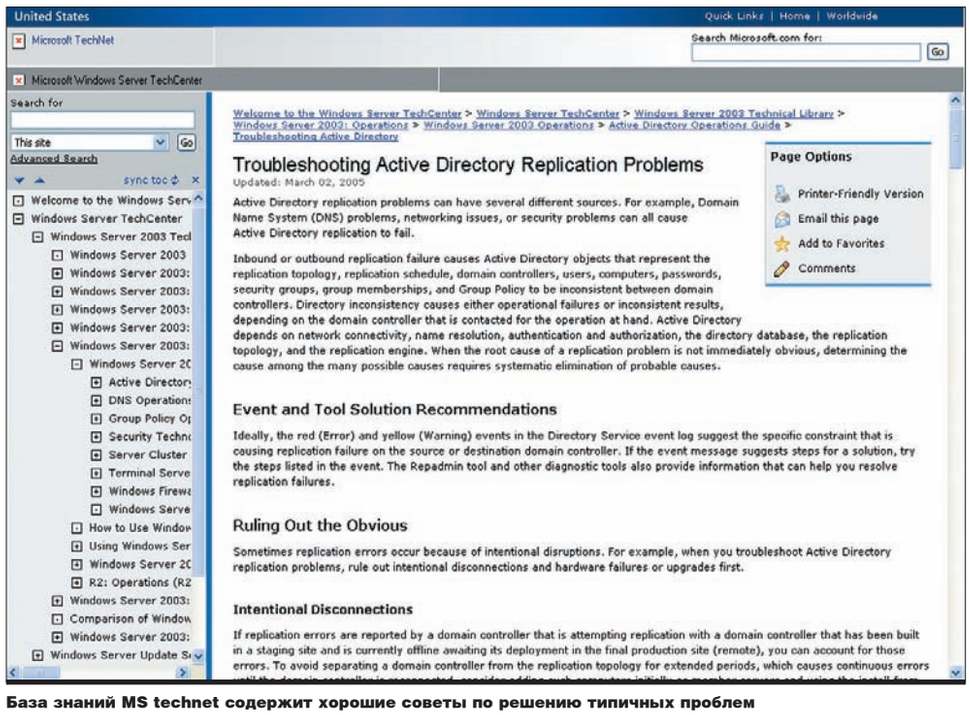


Оснастка User and Computers для настройки Active Directory

По Active Directory, и репликации в частности, могу посоветовать сайт **only4gurus.com** и конкретно ссылочку — **http://www.only4gurus.com/v3/sitemap_active_directory.shtml**. По репликации здесь можно найти хорошие презентации, рисунки которых были взяты за основу данной статьи. Я лишь перевел эти рисунки на родной русский и немного подкорректировал, чтобы они были нагляднее.

➔ **итого.** Надеюсь, читатели убедились, что репликация — это не просто синхронизация, а более продвинутый и интеллектуальный шаг вперед. При правильном подходе этот шаг будет большим. Если ты хорошо разберешься с этой темой, то без проблем сможешь сделать ручную репликацию там, где ее нет изначально. Ведь не во всех базах данных реализована такая возможность.

За кадром данной статьи осталась очень интересная тема — репликация Exchange-сервера. У нее очень много общего с Active Directory и SQL Server, но есть и интересные нюансы **C**



База знаний MS technet содержит хорошие советы по решению типичных проблем

сетевое законодательство

ПЛАНИРОВАНИЕ СЕТИ — ЭТО ПРОСТО!

МНОГИЕ СЧИТАЮТ, ЧТО ПРИ СОЗДАНИИ СЕТИ ДОСТАТОЧНО ВЗЯТЬ ОБОРУДОВАНИЕ И ПРОСТО СОЕДИНИТЬ С НИМ ВСЕ КОМПЬЮТЕРЫ. КАК БЫ НИ ТАК!

ФЛЕНОВ МИХАИЛ AKA HORRIFIC
{www.vr-online.ru}

→ **базовый компонент.** Для домашней сети в качестве базового компонента может использоваться или хаб (концентратор), или коммутатор (свитч). Отстой типа коаксиального кабеля рассматривать не будем, потому что из-за своих ограничений и неудобств соответствующий разъем уже сложно встретить в сетевых картах, да и скорость связи ограничена всего 10 мегабайтами.

На мой взгляд, хабы тоже устарели и стоят не намного дешевле коммутатора, но, на практике, их используют, и очень часто. Поэтому эту тему мы затронем, но везде, где на схемах будет указан хаб, можно смело заменять его на коммутатор, и будет тебе счастье. Если у тебя нет старых хабов, то и не используй их, а сразу закупай коммутаторы: благо у них цена не намного выше, и сейчас можно позволить себе эту железку.

Хочу сразу заметить, что, планируя сеть на картах в 100 мегабит и используя при этом хаб, скорость скорее всего будет 10 мегабит. Большинство хабов не могут работать быстрее. Скорости 10 и 100 — это идеал, которого на практике нереально добиться даже с коммутаторами, но нужно стремиться к лучшему!

Выбирая оборудование, я предпочитаю стоечные решения. Обтекаемые коробки выглядят лучше, но стоечное оборудование можно будет со временем убрать в шкаф, объединить в стойку и т.д.

➔ **и ничего лишнего.** Лишнего кабеля не бывает никогда. Для того, чтобы обезопасить себя от возможных переездов и нехватки кабеля, очень часто его отрезают с запасом. Действительно, никто не хочет перекладывать все заново, если не хватит одного метра до компьютера. Такие люди, наверное, не знают о существовании розеток, которые можно использовать в качестве переходников или вместо скруток для удлинения кабеля.

Получается, что нет смысла оставлять в запасе более 1 метра кабеля. Если наступит день, и этого запаса не хватит, всегда возможно удлинить кабель с помощью установки розетки. Это будет намного удобнее и красивее. Я вообще рекомендую всегда использовать розетки возле каждого рабочего места, но об этом мы еще поговорим.

Если ты все же решился оставить небольшой запас длинной в 15 метров, то никогда не скручивай его на стороне пользовательского компьютера. Лучше отвести для этого НЗ-ящичек на стороне коммутатора. Если что — можно всегда подтянуть кабель, зато он не будет валяться мотками под каждым столом.

➔ **где тянуть кабель?** Вечный вопрос! Очень часто встречаю сети, где кабель протягивают над потолком и к каждому рабочему месту спускают его в кабелегонах. Да, такое решение можно назвать хорошим с эстетической точки зрения, когда в помещении подвесной потолок, и за него можно спрятать все скрутки и даже хабы, но с точки зрения сопровождения такое решение неудачно. Простая перестановка мебели, и ты будешь в шоке, особенно, если кабели обрезаны под самый корешок, т.е. абсолютно без запаса. В этом случае придется выбирать одно из двух:

[1] ПЕРЕНОСИТЬ КАБЕЛЕГОН. ЭТОТ ВАРИАНТ ХОРОШ, ЕСЛИ КАБЕЛЕГОН НЕ НАГЛУХО ПРИКРЕПЛЕН К СТЕНКЕ, И ЕГО ЛЕГКО ОТКЛЕИТЬ И ПЕРЕНЕСТИ НА НОВОЕ МЕСТО.

[2] ОСТАВЛЯТЬ КАБЕЛЕГОН НА РОДИНЕ, А ВДОЛЬ ПОЛА ИЛИ ПЛИНТУСА ВЫТЯГИВАТЬ ОТКРЫТЫЙ (МОЖНО ЗАКРЫТЬ ВСЕ ТЕМ ЖЕ КАБЕЛЕГОНОМ) КАБЕЛЬ.

Всех этих проблем можно избежать, если протянуть кабель внизу стен. Если уж очень сильно хочется увести его под потолок, то стоит ограничиться этим в одном углу.

➔ **кабелегоны.** Не стоит искать в каталогах солидных фирм названия «кабелегон», потому что по-научному они называются кабельными каналами. Это такая штука, в которую укладывают кабели, чтобы они не мешались, не болтались, и все выглядело тип-топ.

Существует масса разновидностей кабельных каналов, и они отличаются по качеству материала, ширине, красоте, цвету, запаху и т.д. Самые лучшие каналы, с которыми мне приходилось работать — производства французской фирмы Legrand. Вот тут действительно ребята продумали все до мелочей, и в этой продукции придраться не к чему. Правда и стоит такой кабелегончик минимум в два раза дороже российского «Made in «Sosednii Garaj».

При выборе размера я бы порекомендовал широкий канал. Единственный его недостаток, с которым мне пришлось столкнуться при данном решении — однажды в кабелегон залезла мышка. Как она туда проникла — ума не приложу. Это животное не только перегрызло кабель, но и отбросило лапки, благодаря чему запах в кабинете был нездоровым. Пришлось разбирать всю конструкцию, чтобы заменить кабель и похоронить вредителя со всеми почестями. Но не стоит обращать внимание на единичный случай проникновения мышки в кабелегон. Я не думаю, что каждый встретится с подобным в своей практике. (Не думаю, что проблема преувеличена — лично у меня дома крыса перегрызла сливной шланг стиральной машинки. Грызуны — очевидный враг компьютерщика! — прим. Лозовского).

У широкого кабельного канала намного больше преимуществ:

— КАБЕЛИ ЛЕЖАТ СВОБОДНО И ДЫШАТ ЛУЧШЕ, ЧЕМ В ПАМПЕРСАХ;

— ЕСЛИ ПРЕДСТОИТ РАСШИРЕНИЕ, ТО Я УВЕРЕН, ЧТО НОВОМУ КАБЕЛЮ ВСЕГДА НАЙДЕТСЯ МЕСТО, И КЛАСТЬ ДОПОЛНИТЕЛЬНЫЕ КАБЕЛЕГОНЫ НЕ ПРИДЕТСЯ;

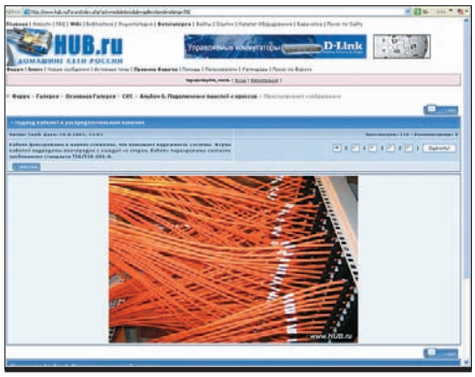
— В ТАКОЙ КАНАЛЬЧИК МОЖНО ВПИХНУТЬ НЕ ТОЛЬКО UTP, НО И КАБЕЛИ НА 220, ТЕЛЕФОННЫЙ ШНУР И ЕЩЕ МНОГО ЧЕГО ИНТЕРЕСНОГО.

➔ **опустить ниже плинтуса.** Если тянуть кабель вдоль стен, то лучше всего делать это на 15-20 сантиметров выше плинтуса. Если кабелегон узкий, то разрезы для вывода кабелей лучше делать внизу. В этом случае, если предстоит переезд на 10 метров в сторону — сделаем новую дырку внизу кабелегона и выведем конец кабеля туда. Старую дырку даже заделывать не нужно, потому что она внизу, и видно ее не будет.

➔ **розетки.** Не стоит экономить на таком удобном аксессуаре, как розетка для RJ-45 кабеля. Да, один экземпляр такого аксессуара хорошего качества стоит около 300 руб., но зато какая эстетичность и удобство от использования — деньгами это не оценить! Можно ограничиться не экранированной розеткой от популярной фирмы NoName за 50 руб. В большинстве случаев ее будет достаточно.

Чем примечательны розетки? Допустим, что мы столкнулись с классической задачей перемещения стола. В этом случае не нужно удлинять весь кабель от коммутатора до компьютера и перекоммутировать весь этаж, достаточно взять более длинный кабель от розетки до компьютера, и никаких проблем.

Дорогой, но очень хороший поставщик фурнитуры решений для сетевика



Обязательно загляни на hub.ru

Тип розетки зависит от того, какой кабелегон мы используем. Если он узкий, то розетка должна быть в виде отдельной коробки, которую можно закрепить немного ниже кабелегона. В принципе, такое решение достаточно удобно и приемлемо.

Но более эстетичным будет использование широкого кабелегона. Специально для таких решений есть розетки, которые вписываются прямо в сам кабелегон и выглядят более чем достойно. Если не стесняют финансы, то лучше выбрать это решение. К тому же, чаще всего такие розетки обладают очень хорошим свойством — разъем закрывается, поэтому, если розетка не используется, то разъем не пылится. Не забывай, что для того, чтобы попки были сухими и чистыми, их не обязательно сушить и чистить, их просто нужно содержать в чистоте и не оставлять открытыми.

➜ **расположение компьютеров.** По поводу расположения компьютеров рекомендовать что-то бесполезно. В домашних условиях железный друг станет там, где есть место или удобно работать. На работе мы стремимся установить монитор так, чтобы его не видел начальник и проходящие мимо зеваки.

Сетевое оборудование чаще всего устанавливают там, где есть розетка в 220 Вольт, где есть место, и где его удобно обслуживать. Все эти три фактора достаточно важные, но все же не стоит забывать о расширяемости. Длина одного сегмента кабеля не бесконечна. Я интересуюсь сетями и регулярно просматриваю то, что рекомендуют производители оборудования при построении сетей. Если объединить личный опыт и рекомендации железячников, то можно выделить следующие решения:

1. Сеть для дома. Домашняя сеть чаще всего строится в многоэтажных домах, где на этаже находятся четыре квартиры. Получается, что строительство должно быть вертикальным. Над каждым подъездом (в Питере почему-то подъезды называют парадными) устанавливаем по коммутатору, и все компьютеры этого подъезда подключаем к нему. Даже если где-то устанавливается два компьютера, не стоит подключать их из другого подъезда, так как в последствии перекоммутация может отнять больше усилий и доставить больше проблем. Лучше потратиться на лишний коммутатор.
2. Офисная сеть. Здесь компьютеры чаще всего распределены горизонтально. В офисных зданиях на одном этаже может быть по 20 кабинетов, и в каждом из них — по 5 компьютеров. Здесь логичнее строить сеть горизонтально. На каждом этаже устанавливаем по коммутатору и соединяем все компьютеры этажа. Вот тут серьезный вопрос с расположением коммутатора. Идеальный вариант — расположить сетевое оборудование в центре этажа, чтобы кабели до самой дальней точки не были слишком длинными. Если компания располагается на нескольких этажах, то чаще всего расположить сетевое оборудование в центре не удается. В этом случае можно использовать два коммутатора в противоположных точках этажа.

Это наиболее распространенные решения для простых офисов и домов. Если ты собираешься осетенять такую организацию, как Газпром, то тут уже структура намного сложнее, и одними коммутаторами не отделаешься. Возможно, что придется внедрять маршрутизаторы и другое оборудование.

➜ **слабое звено.** Как известно, скорость связи определяется скоростью самого слабого звена. Если компьютеров много, а сервер один, то скорость обмена информацией с сервером будет зависеть от количества пользователей, одновременно работающих с этим сервером. Скорость работы коммутаторов и их пропускную способность в данном случае учитывать не будем, к тому же, производители утверждают, что их оборудование способно нормально работать при максимальной нагрузке и даже с большим запасом.

Теперь представим, что к одному серверу обращаются сразу 100 компьютеров по каналу 10 мегабит. Если равномерно разделить скорость канала на всех, то каждый будет работать на 100 килобит. А если учесть, что 10 мегабит — это идеальная скорость, которая на практике недостижима, то реальная скорость будет еще ниже.

Что делать в этом случае? Можно обновить оборудование до гигабитного, но такие сетевые карты стоят не дешево. Обновление 100 компьютеров плюс сетевого оборудования влетит в копе-

SPECIAL ОБЗОР

MEDIUM

UNIX: РУКОВОДСТВО СИСТЕМНОГО АДМИНИСТРАТОРА

М.: ДМК Пресс, 2005
Уэйнгроу К./ 416 страниц
Разумная цена: 160 р.

Предполагается, что ты уже знаком с основными функциями и особенностями системы. Это не учебник по UNIX, но книга доступно рассказывает о том, как автоматизировать рутинную работу и создать командные файлы, которые повысят производительность. В UNIX так много команд, что для выполнения одной задачи очень часто можно пойти разными путями. В книге показаны нестандартные и новые идеи, позволяющие расширить и систематизировать использование разных функций. Рассмотренные примеры были протестированы в разных версиях системы, так что проблем совместимости быть не должно.

HARD

УСТАНОВКА И УПРАВЛЕНИЕ MICROSOFT EXCHANGE SERVER 2003. УЧЕБНЫЙ КУРС MICROSOFT

М.: Издательско-торговый дом «Русская редакция», 2005/ Джесси М. Торрес
384 страницы
Разумная цена: 205 р.

Сценарии — быстрый способ заставить компьютер выполнять набор инструкций. В книге ты найдешь много полезных сценариев, которые помогут тебе выполнять множество трудоемких и часто встречающихся задач при администрировании Windows Server 2003, XP, 2000, NT и 98. Все сценарии написаны с помощью трех инструментов: командная строка, утилита KiXtart и сервер сценариев Windows Script Host (WSH). Поскольку многие сценарии достаточно объемны, автор поместил их на своем сайте — **www.jesseweb.com.**

Ты научишься работать с альтернативными методами: ScriptIt или AutoIt. Книга не страдает общей болезнью других аналогичных, и все примеры реально пригодятся на практике.

ечку. Но есть выход дешевле: можно заменить только коммутаторы и сетевую карту сервера. В этом случае связь между сервером и коммутатором будет гигабитной, а между коммутатором и компьютерами — только 10 или 100 мегабит. Тогда 100 компьютеров смогут работать со скоростью в мегабит. Обновление сетевых карт клиентских компьютеров не даст большого прироста в производительности, потому что если с сервером работает хотя бы 10 человек, более 100 мегабит вы не получите.

Гигабитная карта в клиентском компьютере в любом случае лучше, чем в 100 мегабит, но затраты на ее приобретение не будут оправданы.

➔ **серверы.** Я противник решений «все в одном», когда один сервер выполняет множество задач. Прошли те времена, когда серверы стоили дорого, а программное обеспечение в нашей стране не стоило вообще ничего:). А если серьезно, то если сервер одновременно является базой данных, WEB-сервером, почтовиком и т.д., то о масштабируемости такого решения можно только мечтать, да и уровень безопасности очень низок. Если появится ошибка в одном из сервисов, то хакеру, проникнувшему на сервер, будет доступно все. Если так прикинуть, то наибольших ресурсов требует только база данных. WEB-сервер и почтовик под управлением Linux вполне способны работать даже на стандартном компьютере, если конечно у тебя не хостится google или Microsoft. Корпоративному WEB-серверу будет достаточно второго пентиума или даже первого Pentium 100.

Если каждый сервис разнесен по физическим серверам, то взломав WEB-сервер, хакер не получит доступа к корпоративной базе данных.

➔ **интернет.** Если ты решился выделить под каждую задачу свой сервер, то для сетевого экрана и проксика ты обязан выделить отдельную машину. Именно через нее будет происходить доступ в Сеть и обратно. Таким образом, чтобы взломать WEB-сервер, злоумышленнику придется сначала пройти через сетевой экран. Если этот экран правильно настроен и не дозволяет ничего лишнего, то проникновение сильно усложняется.

Чтобы проще было настраивать политику безопасности на сетевом экране, всегда действуй от запрета. Если WEB-сервер используется только для корпоративных нужд, он не должен быть виден из интернета. Если у тебя два WEB-сервера — публичный и корпоративный (или просто для внутреннего использования), то их лучше разнести по разным машинам. Таким способом проще будет управлять политиками и проще будет следить за каждым из них.

Если к внутреннему серванту запрещен доступ извне, то это не значит, что его не нужно обновлять. Это самая распространенная ошибка. Если хакер получит доступ к одной из машин сети, то через нее он проникнет на запрещенный сервер. Обновлять софт и латать дыры нужно абсолютно на всех серверах. Тем более что даже ближайший сосед может оказаться злым хакером. Никогда и никому не доверяй.

➔ **итого.** Заморочки есть везде и всегда, а возиться с кабелями — занятие не из самых интересных, по крайней мере, для меня. Не люблю перекладывать кабели и что-то переделывать: интереснее строить с нуля и делать это хорошо. Недаром Intel и Del вовсю продвигают свои идеи беспроводных соединений. С каждым днем к этой идее присоединяется все больше производителей и офисов. Мы уже сидим на WiFi, который избавляет нас от лишних розеток и кабелей, а ты? Но это уже совсем другая история. Сначала нужно преодолеть фактор страха перед незащищенностью старых протоколов WiFi C

царь хостинг

АДМИНИСТРИРОВАНИЕ ХОСТИНГА — ОТ «А» ДО «Я»

НА СЕГОДНЯШНИЙ ДЕНЬ СИТУАЦИЯ НА ХОСТИНГОВОМ РЫНКЕ РУНЕТА НАПОМИНАЕТ НОВОГОДНЮЮ ЯРМАРКУ: ОГРОМНЫЙ ВЫБОР ТАРИФНЫХ ПЛАНОВ, ШИРОКИЙ АССОРТИМЕНТ РАЗНООБРАЗНЫХ УСЛУГ. ЛОГИЧНО БУДЕТ ПРЕДПОЛОЖИТЬ, ЧТО ЭТО ОБЪЯСНЯЕТСЯ ДОСТУПНОСТЬЮ ТЕХНОЛОГИИ, ОДНАКО ЭТО НЕ СОВСЕМ ТАК. ДЕЛО В ТОМ, ЧТО СУЩЕСТВУЕТ МНОЖЕСТВО ГОТОВЫХ ХОСТИНГОВЫХ РЕШЕНИЙ, УСТАНОВИТЬ КОТОРЫЕ НЕ СОСТАВИТ ТРУДА — БЫЛИ БЫ ДЕНЬГИ. СЕЙЧАС МЫ ПОСТРОИМ СВОЙ ХОСТИНГ, — С САМОГО НАЧАЛА, И НЕ ПРИБЕГАЯ К ПЛАТНЫМ УСТАНОВОЧНЫМ ПАКЕТАМ ВРОДЕ CPANEL

MIF
{root@securitylab.co.il}

→ **выбор ОС**. На самом деле вариантов не так уж и много. Windows, Linux, BSD, Solaris. У каждой из этих операционок в плане реализации хостинга есть свои плюсы и минусы. Windows дает нам поддержку ASP и еще некоторых MS-only технологий и визуально несложное администрирование, но, в то же время, накладывает существенные ограничения на производительность и увеличивает наши затраты. Linux — достойная кандидатура, но обилие багов в ядре и наличие в паблике вполне рабочих эксплойтов стало уже закономерностью. Solaris — хорошая система, однако платная; встанет не на любое железо, да и с некоторым софтом возникают траблы. Остается BSD. Из BSD я лучше всего знаю FreeBSD, поэтому строить наш хостинг мы будем на примере этой ОС.

→ **нелегкий выбор.** Теперь необходимо сделать выбор версии операционной системы. На сегодняшний день существует всего три основных ветки FreeBSD:

— ВЕРСИЯ 4.* — OLD STABLE (СТАРАЯ СТАБИЛЬНАЯ ВЕТКА). ПОСЛЕДНЯЯ ВЕРСИЯ — 4.11. — ПО СУТИ, ОНА УЖЕ НЕ ПОДДЕРЖИВАЕТСЯ.

— ВЕРСИЯ 5.* — LEGACY PRODUCTION (СТАРАЯ PRODUCTION-ВЕТКА). ПОСЛЕДНЯЯ (НА МОМЕНТ НАПИСАНИЯ СТАТЬИ)

```
ACPI APIC Table: <IntelR AWRDACPI>
Timecounter "i8254" frequency 1193182 Hz quality 0
CPU: Intel(R) Pentium(R) 4 CPU 2.80GHz (2806.37-MHz 686-class CPU)
  Origin = "GenuineIntel"  Id = 0xf33  Stepping = 3
  Features=0xbfebfbff<FPU,VME,DE,PSE,TSC,MSR,PAE,MCE,CX8,APIC,SEP,MTRR,PGE,MCA,CMOV,PAT,PSE36,CLFLUSH,DTS,ACPI,MMX,FXSR,SSE,SSE2,SS,HTT,TM,PBE>
  Hyperthreading: 2 logical CPUs
real memory  = 1073676288 (1023 MB)
avail memory = 1045311488 (996 MB)
ioapic0: Changing APIC ID to 2
ioapic0 <Version 2.0> irqs 0-23 on motherboard
npx0: <math processor> on motherboard
npx0: INT 16 interface
acpi0: <IntelR AWRDACPI> on motherboard
acpi0: Power Button (fixed)
Timecounter "ACPI-fast" frequency 3579545 Hz quality 1000
acpi_timer0: <24-bit timer at 3.579545MHz> port 0x408-0x40b on acpi0
cpu0: <ACPI CPU> on acpi0
acpi_button0: <Power Button> on acpi0
pcib0: <ACPI Host-PCI bridge> port 0xcf8-0xcff on acpi0
pci0: <ACPI PCI bus> on pcib0
agp0: <Intel 82865 host to AGP bridge> mem 0xfb000000-0xfb7fffff at device 0.0 on pci0
pcib1: <PCI-PCI bridge> at device 1.0 on pci0
pci1: <PCI bus> on pcib1
pcib2: <ACPI PCI-PCI bridge> at device 30.0 on pci0
pci2: <ACPI PCI bus> on pcib2
atapci0: <Promise PDC20318 SATA150 controller> port 0x9800-0x987f,0x9400-0x940f,0x9000-0x903f mem 0xf9000000-0xf901ffff,0xf9020000-0xf9020fff irq 16 at device 4.0 on pci2
atapci0: failed: rid 0x20 is memory, requested 4
ata2: channel #0 on atapci0
ata3: channel #1 on atapci0
ata4: channel #2 on atapci0
ata5: channel #3 on atapci0
pci2: <display, VGA> at device 5.0 (no driver attached)
re0: <RealTek 8169S Single-chip Gigabit Ethernet> port 0xa000-0xa0ff mem 0xf9022000-0xf90220ff irq 23 at device 9.0 on pci2
miibus0: <MII bus> on re0
rgephy0: <RTL8169S/8110S media interface> on miibus0
rgephy0:  10baseT, 10baseT-FDX, 100baseTX, 100baseTX-FDX, 1000baseTX, 1000baseTX-FDX, auto
re0: Ethernet address: 00:40:f4:b1:0e:44
xl0: <3Com 3c905C-TX Fast Etherlink XL> port 0xa400-0xa47f mem 0xf9023000-0xf902307f irq 21 at device 10.0 on pci2
miibus1: <MII bus> on xl0
ukphy0: <Generic IEEE 802.3u media interface> on miibus1
ukphy0:  10baseT, 10baseT-FDX, 100baseTX, 100baseTX-FDX, auto
xl0: Ethernet address: 00:01:03:e0:5e:9f
Byte 2490
```

Вывод утилиты dmesg

ВЕРСИЯ — 5.4. СТАБИЛЬНЫЙ, ЗАРЕКОМЕНДОВАВШИЙ СЕБЯ РЕЛИЗ.

— ВЕРСИЯ 6.* — PRODUCTION (PRODUCTION-BETKA). РАЗРАБОТЧИКИ НЕОЖИДАННО СДЕЛАЛИ ПРЫЖОК С 5.4 ДО 6.0, НЕ ВНЕСЯ НИКАКИХ РЕВОЛЮЦИОННЫХ ИЗМЕНЕНИЙ. CHANGELOG 6.0 ДОВОЛЬНО ВЕСОМЫЙ, НО НА ПРАКТИКЕ — КРОМЕ НЕБОЛЬШОГО ПРИРОСТА ПРОИЗВОДИТЕЛЬНОСТИ НА SMP ЯДРАХ — НИЧЕГО НЕ ДАЕТ.

Итог: версия 4.* — уже практически мертва, в 6.* ожидается много изменений, а значит и сюрпризов. Как приятных, так и не очень. Кроме того, релиз 6.0 вышел относительно недавно, и в нем еще могут обнаружиться серьезные недочеты. Поэтому мы остановим свой выбор на 5.4. Собирать хостинговый сервер мы будем на тестовой машине — P4 2.8 Ghz, 512 DDR, 5x200 gb SATA RAID 0+1. Разумеется, если ты планируешь поднять крупный хостинг — стоит подумать о более шустром железе.

➔ **pre-install.** Я не буду рассказывать о том, как установить систему — это довольно не сложно, да и различной документации по этому поводу в Сети хватает. Я остановлюсь лишь на вещах, которые критически важны для нашего хостинга. Очень важно правильно разбить диск. Swap partition должен находиться как можно ближе к началу диска (физически), поэтому его нужно создавать сразу после /. Размер свопа принято рассчитывать по формуле:

```
Swap = количество оперативки * 2+20-30MB
```

Я разбил диск следующим образом:

— / — 512 МБ
— SWAP — 1124 МБ
— /TMP — 512 МБ
— /USR — 30 ГБ
— /VAR — 30 ГБ
— /USR/HOME — ВСЕ ОСТАЛЬНОЕ, В МОЕМ СЛУЧАЕ — ПРИМЕРНО 130 ГБ.

При выборе установки обязательно поставь галочки у src, ports, linux, perl, compat4x.

➔ **the beginning.** Первым делом, после того как система загрузилась, проверяем, что нет никаких проблем с железом, установка прошла без сбоев, и система распознает все корректно:

```
# dmesg | more
# cat /var/log/messages
```

➔ **make.** Так как нам предстоит компилировать ядро и кучу разнообразного софта, то сначала необходимо оптимизировать процесс компиляции. Многие частенько не придают этому значения, забывая, что таким образом мы не только выигрываем время при сборке, но и оптимизируем все под наше железо и ОС. Идем в /etc/make.conf и там пишем:

Листинг файла make.conf

```
# Тип твоего процессора.
# Для AMD — athlon-mp, athlon-xp,
athlon-4, athlon-tbird, athlon, k6-3,
k6-2, k6, k5.
# Для Intel — p4, p3, p2, i686,
i586/mmx, i586, i486, i386.
CPUTYPE?=p4
CPUTYPE=p4
# Совместимость с BSD 4.X
COMPAT4X=true
# Указываем дополнительные флаги
CFLAGS=-O1 -pipe -march=pentium4 -mtune=pentium4
# Говорим, что флаги включать
обязательно
NO_CPU_CFLAGS=false
NO_CPU_COPTFLAGS=false
# Отключаем сборку ненужных
библиотек и софта
MAKE_KERBEROS4=false
MAKE_KERBEROS5=false
NO_BIND=true
NO_SENDMAIL=true
NO_GAMES=true
# Настройки Perl
PERL_VER=5.8.8
PERL_VERSION=5.8.8
PERL_ARCH=mach
NOPERL=no
WITH_PERL=yes
WITHOUT_PERL=no
# Решаем проблемы с портами
FORCE_PKG_REGISTER=yes
```

➔ **update.** В наш век разгула скриптКидисов и прочей нечисти крайне важно держать систему и софт обновленными. Исходники 5.4 обновляются очень редко, только в случае, если обнаружилась критическая уязвимость, а вот порты и документация — довольно часто. Сразу оговорюсь: в FreeBSD все надо ставить из портов. Это очень важно, поскольку в портах лежат уже адаптированные под нужную ось проги со всеми необходимыми патчами. Идем в /usr/ports/net/cvsup-without-gui и собираем порт:

```
# make install clean
```

После окончания процесса сборки нужно написать конфиг для cvsup. Идем в /etc, открываем там файл cvsupfile (я обычно переименовываю в cvsup.conf):

```
# Сервер, с которым будем синхронизироваться.
*default host=cvsup.FreeBSD.org
# Куда будем складывать свеженькое:
*default base=/usr
*default prefix=/usr
*default release=cvs
```

```
# Тег ветки нашей системы
*default tag=RELENG_5_4
*default delete use-rel-suffix
# Используем сжатие при передаче данных
*default compress
# Что будем синхронизировать?
# Все исходники
src-all
*default tag=RELENG_5_4
*default tag=.
# Все порты
ports-all
# Весь RTFM
doc-all
```

После сборки cvsup-without-gui в /usr/local/bin у тебя появился бинарник cvsup. Запускать его надо со следующими параметрами:

```
/usr/local/bin/cvsup -g -L 2 -z
/путь/к/конфигу
```

Согласись, держать команды в памяти неудобно. Поэтому мы напишем скрипт и автоматизируем процесс обновлений. Создаем файл cvs_up:

```
# touch cvs_up
```

Открываем его любым редактором и пишем такой скрипт:

Листинг скрипта cvs_up

```
#!/bin/sh
echo "Starting CVSup..."
case "$1" in
-t)
/usr/sbin/ntpdate -v ru.pool.ntp.org
;;
-q)
/usr/sbin/ntpdate -v ru.pool.ntp.org
2>&1 > /dev/null
/usr/local/bin/cvsup -g -L 2 -z
/etc/cvsup.conf 2>&1 > /dev/null
;;
*)
/usr/local/bin/cvsup -g -L 2 -z
/etc/cvsup.conf
;;
esac
echo "Packages needed to update:"
/usr/sbin/pkg_version -v |grep '<'
exit 0
```

Кладем скрипт в нужное место, выставляем chmod и chown:

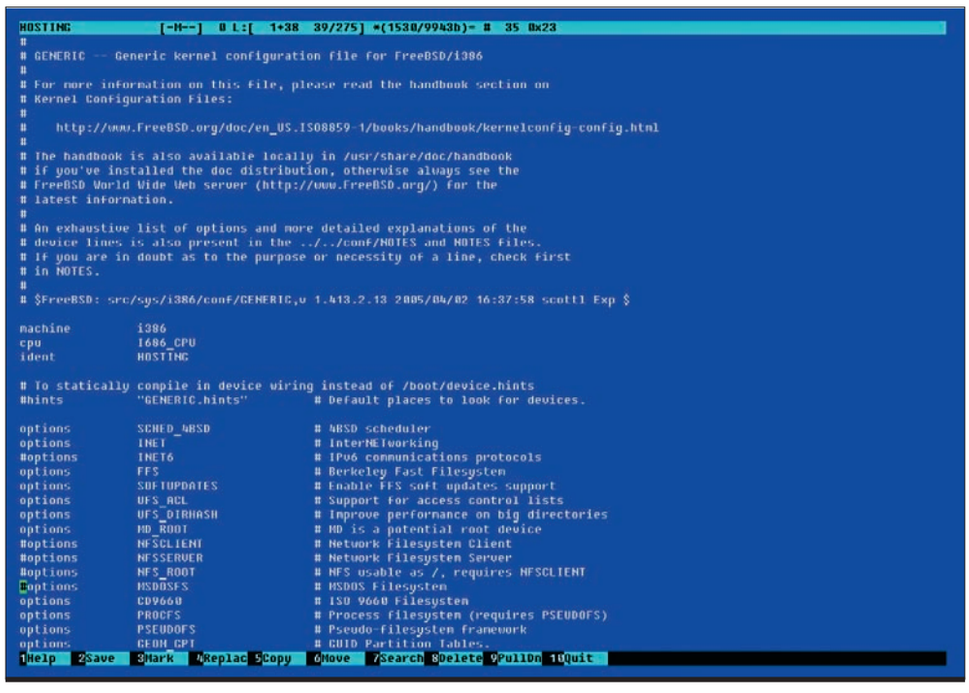
```
# mv cvs_up /usr/local/sbin/cvs_up
# chown root:wheel /usr/
local/sbin/cvs_up
# chmod 0700 /usr/local/sbin/cvs_up
```

Теперь, для того чтобы синхронизировать исходники, порты, документацию и даже время на сервере, у нас есть один скрипт, который после синхронизации еще и покажет, что обновилось. Как видишь, его легко можно запускать с флагом –q, который перенаправит всю отчетность скрипта в /dev/null.

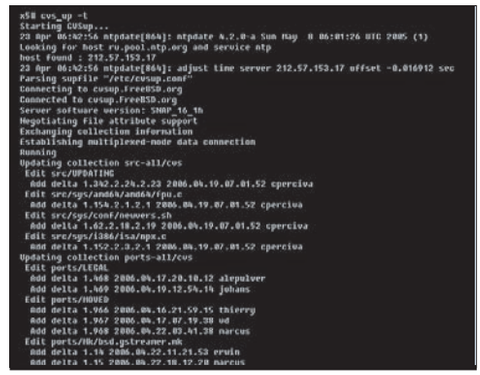
Нам также понадобится утилита, которая займется апгрейдом довольно активно обновляющихся портов. Ставим portupgrade:

```
# cd /usr/ports/sysutils/portupgrade
# make install clean
```

И запускаем наш скрипт. По окончании своей работы скрипт выдаст отчет о том, какие порты требуют обновлений. Обновить софтину или библиотеку очень просто:



Не так страшен кернел, как его конфиг



Наш скрипт в работе

```
# portupgrade порт1 порт2 ... порт22
```

Если хочешь, — можешь прописать этот скрипт в cron на выполнение раз в сутки, желательно ночью, или в то время, когда нагрузка на твой сервер минимальна. Например так:

```
0 4 * * * /usr/local/sbin/cvs_up
>/dev/null 2>&1
```

Лично я предпочитаю запускать его вручную, так как cvsup сервер часто не пускает с первого раза, и скрипт остается висеть в процессах, что не есть хорошо.

```
<Kernel::About>
```

Пора приступать к самой важной части настройки системы — к ядру. При инсталле системы автоматически устанавливается ядро GENERIC. В нем включена поддержка устройств, необходимых для старта системы на любой конфигурации. Оптимизировав ядро под свою систему, мы убираем поддержку ненужных устройств и функций, уменьшая таким образом время загрузки и, что еще важнее, улучшая производительность системы в целом. Давай посмотрим, сколько весит ядро до оптимизации:

```
# ll /boot/kernel/kernel
-r-xr-xr-x 1 root wheel 5940286 Feb 23
2004 /boot/kernel/kernel
#
```

Почти шесть мегабайт — для *BSD это очень много, можешь себе представить. Для сборки своего ядра нам понадобятся исходники (src) системы. Если ты не послушал моей рекомендации и не сделал этого при установке, то вставь диск с операционкой и установи их, используя /stand/sysinstall. Не забудь после этого обновить исходники скриптом cvs_up.

```
[Kernel::Config>]
```

Конфиги ядра лежат в папке /sys/<архитектура>/conf. Если у тебя обычный PC, в /sys/i386/conf. Заходи туда, найди там файл GENERIC и скопируй его с другим названием. Да-да, именно скопируй. Если что-то вдруг пойдет не так как надо, у нас останется рабочий конфиг. Итак, копируем:

```
# cd /sys/i386/conf
# cp GENERIC HOSTING
```

Теперь открываем конфиг HOSTING любимым редактором. Опции настройки ядра указаны в виде устройств (device) и расширений/модулей. Все строчки, которые начинаются с символа «#» — закомментированы, а проще говоря, они не будут учтены при сборке нового ядра. Наша задача — закомментировать ненужные нам строчки, оставив только необходимое (рекомендуется ни в коем случае не удалять, а именно комментировать строки конфига, иначе потом придется долго вспоминать «как же называлась эта опция, после удаления которой ничего не собирается?..» — прим. автора).

Конфиг ядра составляем по принципу «все, что не критично — не нужно». Вряд ли хостинговому серверу так сильно необходимы USB-сканер, десяток драйверов к Wi-Fi карточкам и PCIMCA. Некоторые устройства имеют статус обязательных — без них ядро просто не соберется. Они помечены комментарием required. После того, как ты закомментировал все ненужное, пришло время добавить недостающее:

```
Options IPFIREWALL     # Включаем ipfw
Options IPFIREWALL_VERBOSE
Options IPFIREWALL_VERBOSE_LIMIT=1000
Options TCP_DROP_SYNFIN    # Запрещаем
SYN/FIN пакеты
Options ACCEPT_FILTER_DATA   # Включаем
accept фильтры
Options ACCEPT_FILTER_HTTP
```

Сохраняем конфиг и собираем ядро:

```
# cd /usr/src
# make buildkernel KERNCONF=HOSTING
# make installkernel KERNCONF=HOSTING
```

Все, после ребута загрузится свежесобранное ядро. Но ребутиться мы пока не будем — нам надо отредактировать /etc/rc.conf:

```
# Поддержка линуксовых бинариков
linux_enable="YES"
# Запускаем sshd
sshd_enable="YES"
# Вырубаем лишнее
usbd_enable="NO"
sendmail_enable="NONE"
inetd_enable="NO"
# Включаем сислог
syslogd_enable="YES"
syslogd_flags="-ss"
# Очищаем /tmp при старте системы
clear_tmp_enable="YES"
# Включаем фаервол
firewall_enable="YES"
firewall_script="/etc/rc.firewall"
firewall_type="client"
firewall_quiet="NO"
```

Все. Наша система настроена и готова к бою. Если ты работаешь удаленно, пропиши в /etc/rc.firewall разрешающее правило для себя, иначе после ребута потеряется доступ к машине. Если у тебя локальная консоль, — смело идем в ребут:

```
# init 6
```

Как только сервер поднялся, нужно еще раз проверить, что не возникло проблем с железом, софт не плевался ошибками, и вообще все в шоколаде. Помнишь, мы смотрели размер ядра до пересборки? Посмотрим еще раз:

```
# ll /boot/kernel/kernel
-r-xr-xr-x 1 root wheel 2675196 Mar 10
04:10 /boot/kernel/kernel
#
```

2.6 мегабайт. Совсем другое дело.

➔ **intro::Services.** Итак, в первую очередь важно определиться с тем, какие именно сервисы наш хостинг будет предоставлять клиентам. Основные вещи, которые любой хостинг предоставить обязан — это Web + PHP/Perl, FTP, БД и статистику посещений сайта. Многие хостеры подходят к вопросу поднятия хостинга просто: купили Cpanel, запустили install.sh и продаем аккаунты юзерам. Мы же соберем свой собственный хостинг, с самого начала и до победного конца.

➔ **выбор софта.** Сразу оговорюсь, что предпочитаю использовать стабильный и надежный софт, нежели новый и крутой. Нам важна стабильность и функциональность. А всякие, грубо говоря, свистелки и перделки мы оставим скриптКидисам на разнос. Итак, для www, я думаю, не возникнет сомнений — Apache. Ветка 2.* еще довольно сыровата, да и почти под каждую новую версию двойки появлялся бронебойный эксплойт, зачастую даже в паблике. Использовать будем проверенный временем 1.3. FTP — тут выбор не столь однозначен, есть много разных FTPd, но мы остановимся на pure-ftpd. У него удобный и понятный конфиг, отлично реализована работа с виртуальными юзерами, достаточная функциональность и много других достоинств, о которых — ниже. БД, разумеется, MySQL. И опять мы берем самую стабильную версию — 4.0.*. Статистика: можно взять Webalaizer, но лично я предпочитаю AwStats. Его отчетность намного лучше выглядит, интуитивно более понятна, да и подробности анализа ему не занимать.

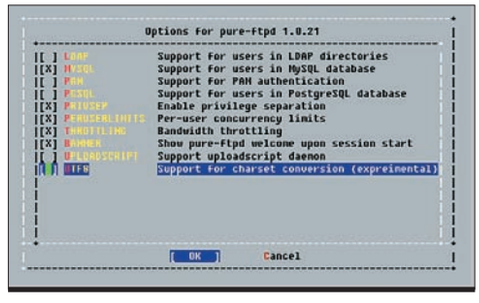
УСЛОВИМСЯ, ЧТО МЫ ИСПОЛЬЗУЕМ СЛЕДУЮЩУЮ СТРУКТУРУ ДИРЕКТОРИЙ:

- /USR/HOME/ЮЗЕР — ДОМАШНЯЯ ДИРА ЮЗЕРА;
- /USR/HOME/ЮЗЕР/WEB — РУТОВАЯ ВЕБ-ПАПКА ЮЗЕРА;
- /USR/HOME/ЮЗЕР/TMP — ТЕМП-ДИРА ЮЗЕРА;
- /USR/HOME/ЮЗЕР/CGI-BIN — CGI-BIN ЮЗЕРА;
- /ETC И /USR/LOCAL/ETC — ПАПКИ С КОНФИГАМИ;
- /ETC/AWSTATS — ПАПКА КОНФИГОВ СТАТИСТИКИ;
- /VAR/DB/AWSTATS — ПАПКА С БД СТАТИСТИКИ;
- /VAR/LOG/WWW — ПАПКА С ЛОГАМИ ВИРТУАЛЬНЫХ ХОСТОВ.

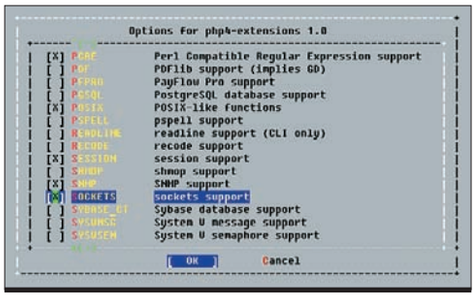
➔ **apache.** Кроме обычных клиентов с мега-порталами (привет VinT) и домашними страничками, услугами хостинга пользуются еще и множество коммерческих организаций, в частности, инет-магазины. Поэтому нам нужна возможность предоставлять им https. На сегодняшний день существуют две основные релизации SSL для Apache. Это Apache-ssl, поддерживаемый самой Apache Group и сторонняя разработка — mod_ssl. Последняя дает намного больше возможностей и намного активней поддерживается, поэтому используем ее. Итак, собираем Apache:

```
# cd /usr/ports/www/apache13-modssl
# make install clean
```

Наконец переходим к настройке. Основной конфиг Апача лежит в /usr/local/etc/apache и зовется httpd.conf. Конфиг совсем не маленький, поэтому я опишу здесь лишь самые основные и важные параметры (а полностью ты сможешь найти его на диске):



Опции pure-ftpd



Не забываем про опции php-extensions

```
# Запускаем сервер через inetd или
самостоятельным демоном, # inetd
у нас в системе выключен, так что выбор
невелик.
ServerType standalone
# Рутовая директория веб-сервера
ServerRoot "/usr/local"
# Таймаут соединений в секундах.
Timeout 300
# А вот об этом — поподробней.
KeepAlive — механизм, позволяющий,
не прерывая # соединения с сервером,
отправить ему несколько запросов.
Это позволяет
# экономить ресурсы за счет того,
что не создается новый процесс,
а на запросы
# отвечает уже существующий. Количество
запросов и таймаут указываются
# следующими опциями:
KeepAlive On
MaxKeepAliveRequests 100
KeepAliveTimeout 15
# Следующие три настройки сильно
зависят от загруженности веб-сервера. Они
# указывают на то, сколько серверов
минимум и максимум может быть загружено,
и сколько # процессов сервера запускать
при старте.
MinSpareServers 10
MaxSpareServers 70
StartServers 10
# Сколько клиентов может одновременно
обслуживать сервер
MaxClients 150
# Сколько запросов может одновременно
обрабатывать один процесс сервера
# (0 — не ограничено). Ноль ставить
не рекомендуется.
MaxRequestsPerChild 7000
```

Дальше у нас идут настройки Listen и Bind — тут ничего хитрого нет. А сразу за ними — список модулей, которые подгружает сервер. Смело комментируй ненужные:

```
mod_userdir, mod_info, mod_proxy,
mod_imap, mod_auth_db
```

Обрати внимание, что каждый модуль нужно закомментировать дважды — в секции LoadModule и в секции AddModule. Дальше идет конфигурация основного сервера, но мы там почти ничего менять не станем, т.к. «основной» сервер использоваться у нас не будет — будем основываться на виртуальном хостинге. Смело стираем блок <mod_userdir> и раскомментируем строки:

```
AddType text/html .shtml
AddHandler server-parsed .shtml
```

Затем находим и раскомментируем строчку «NameVirtualHost *:80» — она включит виртуальные хосты. Настройки SSL — по вкусу, но лучше ничего не трогай, если точно не знаешь, что значит тот или иной параметр. И, наконец, последней строчкой конфига добавим:

```
Include etc/apache/vhosts/
```

Эта строчка скажет серверу, где находятся дополнительные конфиги. Учти, что перед дирой, которую мы укажем, добавляется значение ServerRoot.

➔ **PHP/Perl/CGI**. Веб-сервер это хорошо, но на голом хтмл далеко не уедешь. И сейчас мы добавим использование php, perl и cgi-скриптов. Начнем с php:

```
# cd /usr/ports/lang/php4/
# make config
```

Появится менюшка, поставим галочку на Apache, на zend multibyte support, и, если надо, на IPv6:

```
# make install clean
```

Модуль должен поставиться без проблем и сам вписать себя в конфиг Apache. Открой на всякий случай конфиг и проверь, что все прошло нормально, конфиг жив, и никто не пострадал. Теперь к нашему модулю нужно собрать расширения PHP:

```
# cd /usr/ports/lang/php4-extensions/
# make install clean
```

Опять появится менюшка с кучей расширений на выбор. Нам обязательно установить следующие:

```
Bcmath, bz2, curl, ftp, gd, iconv,
mbstring и sockets.
```

Остается лишь откинуться на спинку стула и наслаждаться установкой :). Как только установка завершится, идем в /usr/local/etc и копируем рекомендуемый конфиг:

```
# cd /usr/local/etc
# cp php.ini-recommended php.ini
```

Открываем php.ini и вносим следующие изменения:

```
; Включаем safe_mode
safe_mode = On
; Максимальное время выполнения скрипта
max_execution_time = 20
; Максимальное время обработки
скриптом данных
max_input_time = 40
; Максимум выделяемой памяти
memory_limit = 10M
; Максимальный размер файла для аплоада
upload_max_filesize = 5M
```

Разумеется, эти настройки варьируются в зависимости от специфики хостящихся сайтов. Я указал наиболее оптимальные значения, проверенные опытным путем, но, разумеется, тебе ничего не мешает указать их по-своему. Некоторые важные настройки, касающиеся безопасности PHP, мы затронем подробнее в разделе «Защита».

Теперь нам нужно установить Zend Optimizer, чтобы юзеры хостинга смогли запускать скрипты, зашифрованые зендом. Тут все не так просто, и придется сделать небольшой финт ушами. Идем на zend.com, выбираем Products → Zend Optimizer, free download. Нас попросят зарегистрироваться: мыло можно вводить любое, оно не проверяется. После регистрации нас перебросит на страницу закачки оптимайзера. В разделе Zend Optimizer 3.0.0 выбирай FreeBSD x86 5.x. Полученный файл ZendOptimizer-3.0.0-freebsd5.4-i386.tar.gz клади в /usr/ports/distfiles и собирай порт:

```
# cd /usr/ports/devel/ZendOptimizer
# make install clean
```

Установка не должна занять много времени. Обрати внимание, что Zend попросит тебя добавить несколько строк в конец файла php.ini. В моем случае:

zend

```
zend_optimizer.optimization_level=15
zend_extension_manager.optimizer="/usr
/local/lib/php/20020429-zts/Optimizer"
zend_extension_manager.optimizer_ts=
"/usr/local/lib/php/20020429-zts/
Optimizer_TS"
zend_extension="/usr/local/lib/php/
20020429-zts/ZendExtensionManager.so"
zend_extension_ts="/usr/local/lib/php
/20020429-zts/
ZendExtensionManager_TS.so"
```

Обычно это происходит автоматически при установке, но проверить лишний раз не помешает. Теперь, по аналогии с php, нам нужно собрать еще и mod_perl. Можно, конечно, дать веб-юзерам использовать системный перл — но делать это крайне не рекомендуется, хотя бы по тем же соображениям безопасности. О производительности я вообще молчу. Собираем mod_perl:

```
# cd /usr/ports/www/mod_perl
# make install clean
```

Модуль перла так же пропишет себя в конфиг httpd.conf, и не лишним будет проверить, что все ок. Таким образом можно добавить многие полезные модули, например поддержку Python, различные модули авторизации, поддержку frontpage extensions и др.

➔ **vhosts**. Как известно, протокол HTTP 1.1 дает возможность передавать в запросе параметр Host, что позволяет держать несколько сайтов на одном IP-адресе. Это называется виртуальным хостингом. Для каждого сайта, который будет у нас хоститься, мы создадим отдельный конфиг, что позволит делать гибкие настройки для каждого домена в отдельности. Первый конфиг, который мы создаем, будет служебного характера. Для начала создадим папку для конфигов, которую мы указали Apache:

```
# mkdir /usr/local/etc/apache/vhosts
# cd /usr/local/etc/apache/vhosts
И создаем там первый конфиг:
# touch 001.hosting.ru
Открываем конфиг и пишем:
<VirtualHost *:80>
# Мыло админа (будет показываться
при HTTP-ошибках)
ServerAdmin admin@hosting.ru
# Рутовая папка вхоста
DocumentRoot /home/revol.ru/web
# Домен и алиасы, по которым мы будем
видеть вхост
ServerName hosting.ru
ServerAlias www.hosting.ru
ServerAlias main.hosting.ru
# Где располагаются логи
ErrorLog /var/log/www/hosting.ru
-error.log
CustomLog /var/log/www/hosting.ru-cu-
stom.log combined
# Настройки .htaccess и запрет просма-
тривать его из браузера
AccessFileName .htaccess
<Files ~ ^.ht>
Order allow,deny
Deny from all
</Files>
</VirtualHost>
```

Чтобы применить настройки апача и вхостов — используй команду apachectl graceful.

➔ **MySQL.** Теперь нам необходимо установить базу данных, в нашем случае — MySQL. Как обычно, собираем из портов, однако, в целях оптимизации, мы немного поправим Makefile:

```
# cd /usr/ports/databases/mysql140-server
```

На всякий случай сделаем бэкап Makefile:

```
# cp Makefile Makefile.back
```

Открываем Makefile, находим там строчку:

```
--enable-thread-safe-client \
```

И после нее добавляем:

```
--with-client-ldflags=-all-static \
--with-mysqld-ldflags=-all-static \
--enable-assembler \
--with-named-thread-libs='-lpthread
-D_THREAD_SAFE'
```

Закрываем, сохраняем и собираем порт с помощью трех магических слов — make install clean. Установка порта MySQL должна пройти без проблем. После установки топаем в /var/db/mysql и находим там несколько дефолтных конфигов:

```
my-huge.cnf — для серверов, работающих
с огромными по размеру базами
(сотни гиг) my-large.cnf — если базы
просто большие.
```

О значении my-medium.cnf и my-small.cnf, думаю, догадаться не сложно. В целом, конфиг my-large.cnf нам подойдет. Оптимизировать MySQL в конфиге имеет смысл только в том случае, когда ты точно знаешь, какие запросы составляют большинство нагрузки. Так как на хостинге сайты будут разные, и работать их движки с БД будут по-разному — оставим пока дефолтные настройки. Потом, исходя из специфики сайтов, некоторые параметры можно будет подкрутить.

➔ **phpMyAdmin.** Однако управлять MySQL из консоли очень и очень неудобно. Поставим phpMyAdmin (свежий дистриб на диске с журнала), и — в бой:

```
# tar zxvf phpMyAdmin-2.8.1.tar.gz
# mkdir /usr/home/hosting.ru/web/pmadmin
# cp -rf phpMyAdmin-2.8.1/* /usr/
home/hosting.ru/web/pmadmin
# chown -R hosting.ru:hosting.ru
/usr/home/hosting.ru/web/pmadmin
# cd /usr/home/hosting.ru/web/pmadmin
```

Открываем файл config.inc.php и меняем там это:

```
$cfg['Servers'][$i]['auth_type'] = 'config';
```

на это:

```
$cfg['Servers'][$i]['auth_type'] =
'http';
```

Идем на **http://hosting.ru/pmadmin/**, вводим свой логин и пароль к SQL и наслаждаемся.

➔ **FTP.** Для FTP-сервиса, как ты помнишь, мы выбрали pure-ftpd. Собираем порт:

```
# cd /usr/ports/ftp/pure-ftpd
# make install clean
```

В менюшке опций сборки поставь галочки на:

- MYSQL — АВТОРИЗАЦИЯ ЮЗЕРОВ ЧЕРЕЗ БД;
- PRIVSEP — РАЗДЕЛЕНИЕ ЮЗЕРСКИХ ПРИВИЛЕГИЙ;
- PERUSERLIMIT — ОГРАНИЧЕНИЕ ПОТОКОВ ДЛЯ КАЖДОГО ЮЗЕРА;
- THROTTLING — ОГРАНИЧЕНИЕ КАНАЛА ДЛЯ КАЖДОГО ЮЗЕРА;
- BANNER — НЕ ОБЯЗАТЕЛЬНО.

После сборки порта в /usr/local/etc появятся дефолтные конфиги фтп-сервера. Создаем отдельную диру, переносим туда нужные конфиги, выставляем чмоды и удаляем ненужное:

```
# cd /usr/local/etc
# mkdir ftp
# mv pure-ftpd.conf.sample ftp/
# mv pureftpd-mysql.conf.sample ftp/
# chown -R root:wheel ftp/ && chmod
-R 0600 ftp/
# rm pure*
```

Заходим в папку с конфигами, переименовываем их, оставляя бэкапы:

```
# cd ftp/
# cp pure-ftpd.conf.sample pure-ftpd.conf
# cp pureftpd-mysql.conf.sample pu-
reftpd-mysql.conf
```

Теперь необходимо настроить наш фтп-сервер. Открываем pure-ftpd.conf:

листинг файла pure-ftpd.conf

```
# Создавать виртуальный chroot для
каждого пользователя
# Папка /home/<юзер> будет выглядеть
как рутовая
ChrootEveryone yes
# Включить поддержку кривых фтп-клиентов
# Не рекомендуется выставлять в yes
из соображений безопасности
BrokenClientsCompatibility no
# Сколько юзеров может одновременно
подключаться
MaxClientsNumber 30
# Сколько юзеров может одновременно
подключаться с одного IP
MaxClientsPerIP 3
# Подробный лог
VerboseLog yes
# Вход только авторизированым
пользователям
NoAnonymous yes
# Не резольвить IP-адреса
DontResolve yes
```

```
# Конфиг сервера для MySQL
MySQLConfigFile /usr/local/etc/ftp
/pureftpd-mysql.conf
# Выключаем PAM и стандартную авторизацию
PAMAuthentication no
UnixAuthentication no
# Диапазон портов для passive mode
PassivePortRange 30000 50000
# Минимальный User ID, который
может залогиниться
MinUID 1002
# Запрещаем/разрешаем FXP (по вкусу)
AllowUserFXP no
# Не создавать папку юзеру, если не
существует
CreateHomeDir no
# Включаем квоты
Quota 1000:10
# Не пускать юзера, если на диске
занято 95% места.
MaxDiskUsage 95
# Включаем лимиты на скорость
download/upload
PerUserLimits 3:20
# Только IPv4
IPV4Only yes
```

Сам сервер сконфигурирован и готов, осталось настроить авторизацию через MySQL. Редактируем /usr/local/etc/ftp/pureftpd-mysql.conf:

```
# Работаем с MySQL через локальный сокет
MYSQLSocket /tmp/mysql.sock
# Юзер, пароль, база
MYSQLUser ftp
MYSQLPassword nhjhf21j
MYSQLDatabase pureftpd
# Храним пароли в открытом виде или
зашифрованые md5
MYSQLCrypt cleartext
# SQL запрос, ответом которого
будет пароль юзера
MYSQLGetPW SELECT Password FROM
users WHERE User="\L"
# SQL запрос, ответом которого будет
uid юзера. По умолчанию uid/gid можно
# указывать цифрами (1003:1003). Чтобы
получить возможность указывать юзеров
# как user:group поменяй тип полей Uid
и Gid в дампе:
# Uid VARCHAR(16) NOT NULL default '-1',
# Gid VARCHAR(16) NOT NULL default '-1',
MYSQLGetUID SELECT Uid FROM users
WHERE User="\L"
MYSQLGetGID SELECT Gid FROM users
WHERE User="\L"
# SQL запрос, ответом которого будет
домашняя директория юзера (она станет для
# него рутовой)
MYSQLGetDir SELECT Dir FROM users
WHERE User="\L"
# SQL запрос, ответом которого будет
лимит на количество файлов
MySQLGetQTAFS SELECT QuotaFiles FROM
users WHERE User="\L"
# SQL запрос, ответом которого
будет квота юзера в мегабайтах
MySQLGetQTASZ SELECT QuotaSize
FROM users WHERE User="\L"
# SQL запрос, ответом которого будет
лимит скорости Upload для юзера (кб/с)
MySQLGetBandwidthUL SELECT ULBandwidth
FROM users WHERE User="\L"
# SQL запрос, ответом которого будет
лимит скорости Download для юзера (кб/с)
MySQLGetBandwidthDL SELECT DLBandwidth
FROM users WHERE User="\L"
```

Конфиг фтп-сервера завершен. Осталось только создать базу MySQL с параметрами, которые мы указали в конфиге, и залить в эту базу дамп. PhpMyAdmin у нас есть, так что с созданием юзера и базы проблем не возникнет. А дамп базы в природе существует в двух местах — глубоко в дебрях оффсайта pure-ftpd и на диске к журналу. Также не забудь: чтобы ftpd запустился при старте системы, — добавь в /etc/rc.conf строчки:

```
pureftpd_enable="YES"
pureftpd_config="/usr/local/etc/ftp/
pure-ftpd.conf"
```

➔ **статистика.** Awstats 6.5 присутствует в портах FreeBSD, но версия 6.5 содержит очень опасную уязвимость, поэтому ставить мы будем ручками версию 6.6. Качай Awstats с оффсайта, или установи с диска к журналу. Разахривируй файл и устанавливай:

```
# mkdir /etc/awstats
# cd awstats-6.6/wwwroot/cgi-bin/
# mv awstats.model.conf /etc/awstats
# cp -rf * /home/пользователь/cgi-bin/
```

Все конфиги статистики будут находиться в папке /etc/awstats. Чтобы добавить там конфиг для определенного домена, — скопируй файл awstats.model.conf, заменив model именем домена (без www). Например:

```
# cd /etc/awstats
# cp awstats.model.conf awstats.
hosting.ru.conf
```

Сам конфиг Awstats довольно длинный, я укажу лишь основные параметры:

```
# Какой лог парсить
LogFile="/var/log/www/hosting.ru-acess.log"

# Тип лога (W – web, F – FTP, M – mail,
S – streaming)
LogType=W
# Домен(ы) сайта
SiteDomain="hosting.ru"
HostAliases="www.hosting.ru REGEX
hosting\.ru$]"
# Путь к БД статистики
DirData="/var/db/awstats"
```

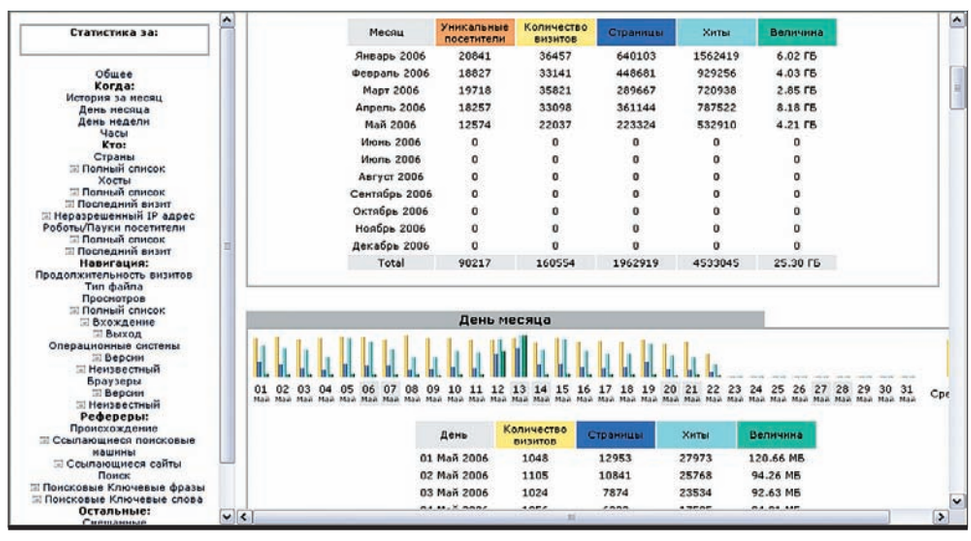
И, наконец, скрипт, который будет обновлять статистику:

```
# cd awstats-6.6
# mkdir /usr/local/awstats
# mv tools/ /usr/local/awstats
```

Добавляем скрипт в крон, чтобы обновлять статистику раз в 9 минут:

```
*/9 * * * * /usr/local/awstats/tools
/awstats_updateall.pl now >/dev/null 2>&1
```

Просмотреть статистику для домена можно по адресу: **http://hosting.ru/cgi-bin/awstats.pl** C



Суровая статистика

сверхдержавный сервер

ЗАЩИЩАЕМ ВЕБ-СЕРВИСЫ ГРАМОТНО

НАШ ЖУРНАЛ УЖЕ МНОГО ПИСАЛ О ТОМ, КАК ХАКЕРЫ ДЕЛАЮТ СВОЕ ЧЕРНОЕ ДЕЛО, СЦЕНЕ И КУЛЬТУРЕ ХАКА. СЕГОДНЯ МЫ ВСТАНЕМ ПО ДРУГУЮ СТОРОНУ БАРРИКАД И ПОГОВОРИМ О МЕТОДИКАХ ЗАЩИТЫ ОТ ВЗЛОМЩИКОВ

MIF
{root@securitylab.co.il}

Сейчас мы попробуем продумать и разработать защитный комплекс, который позволит системному администратору спать чуточку спокойней. Многие сисадмины теорией пренебрегают чаще всего потому, что просто о ней не знают — документаций и статей по этому вопросу практически никто не писал. Ведь объяснить на словах концепцию чего-либо без конкретных примеров — очень и очень сложно. Поэтому, после теоретического ликбеза мы разберем концепцию на примере хостинга, описанного в статье «Могучий хостинг» из этого номера. А начнем мы, пожалуй, с основ — с теории информационной безопасности.

➔ **теория::about.** Немного утрируя, можно сказать, что хакер отличается от скриптКидиса не только тем, что умеет мыслить нестандартно, но и тем, что хорошо знаком с теорией предмета. То же можно сказать и про хорошего крэкера — нужно не только уметь пользоваться дизассемблером, а еще и знать, например, как устроен тот или иной тип бинарика, что такое коллгейт (нет, не паста), и из чего он состоит. Поэтому самый первый кирпичик в основе грамотного системного администрирования — изучение матчасти. Невозможно достойно противостоять напору взломщиков, не понимая, как работает твоя система, и что происходит при вызове того или иного процесса. При разработке защиты так же важно понимать, что хороший хакер, имеющий конкретную цель, взломает любой сервер. C'est la vie. Если кто-то очень сильно захочет посмотреть пару файлов на твоем сервере — он это сделает. Поверь, на Пентагон и ФБР работают не самые плохие специалисты, и, тем не менее, их ломали. И неоднократно. Идеальную защиту можно сравнить с вечным двигателем — теоретически она есть, но пока ее еще никто не создал.

➔ **теория::основные принципы.** По сути, защита любой системы, предоставляющей сервисы, состоит из двух основных направлений — защита от внешней атаки и защита от атаки изнутри. Атака изнутри — это когда атакующий является легальным авторизированным пользователем, который пытается так или иначе поднять свои привилегии в системе. Например, банковский работник, пытающийся просмотреть файлы, к которым ему не давали доступа, или клиент хостинга, у которого есть шелл, пытающийся дефейснуть другой сайт на сервере — это типичные примеры подобной атаки. Атаки второго типа отбивать намного сложнее, ведь у пользователя есть не только данные о системе, но и валидный юзер. Также необходимо учитывать, что, с целью поломать твою систему, хакер может купить аккаунт или украсть пароль у юзера.

➔ **теория::организация.** В вопросах организации и структуры все зависит от масштаба проекта, в данном случае — хостинга. Если речь идет о построении крупного хостинга, — разумным решением будет использование, например, распределенной системы, связанной внутри локальной гигабитной сетью. Один из примеров реализации такого решения может выглядеть как на схеме 1.

В данном случае машины A, B и C являются веб-серверами. На них бегают только веб и фтп-демоны. D — почтовый сервер, обслуживающий наших клиентов. Сервер E представляет собой кластер БД, а F — бэкапный сервер. Как видно на схеме, все серверы хостинга соединены между собой в локалку, причем таким образом, что сервер E и F не имеют доступа в инет. Эта схема имеет довольно серьезные преимущества в плане безопасности — все запросы внутри локальной сети происходят в одностороннем порядке, а значит, ситуацию уже намного легче контролировать. Разумеется, и у такой схемы есть недостатки —

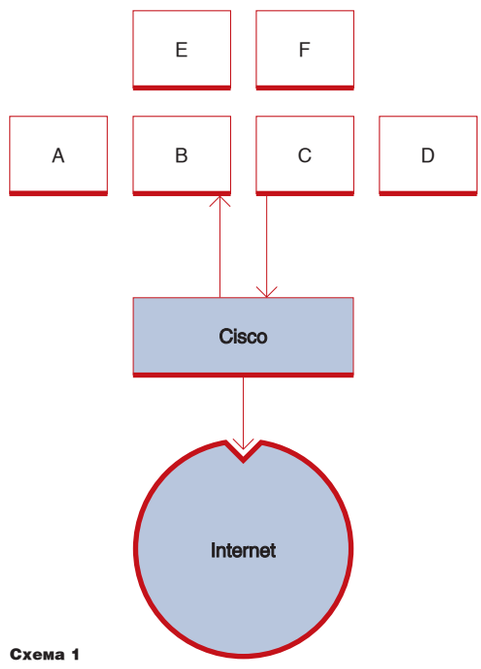


Схема 1

например, время запроса к MySQL возрастает, так как запрос выполняется через TCP, а не через (локальный) unix socket.

Таких вариантов построения хостинга — сотни, и каждый из них имеет свои преимущества и недостатки. Систему, описанную выше, использует, например, весьма солидный хостинг **ipowerweb.com**, о взломе которого я уже рассказывал полтора года назад. Тогда мне помогла лишь полная беспечность админа, оставившего суидный скрипт после инсталляции какого-то софта. Скажу честно: если бы не эта неосторожность с его стороны — я врядли достиг бы цели. Поэтому помни: на систему надейся, а сам не плошай!

➔ **system.** Теперь попробуем реализовать на практике вышеописанные теоретические доводы. Первым делом мы займемся системой. Рассмотрим простой пример — пользователь купил у нас хостинг и запустил мега-движок на PHP, который написал ему приятель-школьник за 100 рублей. Кроме основного действия скрипта функция N зацикливается, попутно производя некое сложное действие. Как результат — высокая загрузка процессора. Это очень типичная ситуация для хостинга. Чтобы предотвратить подобные ненамеренные (и намеренные) атаки, необходимо ограничивать юзера в плане ресурсов. У *BSD для таких целей существует система профилей пользователей. Это значит, что мы можем легко ограничить ресурсы каждого пользователя в отдельности. Открываем /etc/login.conf:

листинг файла /etc/login.conf

```
# Имя профиля
hosting:\
  :copyright=/etc/COPYRIGHT:\
  :welcome=/etc/motd:\
  :setenv=MAIL=/var/mail/$,BLOCKSIZE=K:\
  :path=~/bin /bin /usr/bin /usr/local/bin:\
  :manpath=/usr/share/man /usr/local/man:\
  :nologin=/var/run/nologin:\
# Макс. время использования процессора
  :cputime=1h30m:\
# Макс. кол-во памяти под данные
# Сам код программы и стэк не учитываются
  :datasize=10M:\
# Сколько выделяем для стека программы
  :stacksize=3M:\
# Макс. размер памяти под процесс
  :memoryuse=16M:\
# Макс. размер файла
  :filesize=50M:\
# Макс. размер core файлов
  :coredumpsize=1M:\
# Сколько файлов открывает каждый процесс
  :openfiles=128:\
# Сколько процессов запускает пользователь
  :maxproc=64:\
# Пускать юзера в систему только если
его домашняя дира существует и доступна
# юзеру
  :requirehome:true\
# Время устаревания пароля
  :passwordtime=90d:\
# Остальное берем из профиля default
  :tc=default:
```

Здесь я указал лишь основные параметры. Список всех параметров и их описание можно найти в Handbook.

➔ **hard.** Теперь к вопросу о файловой системе. Самый важный файл настроек в данном случае — /etc/fstab. Он применяется при загрузке, и указывает системе, как работать с тем или иным разделом файловой системы, что с ним может делать пользователь, а что — нет. Открываем /etc/fstab и приводим его примерно в такой вид:

```
/dev/ad1s1b none       swap   sw          0 0
/dev/ad1s1a /          ufs    rw          1 1
/dev/ad1s1e /tmp       ufs    rw,noexec 2 2
/dev/ad1s1f /usr       ufs    rw          2 2
/dev/ad1s1g /usr/home ufs     rw,nos-
                              uid,nodev 2 2
/dev/ad1s1d /var       ufs    rw,nodev   2 2
/dev/acd0   /cdrom     cd9660 ro,noauto 0 0
```

Очень важно поставить параметр noexec на /tmp. Данная опция запрещает запускать что-либо на файловой системе, даже если на файле установлен chmod 777. Я лично видел очень много взломов отлично защищенных серверов именно из-за этой ошибки, которую, почему-то, очень многие допускают. Нельзя забывать, что в /tmp может писать почти любой процесс в системе. Опция nosuid говорит системе игнорировать suid-биты файлов, а nodev запрещает создание/существование в разделе специальных устройств.

➔ **system::sysctl.** Теперь перейдем к тюнингу операционной системы. Открываем /etc/sysctl.conf и пишем туда следующее:

листинг файла /etc/sysctl.conf

```
# Запрещает юзерам видеть процессы
соседа, и, разумеется, рутовые.
security.bsd.see_other_uids=0
# Пускаем запросы на закрытые порты.
net.inet.tcp.blackhole=2
net.inet.udp.blackhole=1
# Указываем размер очереди сокета
kern.ipc.somaxconn=1024
# Отрубаем ip-редиректы
net.inet.icmp.drop_redirect=1
net.inet.icmp.log_redirect=1
net.inet.ip.redirect=0
# Назначаем размеры буфера для TCP-под-
ключений. Если на сервер ожидается
большая # нагрузка, и у него много
памяти — лучше поставить 65535.
# не рекомендуется.
net.inet.tcp.sendspace=32768
net.inet.tcp.recvspace=32768
# Обновляем ARP-таблицу каждые 20 минут
net.link.ether.inet.max_age=1200
# Запрещаем отвечать на все лишние запросы.
net.inet.icmp.maskrepl=0
net.inet.ip.sourceroute=0
net.inet.ip.accept_sourceroute=0
net.inet.icmp.bmcastecho=0
```

Конечно же, здесь указаны не все параметры sysctl. Для полного описания всех возможностей не хватило бы и журнала, поэтому я указал самые основные и необходимые. Многие параметры для sysctl можно изменять и динамически:

```
sysctl <параметр>=<значение>
например:
sysctl kern.maxprocperuid=1000
```

Теперь необходимо продублировать часть настроек в /etc/rc.conf:

```
# Дублируем настройки sysctl
icmp_drop_redirect="YES"
icmp_log_redirect="YES"
icmp_bmcastecho="NO"
tcp_drop_synfin="YES"
```

➔ **логи.** Очень важным аспектом системного администрирования является слежение за поведением сервера. Для этого существует отличная утилита logcheck. Устанавливаем:

```
# cd /usr/ports/security/logcheck
# make install clean
```

Утилита написана на sh-скриптах и занимает всего 29 Кб в архиве. После установки в /usr/local/etc у тебя появятся четыре конфига: переименуй их, убрав из названия файла «sample»:

logcheck.hacking — о каких странностях сообщать;
logcheck.violations — о каких попытках взлома сообщать;
logcheck.ignore — какие странности игнорировать;
logcheck.violations.ignore — какие попытки взлома игнорировать.

В целом и общем, первый файл от второго ничем не отличается, равно как и третий от четвертого. Просто разработчики скрипта решили разнести сообщения о подозрительной активности и сообщения о явной атаке в разные конфиги. Затем необходимо перенести файл logcheck.sh:

```
# mv logcheck.sh /usr/local/sbin
# chmod 0700 /usr/local/sbin/logcheck.sh
# chown root:wheel /usr/local/sbin/logcheck.sh
```

Теперь можно запускать скрипт по крону, хотя бы раз в сутки:

```
0 4 * * * /usr/local/sbin/logcheck.sh
```

Так же следует учесть тот факт, что, при большой активности хостящихся сайтов, логи веб-сервера неумалимо начнут расти и занимать немало места. В то же время их надо сохранять. Тут есть два варианта. Можно использовать утилиту logrotate (/usr/ports/sysutils/logrotate), но я использую небольшой самописный скрипт. Его основной конфиг я поясню, а скрипт целиком можно найти на диске (rLog.sh).

```
# Где лежат логи вхостов?
logs_dir=/var/log/www
# Куда складывать архивы с логами?
arc_logs=/var/wwwlogs
# Кого устанавливать владельцем архивов?
user=root
group=wheel
# Темп-файл
rLog_l=/tmp/rLog.log
```

Скрипт заархивирует все логи виртуальных хостов, создаст архив в указанном тобой месте, обнулит логи и пошлет отчет руту. Разумеется, скрипт нужно прописать в crontab:

```
0 6 * * * /usr/local/sbin/rLog.sh
```

➔ **apache.** К сожалению, на сегодняшний день не существует хотя бы близкой к безупречности модели защиты Apache. Любая конфигурация этого веб-сервера так или иначе оставляет возможности для взлома, даже при использовании suexec или cgi-врапперов. Единственный более-менее интересный вариант — это модуль PerUser для Apache 2. Он позволяет запускать Апач с привилегиями пользователя, который указан в конфиге виртуального хоста. Это значит, что каждый вхост (читай домен) на сервере запускается из-под отдельного системного юзера. Даже если поломают один сайт, то, чтобы добраться до других, хакеру нужно будет поднимать привилегии до рута. А на хорошо настроенной BSD-системе сделать это намного сложнее, нежели залить веб-шелл через багу в скрипте. Однако у модуля PerUser есть три серьезных недостатка. Во-первых, он существует только для Apache второй версии, которая еще не совсем стабильна, во-вторых — проект уже довольно долгое время находится в стадии альфа-тестинга, и в-третьих — модуль (по второй причине) невозможно установить из портов, а значит веб-сервер придется собирать из исходников, а это не только дополнительная возможность наделать ошибок, но и немалый геморрой с апдейтами. Думаю, что если разработчики все же разродятся стабильным релизом этого модуля, — это решит множество проблем для админов хостинговых серверов.

➔ **scripting.** Рассмотрим самое уязвимое место хостинговой системы, а именно — выполняемые файлы, и, в частности, PHP-скрипты. Начнем с того, что открываем конфиг PHP:

```
# vi /usr/local/etc/php.ini
```

Меняем следующие параметры:

```
; Экранирование спецсимволов
magic_quotes_gpc = On
; Выключаем опасные функции:
disable_functions = system, exec, passthru
```

Выключить эти функции очень важно. Хоть они и недоступны при включенном safe mode, пользователь может без труда провести успешную атаку, указав в файле .htaccess:

```
php_flag safe_mode off
```

➔ **виртуальные хосты.** Теперь нам необходимо задать ограничения в конфиге каждого вхоста. Добавляем следующие параметры:

```
<IfModule mod_php4.c>
 # Включаем Safe mode
 php_admin_flag safe_mode on
 php_admin_flag safe_mode_gid on
 # Папка, выше которой скрипт не может видеть
 php_admin_value open_basedir /home/domain.ru
 php_admin_value safe_mode_exec_dir
/home/domain.ru
 # Temp дира юзера
 php_admin_value upload_tmp_dir
/home/domain.ru/tmp
 # Не начинать PHP сессию автоматически
 php_admin_flag session.auto_start off
 # Где сохранять файлы сессий
 php_admin_value session.save_path
/home/domain.ru/tmp
</IfModule>
```

Как известно, немалая часть взломов (SQL Injection, XSS-атаки, инклюдинг) происходит, по сути, посредством хитрого HTTP-запроса. Логично предположить, что эти самые запросы неплохо было бы фильтровать. Решение проблемы существует в виде модуля к Апачу, и называется оно mod_security. Ставим:

```
# cd /usr/ports/www/mod_security/
# make install clean
```

После установки — идем конфигурировать. Открываем любой конфиг виртуального хоста, например, 001.admin.hosting.ru, над которым мы уже экспериментировали. Все значения надо вводить между тегами <Virtualhost *:80> и </Virtualhost>.

```
# Включаем mod_security
SecFilterEngine On
# Проверяем запросы
SecFilterScanPOST On
# Проверяем ответы
SecFilterScanOutput On
# Проверяем, правильно ли закодирован URL
SecFilterCheckURLEncoding On
# Включаем параметр, если сайт в Unicod'e
SecFilterCheckUnicodeEncoding Off
# Задаем диапазон байтов
   SecFilterForceByteRange 1 255
# Сохраняем в лог срабатывания механизма
SecAuditEngine RelevantOnly
# Где живет лог :)
SecAuditLog logs/audit_log
# Возвращаем ошибку 500 при срабатывании
SecFilterDefaultAction "deny,log,status:500"
# Перекрываем dots-bug
SecFilter "\.\./"
# Не забываем про XSS
SecFilter "<(.|\n)+>"
SecFilter "<[[:space:]]*script"
 # SQL injection, куда же без него :)
SecFilter "delete[[:space:]]+from"
SecFilter "insert[[:space:]]+into"
SecFilter "select.+from"
# Перекрываем возможность передачи
переменных PHP
SecFilterSelective ARG_b2inc "!^$"
# Исключаем возможность раскрытия пути
SecFilterSelective OUTPUT "Fatal error:"
```

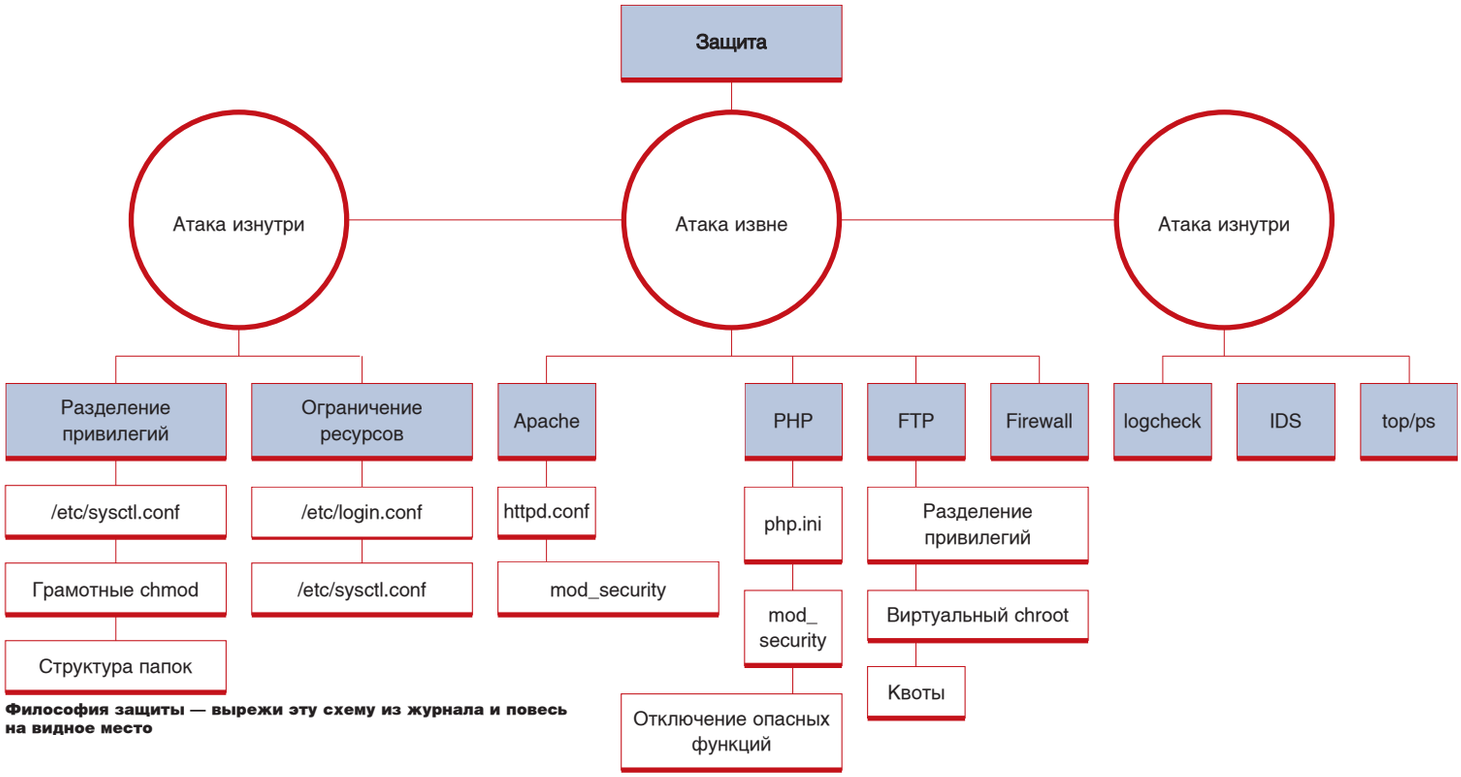
У этого модуля на редкость удачная дефолтная конфигурация. К ней мало что можно добавить, так как большинство настроек — специфичны. Общий принцип составления правил мы рассмотрели, а остальное можно добавить по своему усмотрению.

➔ **firewall.** Ну и, разумеется, ключевой момент защиты — файрвол. Открываем конфиг файрвола (/etc/rc.firewall) и приводим нужную секцию примерно в следующий вид:

```
ip="123.31.123.123" # IP сервера
myip="90.90.90.90" # Твой статический ИП
```

листинг файла /etc/rc.firewall

```
# С этих диапазонов ничего хорошего
за всю историю РуНета не приходило.
${fwcmd} add deny log logamount 1000 ip
from 217.17.248.0/24 to any
${fwcmd} add deny log logamount 1000 ip
from 62.149.64.0/18 to any
${fwcmd} add deny log logamount 1000 ip
from 212.93.192.0/19 to any
${fwcmd} add deny log logamount 1000 ip
from 212.106.64.0/19 to any
${fwcmd} add deny log logamount 1000 ip
from 62.215.0.0/16 to any
${fwcmd} add deny log logamount 1000 ip
from 200.0.0.0/8 to any

# Сервисы
# Пропускаем фтп
${fwcmd} add pass tcp from any to ${ip}
21 setup
```



Философия защиты — вырежи эту схему из журнала и повесь на видное место

```
# Открываем ssh только для себя
${fwcmd} add pass tcp from ${myip} to ${ip}
22 setup
# Веб
${fwcmd} add pass tcp from any to ${ip}
80 setup
# Https
${fwcmd} add pass tcp from any to ${ip}
443 setup
# Разрешаем трафик установленных соединений
${fwcmd} add pass tcp from any to any
established
# Пропускаем IP-фрагменты
${fwcmd} add pass all from any to any frag
# Разрешаем исходящие TCP
${fwcmd} add pass tcp from ${ip} to any setup
# А теперь все идут лесом
${fwcmd} add deny tcp from any to any setup
# Разрешаем DNS-трафик
${fwcmd} add pass udp from ${ip} to any
53 keep-state
# Разрешаем NTP-запросы
${fwcmd} add pass udp from ${ip} to any
123 keep-state
```

В зависимости от того, как ты настроил passive-mode в конфиге pure-ftpd, не забудь открыть нужный диапазон портов.

➔ **chroot.** Когда ко мне прибежал очередной знакомый админ и с выпученными глазами сообщил, что теперь у него стоит mod_chroot для Апача — я задал ему вполне легитимный вопрос: «Зачем?». Ответ был стандартный — «Потому что секурно». Мы с ним рассмотрели минусы решения: потеря производительности, лишний немаленький модуль, дополнительный конфиг. Смотрим плюсы: а что дает модуль? А ничего он не дает. То же можно сказать и про обычный chroot — он ничего не дает в плане безопасности. Дело в том, что грамотно выставленные chmod'ы дают тот же эффект, но без потерь в ресурсах и дополнительных заморочек. Для системы, которую мы рассматриваем на примере, chroot не пригодится. Однако существует множество случаев, когда он необходим. В основном, к помощи chroot'а имеет смысл прибегать, когда требуется обезопасить отдельный сервис. Например, ISC BIND, который, мягко говоря, небезопасен — создавать ему «песочницу» необходимо, даже если DNS — это единственный сервис, запущенный на системе.

➔ **jail.** В связи с тем, что вопрос безопасности сегодня стоит очень остро, постоянно появляются все новые и новые решения. К сожалению, большинство из них далеки от идеала. Выбирая любое решение, необходимо сначала рассматривать его недостатки, и только потом — преимущества, так как обычно игра не стоит свеч. Например, Jail в BSD. С одной стороны — все замечательно и прекрасно, если походить по форумам — везде восторженные отклики «профессионалов» о том, как у них все теперь секурно. На примере того же хостинга давай посмотрим, что будет, если мы поставим туда jail'ы. Во-первых, в джейл нам придется загонять каждый вхост, а значит — мы серьезно теряем в производительности. Во-вторых, jail еще очень плохо документирован, а значит, уже нужно быть готовым к сюрпризам (не всегда приятным). В-третьих, jail еще мало кто использует, и я бы не был на 100% уверен в его стабильности, и, уж тем более, безопасности. В-четвертых, если хакер достаточно квалифицирован, чтобы поднять привилегии внутри джейла, то ему не составит большого труда вылезти из него в основную систему. А теперь рассмотрим плюсы: джейл позволяет нам создавать ОС внутри ОС. Круто. Но как показывают его минусы — в данном случае — бессмысленно. Существуют варианты, когда такие системы необходимы — это при раздаче пользователям шеллов или VDS. Например, проект firstvds.ru работает на основе модифицированного FreeBSD jail.

➔ **резюме.** Суть примеров с Chroot и Jail заключается в том, чтобы донести до нас одну из ключевых аксиом — ОС, софт и настройки следует выбирать исходя из задачи. Не стоит ставить ту или иную фишку, если она не помогает решить задач, которые выполняет сервер. Этим грешат очень многие системщики, и часто именно эти излишки и открывают хакеру лазейку в систему. В целом и общем, можно сказать, что чем больше админ знает о функциях, которые будут выполнять процессы сервера — тем лучше он сможет его защитить.

Разумеется, все вышеописанное не претендует на идеально защищенную систему. Как уже было сказано, идеальная защита — миф. Кому-то данная концепция подойдет, кому-то — нет. В любом случае, надеюсь, что данная статья поможет тебе сориентироваться в основах обеспечения безопасности собственного сервера C

тайная канцелярия

ВНЕДРЕНИЕ IPSEC

РАССМОТРИМ ДВА НАИБОЛЕЕ ЧАСТО ИСПОЛЬЗУЕМЫХ СЦЕНАРИЯ ВЧС (ВИРТУАЛЬНЫХ ЧАСТНЫХ СЕТЕЙ) — «ХОСТ В ХОСТ» И «ХОСТ В СЕТЬ», ПРЕДВАРИТЕЛЬНО БОЛЕЕ ДЕТАЛЬНО РАССМОТРЕВ НЕКОТОРЫЕ ТЕОРЕТИЧЕСКИЕ АСПЕКТЫ IPSEC

КОНСТАНТИН ГАВРИЛЕНКО
{директор компании Архонт}

→ **IPSec** — наиболее признанный, поддерживаемый и стандартизированный из всех протоколов ВЧС на сегодняшний день. Для обеспечения совместной работы различных устройств в гетерогенной сети он подходит лучше прочих, так как основан на полностью открытых стандартах. В отличие от других ВЧС-протоколов, IPSec работает на третьем уровне и может защищать любой ИП-трафик. При его применении совместно с другими протоколами туннелирования на втором уровне, такими как Л2ТП, также появляется возможность защиты в том числе и не ИП-трафика.

→ **внутреннее устройство IPSec.** Нельзя говорить об IPSec'е, как об одном протоколе. На самом деле, под протоколом IPSec подразумевается набор стандартов и черновиков (drafts). Вот основные:

— AH (AUTHENTICATED HEADER) ЗАГОЛОВОК АУТЕНТИФИКАЦИИ, ОБЕСПЕЧИВАЮЩИЙ АУТЕНТИФИКАЦИЮ ИСТОЧНИКА ДАННЫХ, ЦЕЛОСТНОСТЬ И ЗАЩИТУ ОТ АТАК ПОВТОРНОГО ВОСПРОИЗВЕДЕНИЯ.

- ESP (ENCAPSULATED SECURITY PAYLOAD) БЕЗОПАСНО ИНКАПСУЛИРОВАННАЯ ПОЛЕЗНАЯ НАГРУЗКА, ОБЕСПЕЧИВАЮЩАЯ АУТЕНТИФИКАЦИЮ ИСТОЧНИКА ДАННЫХ, ЦЕЛОСТНОСТЬ, ЗАЩИТУ ОТ АТАК ПОВТОРНОГО ВОСПРОИЗВЕДЕНИЯ, КОНФИДЕНЦИАЛЬНОСТЬ ДАННЫХ И, В НЕКОТОРЫХ ТИПАХ ПРИМЕНЕНИЯ, СКРЫТНОСТЬ УПРАВЛЕНИЯ ПОТОКОМ.
- IPCOMP (IP PAYLOAD COMPRESSION PROTOCOL) ПРОТОКОЛ АВТОМАТИЧЕСКОГО СЖАТИЯ ДАННЫХ ПЕРЕД ШИФРАЦИЕЙ. ПОТЕНЦИАЛЬНО УСТРАНЯЕТ НЕГАТИВНОЕ ВЛИЯНИЕ ИНКАПСУЛЯЦИИ ДАННЫХ И СОКРАЩАЕТ ОБЪЕМ ТРАНСЛИРУЕМОЙ ИНФОРМАЦИИ.
- IKE (INTERNET KEY EXCHANGE) МЕХАНИЗМ БЕЗОПАСНОГО АВТОМАТИЧЕСКОГО ОБМЕНА КЛЮЧАМИ, ПРЕДОСТАВЛЯЮЩИЙ СРЕДСТВА СОГЛАСОВАНИЯ КРИПТОГРАФИЧЕСКОГО АЛГОРИТМА И ОТВЕЧАЮЩИЙ ЗА РАСПРЕДЕЛЕНИЕ КЛЮЧЕЙ, ИСПОЛЬЗУЕМЫХ ДЛЯ ШИФРОВАНИЯ ДАННЫХ.

Существуют два режима работы IPSec-соединения: туннельный и транспортный. Транспортный режим работы используется исключительно для защиты соединения между двумя хостами, шифруя только полезные данные в пакете. Туннельный режим работы шифрует весь передаваемый ИП-пакет, вместе с полезными данными, ИП-опциями, исходным и конечным адресом, добавляя новые ИП-заголовки, позволяя создавать защищенное соединение между несколькими сетями. Настоятельно рекомендую использовать туннельный режим работы ESP IPSec, так как он обеспечивает наибольший уровень конфиденциальности передаваемых данных, хотя и увеличивает пакет на несколько дополнительных байтов.

При использовании автоматического режима обмена ключами, создание туннеля происходит в два этапа. В процессе первой фазы соединения происходит формирование ISAKMP SA (соглашения о защите протокола безопасности в интернете и управлении ключами), включая установление аутентификации и защиты IPSec-узлов, согласование политики для защиты обмена информацией, выработку защитного ключа через протокол Диффи-Хельмана и установку туннеля для дальнейших переговоров второй фазы. В процессе второй фазы согласования формируется IPSec SA, включая согласование параметров SA для протокола IPSec, выработку SA для протокола IPSec, периодическую ротацию ключей шифрования.

ДЛЯ СТАТЬИ ИСПОЛЬЗОВАЛОСЬ ПОСЛЕДНЕЕ СТАБИЛЬНОЕ 2.6.16 ЯДРО, IPSEC-TOOLS 0.6.5 И IPROUTE2 2.6.16

Наиболее распространенные методы взаимной аутентификации сторон включают использование предварительно разделенного ключа (PSK) или цифровых сертификатов типа X.509. Оба метода имеют свои преимущества. Хотя считается, что использование цифровых сертификатов — более безопасное решение, но стоит ли утруждать себя созданием CA, выпиской сертификатов и CRL, если нужно соединить только два хоста?

→ **выбор IPSec'a.** На данный момент существует две имплементации IPSec-стэка для Линукса и три вида пользовательского интерфейса. Начиная с 2.6.x версии, ядро Линукса приобрело встроенную поддержку IPSec'a (NETKEY), портированную с FreeBSD, и пользовательский интерфейс, предоставляемый ipsec-tools. Для предыдущих версий ядра (2.2.x и 2.4.x) поддержка протокола IPSec осуществлялась через программный пакет FreeSWAN (KLIPS как часть кернела, и Pluto — как пользовательский интерфейс), который сейчас перешел в новую реинкарнацию и называется OpenSWAN. Третьим пользовательским интерфейсом является Isakmpd, портированный на Линукс с OpenBSD — наименее распространенное решение.

Хотя NETKEY — значительно более молодой стэк, чем KLIPS, и имеет меньшую функциональность, он все равно был интегрирован в текущее древо ядра, в основном из-за различных «политических» проблем, окружающих KLIPS, а также из-за более «чистого» кода.

→ **подготовка к установке.** Большинство современных дистрибутивов базируются на 2.6.x ядре и имеют как предустановленную поддержку IPSec'a в ядре, так и набор утилит в своих системах управления пакетами.

Опустим стандартный процесс сборки и установки, сконцентрировавшись непосредственно на самом процессе конфигурации.

проверь, что в конфигурационном файле ядра следующие опции отмечены для включения в ядро или выбраны как модули

```
CONFIG_XFRM=y          CONFIG_CRYPTO_MD5=y
CONFIG_
XFRM_USER=m            CONFIG_CRYPTO_SHA1=m
CONFIG_NET_KEY=m       CONFIG_CRYPTO_SHA256=m
CONFIG_INET_AH=m       CONFIG_CRYPTO_SHA512=m
CONFIG_INET_ESP=m      CONFIG_CRYPTO_DES=y
CONFIG_
INET_IPCOMP=m          CONFIG_CRYPTO_AES=m
CONFIG_
INET_TUNNEL=m          CONFIG_CRYPTO_DEFLATE=m
```

проверь, что два хоста, между которыми ты собираешься устанавливать туннель, не имеют никаких препятствий для связи (если установлен брандмауэр, то разреши соединения на UDP-порты 500, 4500 и протоколы 50 и 51)

```
iptables -A INPUT -i eth0 -p 50 -j ACCEPT
iptables -A INPUT -i eth0 -p 51 -j ACCEPT
iptables -A INPUT -i eth0 -p udp --
dport 500 -j ACCEPT
iptables -A INPUT -i eth0 -p udp --
dport 4500 -j ACCEPT
```

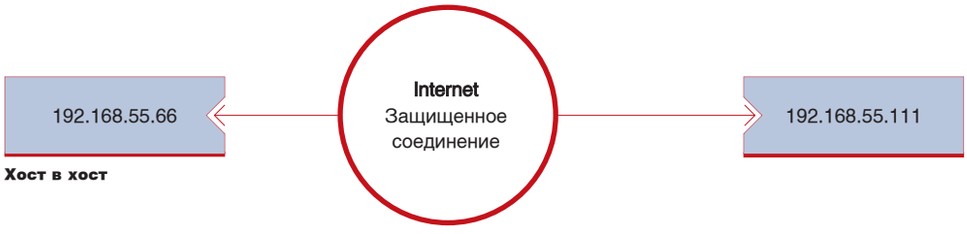
для отделения потока трафика, пришедшего через IPSec-туннель, необходимо пометить входящие ESP-пакеты и разрешить беспрепятственный доступ или перенаправить их в отдельную таблицу

```
iptables -t mangle -A PREROUTING -i
eth0 -p esp -j MARK --set-mark 50
iptables -A INPUT -i eth0 -m mark --
mark 50 -j ACCEPT
```

→ **конфигурация «хост в хост».** Существует достаточно возможностей установления безопасного соединения между двумя статическими хостами, начиная с использования SSH для защиты административного канала управления или инкапсуляции всего трафика в PPP-канал связи с последующей защитой через SSH или SSL. Хотя наиболее простым и правильным решением в данном случае будет установка «хост в хост» IPSec-соединения, используя PSK для аутентификации сторон.

Ракун — достаточно сложный в конфигурации демон с огромным количеством опций, большинство из которых, к счастью, можно оставить по умолчанию, что значительно облегчает задачу.

В первую очередь нужно установить пароль. Значение ключа устанавливается в файле psk.txt (проверь, чтобы права доступа были 400, -r-------- 1 root root, иначе Ракун не запустится).



Хост в хост

генерирование случайного ключа

```
arhontus / # dd if=/dev/random bs=16
count=1 | xxd -ps
1+0 records in
1+0 records out
16 bytes (16 B) copied, 4.4e-05
seconds, 364 kB/s
cc0c6778f478f5aff03caa38779090c1
```

помести ключ в файл psk.txt

```
arhontus racoon # cat psk.txt
192.168.55.66
cc0c6778f478f5aff03caa38779090c1
```

В первом столбце указывается идентификатор хоста, будь-то ИП-адрес или имя хоста, а во втором — сам ключ. Такую же операцию проведи и на втором хосте, заменив ИП на противоположный.

Далее необходимо задать политику безопасности IPSec, а именно: какие каналы коммуникации необходимо защитить, и каким образом будет осуществляться защита соединения. Политику безопасности возможно определить для хостов и для направления соединения, а также и на уровне сокета, которым пользуется программа. При запуске Ракун не пытается немедленно установить соединение, а ждет уведомления от ядра о том, что данное соединение становится активным и нуждается в защите, после чего инициирует обмен ключами.

как правило, конфигурация политики безопасности заносится в файл ipsec.conf или setkey.conf (зависит от особенностей дистрибутива)

```
arhontus racoon # cat ipsec.conf
#!/usr/sbin/setkey -f
# Flush the SAD and SPD
flush;
spdflush;
spdadd 192.168.55.111/32
192.168.55.66/32 any -P out ipsec
 ipcomp/transport//use
 esp/transport//unique;
spdadd 192.168.55.66/32
192.168.55.111/32 any -P in ipsec
 ipcomp/transport//use
 esp/transport//unique;
```

В данном примере мы создали две политики, описывающие входящий и исходящий трафик, для двухсторонней коммуникации с соседним хостом. В зависимости от используемого режима протокола и алгоритма шифрования, конечный отправляемый пакет увеличивается в размере. Соответственно, для уменьшения количества передаваемых данных, а так же для того, чтобы избежать ненужной фрагментации пакетов, мы сначала сжимаем пакет и только потом его шифруем, что и отображено в файле конфигурации. Ты неограничен в выборе используемой комбинации протоколов (AH, ESP, IPCOMP) и, ради эксперимента, можешь попробовать провести даже двойное шифрование пакета.

настройка конфигурационного файла IKE-демона, чем, собственно, и является Ракун

```
arhontus racoon # cat racoon.conf
path pre_shared_key "/etc/raco-
on/psk.txt";
listen {
 isakmp 192.168.55.111 [500];
  isakmp_natt 192.168.55.111 [4500];
 strict_address;
 }

remote 192.168.55.66 {
 exchange_mode main;
 my_identifier address;
 peers_identifier address;
 verify_identifier on;

 dpd_delay 60;
 proposal {
  lifetime time 120 min;
  encryption_algorithm rijndael256;
  hash_algorithm sha256;
  authentication_method pre_shared_key;
  dh_group modp4096;
  }
 proposal_check strict;
}

sainfo anonymous {
 lifetime time 30 minutes;
 encryption_algorithm rijndael;
 authentication_algorithm hmac_sha1;
 compression_algorithm deflate;
 pfs_group modp2048;
}
```

SPECIAL МНЕНИЕ

КОНСТАНТИН ГАВРИЛЕНКО
Консультант по безопасности, директор компании Архонт. Соавтор книг: «Wi-Фу: Секреты беспроводного взлома» и «Секреты Хакеров: Безопасность сетей Циско».

КАКОВО ИСТИННОЕ ПРЕДНАЗНАЧЕНИЕ VPN (VIRTUAL PRIVATE NETWORK)?

В те давние времена, когда интернет был доступен ограниченному количеству пользователей, в основном академической направленности, особых вопросов о конфиденциальности передаваемых данных не возникало. С ростом количества пользователей и приходом громадных корпораций претерпела изменения и сама природа интернета. Из академического инструмента она превратилась в глобальную распределенную Сеть, в которой хранится и передается огромное количество конфиденциальных данных и проводится множество финансовых транзакций.

Такие изменения не могли долго оставаться без внимания лиц, пытающихся извлечь выгоду из доступа к конфиденциальной информации. Соответственно, с особой остротой встал вопрос безопасной передачи данных. Одно из возможных решений этой проблемы — развертывание ВЧС. Их применение оправдано по двум мотивам:

— стремление сократить расходы, например, заменив безопасные линии дозвона для удаленных корпоративных пользователей на доступ через IPSec;

— желание обеспечить конфиденциальность передаваемых данных между узлами сети во враждебном окружении, например, защита коммуникаций между клиентом и точкой беспроводного доступа.

Обычная конфигурация хранится в файле racoon.conf. В нем содержится описание особенностей всех туннелей, для которых необходима автоматическая генерация ключей.

Теперь более подробно рассмотрим используемые опции:

- PATH PRE_SHARED_KEY
  МЕСТОНАХОЖДЕНИЕ ФАЙЛА С КЛЮЧАМИ;
- ISAKMP 192.168.55.111 [500]
  АДРЕС, НА КОТОРОМ БУДЕТ СЛУШАТЬ ДЕМОН IKE;
- ISAKMP_NATT 192.168.55.111 [4500]
  АДРЕС, НА КОТОРОМ БУДЕТ СЛУШАТЬ ДЕМОН IKE В РЕЖИМЕ РАБОТЫ ЧЕРЕЗ NAT;
- STRICT_ADDRESS
  УКАЗЫВАЕТ, ЧТО ИНТЕРФЕЙС ДОЛЖЕН ПРИСУТСТВОВАТЬ ПЕРЕД НАЧАЛОМ РАБОТЫ;
- REMOTE 192.168.55.6
  ОТКРЫВАЕТ СЕКЦИЮ КОНФИГУРАЦИИ ОТДЕЛЬНО ВЗЯТОГО ТУННЕЛЯ И УКАЗЫВАЕТ АДРЕС СОСЕДА IPSEC-ТУННЕЛЯ;
- EXCHANGE_MODE MAIN
  ОПРЕДЕЛЯЕТ РЕЖИМ РАБОТЫ ПЕРВОЙ ФАЗЫ;
- MY_IDENTIFIER ADDRESS
  ПОСЫЛАЕМЫЙ ИДЕНТИФИКАТОР;
- PEERS_IDENTIFIER ADDRESS
  ОЖИДАЕМЫЙ ИДЕНТИФИКАТОР СОСЕДА;
- VERIFY_IDENTIFIER ON
  ВКЛЮЧЕНИЕ ПРОВЕРКИ ИДЕНТИФИКАТОРА СОСЕДА;
- DPD_DELAY 60
  ОПРЕДЕЛЕНИЕ ИНТЕРВАЛА РАБОТЫ РЕЖИМА ОБНАРУЖЕНИЯ НЕРАБОТАЮЩЕГО ХОСТА;
- PROPOSAL
  ОТКРЫВАЕТ СЕКЦИЮ КОНФИГУРАЦИИ ПАРАМЕТРОВ ПРЕДЛОЖЕНИЯ ПЕРВОЙ ФАЗЫ;
- LIFETIME TIME 120 MIN
  ВРЕМЯ ЖИЗНИ КЛЮЧА ШИФРОВАНИЯ ПЕРВОЙ ФАЗЫ;
- ENCRYPTION_ALGORITHM RIJNDAEL256
  АЛГОРИТМ ШИФРОВАНИЯ, ИСПОЛЬЗУЕМЫЙ В ПРОЦЕССЕ ПЕРВОЙ ФАЗЫ;
- HASH_ALGORITHM SHA256
  АЛГОРИТМ ХЭШИРОВАНИЯ, ИСПОЛЬЗУЕМЫЙ В ПРОЦЕССЕ ПЕРВОЙ ФАЗЫ;
- AUTHENTICATION_METHOD PRE_SHARED_KEY
  ИСПОЛЬЗУЕМЫЙ МЕТОД АУТЕНТИФИКАЦИИ;
- DH_GROUP MODP4096
  ПАРАМЕТРЫ ФУНКЦИИ ИДЕАЛЬНОЙ СЕКРЕТНОСТИ ПЕРЕНАПРАВЛЕНИЯ ПЕРВОЙ ФАЗЫ;
- PROPOSAL_CHECK STRICT
  ОПРЕДЕЛЯЕТ УРОВЕНЬ СООТВЕТСТВИЯ ДВУХ ПРЕДЛОЖЕНИЙ;
- SAINFO ANONYMOUS {
  ОТКРЫВАЕТ СЕКЦИЮ КОНФИГУРАЦИИ ПАРАМЕТРОВ ПРЕДЛОЖЕНИЯ ВТОРОЙ ФАЗЫ;
- LIFETIME TIME 30 MINUTES
  ВРЕМЯ ЖИЗНИ КЛЮЧА ШИФРОВАНИЯ;
- ENCRYPTION_ALGORITHM RIJNDAEL
  АЛГОРИТМ ШИФРОВАНИЯ, ИСПОЛЬЗУЕМЫЙ В ПРОЦЕССЕ ВТОРОЙ ФАЗЫ;
- AUTHENTICATION_ALGORITHM HMAC_SHA1
  АЛГОРИТМ ХЭШИРОВАНИЯ, ИСПОЛЬЗУЕМЫЙ В ПРОЦЕССЕ ВТОРОЙ ФАЗЫ;
- COMPRESSION_ALGORITHM DEFLATE
  АЛГОРИТМ СЖАТИЯ, ИСПОЛЬЗУЕМЫЙ В ПРОЦЕССЕ ВТОРОЙ ФАЗЫ;
- PFS_GROUP MODP2048
  ПАРАМЕТРЫ ФУНКЦИИ ИДЕАЛЬНОЙ СЕКРЕТНОСТИ ПЕРЕНАПРАВЛЕНИЯ ВТОРОЙ ФАЗЫ.

Стоит отметить, что для второй фазы были выбраны менее мощные алгоритмы шифрования и хэширования, так как они используются непосредственно для шифрования отправляемого трафика, что, в свою очередь, сказывается на производительности системы. В зависимости от мощности и архитектуры процессора, необходимой пропускной способности и желаемого уровня безопасности данных, различные алгоритмы будут более или менее приемлемы в каждой конкретной ситуации. Включение режима сжатия данных так же добавляет дополнительную нагрузку на центральный процессор, но при подходящем для компрессии типе данных, ты можешь обеспечить значительный прирост скорости передачи.

Не забудь, что файлы конфигурации должны, за исключением ИП-адресов, зеркально отображать себя на обоих хостах. Иначе возможны несостыковки в политиках безопасности, что приведет к невозможности согласования параметров туннеля.

для установки политик безопасности

```
arhontus racoon # setkey -f ./ipsec.conf
```

запуск демона Ракун

```
arhontus racoon # racoon -f ./racoon.conf -F -v
```

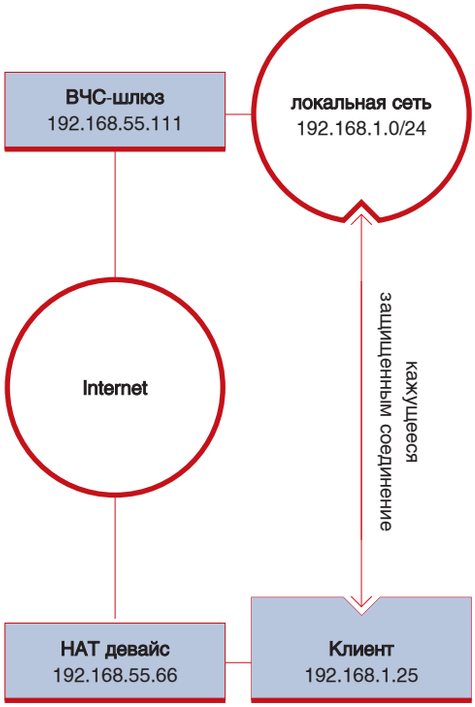
соединение инициировано простым пингом

```
arhontus racoon # ping -c 1 192.168.55.66

May 21 14:18:44 pingo racoon: INFO:
respond new phase 1 negotiation:
192.168.55.111[500]<=>192.168.55.66[500]
May 21 14:18:44 pingo racoon: INFO:
begin Identity Protection mode.
May 21 14:18:44 pingo racoon: INFO:
received Vendor ID: DPD
May 21 14:18:45 pingo racoon: INFO:
ISAKMP-SA established
192.168.55.111[500]-192.168.55.66[500]
spi:8dc4793f80eb71da:b0fd7a67799645da
May 21 14:18:47 pingo racoon: INFO:
respond new phase 2 negotiation:
192.168.55.111[500]<=>192.168.55.66[500]
May 21 14:18:47 pingo racoon: INFO:
IPsec-SA established: ESP/Transport
192.168.55.66[0]->192.168.55.111[0]
spi=26208972(0x18feacc)
May 21 14:18:47 pingo racoon: INFO:
IPsec-SA established: IPCOMP/Transport
192.168.55.66[0]->192.168.55.111[0]
spi=11347(0x2c53)
May 21 14:18:47 pingo racoon: INFO:
IPsec-SA established: ESP/Transport
192.168.55.111[0]->192.168.55.66[0]
spi=64639354(0x3da517a)
May 21 14:18:47 pingo racoon: INFO:
IPsec-SA established: IPCOMP/Transport
192.168.55.111[0]->192.168.55.66[0]
spi=20799(0x513f)
```

→ **конфигурация «хост в сеть».** Часто возникает ситуация, когда клиенту необходим доступ к ресурсам сети, но он использует динамический доступ к интернету посредством дозвона, беспроводного хот-спота и т.д. Заранее невозможно прописать его динамический ИП в политике безопасности для установки туннеля, поэтому для аутентификации таких хостов приходится применять другие методы.

Рассмотрим пример настройки ВЧС-шлюза для приема соединений таких клиентов, используя аутентификацию через x509 сертификаты, проверку их подлинности через центральный CA и использование поддержки режима работы через NAT- устройства.

→ **пример конфигурации сервера.** Опустим детальное описание настройки x509 сертификатов, благо, об этом существует достаточное количество информации как в Сети, так и в печатных изданиях, которых предостаточно в книжных магазинах. Вкратце, используя openssl, необходимо



Хост в сеть

создать свой CA (центр сертификации), а затем — подписанные сертификаты для сервера и для каждого из клиентов. Для контроля годности сертификатов необходимо выпустить CRL (список аннулирования сертификатов). Теперь помести открытый сертификат CA, а также открытую и секретную части сертификата сервера и CRL в директорию, используемую Ракуном, или сделай символический линк к директории по умолчанию (/etc/racoon/certs/).

чтобы openssl мог найти CA и CRL, их надо переименовать или слинковать к их хэшу

```
arhontus certs # ln -s cacert.pem
`openssl x509 -in cacert.pem -noout -hash`.0
arhontus certs # ln -s rootca.crl
`openssl crl -in rootca.crl -noout -hash`.r0
```

директория с сертификатами на сервере

```
arhontus certs # ls -1
8bc54ff5.0 -> cacert.pem
8bc54ff5.r0 -> rootca.crl
cacert.pem -> /etc/ssl/cacert.pem
rootca.crl -> /etc/ssl/rootca.crl
stalin.arhont.com.crt
stalin.arhont.com.key
```

файл описания политик безопасности (ipsec.conf)

```
arhontus racoon # cat ipsec.conf
#!/usr/sbin/setkey -f

# Flush the SAD and SPD
flush;
spdflush;
```

файл настройки Ракуна

```
arhontus racoon # cat racoon.conf
path certificate "/etc/racoon/certs";

listen {
 isakmp 192.168.55.111 [500];
 isakmp_natt 192.168.55.111 [4500];
 strict_address;
 }

remote anonymous {
 exchange_mode aggressive;
 generate_policy on;
 nat_traversal force;
 ike_frag on;
 esp_frag 552;
 dpd_delay 60;

 ca_type x509 "cacert.pem";
 certificate_type x509
"stalin.arhont.com.crt"
"stalin.arhont.com.key";
 verify_cert on;

 my_identifier asn1dn;
 peers_identifier asn1dn;
 verify_identifier off;

 proposal {
   lifetime time 120 min;
   encryption_algorithm rijndael256;
   hash_algorithm sha256;
   authentication_method hybrid_rsa_server;
   dh_group modp4096;
   }
 proposal_check claim;
}

mode_cfg {
 network4 192.168.1.1;
 pool_size 128;
 auth_source system;
 dns4 192.168.1.121;
 banner "/etc/racoon/motd";
}

sainfo anonymous {
 lifetime time 30 minutes;
 encryption_algorithm rijndael;
 authentication_algorithm hmac_sha1;
 compression_algorithm deflate;
 pfs_group modp2048;
}
```

Итак, теперь приступим к более подробному рассмотрению новых опций, которые будем использовать:

— `PATH CERTIFICATE "/ETC/RACOON/CERTS"`
МЕСТОНАХОЖДЕНИЕ ДИРЕКТОРИИ С СЕРТИФИКАТАМИ;

— `REMOTE ANONYMOUS {`
ОТКРЫВАЕТ СЕКЦИЮ КОНФИГУРАЦИИ ТУННЕЛЕЙ, ДЛЯ КОТОРЫХ НЕ ПРОПИСАНА ПОЛИТИКА;

— `GENERATE_POLICY ON`
ВКЛЮЧАЕТ РЕЖИМ УСТАНОВЛЕНИЯ ПОЛИТИКИ БЕЗОПАСНОСТИ, ПОЛУЧЕННОЙ ОТ КЛИЕНТА;

— `NAT_TRAVERSAL FORCE`
ИСПОЛЬЗОВАНИЕ МЕХАНИЗМА ПРЕОДОЛЕНИЯ NAT ВО ВСЕХ СЛУЧАЯХ;

— `IKE_FRAG ON`
ВКЛЮЧЕНИЕ РЕЖИМА ПОДДЕРЖКИ ФРАГМЕНТАЦИИ IKE;

— `ESP_FRAG 552`
ВКЛЮЧЕНИЕ РЕЖИМА ПОДДЕРЖКИ ФРАГМЕНТАЦИИ ПАКЕТА ДО ИНКАПСУЛЯЦИИ В ESP;

— `CA_TYPE X509 "CACERT.PEM"`
ИМЯ ФАЙЛА CA;

— `CERTIFICATE_TYPE X509 "STALIN.ARHONT.COM.CRT" "STALIN.ARHONT.COM.KEY"`
ТИП И ИМЯ ОТКРЫТОГО СЕРТИФИКАТА И СЕКРЕТНОГО КЛЮЧА СЕРВЕРА;

— `VERIFY_CERT ON`
ВКЛЮЧЕНИЕ ПОДДЕРЖКИ ПРОВЕРКИ СЕРТИФИКАТА КЛИЕНТА;

— `AUTHENTICATION_METHOD HYBRID_RSA_SERVER`
ВЫБОР HYBRID_RSA_SERVER МЕТОДА АУТЕНТИФИКАЦИИ;

— `MODE_CFG {`
ОТКРЫТИЕ СЕКЦИИ КОНФИГУРАЦИИ ИНФОРМАЦИИ ДЛЯ КЛИЕНТА;

— `NETWORK4 192.168.1.1`
ОПРЕДЕЛЕНИЕ РЯДА ИП-АДРЕСОВ, НАЗНАЧАЕМЫХ КЛИЕНТАМ;

— `POOL_SIZE 128`
РАЗМЕР РЯДА ИП-АДРЕСОВ, НАЗНАЧАЕМЫХ КЛИЕНТАМ;

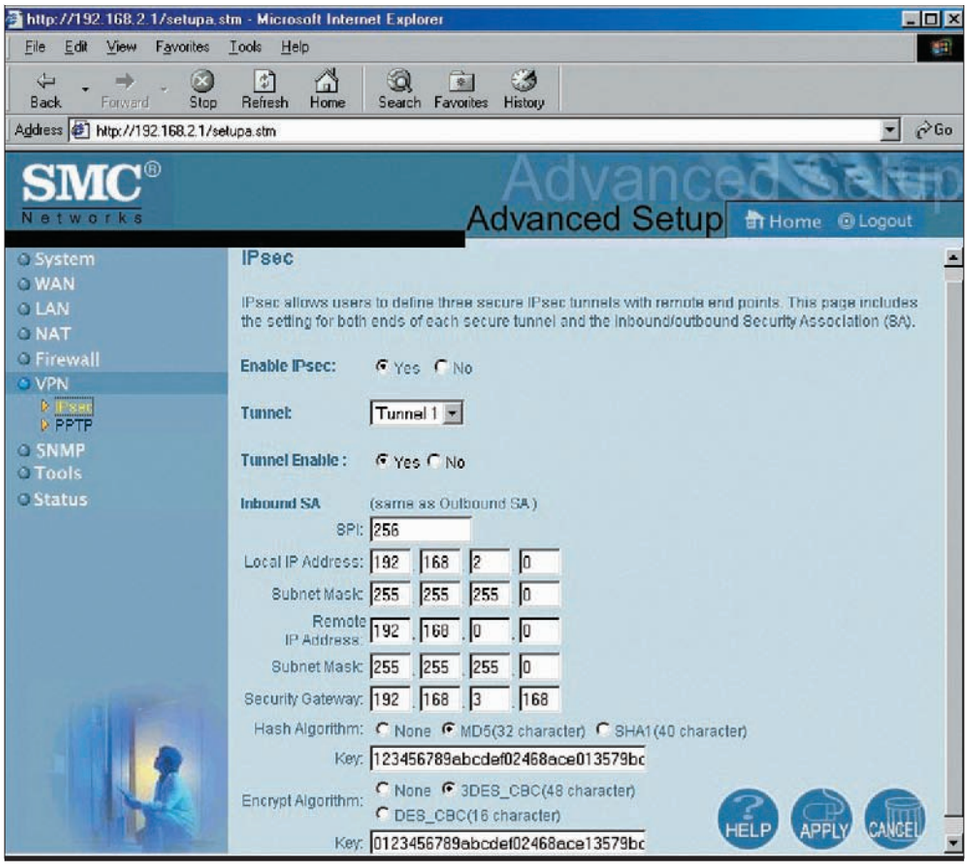
— `AUTH_SOURCE SYSTEM`
МЕХАНИЗМ АУТЕНТИФИКАЦИИ;

— `DNS4 192.168.1.121`
ИП-АДРЕС DNS-СЕРВЕРА, НАЗНАЧАЕМОГО КЛИЕНТАМ;

— `BANNER "/ETC/RACOON/MOTD"`
ПУТЬ К ФАЙЛУ ЗАГОЛОВКА, ПЕРЕДАВАЕМОМУ КЛИЕНТАМ.

➔ **конфигурация клиента.** Процесс конфигурации клиента практически такой же, как и для сервера, за исключением некоторых опций в файле конфигурации Ракуна.

```
dyno racoon # cat racoon.conf
path certificate "/etc/racoon/certs";

listen {
 isakmp 192.168.55.66 [500];
 isakmp_natt 192.168.55.66 [4500];
 strict_address;
 }

remote 192.168.55.111 {
 exchange_mode aggressive;
 nat_traversal force;
 ike_frag on;
 esp_frag 552;
 dpd_delay 60;

 ca_type x509 "cacert.pem";
 certificate_type x509
"berija.arhont.com.crt"
"berija.arhont.com.key";
 verify_cert on;

 my_identifier asn1dn;
 peers_identifier asn1dn;
 verify_identifier off;

 mode_cfg on;
 script "/etc/racoon/phase1-up.sh"
phase1_up;
 script "/etc/racoon/phase1-down.sh"
phase1_down;
 passive off;

 proposal {
  lifetime time 120 min;
  encryption_algorithm rijndael256;
  hash_algorithm sha256;
  authentication_method
hybrid_rsa_client;
  dh_group modp4096;
  }
 proposal_check obey;
}

sainfo anonymous {
 lifetime time 30 minutes;
 encryption_algorithm rijndael;
 authentication_algorithm hmac_sha1;
 compression_algorithm deflate;
 pfs_group modp2048;
}
```



Пример настройки IPSec на роутере

Обзор новых опций в файле конфигурации клиента:

— `MODE_CFG ON`
ВКЛЮЧЕНИЕ РЕЖИМА ЗАПРОСА ОПЦИЙ КЛИЕНТА;

— `SCRIPT "/ETC/RACOON/PHASE1-UP.SH" PHASE1_UP`
ПУТЬ К СКРИПТУ, ИСПОЛЬЗУЕМОМУ ПРИ ВЫПОЛНЕНИИ ПЕРВОЙ ФАЗЫ ОБМЕНА;

— `SCRIPT "/ETC/RACOON/PHASE1-DOWN.SH" PHASE1_DOWN`
ПУТЬ К СКРИПТУ, ИСПОЛЬЗУЕМОМУ ПРИ ОКОНЧАНИИ ПЕРВОЙ ФАЗЫ ОБМЕНА.

После завершения конфигурации клиента запусти демон Ракун. В настоящей конфигурации политика безопасности не прописана, соответственно, ядро не знает, какие пакеты нуждаются в защите, и не инициирует соединение — это нужно сделать вручную.

инициирование туннеля

```
arhontus racoon # racoonctl vpn-connect
-u g_kos 192.168.55.111
Password:
Bound to address 192.168.1.1
=======================================
=====================
# This is a PROTECTED device — UNAUTHO-
RIZED ACCESS IS PROHIBITED! #
```

Для успешного подключения необходимо иметь годный сертификат, подписанный центром сертификации, учетную запись и пароль на ВЧС-шлюзе.

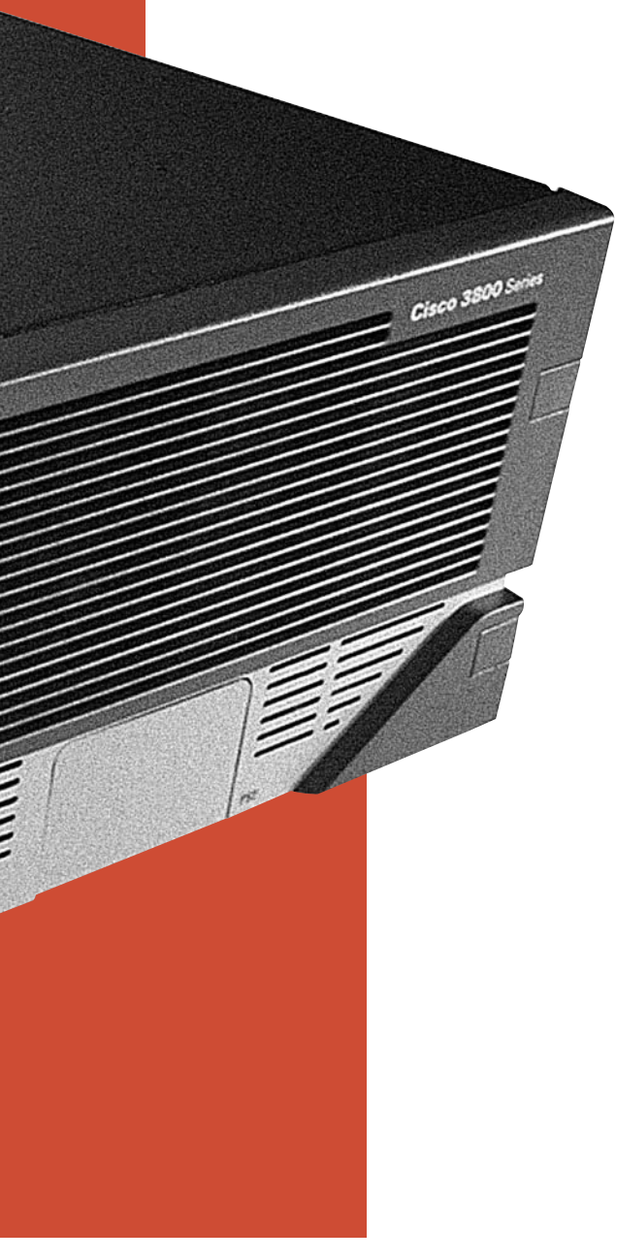
➔ **эпилог.** Всегда имей в виду, что IPSec — достаточно сложный протокол, особенно для начинающего пользователя, что увеличивает вероятность возникновения крупной ошибки. Дополнительные затруднения при установлении соединения могут возникать при использовании различных версий одного продукта и, что более вероятно, различных имплементаций от разных производителей. Начинай с простых решений: меньше вероятность того, что что-нибудь выйдет из под контроля. Не стремись устанавливать самые мощные алгоритмы шифрования. Даже для очень продвинутого хакера проще, и обычно результативнее, попытаться найти уязвимости в ВЧС-шлюзе, чем расшифровать закриптованный пакет. А в случае, если твоими данными заинтересовались спецслужбы, то они скорее всего не станут заниматься криптоанализом трафика, а применят более эффективный метод ректотермального криптоанализа. Так что рассматривай IPSec не как панацею, а только как одну из частей многогранной мозаики систем безопасности C


NM-AIR-WLC6
NOT SUPPORTED
LINK
ACT
PWR
EN
Fast Ethernet 0
Cisco Systems
SYS
ACT
SYS PWR1
AUX PWR1
SYS PWR2
AUX PWR2
PS1

63

КОНТРОЛЬ ЖЕЛЕЗА

в разделе:



скрытая мощь

МЕХАНИЗМЫ ЗАЩИТЫ МАРШРУТИЗАТОРОВ CISCO

ЕСЛИ О НАДЕЖНОСТИ И ФУНКЦИОНАЛЬНОСТИ МАРШРУТИЗАТОРОВ И КОММУТАТОРОВ CISCO ВСЕ НАСЛЫШАНЫ, ТО О БЕЗОПАСНОСТИ МАЛО КТО ЗНАЕТ

АЛЕКСЕЙ ЛУКАЦКИЙ
{alukatsk@cisco.com}

В любой маршрутизатор Cisco встроены: прозрачный межсетевой экран Cisco IOS Firewall, средство построения VPN (IPSec или SSL) Cisco IOS VPN, прозрачная система предотвращения атак (Intrusion Prevention System) Cisco IOS IPS. Помимо этих хорошо известных механизмов существует и множество других, не менее важных и полезных функций, делающих из обычного маршрутизатора полноценное защитное устройство, ориентированное на защиту небольших и средних офисов. Аналогичный тезис применим и к коммутаторам.

→ **с чего начинается администрирование маршрутизатора.** Администрирование функций безопасности нужно для защиты сети (внешней и внутренней) от несанкционированной активности. А значит, прежде чем начинать копаться в настройках оборудования, необходимо понять, что и от чего ты защищаешь. Начинай с политики безопасности, которая должна:

- ОПИСЫВАТЬ, КАКИЕ РЕСУРСЫ, КОМУ, КОГДА И КАК МОЖНО ИСПОЛЬЗОВАТЬ;
- ОПИСЫВАТЬ ВСЕ ИНФОРМАЦИОННЫЕ ПОТОКИ В ЗАЩИЩАЕМОЙ СЕТИ;
- НЕ ЗАБЫВАТЬ О ЗАЩИТЕ САМИХ СРЕДСТВ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ;

— БЫТЬ ТЕХНИЧЕСКИ РЕАЛИЗУЕМОЙ;

— БЫТЬ ПОСЛЕДОВАТЕЛЬНОЙ;

— БЫТЬ ГЛОБАЛЬНОЙ И ПРИМЕНИМОЙ КО ВСЕЙ СЕТИ, А НЕ К ОТДЕЛЬНЫМ ЕЕ СЕГМЕНТАМ;

— ЧЕТКО ОПИСЫВАТЬ РОЛИ И ОТВЕТСТВЕННОСТЬ ВСЕХ ЗАИНТЕРЕСОВАННЫХ ЛИЦ;

— БЫТЬ ГИБКОЙ К ПОСТОЯННО ИЗМЕНЯЮЩИМСЯ ТЕХНОЛОГИЯМ И БИЗНЕС-ПРОЦЕССАМ;

— БЫТЬ ПОНЯТНОЙ;

— ВКЛЮЧАТЬ В СЕБЯ НЕ ТОЛЬКО ЗАДАЧИ ОТРАЖЕНИЯ УГРОЗ, НО И ПРОЦЕССЫ РАССЛЕДОВАНИЯ И РЕАГИРОВАНИЯ НА АТАКИ.

И еще грамотная политика безопасности не должна диктовать бизнесу, как ему работать — все должно быть с точностью наоборот. При этом политика не должна зависеть от используемых средств защиты. Сегодня это может быть маршрутизатор Cisco 871W, завтра маршрутизатор Cisco ISR 3845, а послезавтра многофункциональное защитное устройство «все в одном» Cisco ASA 5550. Грамотная политика будет без изменений «работать» для любого из этих устройств. Более того, если требования по защите не очень специфичны, то эта же политика может быть использована и для других производителей средств защиты.

→ **принципы безопасности маршрутизаторов Cisco.** Маршрутизатор может быть логически разделен на 4 функциональных компонента, отвечающих за решение своих задач:

[1] DATA PLANE — УРОВЕНЬ ДАННЫХ, ЧЕРЕЗ КОТОРЫЙ ПРОХОДИТ ВЕСЬ СЕТЕВОЙ ТРАФИК.

[2] CONTROL PLANE — УРОВЕНЬ ПОСТРОЕНИЯ И ОБНОВЛЕНИЯ ТАБЛИЦ МАРШРУТИЗАЦИИ.

[3] MANAGEMENT PLANE — УРОВЕНЬ УПРАВЛЕНИЯ МАРШРУТИЗАТОРОМ (SSH, SNMP, SYSLOG И Т.Д.)

[4] SERVICE PLANE — УРОВЕНЬ ОБЕСПЕЧЕНИЯ КАЧЕСТВА СЕРВИСА И ОБСЛУЖИВАНИЯ.

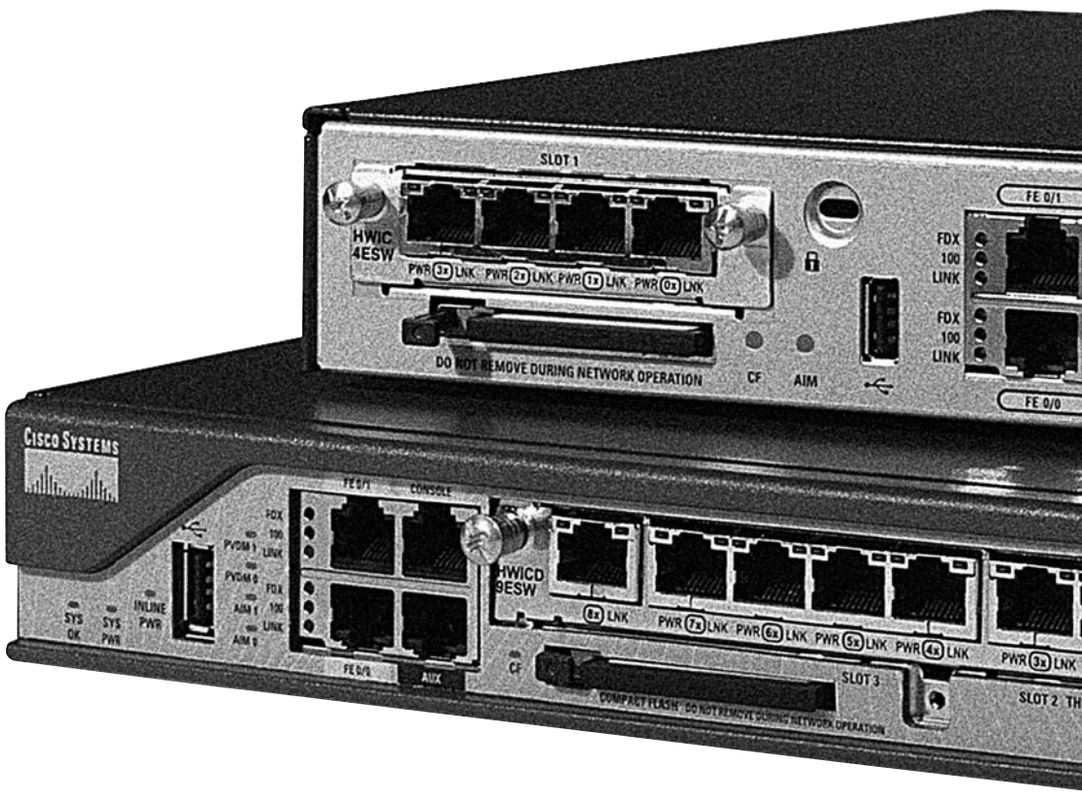
Очевидно, что механизмы защиты маршрутизаторов должны быть применены ко всем этим уровням без исключения. Причем защита уровней управления и контроля зачастую является даже более важной, чем уровень безопасности данных. Списки контроля доступа (Access Control List, ACL), однонаправленная проверка передачи по обратному маршруту (Unicast Reverse Path Forwarding, uRPF), ограничение полосы пропускания (Committed Access Rate, CAR) и так далее, очень важны, но позволяют ограничить только определенные типы трафика. А вот недооценка вопросов самозащиты самого маршрутизатора может повлечь за собой печальные последствия — захват и компрометация всего устройства, локальное или дистанционное изменение таблиц маршрутизации, перехват трафика, реализация атак «отказ в обслуживании» (Denial of Service, DoS) и т.п.

→ **autosecure**. Несколько лет назад по интернету ходил анекдот: «Чем отличается Windows 95 от Windows 98? Тем, что в Windows 95 не используется 95% возможностей, а в Windows 98 не используется 98% возможностей». Отчасти это так. Производители, чтобы удовлетворить как можно больше запросов со стороны своих заказчиков, оснащают свои продукты очень большим количеством функций, которые зачастую висят «мертвым» грузом и у многих попросту не используются (многие ли используют асимметричную маршрутизацию?). Хорошо, если эти функции просто не мешают. А если они становятся каналом проникновения злоумышленников?

При администрировании операционных систем существует правило — «отключить все, что не нужно для выполнения поставленных задач». Аналогичное правило применимо и к сетевому оборудованию. Вручную отключать десятки неиспользуемых механизмов — дело неблагодарное (можно что-то и забыть). Поэтому в маршрутизаторах Cisco, начиная с версии IOS 12.3, появился механизм AutoSecure, который:

— ЗАПРЕЩАЕТ ПОТЕНЦИАЛЬНО ОПАСНЫЕ ГЛОБАЛЬНЫЕ СЕРВИСЫ (FINGER, PACKET ASSEMBLER AND DISASSEMBLER, TCP/UDP SMALL SERVICES, BOOTP SERVER, HTTP SERVER, CDP, NTP, SOURCE ROUTING...);

— ЗАПРЕЩАЕТ ПОТЕНЦИАЛЬНО ОПАСНЫЕ СЕРВИСЫ ПО ИНТЕРФЕЙСАМ (ICMP, PROXY-ARP, BROADCAST, MOP, ICMP UNREACHABLE, ICMP REPLY);



— ВКЛЮЧАЕТ РАСШИРЕННЫЕ МЕХАНИЗМЫ ЗАЩИТЫ (ШИФРОВАНИЕ ПАРОЛЕЙ, НАСТРОЙКА БАННЕРОВ, ВЗАИМОДЕЙСТВИЕ С СЕРВЕРАМИ АУТЕНТИФИКАЦИИ, АНТИСПУФИНГ, CISCO EXPRESS FORWARDING, БЛОКИРОВАНИЕ ЗАРЕЗЕРВИРОВАННЫХ АДРЕСОВ IANA, УСТАНОВКА МАРШРУТА ПО УМОЛЧАНИЮ NULL 0, CBAC, NETFLOW...);

— ОБЕСПЕЧИВАЕТ ЗАЩИТУ САМОГО МАРШРУТИЗАТОРА (SSH И SCP, НАСТРОЙКА ПАРОЛЕЙ И УЧЕТНЫХ ЗАПИСЕЙ, БЛОКИРОВАНИЕ SNMP...);

— ВКЛЮЧАЕТ РЕГИСТРАЦИЮ СОБЫТИЙ БЕЗОПАСНОСТИ.

Cisco AutoSecure может функционировать в двух режимах — интерактивном и автоматическом. В первом случае администратор отвечает на вопросы по своей собственной сети, а во втором — настройка осуществляется автоматически, в соответствие с параметрами по умолчанию. Причем включить Cisco AutoSecure можно всего одной командой: Router# auto secure.

По окончании работы сервиса на экран выводится список всех сделанных настроек, и администратор должен разрешить все сделанные изменения. Проверка может быть осуществлена двумя путями — с помощью Security Device Manager (SDM) и команды IOS EXEC, которая показывает настройки, сделанные после AutoSecure. Наиболее интересен именно первый путь (функция Security Audit), так как он позволяет в удобном виде получить ответ на вопрос: «Какие из существующих механизмов защиты включены, а какие нет?».

➔ **расширения ios login**. Начиная с версии IOS 12.2(25)S, маршрутизаторы Cisco могут существенно усложнить жизнь злоумышленникам, желающим получить несанкционированный доступ к сетевому оборудованию. Одна из распространенных атак, позволяющих получить такой доступ, — подбор пароля. Для этого используются различные утилиты, к примеру, THC-Hydra или Brutus. Самый простой путь блокировать эту атаку — увеличить время задержки между попытками ввода логина и пароля. Сделать это можно тремя путями: через уже описанную функцию AutoSecure или с помощью специальных команд — login delay и login block-for. Эти команды можно использовать и в паре:

```
Router(config)# login block-for 100
attempts 5 within 50
Router(config)# login quiet-mode
access-class myacl
Router(config)# login delay 10
Router(config)# login on-failure log
Router(config)# login on-success log
```

Первая команда должна вводиться до использования любых других команд login. Она на 100 секунд блокирует любые попытки подключения к устройству, если в течение 50 секунд было осуществлено 5 неудачных регистраций на маршрутизаторе. Если есть адреса, которые не должны быть блокированы (например, административные), то они описываются командой login quiet-mode access-class. Команда login delay определяет время задержки перед разрешением повторной регистрации. Если ее не указать, то автоматическая задержка будет осуществлена по команде login block-for на 1 секунду. Последние 2 команды включают регистрацию успешных и неудачных попыток подключения к маршрутизатору.

Проверить настройки подсистемы регистрации можно путем использования команды show login. А команда show login failures показывает все неудачные попытки подключения к устройству.

➔ **защита уровня контроля.** Почти все архитектуры уязвимы к атакам «отказ в обслуживании». При воздействии на сетевое оборудование она несет серьезную опасность, так как выведение его из строя приводит к неработоспособности всей сети. Необходимо оградить процессор маршрутизатора от обработки вредоносного трафика, и, начиная с версии IOS 12.2, такая возможность появилась и стала носить название Control Plane Policing. С ее помощью можно:

— КЛАССИФИЦИРОВАТЬ И ОГРАНИЧИТЬ КАЖДЫЙ КЛАСС ТРАФИКА, ПОСТУПАЮЩИЙ НА ОБРАБОТКУ В УРОВЕНЬ КОНТРОЛЯ;

— ОБЕСПЕЧИТЬ МЕХАНИЗМ РАННЕГО ОТБРАСЫВАНИЯ ПАКЕТОВ, НАПРАВЛЕННЫХ НА ЗАКРЫТЫЕ ИЛИ ИНЫЕ TCP/UDP-ПОРТЫ;

— ОБЕСПЕЧИТЬ ЗАЩИТУ ОТ ПРОТОКОЛЬНОГО ФЛУДИНГА;

— ОБЕСПЕЧИТЬ QOS ДЛЯ ПАКЕТОВ, НАПРАВЛЕННЫХ НА УРОВЕНЬ КОНТРОЛЯ;

— ОБЕСПЕЧИТЬ НАДЕЖНОСТЬ, ЗАЩИЩЕННОСТЬ И ДОСТУПНОСТЬ.

Для реализации данного механизма необходимо пройти 4 обязательных и 2 опциональных шага:

1. ЗАДАТЬ КРИТЕРИИ ДЛЯ КЛАССИФИКАЦИИ ПАКЕТОВ.
2. ОПРЕДЕЛИТЬ ПОЛИТИКИ СЕРВИСА.
3. ПЕРЕЙТИ В РЕЖИМ НАСТРОЙКИ.
4. ПРИМЕНИТЬ ПОЛИТИКИ.
5. НАСТРОИТЬ ПОЛИТИКИ ФИЛЬТРАЦИИ ПОРТОВ (ДЛЯ РАННЕГО ОТБРАСЫВАНИЯ ПАКЕТОВ).
6. НАСТРОИТЬ ПОЛИТИКИ ПОРОГОВЫХ ЗНАЧЕНИЙ (ЗАЩИТА ОТ ПРОТОКОЛЬНОГО ФЛУДИНГА).

Для реализации первой задачи необходимо использовать 2 команды: задающую имя класса трафика (class-map) и описывающую критерии для данного трафика (match). Параметр match-any говорит о том, что хотя бы один критерий классификации должен встретиться в трафике (использование параметра match-all требует обнаружения всех критериев):

```
Router(config)# class-map match-any
control-plane-class
Router(config-cmap)# match access-group
name cpp-icmp-ac1
```

Для определения политики необходимо выполнить 3 команды: задающую имя политики (policy-map), класс (class) и определяющую политику (police):

```
Router(config)# policy-map
control-plane-policy
Router(config-pmap)# class
control-place-class
Router(config-pmap-c)# police rate
50000 pps conform-action transmit
exceed-action drop
```

Применение политики осуществляется в 2 задачи — связывание политики с субинтерфейсом (control-plane) и указание имени используемой политики:

```
Router(config)# control-plane host
Router(config-cp)# service-policy input
control-plane-policy
```

Для оставшихся 2-х опциональных задач необходимо использование команды class-map type, схожей по синтаксису с командами, описанными выше. Фильтрация портов и пороговых значений описывается следующим образом:

```
Router(config)# class-map type
port-filter match-all pf-class
Router(config-cmap)# match closed-ports
Router(config-cmap)# exit
Router(config)# policy-map type
port-filter cppr-pf-policy
Router(config-pmap)# class pf-class
Router(config-pmap-c)# drop
Router(config-pmap-c)# end
Router(config)# control-plane host
Router(config)# service-policy
input cppr-pf-policy

Router(config)# class-map type
queue-threshold qt-snmp-class
Router(config-cmap)# match protocol snmp
Router(config-cmap)# class-map type
queue-threshold qt-telnet-class
Router(config-cmap)# match protocol telnet
Router(config-cmap)# class-map type
queue-threshold qt-other-class
Router(config-cmap)# match host-protocols
Router(config-cmap)# exit
Router(config)# policy-map type
queue-threshold qt-policy
Router(config-pmap)# class qt-snmp-class
Router(config-pmap-c)# queue-limit 50
Router(config-pmap-c)# class
qt-telnet-class
Router(config-pmap-c)# queue-limit 50
Router(config-pmap-c)# class
qt-other-class
Router(config-pmap-c)# queue-limit 150
Router(config-pmap-c)# end
```

Проверить настройки подсистемы регистрации можно путем использования команды show policy map control-plane.

➔ **защита уровня управления.** Механизм Control Plane Policing (CoPP) позволяет защитить маршрутизатор от обработки вредоносного трафика и не дать ему попасть в защищаемую сеть. Однако, все равно остается проблема защиты самого устройства от несанкционированного доступа. Эту задачу решает механизм Management Plane Policing (MPP), который позволяет описать один или несколько интерфейсов маршрутизатора как управляющие, что, в свою очередь, блокирует любые попытки управления с «неуправляющих» интерфейсов. Иными словами, ты ограничиваешь доступ по протоколам FTP, HTTP, HTTPS, SSH, Telnet, SNMP и TFTP. Это, конечно, можно было бы реализовать и с помощью списков контроля доступа (ACL), но в этом случае снижается производительность и масштабируемость маршрутизатора, вынужденного тратить ресурсы на обработку ACL. Настройка данного механизма осуществляется достаточно просто:

```
Router(config)# control-plane host
Router(config-cp-host)# management-in-
terface FastEthernet 0/0 allow ssh snmp
```

Первая команда включает режим конфигурации, а вторая — задает его настройки. После параметра allow можешь указать протоколы, которые разрешаются на данном интерфейсе (в приведенном примере только SSH и SNMP).

Проверить наличие и настройки управляющих интерфейсов можно командой Router# show management-interface.

➔ **CPU и Memory Thresholding Notification.** Очень часто признаком атаки «отказ в обслуживании» или другой вредоносной активности является перегрузка центрального процессора или нехватка памяти, вызванные наличием какого-нибудь процесса, «забирающего» все ресурсы «под себя». Механизм контроля аналогичных действий есть в маршрутизаторах Cisco: в CPU и Memory Threshholding Notification.

В первом случае можешь сигнализировать, когда загрузка процессора начнет превышать максимально заданную или падает ниже минимально заданной границы. Делается это следующим образом:

```
Router(config)# snmp-server enable
traps cpu threshold
Router(config)# snmp-server host
192.168.0.0 traps public cpu
Router(config)# process cpu threshold
type total rising 80 interval 5 falling
20 interval 5
```

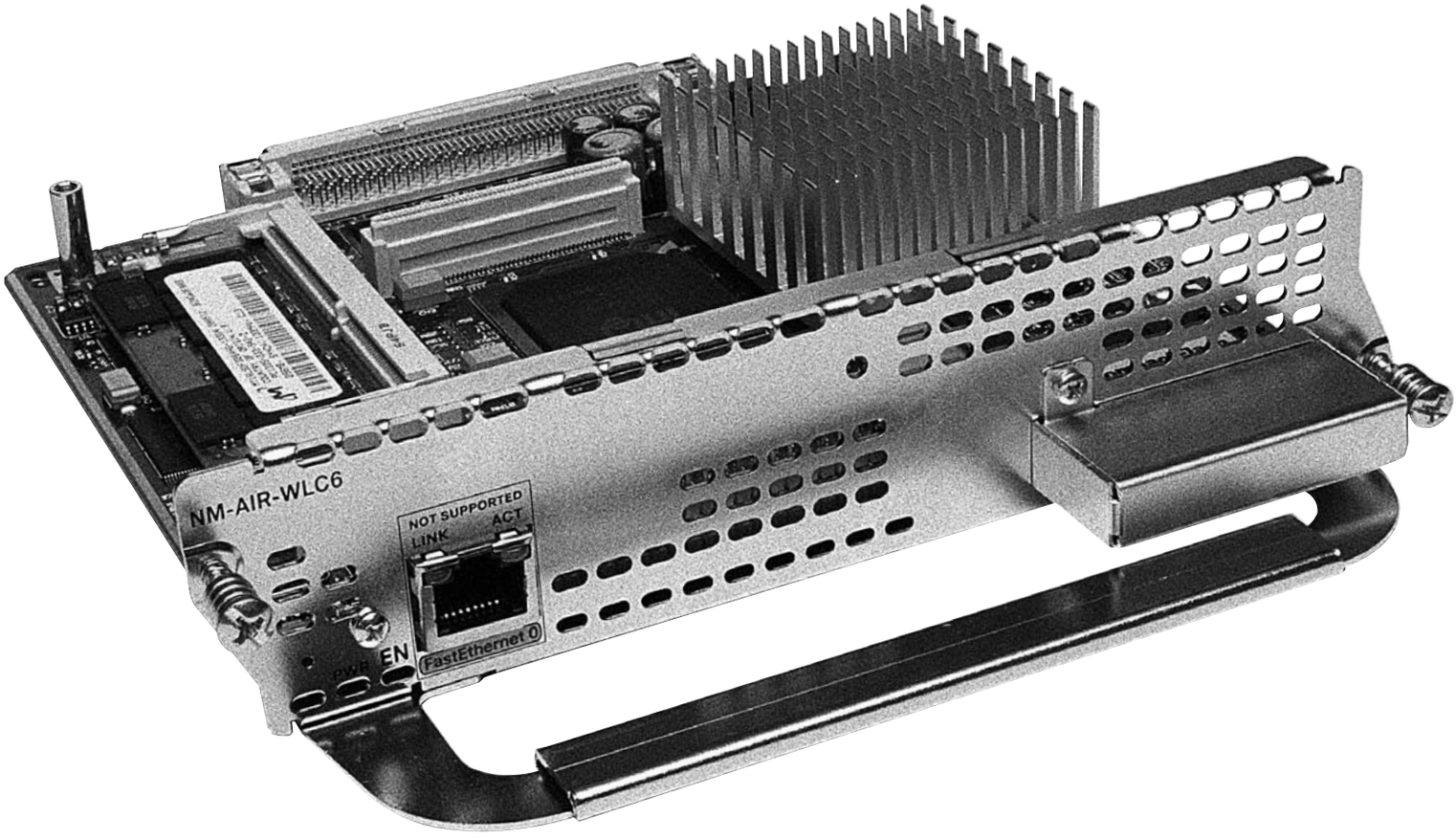
Первая команда разрешает посылать уведомления о нарушении, связанном с загрузкой процессора. Вторая описывает адрес, на который посылается SNMP Trap. Третья команда устанавливает пороговые значения: верхняя граница — 80% и нижняя граница — 20% (5 — это интервал запроса значения загрузки CPU).

Задание уведомления о критическом превышении доступной памяти выполняется аналогичным образом. При этом ты видишь генерацию сигнала тревоги, когда в маршрутизаторе остается меньше 20 Кб свободной процессорной памяти или памяти ввода/вывода:

```
Router(config)# memory free
low-watermark processor 20000
или
Router(config)# memory free
low-watermark io 20000
```

С сигнализацией о нехватке памяти связан механизм выделения определенного объема памяти под критичные задачи (например, под регистрацию событий). Это позволяет быть уверенным, что важная операция все равно будет произведена даже при условии нехватки памяти. При этом резервируемая память не должна превышать 25% от всего объема доступной памяти:

```
Router(config)# memory reserve critical 1000
```



➔ **IOS Software Image Verification.** Регулярно на различных форумах всплывает тема встраивания «чужого» кода в Cisco IOS, и какая это огромная угроза всему интернету. Но с самого начала целостность кода, загружаемого на маршрутизатор, можно проверять — достаточно сравнить контрольную сумму MD5 имиджа IOS, установленного на устройство, с суммой, показанной на сайте **cisco.com**. Однако не многие пользователи делали это, ссылаясь на сложность и длительность процедуры. Чтобы облегчить такую «непростую» задачу, у пользователей в версии 12.0(26)S появилась команда verify, которую можно и удобно использовать в трех случаях:

1 ГЛОБАЛЬНАЯ И АВТОМАТИЧЕСКАЯ ПРОВЕРКА ЦЕЛОСТНОСТИ ИМИДЖА (ПОСЛЕ ЛЮБОЙ ПОПЫТКИ КОПИРОВАНИЯ ИЛИ ПЕРЕЗАГРУЗКИ):

```
Router(config)# file verify auto
```

2 ПРОВЕРКА ЦЕЛОСТНОСТИ ИМИДЖА ПОСЛЕ КОПИРОВАНИЯ ИЗ КАКОГО-ЛИБО ИСТОЧНИКА:

```
Router(config)# copy /verify
tftp://10.1.1.1/jdoe/c7200-js-mz
disk0:
```

3 ПРОВЕРКА ЦЕЛОСТНОСТИ ИМИДЖА ПОСЛЕ ПЕРЕЗАГРУЗКИ УСТРОЙСТВА:

```
Router# reload /verify
```

➔ **Flexible Packet Matching.** Многие слышали о том, что в маршрутизаторы Cisco встроена система предотвращения атак Cisco IOS IPS. Но очень мало кто слышал о Flexible Packet Matching, которая позволяет описывать и обнаруживать любые интересующие события, например, атаки, для которых еще никто не написал сигнатуры. Делается это с помощью XML, который позволяет описать любые поля заголовка пакета и тела данных любого протокола. Для наиболее распространенных из них существуют специальные файлы описания заголовка протокола — Protocol Header Definition File, PHDF.

фрагмент PHDF файла для протокола IP:

```
<?xml version="1.0" encoding="UTF-8"?>
<phdf>
 <version>1</version>
 <protocol name="ip" description=
"Definition-for-the-IP-protocol">
  <field name="version"
description="IP-version">
   <offset type="fixed-offset"
units="bits">0</offset>
   <length type="fixed"
units="bits">4</length>
  </field>
  <field name="ihl" description="IP-He-
ader-Length">
   <offset type="fixed-offset"
units="bits">4</offset>
   <length type="fixed"
units="bits">4</length>
  </field>
  <field name="tos" description="IP-Ty-
pe-of-Service">
   <offset type="fixed-offset"
units="bits">8</offset>
   <length units="bits" type="fi-
xed">8</length>
  </field>
…
  <headerlength type="fixed" va-
lue="20"></headerlength>
  <constraint field="version" value="4"
operator="eq"></constraint>
  <constraint field="ihl" value="5"
operator="eq"></constraint>
 </protocol>
</phdf>
```

Описать же любую атаку с помощью FPM становится совсем нетрудно (если понимать критерии этой атаки).

классический SYN Flood:

```
! Загружаем файлы описания заголовков
IP и TCP
Router(config)# load protocol
flash:ip.phdf
Router(config)# load protocol
flash:tcp.phdf
! В классе stack определяем
последовательность заголовков
Router(config)# class-map type stack
match-all ip_tcp
Router(config-cmap)# description "match
TCP over IP packets"
Router(config-cmap)# match field ip
protocol eq 0x6 next tcp
! Определяем критерии для атаки SYN Flood
Router(config)# class-map type
access-control match-all tcpsynflood
Router(config-cmap) # description
"match on tcp syn packets from source
```

```
address 10.10.10.3"
Router(config-cmap)# match field ip
source-addr eq 10.10.10.3
Router(config-cmap)# match field tcp
control bits eq 2 mask 0x3D
! Определяем действие для данного
трафика (блокирование), а потом
применяем данную политику (!) к нужному
интерфейсу
Router(config)# policy-map type
access-control fpm_tcp_syn_policy
Router(config-pmap)# description
"policy for TCP SYN flood attacks"
Router(config-pmap)# class tcpsynflood
Router(config-pmap-c)# drop
Router(config)# policy-map type
access-control fpm_policy
Router(config-pmap)# description
"drop tcp syn packets from source
address 10.10.10.3"
Router(config-pmap)# class ip_tcp
Router(config-pmap-c)# service-policy
fpm_tcp_syn_policy
Router(config)# interface GigabitEthernet 0/1
Router(config-if)# service-policy type
access-control input fpm_policy
```

➔ **Advanced Application Inspection and Control.** Решения Cisco давно вышли из определения, данного в любом компьютерном словаре термину «маршрутизатор». Например, когда говорят о контроле доступа к защищаемым ресурсам (внешним или внутренним), то обычно первое, что приходит в голову — списки контроля доступа (Access Control List, ACL), существующие в любом маршрутизаторе. Однако, как только заговаривают о контроле прикладного трафика (например, блокировании Instant Messaging или P2P), то все начинают смотреть в сторону отдельных устройств. А ведь в маршрутизаторах Cisco есть и такие функции защиты. И это не только описанный выше Flexible Packet Matching или известный не первый год механизм Network-Based Application Recognition (NBAR). Для контроля того же прикладного трафика можно использовать команду ip inspect.

фрагмент конфигурации для дополнительной проверки популярных протоколов на соответствие политике безопасности:

```
ip inspect name my-ios-fw http
ip inspect name my-ios-fw https
ip inspect name my-ios-fw esmtp
ip inspect name my-ios-fw pop3
ip inspect name my-ios-fw imap3
ip inspect name my-ios-fw dns
ip inspect name my-ios-fw ftp
ip inspect name my-ios-fw ntp
ip inspect name my-ios-fw icmp
```

Для не столь популярных протоколов ситуация сильно не меняется — надо добавить всего одну команду:

```
ip port-map user-vnc port tcp 5900
ip inspect name my-ios-fw user-vnc
```

После этого можно применить данные правила к нужному интерфейсу маршрутизатора:

```
interface fastethernet 0/1
ip inspect my-ios-fw in
```

А для инспекции разрешенного трафика, внутри которого может скрываться трафик запрещенный (именно так часто инкапсулируется Instant Messaging или P2P), достаточно использовать команды:

```
appfw policy-name abuse-control
application http
port-misuse default action reset alarm
ip inspect name my-ios-fw appfw
abuse-control
```

➔ **IP Source Tracker.** Итак, есть достаточное количество механизмов обнаружения и отражения атак и другой подозрительной активности. Что теперь делать, когда пришел сигнал о попытке несанкционированного доступа? Сидеть, сложа руки, — не совсем правильно :). Надо быстро отследить источник атаки и собрать доказательства его вредоносной деятельности, чтобы разобраться самому или передать дело в руки правоохранительных органов. Особенно важно сделать это при подмене адреса, когда ты не знаешь, с какого интерфейса маршрутизатора пришел вредоносный трафик, и куда двигаться в дальнейшем расследовании. Для решения этой задачи можно использовать механизмы маршрутизаторов Cisco IOS: ACL, NetFlow, uRPF и т.д. Но наиболее эффективный способ — задействование специальной функции IP Source Tracker. Фрагмент конфигурации будет выглядеть следующим образом:

```
Router(config)# ip source-track 192.168.1.1
```

Эта команда позволяет отслеживать трафик, получаемый с адреса 192.168.1.1. Посмотреть статистику по данному адресу можно командой show ip source-track.

➔ **финал.** Выше было кратко описано 10 механизмов защиты маршрутизаторов Cisco... Это много или мало? Для статьи — безусловно, немало. Для понимания всей мощи защитных механизмов оборудования Cisco — капля в море. Всего в маршрутизаторах Cisco существует свыше сотни различных механизмов, которые позволяют обнаруживать, отражать и расследовать различные нарушения политики безопасности. Зачастую достаточно просто настроить существующий функционал, чтобы покрыть все потребности небольшого офиса в защите. А если добавить сюда возможность маршрутизаторов Cisco ISR выполнять функции беспроводной точки доступа, коммутатора начального уровня, телефонной станции и так далее, то становится ясно, что для эффективного и надежного подключения небольшой сети к интернету достаточно всего одного устройства.

Его цена может быть несколько выше, чем цена на маршрутизаторы D-Link, Zyxell, 3Com и других производителей. Но если суммировать цену нескольких коробок, решающих те же задачи, что и один маршрутизатор Cisco, то выгода станет очевидной **C**

сэкономь деньги — закажи журнал в редакции

ВЫГОДА

Цена подписки до 15% ниже, чем в розничной продаже
Бонусы, призы и подарки для подписчиков
Доставка за счет редакции

ГАРАНТИЯ

Ты гарантированно получишь все номера журнала
Единая цена по всей России

СЕРВИС

Заказ удобно оплатить через любое отделение банка
Доставка осуществляется заказной бандеролью или курьером

КАК ОФОРМИТЬ ЗАКАЗ

1 Заполнить купон и квитанцию
2 Перечислить стоимость подписки через любой банк
3 Обязательно прислать в редакцию копию оплаченной квитанции с четко заполненным купоном любым из перечисленных способов:

— по электронной почте: **subscribe@glc.ru**;
— по факсу: (495) 780-88-24;
— по адресу: 119021, Москва, ул. Тимура Фрунзе, д. 11, стр. 44-45, ООО «Гейм Лэнд», отдел подписки.

Внимание!
Подписка оформляется в день обработки купона и квитанции.

— купоны, отправленные по факсу или электронной почте, обрабатываются в течение 5 рабочих дней.
— купоны, отправленные почтой на адрес редакции, обрабатываются в течение 20 дней.

Рекомендуем использовать электронную почту или факс. Подписка производится с номера, выходящего через один календарный месяц после оплаты. Например, если произвести оплату в сентябре, то подписку можно оформить с ноября.

ПОДПИСКА ДЛЯ ЮРИДИЧЕСКИХ ЛИЦ

Москва: ООО «ИНТЕР-ПОЧТА» (495) 500-00-60 www.interpochta.ru

Для получения счета на оплату подписки нужно прислать заявку с названием журнала, периодом подписки, банковскими реквизитами, юридическим и почтовым адресом, телефоном и фамилией ответственного за подписку лица.

подписной купон

стоимость заказа на Хакер Спец + CD

6 месяцев — 900 руб. 00 коп. | **12** месяцев — 1740 руб. 00 коп.

стоимость заказа на комплект Хакер Спец + Хакер + Железо

6 месяцев — 2550 руб. 00 коп. | **12** месяцев — 5040 руб. 00 коп.

прошу оформить подписку:
☐ на журнал Хакер Спец + CD
☐ на комплект Хакер Спец + Хакер + Железо
на _____ месяцев
начиная с _____ 200 г.
☐ Доставлять журнал по почте на домашний адрес
☐ Доставлять журнал курьером на адрес офиса (по г. Москве)
Подробнее о курьерской доставке читайте ниже*
(отметьте квадрат выбранного варианта подписки)
Ф.И.О.
дата рождения
адрес доставки:
индекс
область/край
город
улица
дом _____ корпус
квартира/офис
телефон ( )
e-mail
сумма оплаты

*Курьерская доставка осуществляется только по Москве на адрес офиса. Для оформления доставки курьером укажите адрес и название фирмы в подписном купоне.

Извещение

ИНН 7729410015 ООО «Гейм Лэнд»
ЗАО ММБ
р/с № 40702810700010298407
к/с № 30101810300000000545
БИК 044525545 КПП - 772901001
Плательщик
Адрес (с индексом)

Назначение платежа	Сумма
Оплата за «_____» с _____ 200_ г. (месяц)	

Ф.И.О.
Подпись плательщика

Кассир

Квитанция

ИНН 7729410015 ООО «Гейм Лэнд»
ЗАО ММБ
р/с № 40702810700010298407
к/с № 30101810300000000545
БИК 044525545 КПП - 772901001
Плательщик
Адрес (с индексом)

Назначение платежа	Сумма
Оплата за «_____» с _____ 200_ г. (месяц)	

Ф.И.О.
Подпись плательщика

Кассир

ПО ВСЕМ ВОПРОСАМ, СВЯЗАННЫМ С ПОДПИСКОЙ, ЗВОНИТЕ ПО БЕСПЛАТНЫМ ТЕЛЕФОНАМ: **780-88-29** (ДЛЯ МОСКВИЧЕЙ) И **8-800-200-3-999** (ДЛЯ РЕГИОНОВ И АБОНЕНТОВ МТС, БИЛАЙН, МЕГАФОН). ВСЕ ВОПРОСЫ ПО ПОДПИСКЕ МОЖНО ПРИСЫЛАТЬ НА АДРЕС: **info@glc.ru**

с корабля на бал

НАСТРОЙКА МАРШРУТИЗАТОРА ЗА 5 МИНУТ

В НАШИ ДНИ РАЗВИТИЕ СЕТЕВЫХ ТЕХНОЛОГИЙ ДВИЖЕТСЯ ВПЕРЕД СЕМИМИЛЬНЫМИ ШАГАМИ. ПОЯВЛЯЮТСЯ НОВЫЕ ПРОТОКОЛЫ И СТАНДАРТЫ, ВЫХОДЯТ В СВЕТ НОВЫЕ УСТРОЙСТВА, ПРОИЗВОДИТЕЛИ ПРИДУМЫВАЮТ МНОЖЕСТВО НОВЫХ СПОСОБОВ ПРИМЕНЕНИЯ ТЕХНОЛОГИЙ В НАШЕЙ ПОВСЕДНЕВНОЙ ЖИЗНИ

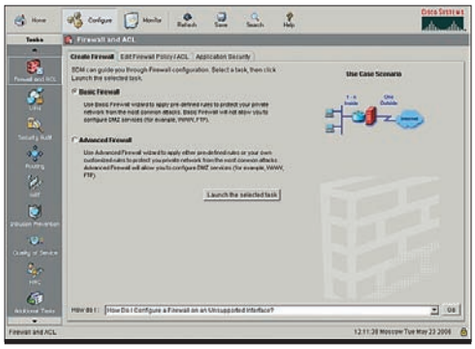
ДМИТРИЙ РЫЖАВСКИЙ
{системный инженер Cisco Systems}

В силу все более широкого распространения сетевых технологий, потребность в настройке оборудования часто возникает не только у профессионалов, виртуозно владеющих языком командной строки и помнящих наизусть все параметры протоколов, но и у обычных пользователей и специалистов в смежных областях высоких технологий. При этом далеко не у каждого спеца есть возможность отслеживать все новые веяния и постоянно находиться в курсе новинок сетевых технологий. Это приводит к тому, что даже самое функциональное устройство, если его функции нельзя быстро и просто настроить, не штудируя предварительно тома документации, никогда не будет использоваться эффективно.

Возможность настройки оборудования через графический интерфейс с применением мастеров и шаблонов конфигураций становится в телекоммуникационной индустрии стандартом де-факто. В последние годы возможности встроенных в маршрутизаторы Cisco графических средств управления возросли настолько, что теперь можно сравнивать их со специализированными сетевыми системами управления.

→ **первоначальная настройка с интеграцией сервисов.** Cisco Security Device Manager (SDM) — web-утилита для настройки маршрутизаторов Cisco. SDM предназначена для использования с широким спектром маршрутизаторов Cisco, начиная с серии 800 и заканчивая серией 7301. Она предустановленна на каждый маршрутизатор Cisco с интеграцией сервисов и обеспечивает графический инструментарий для безопасной настройки маршрутизатора. SDM поддерживает конфигурации LAN/WAN, VPN и межсетевых экранов в рамках программной среды Cisco IOS.

Кроме того, SDM выполняет функции аудита системы безопасности, применяемые для проверки конфигурации маршрутизатора, и предлагает варианты повышения уровня защиты в соответствии с рекомендациями ICSA Labs и Cisco Technical Assistance Center. SDM предлагает простой и экономичный способ управления всеми функциями безопасности, имеющимися в маршрутизаторах доступа Cisco, и настройку маршрутизатора своими силами.



Настройка SDM

→ перед тобой лежит новый маршрутизатор Cisco. Чтобы установить последнюю версию SDM и получить возможность быстрой настройки большей части основных функций через графический интерфейс, нужно выполнить определенные действия...

Рассмотрим наиболее «сложную» ситуацию. Конфигурационный файл удален, поэтому получить доступ к командной строке устройства можно только с помощью консольного кабеля. Такой кабель всегда входит в комплект поставки, но при желании его довольно просто изготовить самостоятельно, воспользовавшись инструкцией на сайте Cisco (**www.cisco.com**).

Если для администрирования используешь Windows, то для получения доступа к командной строке через консольный порт достаточно запустить HyperTerminal. В нем нужно создать новое соединение с настройками, которые автоматически будут установлены при нажатии Restore Defaults.

Предположим, в флеш-памяти маршрутизатора нет ничего, кроме файла-образа операционной системы IOS с расширением bin.

вход в привилегированный режим

```
router&gt;enable
```

вход в режим настройки конфигурации

```
router#configure terminal
```

установка пароля для привилегированного режима

```
router(config)#enable secret
&lt;password&gt;
```

включение и настройка IP-адреса на интерфейсе (через который будет происходить загрузка ПО и дальнейшее конфигурирование устройства)

```
router(config)#interface fastethernet 0
router(config-if)#ip address
192.168.0.1 255.255.255.0
router(config-if)#no shutdown
router(config-if)#exit
```

включение http и https серверов (для контроля доступа по http/https будут использоваться учетные записи из локального конфигурационного файла)

```
Router(config)# ip http server
Router(config)# ip http secure-server
Router(config)# ip http authentication local
```

добавление в конфигурационный файл учетной записи пользователя с высшим уровнем доступа

```
Router(config)# username &lt;username&gt;
privilege 15 password 0 &lt;password&gt;
```

активация доступа к командной строке по протоколам telnet и http

```
Router(config)# line vty 0 4
Router(config-line)# privilege level 15
Router(config-line)# login local
Router(config-line)# transport input telnet
Router(config-line)# transport input
telnet ssh
Router(config-line)# exit
```

В Cisco IOS по умолчанию доступ к этим протоколам закрыт, поскольку при пустом конфигурационном файле отсутствуют какие-либо пароли по умолчанию, которые могли бы воспрепятствовать захвату контроля над подключенным к сети устройством.

→ все необходимые подготовительные действия произведены. Чтобы скачать дистрибутив последней версии SDM с сайта Cisco, понадобится учетная запись с гостевым уровнем доступа. Для ее получения достаточно пройти процедуру регистрации. После этого можно запускать процедуру установки, во время которой нужно будет ввести ранее настроенный IP-адрес и учетную запись пользователя. Всю дальнейшую настройку маршрутизатора можно производить через графический интерфейс.

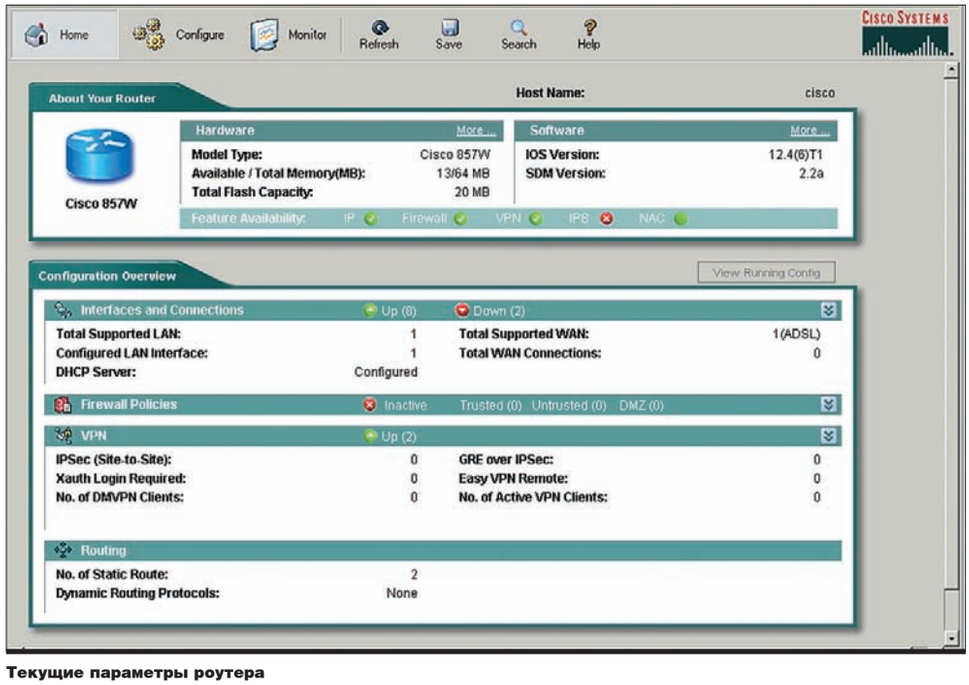
Доступны три варианта установки файлов SDM: на компьютер, во флеш-память маршрутизатора и в оба места одновременно. Интерфейс SDM написан на JAVA, и в любом случае будет выполняться на компьютере. Это сделано для сохранения вычислительных ресурсов маршрутизаторов при решении основных задач. Установка SDM во флеш-память дает возможность настраивать маршрутизатор с любого компьютера, даже если файлы SDM на нем не установлены.

Если устанавливаешь SDM во флеш, на основе доступного объема памяти можно установить полнофункциональный SDM или его сокращенную версию — SDM Express. Версия Express позволяет настраивать базовые функции маршрутизатора и контролировать работу различных подсистем. Она идеально подходит для настройки маршрутизаторов неопытными пользователями.

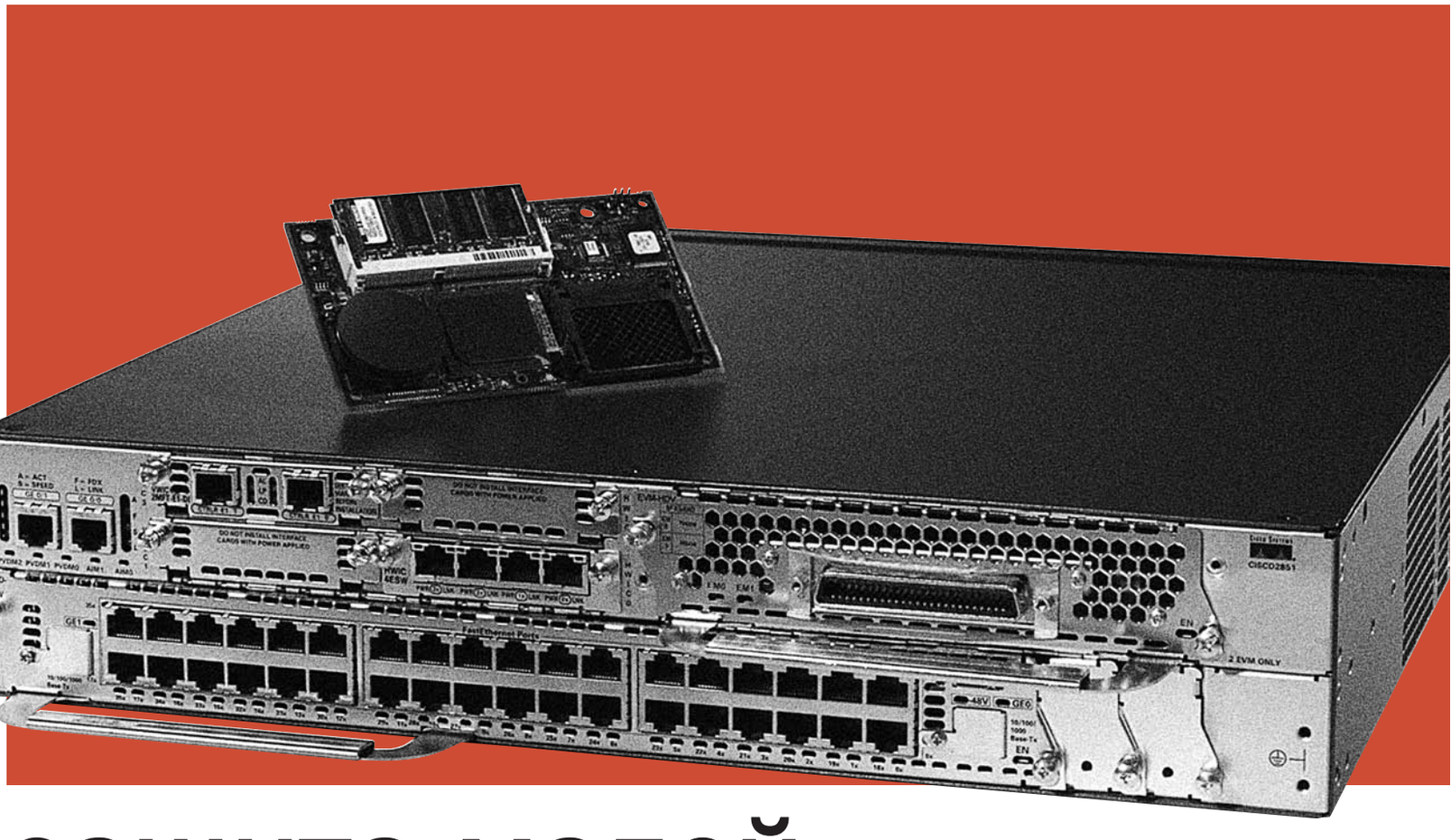
Если маршрутизатор содержит встроенную беспроводную точку доступа, можешь установить во флеш-память файлы для настройки Wi-Fi через web-интерфейс. Они устанавливаются одновременно с SDM'ом, но, в отличие от него, не могут выполняться с компьютера. Обычно настройку беспроводной точки доступа значительно удобнее производить через web-интерфейс. Только в исключительных случаях может потребоваться изменение параметров беспроводной сети в режиме командной строки.

Профессионалам, привыкшим настраивать оборудование из командной строки, SDM позволит сэкономить время при проведении рутинных операций и создании простых конфигураций. Любые настройки, сделанные в командной строке, незамедлительно отображаются в графическом интерфейсе.

По-прежнему, многие функции недоступны для настройки через графический интерфейс. Их конфигурация осуществляется из командной строки. Последующее изменение конфигурации в графическом интерфейсе SDM никак не затрагивает сделанные через CLI изменения **C**



Текущие параметры роутера



защита малой кровью

EASY VPN

РОСТ ЧИСЛА НАДОМНЫХ РАБОТНИКОВ И ВОЗРОСШАЯ МОБИЛЬНОСТЬ ПОЛЬЗОВАТЕЛЕЙ ВСЕ ЧАЩЕ СТАВЯТ ПЕРЕД НЕБОЛЬШИМИ КОМПАНИЯ ЗАДАЧУ ОБЕСПЕЧЕНИЯ УДАЛЕННОГО ДОСТУПА К КОРПОРАТИВНЫМ РЕСУРСАМ (REMOTE ACCESS VPN). А ПОВСЕМЕСТНОЕ РАСПРОСТРАНЕНИЕ НЕДОРОГОГО ШИРОКОПОЛОСНОГО ДОСТУПА ПО ТЕХНОЛОГИЯМ DSL, WIFI И ETHERNET СОЗДАЕТ ВСЕ УСЛОВИЯ ДЛЯ ТОГО, ЧТОБЫ УДАЛЕННЫЙ ДОСТУП СТАЛ РЕАЛЬНОСТЬЮ

ДМИТРИЙ РЫЖАВСКИЙ
{системный инженер Cisco Systems}

Работу любой технологии, обеспечивающей защищенную передачу данных через неподконтрольную, а потому всегда потенциально опасную среду, можно условно разделить на две фазы. Первая фаза представляет собой установление соединения с обязательной проверкой подлинности взаимодействующих сторон (аутентификацию), применением политик безопасности (авторизацию) и установлением ключей шифрования для второй фазы. На второй фазе происходит непосредственно передача зашифрованных ранее установленными ключами данных, целостность (неизменность) которых обязательно проверяется при приеме.

→ **первая фаза на примере технологии IPSec Easy VPN.** Перед тем, как пользователь сможет передавать зашифрованные данные в удаленную сеть, он должен осуществить процесс подключения. При этом происходит процедура аутентификации, во время которой пользователь должен подтвердить, что он именно тот, за кого себя выдает, и действительно имеет право произвести удаленное подключение. Аналогом этого процесса из реальной жизни является предъявление паспорта сотруднику банка. В IPSec VPN-сетях для аутентификации удаленных пользователей может использоваться заранее заданное на клиентских устройствах и сервере секретное значение (ключ), цифровые сертификаты формата x.509, основанные на использовании технологий цифровой подписи, групповые и персональные имена пользователей и пароли, а так же различные комбинации этих методов.

В настоящее время наиболее защищенным способом аутентификации является использование цифровых сертификатов. Аутентификация с использованием цифровых сертификатов не подвержена наиболее совершенному методу атак «man in the middle» (MITM, «человек посередине»). Суть этого метода состоит в том, что злоумышленник некоторым образом получает возможность пропустить через себя весь трафик между двумя взаимодействующими устройствами. При этом, он выступает в качестве своеобразного proxy-сервера, который может выборочно пропускать через себя трафик легитимных устройств, подменяя часть данных на собственные. Из перечисленных методов только использование цифровых сертификатов позволяет полностью исключить возможность успешного проведения подобного типа атак. Но для того, чтобы использовать цифровые сертификаты, в сети обязательно должен присутствовать сервер цифровых сертификатов (Certification Authority).

Операционная система Cisco IOS, под управлением которой работают все маршрутизаторы Cisco, содержит встроенный сервер цифровых сертификатов, предназначенный для использования совместно с технологиями IPSec VPN и SSL VPN.

➔ **Remote Access VPN.** Представь себе следующую ситуацию. Тебе нужно обеспечить удаленный доступ к корпоративной сети нескольким десяткам сотрудников. Ты можешь использовать для этого технологию шифрованных VPN. Но чем больше сотрудников будет пользоваться удаленным доступом, тем больше компьютеров со всеми детальными политиками безопасности нужно будет настроить. Как же избежать головной боли с настройкой и поддержкой столь большого числа клиентских устройств? А если не все сотрудники используют ноутбуки? И кто-то из надомных сотрудников захочет получать доступ со своего домашнего компьютера, который он настраивает сам. Сможет ли он так же аккуратно и правильно настроить свой компьютер для удаленного доступа к корпоративной сети, как это сделает системный администратор? Ответом на эти вопросы является использование технологии Cisco Easy VPN. Ее основное преимущество — использование «глупых» клиентов, конфигурирование которых сведено к минимуму.

Когда пользователю уже выдан цифровой сертификат, для создания VPN-соединения в Cisco Easy VPN Client достаточно настроить IP-адрес маршрутизатора компании, подключенного к интернету. Никаких настроек, связанных с использованием алгоритмов шифрования, аутентификации, хеширования для обеспечения целостности, распространения ключей шифрования для протоколов второй фазы и т.п., производить не нужно. Причем для установления VPN-соединения клиентским устройствам совсем не обязательно иметь публичные IP-адреса. За счет передачи IPSec-трафика поверх протокола TCP или UDP пользователи могут находиться за устройствами, осуществляющими трансляцию адресов с использованием технологий NAT/PAT.

При выдаче сертификата пользователю, ему автоматически передается корневой сертификат сервера цифровых сертификатов, содержащий только публичный ключ. Он будет использоваться при подключении перед аутентификацией, для проверки подлинности сервера, к которому производится подключение, и исключения атаки MITM.

Итак, есть задача — в короткие сроки развернуть для сотрудников компании защищенную по последнему слову техники сеть удаленного доступа. При этом нужно постараться избежать использования дополнительных компонентов, усложняющих и удорожающих решение.

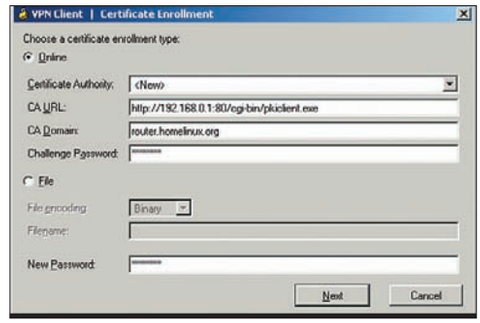
Для этого возьмем маршрутизатор Cisco 857W. Помимо всех функций маршрутизации и обеспечения безопасности у этого устройства есть еще и встроенная беспроводная точка доступа и RADIUS-сервер. Наличие RADIUS-сервера позволяет защитить небольшую сеть на несколько точек доступа в соответствии с последними рекомендациями WiFi-форума по защите корпоративных беспроводных сетей.

➔ **синхронизация времени по протоколу NTP.** Для нормальной работы инфраструктуры PKI очень важно, чтобы на всех взаимодействующих устройствах было установлено точное время и дата. В цифровом сертификате формата x.509 присутствуют поля с явным указанием его срока действия. В случае сильного расхождения времени на двух устройствах при проведении процедуры аутентификации одно из них решит, что срок действия сертификата другого устройства уже истек или еще не наступил. При этом сертификат считается недействительным, и успешное завершение процедуры аутентификации становится невозможным.

На любых устройствах, работающих под управлением ОС Cisco IOS, точное время можно устанавливать при помощи протокола NTP (Network Time Protocol). Рекомендуется использовать NTP-серверы, имеющие наивысший Stratum1. Это означает, что NTP-сервер напрямую подключен к источнику точного времени, такому как атомные часы или GPS-приемник. В свою очередь, Stratum2 получает точное время от Stratum1 и т.д. Если у тебя нет подконтрольного NTP-сервера, рекомендуется настроить для синхронизации сразу несколько внешних серверов. На любом NTP-сервере может произойти сбой, в результате которого он начнет распространять значительно отличающееся от реального время. Если на маршрутизаторе настроено несколько NTP-серверов, алгоритм тут же определит неожиданно большую разницу между получаемыми значениями и не будет использовать вышедший из строя сервер.

```
!указано отличие московского времени
от времени по Гринвичу
clock timezone Moscow 3
!алгоритм перевода часов для соответствия
российскому летнему времени
clock summer-time Moscow recurring last
Sun Mar 3:00 last Sun Oct 4:00
!не обязательно использовать
приведенные ниже серверы
!список публичных серверов Stratum 1
и 2 найдешь на сайте www.ntp.org
ntp server 195.68.135.5
ntp server 193.79.237.14
ntp server 195.2.64.5
ntp server 193.190.230.65
```

➔ **сервер сертификатов Cisco IOS.** Сервер сертификатов Cisco IOS Certificate Server внедрен в программное обеспечение Cisco IOS и дает маршрутизатору возможность действовать в сети в качестве центра сертификации (выпускать и отзывать цифровые сертификаты). Традиционно, генерирование криптографической информации и управление ею — непростая задача, по мере роста количества VPN. Сервер сертификатов Cisco IOS решает эти проблемы при помощи масштабируемого и несложного в управлении центра сертификации, который встроен в ту же аппаратуру поддержки IPSec VPN. Программное обеспечение Cisco IOS также поддерживает встроенные клиентские функции PKI, которые взаимодействуют с сервером сертификатов и с центрами сертификатов сторонних производителей.



Цифровой сертификат для VPN

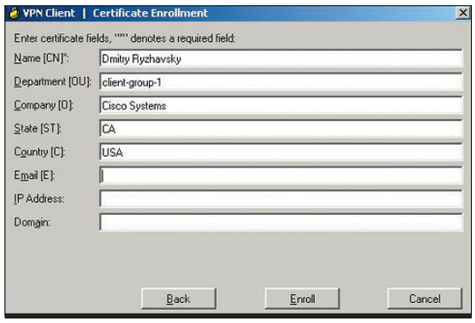
возможности PKI-клиента:

- ПОДДЕРЖКА ЛОКАЛЬНЫХ СПИСКОВ ACL ДЛЯ ПРИНЯТИЯ ИЛИ ОТКЛОНЕНИЯ СЕРТИФИКАТОВ НА ОСНОВАНИИ ПОЛЕЙ СЕРТИФИКАЦИИ;
- ИНТЕГРАЦИЯ С AAA ДЛЯ АВТОРИЗАЦИИ СЕРТИФИКАТОВ НА БАЗЕ ИМЕНИ ПОЛЬЗОВАТЕЛЯ И ДРУГИХ АТРИБУТОВ;
- ПОДДЕРЖКА ОНЛАЙНОВОГО ПРОТОКОЛА СТАТУСА СЕРТИФИКАТА (ONLINE CERTIFICATE STATUS PROTOCOL, OCSP);
- ПОДДЕРЖКА СПИСКОВ ОТЗЫВА СЕРТИФИКАТОВ И АВТОМАТИЧЕСКОГО ПЕРЕИЗДАНИЯ.

➔ **настройка сервера цифровых сертификатов на маршрутизаторе.** Встроенный в Cisco IOS-сервер цифровых сертификатов имеет богатые возможности по настройке. Приведем минимально необходимое количество команд для создания работоспособной конфигурации:

```
!задай имя для сервера цифровых
сертификатов
crypto pki server certsrv
database level names
issuer-name CN=certsrv,
OU=client-group-1, O=Cisco Systems
grant auto
!настройку параметров можно производить
только в выключенном состоянии, после
завершения настройки сервер нужно пере
вести в рабочее состояние
no shutdown
```

После этого будет сгенерирована ключевая пара для корневого сертификата сервера. При помощи ее частного ключа в дальнейшем будут подписываться все выдаваемые сервером сертификаты.



Цифровой сертификат для VPN

Команда grant auto позволяет автоматически выдавать сертификаты на запросы пользователей, что значительно упрощает процедуру выдачи сертификатов большому числу клиентов. Если канал между клиентом и сервером цифровых сертификатов во время выписки защищен, то сохраняется должный уровень безопасности. Например, выдачу сертификатов онлайн можно разрешить только пользователям внутри корпоративной сети.

➔ **технология Cisco Easy VPN.** Технология Cisco Easy VPN упрощает администрирование и управление сетями VPN, которые связывают различные узлы сети между собой, за счет активного продвижения новых политик безопасности из головного узла в сети на удаленные площадки. Для простоты конфигурации и высокой масштабируемости в решении Easy VPN применяется технология «проталкивания политики» (policy-push), но при этом сохраняется широкий спектр настроек и контроль над соблюдением политики.

Сервер Easy VPN, сконфигурированный в центральном офисе компании, передает политики безопасности на удаленные устройства VPN, обеспечивая реализацию на таких соединениях действующих политик еще до установки соединения.

➔ **Cisco Easy VPN Client.** Программное обеспечение Cisco VPN Client предназначено для удаленного подключения к корпоративной сети с помощью VPN-туннеля. Cisco VPN Client не требует почти никакой настройки со стороны пользователя. Все параметры соединения и политики безопасности передаются клиенту во время подключения к шлюзу доступа. Cisco VPN Client бесплатно доступен всем пользователям продуктов Cisco со встроенной функциональностью Easy VPN-сервера. К таким продуктам относятся маршрутизаторы с интеграцией сервисов, VPN-концентраторы, межсетевые экраны Cisco PIX и многофункциональные защитные устройства Cisco ASA.

➔ **снастройка Cisco Easy VPN Client.** Для настройки VPN-клиента достаточно создать соединение, указав IP-адрес сервера. Нужно использовать IP-адрес подключенного к интернету интерфейса маршрутизатора. На этот интерфейс был назначен crypto map при настройке Easy VPN-сервера.

Чтобы начать процедуру получения цифрового сертификата в меню VPN-клиента, нужно выбрать Certificates -> Enroll. Для выдачи сертификата пользователю должна существовать IP-достижимость между компьютером и интерфейсом локальной сети маршрутизатора:

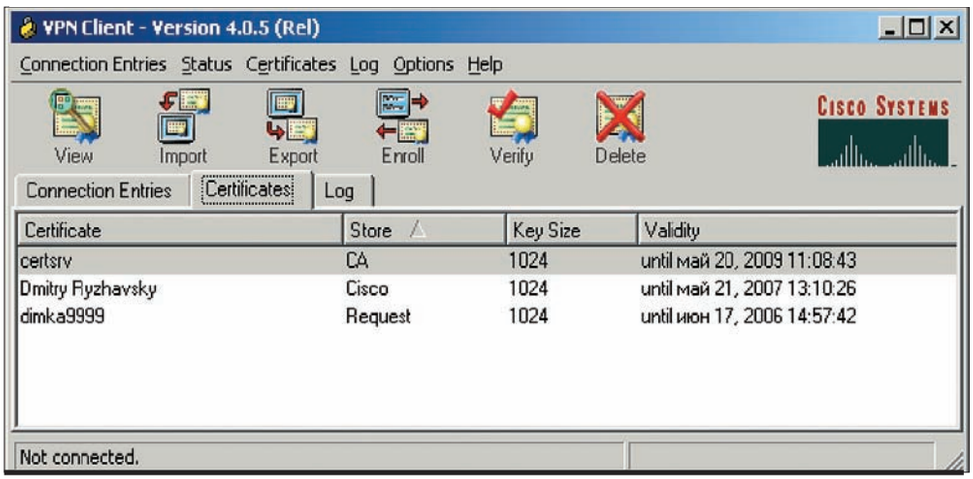
```
CA URL: http://192.168.0.1:80/
cgi-bin/pkiclient.exe
CA Domain: router.homelinux.org
```

Обязательно нужно указать домен, даже если он не настроен на маршрутизаторе. Без указания домена выдача сертификата невозможна!

```
Name[CN]: Dmitry Ryzhavsky
(имя пользователя)
Department [OU]: client-group-1 (должен
совпадать crypto isakmp client configu
ration group, задаваемой при настройке
Easy VPN-сервера)
```

При выдаче сертификата пользователю в VPN-клиенте также будет передан корневой сертификат CA, содержащий публичный ключ сервера цифровых сертификатов. С его помощью при установлении соединения будет проверяться подлинность сертификата Easy VPN-сервера. За счет этого становится возможным исключение атаки типа MITM.

Если обеспечить доступ клиента по IP к серверу цифровых сертификатов невозможно, выписку сертификатов пользователям можно осуществлять в ручном режиме. При этом сгенерированный клиентом запрос на получение цифрового сертификата в виде двоичной последовательности вводится в командную строку сервера цифровых сертификатов. Выданный пользователю сертификат в том же виде импортируется в Cisco VPN Client.



Список цифровых сертификатов и срок их действия

преимущества easy vpn

1. Easy VPN Server и Easy M3T Client поддерживается на маршрутизаторах с интеграцией сервисов, VPN-концентраторах, межсетевых экранах Cisco PIX и многофункциональных защитных устройствах Cisco ASA.
2. Клиентское программное обеспечение Cisco VPN Client можно инсталлировать без дополнительных затрат на компьютерах PC, Mac и в системах UNIX, для удаленного доступа к VPN-маршрутизатору. Поскольку одна и та же технология (Easy VPN) используется на аппаратуре у клиента (CPE) и в программном обеспечении, общая стоимость владения снижается за счет упрощения и унификации в обслуживании и мониторинге сервисов AAA.
3. В Easy VPN предусмотрены опции локальной (на базе маршрутизаторов) и централизованной аутентификации RADIUS. Аутентификацию на базе стандарта 802.1x также можно использовать для аутентификации хостов в каждом местоположении CPE.
4. Easy VPN предлагает цифровые сертификаты, повышая уровень безопасности по сравнению с preshared keys.
5. Балансировка нагрузки для нескольких находящихся на центральной площадке концентраторов Easy VPN автоматически распределяет нагрузку между несколькими серверами Easy VPN. Принудительная передача политик с резервных концентраторов на CPE позволяет компаниям масштабировать решение без переконфигурации CPE.
6. Easy VPN предлагает полнофункциональную интеграцию, включая динамическое назначение политики QoS, межсетевые экраны и IPS, раздельное туннелирование и Cisco Service Assurance Agent и NetFlow для мониторинга.
7. Cisco SDM дает возможность на базе мастер-программы быстро развернуть Easy VPN совместно с сервисами AAA и межсетевым экраном, а также возможность графического мониторинга удаленных клиентов Easy VPN в режиме реального времени

ЖУРНАЛ ДЛЯ МУЖЧИН, ЖИВУЩИХ В МИРЕ ТЕХНОЛОГИЙ

неприступная крепость

БЕЗОПАСНОСТЬ КОММУТАТОРОВ

ЕСЛИ О ЗАЩИТЕ ПЕРИМЕТРА НАПИСАНО МНОГО, ТО О ТОМ, КАК ЗАЩИТИТЬ ВНУТРЕННЮЮ СЕТЬ ОТ АТАК И НАРУШИТЕЛЕЙ, ПИШУТ РЕДКО.

АЛЕКСЕЙ ЛУКАЦКИЙ
{ALUKATSK@CISCO.COM}

И если стоимость выбранного коммутатора изначально невелика, то добавление в его комплектацию системы защиты полностью отбрасывает цену, как главный конкурентный показатель, которым часто оперируют производители коммутационного оборудования. Не говоря уже о том, что внедрить систему защиты в коммутируемую сеть не так-то и просто. Но зато если твоя сеть построена на оборудовании Cisco, ситуация меняется: в различные модели коммутаторов Cisco Catalyst уже встроено большое количество функций защиты, о части из которых мы и поговорим. Причем не будем касаться базовых механизмов (VLAN, баннеры, пароли и учетные записи), а перейдем сразу к ключевым особенностям.

➔ **oport security.** Первое, что мы хотим реализовать в коммутируемой сети с точки зрения безопасности, — это предотвращение подключения чужих устройств. Сделать это можно достаточно легко, и многие производители предлагают такую возможность (в Cisco это Port Security).

реализация блокировки подключения чужих устройств (третья команда блокирует порт на 600 минут):

```
set port security 2/1 enable
set port security 2/1 enable 00-90-2b-03-34-08
set port security 2/1 shutdown 600
```

Коммутаторы Cisco могут работать под управлением двух различных операционных систем — CatOS и IOS. Поэтому примеры конфигурации в дальнейшем будем приводить для разных ОС.

Чем плох описанный выше подход? Он слишком сложен в администрировании и абсолютно не масштабируем. Представь, что к тебе приехал представитель компании-партнера или клиент со своим лэптопом. Ты хочешь подключить его к твоей сети. Жесткая привязка портов коммутатора к MAC-адресам сделает эту задачу трудновыполнимой. Тем более что подделка MAC-адреса сегодня не является сложной задачей. Поэтому рекомендуется пойти немного другим путем. С помощью механизма 802.1x блокировать подключение несанкционированных устройств, а функцию Port Security использовать для динамической авторизации на коммутаторе.

Иными словами, вместо указания самих MAC-адресов, ты указываешь количество адресов, которые могут работать на данном порту. Порт коммутатора в динамическом режиме запоминает первые адреса, которые к нему «обратились», и в течение заданного администратором времени разрешает трафик только с них. При этом, если на порт попал трафик с неразрешенных адресов, возможно применение двух режимов —

shutdown и restricted. В первом случае блокируется работа самого порта, во втором — блокируется прием трафика с неразрешенных адресов.

реализация механизма Port Security для CatOS:

```
set port security 5/1 enable
set port security 5/1 port max 3
set port security 5/1 violation restrict
set port security 5/1 age 2
set port security 5/1 timer-type
inactivity
```

реализация механизма Port Security для IOS:

```
switchport port-security
switchport port-security maximum 3
switchport port-security violation
restrict
switchport port-security aging time 2
switchport port-security aging type
inactivity
```

В примере авторизуем только 3 MAC-адреса на порту, и, при превышении их числа, порт не блокируется. Время «привязки» адресов к порту (время устаревания информации об авторизованных адресах) составляет 2 минуты. Если ты используешь IP-телефонию, то на каждом порту нужно разрешать 3 адреса (рабочая станция, IP-телефон и мини-коммутатор в IP-телефоне). При подключении только рабочей станции достаточно указать максимальное количество адресов на порту, равное единице.

Механизм Port Security помимо блокирования «чужих» адресов может быть использован и для предотвращения атак, например, переполнения таблицы коммутации (MAC Flood) или истощения DHCP (DHCP Starvation).

➔ **dhcp snooping.** Еще одна распространенная атака, которая встречается в локальных сетях, — перехват трафика путем его перенаправления на себя. Делается это достаточно просто. Злоумышленник, выдавая себя за DHCP-сервер, подменяет адреса отдельных узлов в сети (например, маршрутизатора), тем самым меняя маршруты информационных потоков. Другим применением этой атаки может служить атака «отказ в обслуживании», когда на определенные адреса трафик может вообще не доходить.

И, наконец, последний пример атак с применением DHCP — истощение адресов (DHCP Starvation). Генерируя большой поток ложных служебных сообщений о выделении адресов, злоумышленник может «выбрать» весь пул адресов, и для авторизованных пользователей их просто не останется, что приведет к невозможности их работы. Защититься от этого позволит встроенная функция коммутаторов Cisco Catalyst — DHCP Snooping.

настройка DHCP Snooping для CatOs:

```
set security acl ip snoop1 permit dhcp-
snooping
set security acl ip snoop1 permit
ip any any
commit security acl all
set security acl map snoop1 183
set port dhcp-snooping 1/3 trust enable
set security acl feature ratelimit 15
```

➔ **dynamic arp inspection.** С протоколом ARP также немало проблем. И также, как и в случае с DHCP, некорректная настройка данного протокола позволяет злоумышленникам осуществлять перехват данных, «отказывать в обслуживании» и вносить хаос в работу сети. Для защиты от ARP-атак в коммутаторах Cisco существует специальный механизм — Dynamic ARP Inspection (DAI) .

настройка DAI для CatOS:

```
set security acl arp-inspection
dynamic enable 183
set port arp-inspection 1/3  trust enable
set security acl feature ratelimit 500
```

Первая команда связывает определенную VLAN с механизмом DAI, вторая — определяет порты, которым «доверяем», а третья — ограничивает полосу пропускания для защиты от DoS-атак.

настройка DAI для IOS:

```
ip arp inspection vlan 4,104
ip arp inspection trust
ip arp inspection limit rate 15
```

➔ **ip source guard.** Злоумышленник может подменять не только MAC-адреса, реализуя различные ARP-атаки, но и организовывать IP-спуфинг. Например, до 95% DoS-атак осуществляется именно с подменой IP-адреса, поэтому защита от этой угрозы является достаточно актуальной. Но если на периметре это сделать достаточно просто, и любой маршрутизатор и межсетевой экран делает это «влет», то в локальной сети это достаточно серьезная проблема. В коммутаторах Cisco Catalyst существует еще один механизм — IP Source Guard.

настройка IP Source Guard для CatOS:

```
set port security-acl 1/2 port-based
set port dhcp-snooping 1/2 source-guard
enable
```

настройка IP Source Guard для IOS (Cisco Catalyst 4500):

```
ip verify source vlan dhcp-snooping
port-security
```

настройка IP Source Guard для IOS (Cisco Catalyst 3750):

```
ip verify source port-security
```

➔ **bpdu guard и root guard.** Другой часто упоминаемой проблемой для локальных сетей является набор уязвимостей протокола Spanning Tree (STP), которые были обнаружены российскими экспертами в области безопасности — Олегом Артемьевым и Владиславом Мяснянкиным. С тех пор много воды утекло, но и по сей день встречается оборудование известных сетевых вендоров, которое подвержено данным уязвимостям, что приводит к хаосу в сети и ее отказу в обслуживании. В коммутаторах Cisco существует 2 механизма: BPDU Guard и Root Guard.

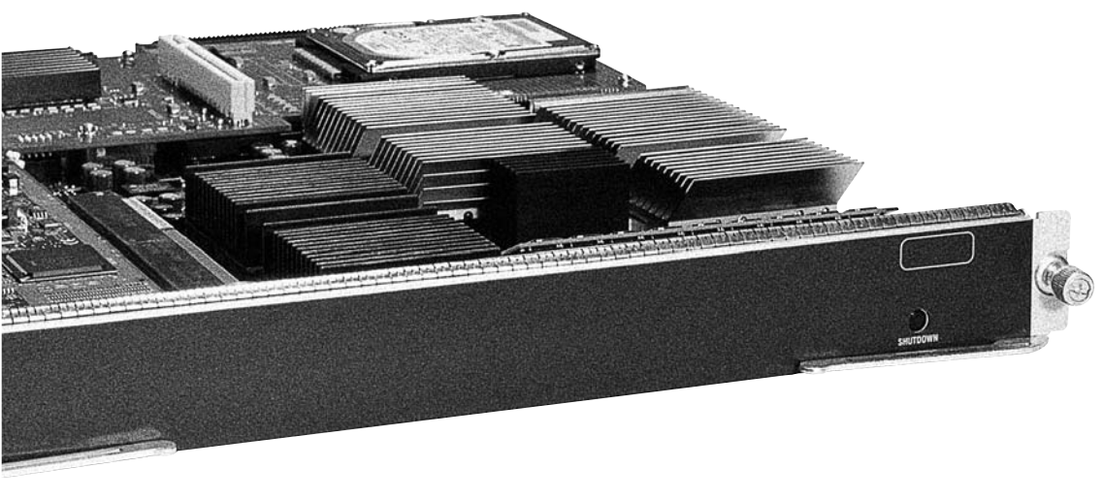
активация BPDU Guard и Root Guard для CatOS:

```
set spantree portfast bpdu-guard enable
set spantree guard root 1/1
```

активация BPDU Guard и Root Guard для IOS:

```
spanning-tree portfast bpduguard
spanning-tree guard root или
spanning-tree rootguard
```

Осталось множество интересных встроенных функций catalyst, обеспечивающих защиту локальной сети: использование списков контроля доступа (access control list, acl), протокола 802.1X и технологии network admission control, broadcats supression (storm control) и qos scavenger class, cisco express forwarding и cpp limiting и т.д. Все вместе, эти механизмы позволяют использовать коммутаторы cisco catalyst не только по своему прямому назначению, но и возложить на них базовые функции защиты локальной сети, не тратясь на приобретение дорогостоящего навесного оборудования



SPECIAL ИНТЕРВЬЮ

ЧЕМ ВСЕ-ТАКИ ЗАНИМАЕТСЯ АДМИНИСТРАТОР? К ПРИМЕРУ, НАСТРОЙКА, ОПТИМИЗАЦИЯ И БЕЗОПАСНОСТЬ — ЕГО КРУГ ПРОБЛЕМ?

ЗАРАЗА: Терминология — вещь всегда непростая. Начнем с того, что профессии «администратор» нет. Есть, например, «системный администратор», а есть «администратор безопасности». Это две разные должности. Понятно, что в небольшой конторке человек, которого называют системным администратором, может реально выполнять функции «специалиста поддержки пользователей», «инженера-электронщика», «администратора баз данных», а собственно администрированием системы и не заниматься вовсе. В конторе покрупней роли, наверняка, расписаны более четко. Кроме того, может встретиться человек, у которого на визитке написано «системный инженер» или «системный архитектор». Это человек, отвечающий за дальнейшее развитие или построение вычислительной системы. Системный администратор такими вещами заниматься не обязан.

То есть сформулировать определение понятия «системный администратор» можно следующим образом. Это человек, обеспечивающий решение повседневных задач: создание/настройка учетных записей; установка и настройка приложений согласно разработанным инструкциям; иногда — развертывание системы, опять же по инструкциям; наблюдение за системой (журналы системы, производительность); решение проблем.

ТОГДА КАКОЕ УСЛОВНОЕ ДЕЛЕНИЕ МОЖНО СЧИТАТЬ ОПТИМАЛЬНЫМ?

ЗАРАЗА: Если брать технических специалистов, то можно говорить о классификации «по уровню»: оператор; администратор; инженер. Администратор — это технический специалист с достаточно высокими навыками и опытом работы. Но нельзя забывать о специализации: «системный администратор», «администратор безопасности», «администратор баз данных». Хотя, чем выше уровень человека, чем более высокую должность он занимает — тем шире его специализация. Гради Буч называет таких людей «широкими коротышками», в отличие от «длинных тонких» специалистов. То есть начинать надо с какой-то одной специализации, стать профессионалом в ней, а потом уже расти вширь, развивая квалификацию в соседних областях, пусть даже за счет некоторого снижения профессионального уровня в основной области.

Вообще, компьютерные профессии можно разбить условно на четыре направления: обслуживание оборудования, поддержка пользователей, системное, сетевое и прочее администрирование и проектирование, разработка ПО.

Каждым из направлений занимаются свои специалисты. Хотя системный администратор должен владеть минимальными навыками разработки и поддержки пользователей, разработчик — минимальными навыками системного администрирования и обслуживания оборудования и т.д.

МЕЧТА КАЖДОГО АДМИНИСТРАТОРА — ПОЛНАЯ АВТОМАТИЗАЦИЯ. ВОЗМОЖНО ЛИ ТАКОЕ?

ЗАРАЗА: В любой момент времени! Вот только в следующий момент возникнет задача, которая еще не автоматизирована... Например, решение очередной задачи автоматизации. Собственно это и определяет уровень администратора. Специалист в небольшой компании все делает руками. Специалист в компании побольше решает задачи автоматизации. Специалист в крупной фирме решает задачи автоматизации решения задач автоматизации... И так далее. Причем для всех находится работа, так как компьютерная техника и программное обеспечение довольно быстро устаревают.

КАК ОПРЕДЕЛИТЬ ЗОЛОТУЮ СЕРЕДИНУ СТРАДАНИЙ ПОЛЬЗОВАТЕЛЕЙ, ЧТОБЫ ОДНОВРЕМЕННО СЭКОНОМИТЬ НА ЖЕЛЕЗЕ И ГЛОБАЛЬНО НЕ ПОТЕРЯТЬ В КАЧЕСТВЕ?

ЗАРАЗА: Сложный вопрос. Экономия — это правильно. Но экономить надо с умом. Любые затраты, начиная с перехода на новое железо и софт и заканчивая зарплатой тех же системных администраторов, должны быть обоснованы. На западе, да и у нас, в крупных организациях, подход гораздо экономичнее. Например, до сих пор используется MS-DOS с соответствующей техникой.

Другой вопрос, что пытаться «соптимизировать» явно слабое железо — это глупо. Через несколько месяцев потребности возрастут, и все равно придется вкладывать деньги. Потраченное администратором время, не говоря о возможных потерях времени пользователей — это впустую потраченные ресурсы.

Задачи перехода на новое железо или софт вообще решает не администратор, а, например, начальник отдела АСУ. Подход должен быть простым. Есть стоимость затрат на новую технику. Есть срок использования этой техники (например, 5-6 лет). Есть стандартные бизнес-операции, например, выписывание счета клиенту. Можно рас-

Большинство знают **Заразу** как автора ресурса по безопасности (*www.security.nnov.ru*), но в реальной жизни круг его интересов и профессиональной деятельности значительно шире. Основная профессия Заразы — руководство службой поддержки пользователей довольно крупного ISP. Такая работа требует знаний во многих областях: железа, системного администрирования, информационной безопасности, психологии, педагогики и менеджмента. А в качестве хобби — разработка программного обеспечения, в частности — проект 3proxy (*www.security.nnov.ru/soft/3proxy/*).

считать, насколько меньше будет тратиться времени на типовые операции, подсчитать сэкономленное время и деньги (зарплата работника, стоимость поддержки рабочего места и т.п.). Когда затраты на технику окупятся прибылью от ее внедрения — тогда и нужно обновляться.

ЧТО КАСАЕТСЯ СРЕДСТВ... LINUX ИЛИ WINDOWS? КОГДА И ЧТО ЛУЧШЕ?

ЗАРАЗА: Linux или Windows — опять же решается по деньгам. При этом учитывается не столько стоимость системы, поскольку она составит лишь небольшой процент затрат даже в случае самых дорогих Windows'ов, сколько софт, который будет установлен и система, которой он требует. Софт, как правило, выбирается исходя из удобства пользователей. Нужно, чтобы он максимально экономил им время. Время — деньги. Нужно, чтобы клиентский софт легко устанавливался и разворачивался, так как опять: время — деньги. Нужно, чтобы требовалось минимум обучения, так как это — тоже деньги. И чтобы не сложно было найти администраторов, их обучить и заменить, если они перебегут куда-то на большую зарплату.

А уж каждый администратор для себя должен выбрать, что он любит и с чем будет работать. При этом давно замечено, что ту или иную систему ругают только «недообученные» администраторы. Человек, знающий Windows досконально, никогда не будет кричать «мастдай!». Но и отворачиваться от возможности сэкономить на бесплатных системах тоже не стоит, так как любая возможность должна быть просчитана, а выбор — экономически обоснован. Windows гораздо чаще используется в корпоративных сетях, но иногда причиной становится банальное нежелание проектировщика «рисковать» на бесплатном решении. Если в конечном итоге выяснится, что Linux оказался менее эффективным, то можно оказаться за бортом. Если наоборот — то вряд ли.

ЧТО ДОЛЖЕН ЗНАТЬ И УМЕТЬ АДМИНИСТРАТОР БЕЗОПАСНОСТИ? КАК ПРОТИВОСТОЯТЬ ХАКЕРАМ, КОТОРЫЕ ПОРОЙ ЗНАЮТ БОЛЬШЕ, И КОТОРЫХ — СОТНИ И ТЫСЯЧИ?

ЗАРАЗА: Ну, только не что угодно, а кого угодно — в смысле, любую организацию. На самом деле, администратор безопасности — человек опять же небольшой. Он следит за работой средств безопасности и анализирует журналы, донастраивает/доводит какие-нибудь параметры. Ему нужно знать инструментарий. Но на деле это — не защита. Защита разрабатывается гораздо раньше. И защищаются не от хакеров. Защищаются от угроз. Администратор баз данных, забывший дописать WHERE в SQL-запросе, может наломать дров побольше любого хакера.

Поэтому прежде всего думают о том, что и где защищать. Потом о рисках, то есть о том нехорошем, что может грозить защищаемой информации. И только потом о тех, кто эти риски может реализовать, и насколько это вероятно. Дальше выбираются адекватные и оптимальные методы защиты. И только когда все выбрано, и сформирована политика безопасности — все это попадает к администратору безопасности, который следит за реализацией и соблюдением задуманного.

КАКИЕ МЕТОДЫ ЗАЩИТЫ НАИБОЛЕЕ АДЕКВАТНЫЕ И ОПТИМАЛЬНЫЕ?

ЗАРАЗА: Смотря, от какого риска. Например, у нас есть внутренняя база данных. Если мы потеряем эту базу данных, то наши убытки составят $1000000, так как мы не сможем дальше функционировать. Если она попадет конкурентам, то наши убытки составят $50000. Час простоя без доступа к информации обходится нам в $1000.

Проанализируем, как информация может попасть к конкурентам:

1. ФИЗИЧЕСКИЙ ДОСТУП (К КОМПЬЮТЕРУ С ИНФОРМАЦИЕЙ, АРХИВАМ НА ЛЕНТАХ И Т.Д.)
2. ДОСТУП К КАНАЛАМ СВЯЗИ.
3. ДОСТУП К ДАННЫМ ЧЕРЕЗ АВТОМАТИЗИРОВАННУЮ СИСТЕМУ.

Кто может получить физический доступ:

1. СИСТЕМНЫЕ АДМИНИСТРАТОРЫ.
2. СОТРУДНИКИ (ТУТ ВСЕГДА АНАЛИЗИРУЮТСЯ ДВЕ КАТЕГОРИИ — И СОТРУДНИКИ, И БЫВШИЕ СОТРУДНИКИ).
3. ОБСЛУЖИВАЮЩИЙ ПЕРСОНАЛ.
4. ПОСЕТИТЕЛИ.
5. ПОСТОРОННИЕ.

Какие будут адекватные меры защиты, если максимальный ущерб может составить $50000? Посадить вахтера на входе и проверять пропуска — наверное, неплохо. Хороший замок в серверной — да. Сейф для хранения бэкапов. А ввод системы разграничения доступа, камер видеонаблюдения и систем самоуничтожения данных — будет явным перебором.

При рассмотрении рисков потери информации вероятность, что уволенный со скандалом сисадмин оставит «бомбу», которая потрет всю информацию — довольно высока. Потери при этом могут быть значительные, особенно если он же следил и за бэкапом. Значит, можно потратить довольно много денег, чтобы убедиться в том, что он этого не сделает. Например, дать ему хорошие отступные и уволить без скандала.

Идея в том, что рассчитывается вероятность реализации угрозы и риски (вероятные финансовые потери). Определяются средства минимизации рисков, например — защитный софт или железо. По каждому из таких решений рассчитывается, насколько и какие риски они снижают, и какова стоимость решения (с учетом стоимости внедрения и поддержки на планируемый период). А дальше решается очень сложная математическая задача расчета средств, которые нужно внедрить, чтобы риски минимизировать.

Конечно, все это в теории. На практике большая часть оценок производится на глаз, главное — не упустить в защите что-то важное и не вбухать деньги в дорогую, но малоэффективную систему.

ПОЧЕМУ ЖЕ ТОГДА ДЕФЕЙСЯТ ТЕХ, КТО РЕАЛЬНО ОЦЕНИВАЕТ СВОИ РИСКИ, ТРАТИТ КРУПНЫЕ СУММЫ НА БЕЗОПАСНОСТЬ И ИМЕЕТ В ШТАТЕ НЕ ОДНОГО АДМИНИСТРАТОРА?

ЗАРАЗА: Ну, во-первых, дефейс — это не самая большая угроза. Что такое дефейс? Это модификация публично доступной информации. Если основной бизнес компании не связан с веб-сервером, то прямые финансовые потери от этого небольшие. Потеря репутации — вещь довольно скользкая... А некоторая реклама за счет отзывов в прессе, пусть даже и негативных, обеспечена.

При этом веб-приложения — это приложения, разрабатываемые «на заказ» в штучном исполнении. Естественно, что они хуже отлажены и проверены, чем приложения, которые используются массово. Обеспечить безопасность таких приложений можно лишь проводя аудит исходного кода, что очень дорого. Поэтому выходит, что при небольших рисках стоимость защиты получается большой, и защитой веб-серверов часто пренебрегают.

А во-вторых, сломать можно кого угодно. Любая защита снижает риски, но ни одна не устраняет их! Если есть один шанс из миллиона, и если есть миллион людей, которые попробуют, — то вероятность, что кому-то повезет, очень высока.

А ЕСЛИ ЭТИ ЛЮДИ ИЗ КИТАЯ, ТО ВЕРОЯТНОСТЬ РАВНА ЕДИНИЦЕ?

ЗАРАЗА: Нет, вероятность равна единице не будет и в этом случае. Это уже следует чисто из математики. Вероятность, что систему взломают, равна: (1 — (1-p)^n), где p — вероятность взлома, а n — число попыток. Но порой теория вероятности к реальной жизни отношения не имеет. Например, что такое «вероятность взлома», не скажет никто. Система либо взламывается, либо нет — без всяких вероятностей **C**

BSD

В СЛЕДУЮЩЕМ НОМЕРЕ МЫ РАСКРОЕМ ТАЙНЫ BSD-СИСТЕМ:

СИСТЕМНЫЙ СКРИПТИНГ
ГРАМОТНОЕ ОБНОВЛЕНИЕ
ПОчЕМУ BSD СЛОЖНЕЕ АТАКОВАТЬ, ЧЕМ LINUX
ЗАПИСЬ ДИСКОВ В BSD
МЕХАНИЗМ SYSCTL
ОПТИМИЗАЦИЯ ПОД ДЕСКТОП
ВОССТАНОВЛЕНИЕ УДАЛЕННЫХ ФАЙЛОВ

А ТАКЖЕ ОТВЕТИМ НА КУЧУ ТВОИХ ВОПРОСОВ ПО BSD В БОЛЬШОМ FAQ'E!

СКОРО В СПЕЦЕ:

WINDOWS VISTA
ВЗГЛЯД ИЗНУТРИ. ПОДРОБНЫЙ АНАЛИЗ НОВОЙ ОС ОТ MICROSOFT.
НОВЕЙШИЕ ТЕХНОЛОГИИ. УДОБСТВО, БЫСТРОТА РАБОТЫ.

SPYWARE
ТРОЯНЫ. ADWARE. БОТНЕТЫ.
СПАМ. ВИРУСЫ.

SPECIAL ОБЗОР

HARD

Технологии клонирования компьютеров

СПб.: БХВ-Петербург, 2006 /
Медведев Ю.Г. / 304 страницы
Разумная цена: 135 рублей

Под клонированием компьютеров понимается клонирование жестких дисков — процесс снятия точной копии жесткого диска, и использование этой копии для построения другой идентичной системы, включая операционную систему, различные настройки и программное обеспечение. Книга посвящена технологиям клонирования, позволяющим устанавливать ОС и ПО на сотни компьютеров достаточно быстро и без особых проблем. Рассмотрены программы Symantec Ghost 8.x, Norton Ghost 2003 и 9. Плюс практические рекомендации по вопросам массового клонирования компьютеров.
Обладая этой информацией, ты сэкономишь свое время, средства и силы.

MEDIUM

Администрирование сети на примерах

СПб.: БХВ-Петербург, 2005 /
Поляк-Брагинский А.В. /
320 страниц
Разумная цена: 123 рубля

С ростом числа сетей увеличивается и армия сетевых администраторов. И многие из них сталкиваются либо с тем, что большинство справочных материалов дают отрывочную информацию о решении проблем, либо с тем, что на теоретическом уровне они доступны лишь специалисту, который итак уже разобрался в данной проблеме. А время на поиск решения иногда весьма ограниченно. В этой книге ты почти не встретишь теоретических сведений: здесь масса именно практических примеров реализации различных задач администратора локальной сети (в основном по работе с сервером Windows 2000 или Windows Server 2003). Но учти, что для реализации примеров может потребоваться знание сценариев на языке VBScript, JScript и несложных программ на языке Visual Basic.

Если заинтересовался, можешь заказать любую книгу из обзора (по разумным ценам), не отрывая пятой точки от дивана или стула, в букинистическом интернет-магазине **«OS-книга»** (*www.osbook.ru*). Книги для обзора мы берем именно там

EASY

Самоучитель системного администратора

СПб.: БХВ-Петербург, 2006 / Кенин А.М. / 464 страницы
Разумная цена: 172 рубля

Круг обязанностей системного администратора достаточно сложно формализовать. Некоторые полагают, что он осуществляет только текущие контрольные функции, другие возлагают на него все работы по поддержанию и развитию информационной сети. Истина, как известно, лежит где-то посередине. Хороший системный администратор «зреет» не один год: необходим опыт и комплексный взгляд на систему. Автор книги хочет поделиться своим опытом и помочь советами начинающим администраторам, объясняя основные принципы, заложенные в основу различных технологий, которыми придется управлять. То есть перед тобой — «наглядная почему и зачем» для администратора.

MEDIUM

Как работать с маршрутизаторами Cisco

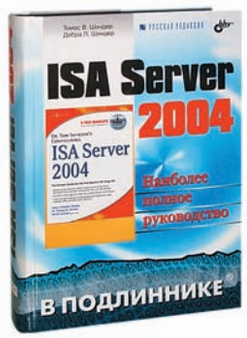
М.: ДМК Пресс, 2005 / Хабракен Д. / 320 страниц
Разумная цена: 190 рублей

По мере роста, любая компания ищет способы сохранить пропускную способность своих локальных сетей. Одно из популярных решений этой проблемы — сегментация локальных сетей с помощью маршрутизаторов. Но хороших книг об основах межсетевого взаимодействия практически нет. Либо это узкоспециализированные справочники для опытных специалистов, либо теоретизированные данные, больше напоминающие лекции в институте. Здесь же доступно и наглядно рассказано о межсетевом взаимодействии и конфигурировании маршрутизаторов Cisco, которые очень часто используются на практике. И если ты столкнулся с ними в работе, книга не даст потеряться.

HARD

ISA Server 2004

М.: Издательско-торговый дом «Русская Редакция», 2006 / Шиндер Т. / 1088 страниц
Разумная цена: 518 рублей



Некоторые изменения в ISA Server 2004 оказались настолько радикальными, что Microsoft серьезно подумывала о смене названия, но в итоге оставила Internet Security and Acceleration Server (ISA Server), чтобы не потерять пользователей предыдущей версии. В книге подробнейшим образом описаны функциональные возможности брандмауэра ISA Server 2004, конфигурация сетей с использованием ISA Server 2004, типы клиентов и способы их настройки, установка и конфигурирование ISA Server 2004. Использовать книгу можешь как огромный справочник, изучая нужные разделы, либо как пошаговый путеводитель, если ты еще не знаком с этим брандмауэром.

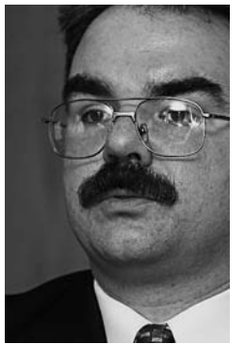
MEDIUM

TCP/IP и DNS в теории и на практике. Полное руководство

СПб.: Наука и Техника, 2006 / Досталек Л. / 608 страниц
Разумная цена: 296 рублей

Компьютеры в компьютерных сетях для взаимной коммуникации используют сетевые протоколы, в интернете — сетевые протоколы TCP/IP. В книге показано, как работают протоколы семейства TCP/IP и служба DNS, их функциональные особенности и характерные примеры из жизни. Разбираются реальные ситуации и даются профессиональные рекомендации по решению тех или иных проблем для Windows, Linux(Unix) и IOS — операционной системы CISCO. Отдельно рассмотрены проблемы безопасности и уязвимости TCP/IP и DNS **C**

SPECIAL ОПРОС



АЛЕКСЕЙ ЛУКАЦКИЙ
Бизнес-консультант по безопасности «Cisco Systems». В «Cisco» отвечает за развитие направления безопасности в России и странах СНГ.

АЛЕКСАНДР АНТИПОВ
Руководитель проекта, автор/соавтор/корректор многочисленных статей ведущего отечественного портала по информационной безопасности *SecurityLab.ru*.

АНТОН ПАЛАГИН
Директор по развитию компании «Eykon». Его первая должность — как раз администратор.

ЗАРАЗА
Руководитель службы поддержки пользователей довольно крупного ISP. Хобби — разработка программного обеспечения, в частности проект «3proxy» (*www.security.nnov.ru/soft/3proxy/*).

КОНСТАНТИН ГАВРИЛЕНКО
Консультант по безопасности и по совместительству директор компании «Архонт». Специализируется на безопасности сетевой инфраструктуры и безопасности беспроводной связи.

У АДМИНИСТРАТОРА СЛОЖНЫЙ ГРАФИК РАБОТЫ. СБОИ И АТАКИ МОГУТ БЫТЬ КАК ДНЕМ, ТАК И НОЧЬЮ. КАК БЫТЬ?

ЗАРАЗА: Это все определяется масштабами фирмы. Крупная компания может себе позволить дежурного администратора, который будет на рабочем месте и ночью. Помельче — администратора, который будет дежурить дома с трубкой в пределах досягаемости... Ну а если это компания, которой не выгодно иметь более одного администратора, то можно и одного администратора не брать. А заказать услуги администрирования организации, которая этим занимается профессионально, и в штате которой — несколько администраторов. То есть отдать администрирование на аутсорсинг. Тогда можно и отпусков не бояться...

ЧТО САМОЕ ГЛАВНОЕ В АДМИНИСТРИРОВАНИИ?

ЗАРАЗА: В администрировании все главное. Любая ошибка, сделанная администратором, не важно на каком этапе — планирования или реализации — может обернуться большими, очень часто невосполнимыми, потерями. Поэтому очень важно, чтобы задачи, которые решает системный администратор, были четко сформулированы и находились в пределах его компетенции. Ошибки в системном администрировании чаще всего делаются руководителями. Они рассуждают так: «я ничего в этом не понимаю, поэтому я найму технического человека, пусть он решает все технические вопросы». В резуль-

тате получается, что технический специалист начинает заниматься решением задач постановки технологического процесса, то есть совсем не технических. Кроме того, его действия никому не подконтрольны. Никто не может оценить качество работы.

При правильной организации системного администрирования все действия администратора четко регламентированы и подотчетны. Любое действие в системе происходит не само по себе, а по какому-то документу. Это снимает большую часть ответственности с администратора и перекладывает ее на того, кто подписал документ. Такая «бюрократизация» процедуры системного администрирования устраняет необдуманные действия со стороны администратора, значительно снижая вероятность ошибки. Постановка системного администрирования — это как раз и есть весьма трудоемкая задача по превращению набора неких хаотических и плохо понятных действий в хорошо отлаженный процесс.

АЛЕКСАНДР АНТИПОВ: Самое главное — выполнять все распоряжения начальства! Кто такой системный администратор? Человек подневольный, которого не замечают, когда все нормально работает, и на которого сыпятся все шишки, если что-то сломалось. Хорошо, если только сломалось, и он смог быстро решить возникшую проблему. Например, часто оказывается, что после того, как в течение месяца вдруг резко уменьшается поток писем от возможных клиентов компании, начальство узнает об установленном спам-фильтре. И тут бесполезно рассказывать про заботу о пользователях, постоянно жалующихся на увеличенное количество спама, — все равно окажешься виноватым, так как твоя инициатива нанесла прямой ущерб бизнесу.

Бывает плохой админ, хороший админ, а бывает правильный админ. Плохой — это тот, у которого ничего и никогда нормально не работает, а виноват в этом всегда Билл Гейтс и его глючные Винды. Хороший админ тихо делает всю свою работу, получает шишки от начальства и никогда не добьется повышения зарплаты или более высокой должности. Правильный же админ всегда перед тем, как нажать на кнопку, напишет внутреннюю инструкцию по тому, как нужно нажимать на эту кнопку, напишет докладную записку начальнику с аргументами о необходимости нажатия этой кнопки (пусть начальник представляет отделу продаж твои аргументы), а только потом нажмет на нее. Правильный админ всегда будет на хорошем счету у начальства, никогда не будет виноват и, вполне вероятно, быстро дослужится до более высокой должности с более высокой зарплатой.

АНТОН ПАЛАГИН: Главное для администратора — не становиться священной коровой, к которой несут дароносицу. К несчастью, это случается слишком часто, и зарвавшегося администратора приходится менять, со всеми вытекающими отсюда последствиями. Так что получается, что самое главное умение администратора — это умение взаимодействовать с людьми. Недаром на должность, так сказать, «штатского» администратора всегда назначают приятных и умеющих общаться девушек. На приличном ресепшене сидит человек, который тебе всегда поможет и подскажет, а не обложит матом и не попросит литр пива и рыбки к нему за ерундовую услугу.

Соответственно, для объекта администрирования важно, чтобы людям было удобно работать. Девушку Таню ведь не волнуют проблемы безопасности, связанные с дырками в IIS 6.0, ей интересно послушать музыку и посплетничать с соседкой Ксюшей о новом галстуке начальника. Но она не может сделать этого, потому что администратор Эммануил считает, что аська несет потенциальную угрозу безопасности. Бред? Конечно. А если начальник Зиновий Галактионович считает, что использование аськи пагубно сказывается на удоях... тьфу, то есть на работоспособности, то хороший администратор должен убедить его в обратном. Потому что девушки все равно будут сплетничать (с помощью гугл-тока или просто в туалете), и на работоспособность это никак не повлияет.

И, конечно, безопасность, — от нее никуда не денешься. Скажи мне, пожалуйста, о какой безопасности можно говорить, если сложный пароль секретарша записывает на бумажку и кладет ее под клавиатуру или наклеивает на монитор. А если ее за это отругать, то она сменит пароль на «123», чтобы было проще запомнить. И здесь администратор должен проявить умение общаться и убеждать (учить) секретаршу пользоваться специальными программами для записи конфиденциальной информации. Так что хороший администратор, в моем понимании, это тот, кто умеет решать проблемы пользователей, а не создавать им проблемы. Тогда глядишь, коллеги не будут зло смеяться над его внешностью, грязными ногтями и желтыми от кофе и курева зубами. Этих атрибутов просто не будет. А еще я за то, чтобы администратора, как и футбольного арбитра, не было заметно.

КОНСТАНТИН ГАВРИЛЕНКО: На этот вопрос невозможно дать однозначный ответ, и выделить единственный архиважный компонент. Принцип администрирования определяется ИТ-политикой компании, и в зависимости от этого можно определить некоторые направления, которые и будут являться доминирующими в работе администратора.

В первую очередь, любой человек, занимающийся администрированием, должен руководствоваться двумя основными принципами: стабильность и безопасность. Следом за ними идут функциональность и автоматизация. На самом деле, все четыре составляющие достаточно тесно переплетены между собой. Квалифицированный администратор должен уметь просчитать последствия во взаимодействии перечисленных составных частей от изменений, вносимых в структуру администрируемого объекта.

Но вне зависимости от типа администрируемой сети и потенциального материального ущерба от ее взлома, безопасность является одним из наиболее важных компонентов. Степень безопасности напрямую воздействует, по крайней мере, на стабильность и функциональность. Для каждой из других частей, при условии самого неприятного исхода, существует возможность исправить и вернуть все на свои места. В случае с безопасностью такая возможность отсутствует.

Останавливаясь на качествах администратора, особо стоит отметить отсутствие туннельного мышления и нестандартного подхода к решению проблем. А также любви к пицце, кофе и хорошему пиву.

АЛЕКСЕЙ ЛУКАЦКИЙ: В администрировании главное — планирование, как бы непривычно это не звучало. Причем планирование не в его советском понимании, а классический план, включающий в себя ответы на вопросы:

— ЧТО И ЗАЧЕМ НАДО СДЕЛАТЬ (ПО-КРУПНОМУ)?
ОТВЕТ НА ЭТОТ ВОПРОС ДОЛЖЕН БЫТЬ ТЕСНО СВЯЗАН С ЦЕЛЯМИ ОРГАНИЗАЦИИ. НАПРИМЕР, ВНЕДРЕНИЕ IP-ТЕЛЕФОНИИ ПОЗВОЛИТ СЭКОНОМИТЬ НА МЕЖДУГОРОДНИХ ПЕРЕГОВОРАХ И ПОЛУЧИТЬ НОВЫЕ ПРЕИМУЩЕСТВА ОТ ИСПОЛЬЗОВАНИЯ ТЕЛЕФОНИИ (НАПРИМЕР, ИНТЕГРАЦИЯ С CRM-СИСТЕМОЙ И ПОЛУЧЕНИЕ ВСЕЙ ИСТОРИИ ЗАКАЗОВ ИЛИ TROUBLESHOTING CASE'ОВ ЗВОНИВШЕГО).

— ЧТО НАДО СДЕЛАТЬ КОНКРЕТНО?
ДАЛЬШЕ МЫ ОПРЕДЕЛЯЕМ КОНКРЕТНЫЕ ДЕЙСТВИЯ, ПОЗВОЛЯЮЩИЕ ДОСТИЧЬ ПОСТАВЛЕННОЙ ЗАДАЧИ.

— КОГДА ЭТО НАДО СДЕЛАТЬ, И КТО ЭТИМ ЗАЙМЕТСЯ?
УСТАНАВЛИВАЕМ СРОКИ И ОТВЕТСТВЕННЫХ. ЕСЛИ ОРГАНИЗАЦИЯ НЕБОЛЬШАЯ, ТО ОТВЕТСТВЕННЫЙ ВСЕГДА БУДЕТ ТОЛЬКО ОДИН.

— КАК ИЗМЕРИТЬ ЭФФЕКТИВНОСТЬ?
ЭТО ОЧЕНЬ ВАЖНЫЙ МОМЕНТ, КОТОРЫЙ ОБЫЧНО ИЗ ВИДУ УПУСКАЕТСЯ. СДЕЛАТЬ ЧТО-ТО — СДЕЛАЛИ, А ВОТ ПРОВЕРИТЬ, НАСКОЛЬКО СДЕЛАННЫЕ ИЗМЕНЕНИЯ КОРРЕКТНЫ И ПРИВОДЯТ К НУЖНОМУ РЕЗУЛЬТАТУ, ЗАБЫВАЮТ. ИНОГДА РЕЗУЛЬТАТ, ТАК СКАЗАТЬ, НАЛИЦО. НО ЗАЧАСТУЮ ПРИХОДИТСЯ ПРОВОДИТЬ ДОСТАТОЧНО СЛОЖНЫЕ ИССЛЕДОВАНИЯ И ИСПЫТАНИЯ, ЧТОБЫ ПОНЯТЬ, ЧТО ВСЕ РАБОТАЕТ «КАК ЗАДУМАНО».

И только после ответа на все эти вопросы надо переходить непосредственно к конкретным действиям, которые многие и понимают как истинное администрирование **C**

SPECIAL FAQ

На вопросы отвечает эксперт этого номера, известная личность в Сети — **Яков Харон**

Q ЧТО САМОЕ СЛОЖНОЕ В РАБОТЕ СИСТЕМНОГО АДМИНИСТРАТОРА?

A Как это ни странно, но самое сложное — это понять, в чем заключается проблема. Хороший системный администратор в первую очередь должен уметь работать не с «железом», а с людьми, быть и психологом, и инженером. Четко поставленную техническую задачу решить легко (даже если эта задача из разряда «тяжелых»), а вот разобраться, чего хочет обратившийся к нему пользователь, с первого раза удается далеко не всегда. «Для того, чтобы правильно задать вопрос, нужно знать как минимум 80% ответа» (с) Азимов. Все пользователи делятся на две категории: те, кто знает, что они ничего не знают, и те, кто думает, что они знают все.

В первом случае к тебе обращаются с претензией типа: «у меня не работает интернет». Ты смотришь таблицу ARP'ов на его порте и видишь, что все должно работать... Можно, конечно, на этом и закончить, но пользователь приносит тебе деньги. Это он их зарабатывает, а ты их получаешь, так что надо разбираться дальше. Приходится учить людей владеть компьютером хотя бы в такой степени, чтобы первичную диагностику возможно было провести по телефону, подсказывая пользователю, на что нажимать. Плюс, постоянно сталкиваясь с однотипными звонками, администратор постепенно вырабатывает набор простых вопросов, на которые ответит кто угодно.

Со второй категорией общаться намного сложнее. Они уверены, что гораздо лучше знают, в чем проблема, и отказываются как-то реагировать на твои доводы, затягивая ее решение на неопределенный срок. Например, однажды мне пришлось устраивать конференцию с админом крупной компании и админом банка. Админ клиента уверенно рассказывал мне, как наш firewall мешает работать его клиент-банку (в действительности, никакого firewall'а для этого клиента у нас не было). А админ банка отказывался верить, что у него «вклинило» маршрутизацию, в результате чего сервер, обслуживающий клиент-банк, остался без связи с доброй половиной России! Но главным аргументом оба админа считали: «все остальное же

работает!». Хуже всего, что из-за таких пользователей страдают действительно разбирающиеся профи, которых рефлекторно принимаешь за вышеописанный тип людей и изначально не обращаешь внимания на то, что они говорят.

НЕУЖЕЛИ ВСЕ СЛОЖНОСТИ ИЗ-ЗА ПОЛЬЗОВАТЕЛЕЙ?

Конечно нет. Администраторы так же успешно сами создают себе проблемы. Всем нам часто кажется, что мы уже сталкивались с точно такой же проблемой. И вместо того, чтобы проделать стандартный набор действий (в зависимости от ситуации и проблемы), позволяющих диагностировать неисправность, пытаемся «починить» то, что, как нам кажется, «поломалось». Тем самым можно на несколько часов загнать себя в состояния поиска черной кошки в темной комнате, которая там и не ночевала. После чего ты все-таки вернешься к началу и поймешь, что решение было тривиально, и следующие полчаса пройдут в воспоминаниях, что же ты успел поменять, дабы вернуть все в исходное состояние.

В целом, у администратора должно быть два основных качества. Первое — умение выуживать из людей нужную информацию. Второе — необходимо иметь «систему» отладки/поиска проблемы, развитую на подсознательном уровне. Надо уметь шаг за шагом отсекать не имеющие отношения к делу звенья, чтобы в конце найти неисправное. Очень часто администраторы устраняют не причину проблем, а ее следствия. Это из серии: не видно — значит все хорошо. Если администратор обладает всеми вышеперечисленными качествами, то ни новое оборудование, ни новое программное обеспечение не станут для него большой проблемой.

МНОГИЕ УТВЕРЖДАЮТ, ЧТО МОГУТ ЗАЩИТИТЬ СВОЮ СЕТЬ ТАК, ЧТО НИКТО НЕ СМОЖЕТ СЛОМАТЬ ЕЕ. РЕАЛЬНО?

Разумеется, нет! Что сделал один человек, сможет сломать другой. Это вопрос времени и средств, которые хакер готов потратить на взлом. Ну и конечно, все зависит от цели, которую преследует атакующий. А цели бывают разными: получить доступ к конфиденциальным данным, уничтожить информацию, не дать работать неделю и т. д. Более того, достаточно важный вопрос: какие усилия способен приложить взломщик, чтобы остаться незамеченным и не пойманным.

КАК ПРОЩЕ ВСЕГО ХАКЕР МОЖЕТ ОБЕЗОПАСИТЬ СЕБЯ?

Проще всего отрезать кабель, когда никто не видит. По крайней мере передающую жилу Ethernet'а при sniffing'е отрезать стоит наверняка, поскольку существует масса противохакерских способов, обнаруживающих даже пассивный грабеж трафика. Как вариант, можно вести взлом чужими «руками».

НО ВЕДЬ МОЖНО ЖЕ ОТСЛЕДИТЬ, ОТКУДА ИДЕТ АТАКА?!

Ну, предположим, что мы хотим атаковать своего конкурента, сидящего в соседней комнате. Возьмем диапазон его IP-адресов и, подставив их в качестве source, будем посылать пакеты всему миру. И мир ответит. На эти адреса. Жертва увидит поток мусора, падающий со всех сторон, который загружает канал и не дает нормально работать. Но противостоять этому не сможет, даже если поставит «персональный» брандмауэр, создающий видимость «защиты» от атак такого типа, но бессильный «очистить» канал. Никакой защиты от DoS-атак не будет, пока все операторы не поменяют магистральное оборудование (которого на сегодняшний день просто нет). Либо не будет принципиально изменена идеология динамической маршрутизации. Иначе как только у меня есть подключения по BGP, ко мне беспрепятственно могут приходить пакеты, идущие откуда угодно и куда угодно.

ПРАВДА, ЧТО СИГНАЛ В МЕДНОМ КАБЕЛЕ МОЖНО «ПОДСЛУШАТЬ» БЕЗ РАЗРЫВА?

Абсолютно верно! Если у тебя есть возможность подойти к кабелю так, чтобы до него дотронуться, то это делается без проблем. Из школьного курса физики известно, что вокруг провода, в котором «живет» электричество, всегда присутствует электромагнитное поле. Существует миф о том, что экранированный кабель или кабель с двойным экраном (когда экран есть у каждой пары и есть общий экран) полностью «нейтрализует» это поле. Но в действительности все не так. Оборудование, перехватывающее сигнал, может быть построено по разным принципам, но «спрятать» сигнал за фольгой не получится. Более того, нет особых проблем, чтобы считать сигнал и на расстоянии в метр.

ГОВОРЯТ, ЧТО СВЯЗЬ ПО ОПТОВОЛОКНУ БЕЗОПАСНЕЕ, ЧЕМ СВЯЗЬ ПО МЕДИ. ЭТО ТАК?

Это не так! Люди, которые так говорят, сами не работали с оптоволокном или не до конца знают, как и для чего его можно использовать. Им кажется, что параллельно подключиться к медным проводам можно, а к оптоволокну — нельзя. На деле к оптоволокну подключаются точно так же, только вместо скруток используются делители сигнала: одно волокно разводится, и одинаковые сигналы меньшей мощности идут в оба волокна. Дальше — техника та же, что и с медью.

ПО ЛОГИКЕ ОПТИКА ГОРАЗДО НАДЕЖНЕЕ, ЭЛЕКТРИЧЕСТВА В НЕЙ НЕТ И, ЗНАЧИТ, БЕЗ РАЗРЫВА ЕЕ ПРОСЛУШАТЬ НЕ УДАСТСЯ?

По логике да, но логика и современные технологии — это две несовместимые вещи. Существует общедоступный прибор, часто используемый при работе с оптикой. Если его поднести к кабелю, он покажет, присутствует ли в нем сигнал, и в какую сторону он направлен. Технические подробности и принцип работы мне не известны, но раз он работает, то, следовательно, часть фотонов все-таки просачивается наружу.

СКЛАДЫВАЕТСЯ ВПЕЧАТЛЕНИЕ, ЧТО НЕТ НИКАКОГО СПОСОБА СДЕЛАТЬ СЕТЬ БЕЗОПАСНОЙ.

Смотря что понимать под «безопасностью». Абсолютная «абстрактная защита» существует лишь на бумаге. В реальной же жизни ты всегда защищаешь что-то конкретное: документы, которые ты посылаешь по почте, файлы, которые лежат у тебя на компьютере, или что-то еще. Прежде чем говорить о «защите», необходимо оценить условную стоимость охраняемого объекта для тебя и потенциального злоумышленника (с поправкой взлома на «интерес» и стремления кому-то отомстить или напакостить). После этого остается выбрать адекватный способ защиты, гарантирующий, что стоимость взлома будет выше стоимости охраняемой информации, в результате чего взлом становится экономически нецелесообразным и нерентабельным. Остаются только месть типа «вендетты» и вандализм. А вот с этими типами сложнее. Если кто-то очень умный, очень влиятельный и очень-очень-очень сильно разозленный захочет сломать твой сервер, то с высокой степенью вероятности он его сломает.

А ЕСЛИ ДАННЫЕ ПРАКТИЧЕСКИ БЕСЦЕННЫ?

В этом случае, в первую очередь, необходимо обеспечить безопасность на административном уровне: компьютеры в железных клетках, вход только по пропускам, камеры наблюдения на каждом шагу и т.д. Плюс служба охраны — отобрать данные «физическим» путем гораздо проще. Если же ты интересуешься, как максимально защитить данные, передаваемые по сети, ответ очень прост — не используй ничего стандартного! Если ты используешь свое оборудование, свои протоколы связи, свои алгоритмы шифрации (пусть и достаточно простые, которые ты сделал сам или кто-то сделал специально для тебя), у того, кто покушается, не будет возможности экспериментировать и искать дыры. Скорее всего он будет очень долгое время пытаться понять, что же это такое, а потом и вовсе бросит это занятие **C**

hard

споет и покажет

В СТАРОДАВНИЕ ВРЕМЕНА В МОЛОДЕЖНЫХ КРУГАХ БЫЛО ОЧЕНЬ ПОЧЕТНО ИМЕТЬ КАССЕТНЫЙ ПЛЕЕР. ПОМНИШЬ? СЕГОДНЯ ВЫДЕЛИТЬСЯ ПОДОБНЫМ ОБРАЗОМ СТАЛО СЛОЖНЕЕ. А ВСЕ-ТАКИ ХОЧЕТСЯ, ПРАВДА? НУ ЧТО Ж, СЕГОДНЯ МЫ ПРЕДОСТАВИМ ТЕБЕ ТАКОЙ ШАНС

СЕРГЕЙ НИКИТИН, АЛЕКСЕЙ МАЛАШИН

тестовый стенд:

ПРОЦЕССОР:	**AMD Athlon XP 2400+**
СИСТЕМНАЯ ПЛАТА:	**JetWay N2View (nForce 2)**
ОПЕРАТИВНАЯ ПАМЯТЬ:	**512 Мб, DDR 333**
ВИДЕОПЛАТА:	**128 Мб, GeForce Ti 4200**
ЖЕСТКИЙ ДИСК:	**120 Гб, Seagate Barracuda 7200 RPM**

Протестированные устройства — не банальные проигрыватели музыки, а многофункциональные устройства, которые могут работать и с видеофайлами, и с фото, и с текстом, да и кучу всего они еще могут. Такие изделия пока не очень распространены, так что читай наш тест, чтобы выбрать лучшее!

➜ **методика тестирования.** Для наиболее точного выявления возможностей этих устройств мы разработали методику тестирования с предельно прикладной направленностью. Испытаний было три. Первое заключалось в закачивании на плеер тестового пакета DivX Test CD. Это множество файлов, записанных при помощи разных кодеков, а так же с использованием разных разрешений и аудиопотоков. Потом они запускались, и тем самым мы проверяли, с каким видео плеер реально может работать. Дальше идет тест на скорость — копирование с компьютера на плеер 700 Мб фильма. Что может быть типичнее такой задачи? Время копирования засекалось. Третий тест был на продолжительность работы. На плеере с полностью заряженным аккумулятором запускался только что закачанный на него фильм и шел до тех пор, пока батарея устройства не садилась. Помимо этого, мы обращали внимание на внешний вид и габариты устройств, на удобство и простоту управления, комплект поставки, качество поставляемых наушников и множество других параметров. Результаты этих наблюдений нашли себя в описаниях конкретных устройств.

➜ **технологии.** Объясним вкратце, что обозначают значения из таблиц и какие типы кодирования используются на тестовом диске.

➜ **кодеки**. Здесь можно провести аналогию с архиватором, то есть кодек призван сжимать исходное видео, однако, делается это также и за счет потери качества изображения. Поэтому стали разрабатывать алгоритмы для обеспечения наименьших потерь путем применения разнообразных технологий, которые различаются у разных версий кодеков.

DivX 3 — наиболее старый кодек, алгоритм которого изначально был заимствован у Microsoft, представляет собой несколько измененную версию MPEG4.3 (здесь отсутствуют некоторые ограничения, сам же алгоритм не изменен). Обозначение складывается так: <видеокодек><битрейт в kb/s * 1000><аудиокодек> (по умолчанию, аудиокодек = MP3 128 kb/s). То есть, например, «fast3k» обозначает, что этот файл закодирован при помощи Fast Motion (для быстрых сцен) с потоком ~3000 kbps (а если быть точнее, то 2649 kbps), звуковая же дорожка представлена в формате MP3. Тогда как «low3k-DivXTon» говорит о том, что фрагмент представляет из себя Low Motion (для медленных сцен) ~3000 kbps с аудио в форме DivX Audio 64kb/s.

DivX5 — версия кодека, значительно отличающаяся от предыдущей (включает множество дополнительных возможностей) с улучшенными алгоритмами кодирования. Здесь нам предлагаются такие вкусности, как поддержка GMC (Global Motion Compensation — глобальная компенсация движения, — что помогает снизить потери при сжатии кадров), Quarter Pixel (обработка векторов движения с точностью до четверти пикселя), а также моделирование восприятия изображения человеком (снижение качества картинки из расчета того, что глаз этого просто не заметит). Тестовые позиции обозначаются здесь так: <режим сжатия (по умолчанию 1pass)><битрейт видео в kbps * 1000><алгоритм обработки><битрейт аудио (по умолчанию MP3 129 kbps)>. Покажем пример: «6k-gmc-bf-320» — говорит о том, что это однопроходное кодирование, с видеобитрейтом ~6000 kbps, примененными алгоритмами GMC и B-Frames и аудио в формате MP3 320 kbps, а «1k-qpel» означает сжатие за один проход с ~1000 kbps алгоритмом Quarter Pixel и аудио по умолчанию.

XviD — изначально это альтернативная разработка «сжимателя» MPEG4 с открытым исходным кодом, причем являющаяся конкурентом предыдущих двух (можно заметить, что XviD это обратное написание DivX). Тут надо сказать о том, что до недавнего времени кодер был весьма нестабильным, а результат его работы был далеким от приемлемого. Однако, последнее время позиции этого формата становятся довольно крепкими, и он начинает получать распространение среди пользователей. Алгоритмы работы весьма близки к DivX5, а обозначения тестовых трэков из тестового пакета совпадают.

➜ **режимы сжатия**. Однопроходный (1 pass):

— С ПОСТОЯННЫМ БИТРЕЙТОМ (CBR — CONSTANT BIT RATE): РЕЖИМ, КОГДА КАЖДАЯ ГРУППА КАДРОВ (НАПРИМЕР, 25 = 1 СЕКУНДЕ ВИДЕО) ИМЕЮТ ОДИН И ТОТ ЖЕ РАЗМЕР. ЗДЕСЬ ХОРОШО ТО, ЧТО ТАКОЙ РЕЖИМ ПРОСТ ДЛЯ КОДИРОВАНИЯ И, СООТВЕТСТВЕННО, ТРЕБУЕТ МАЛЫХ СИСТЕМНЫХ РЕСУРСОВ. ИЗ МИНУСОВ ЖЕ НАДО ОТМЕТИТЬ НИЗКОЕ КАЧЕСТВО ПОЛУЧАЕМЫХ ФРАГМЕНТОВ.

— С ПЕРЕМЕННЫМ БИТРЕЙТОМ (VBR — VARIABLE BIT RATE): ЗДЕСЬ УЖЕ ПРИСУТСТВУЕТ НЕКОТОРАЯ ОБРАБОТКА, ТАК ДЛЯ ПРОСТЫХ КАДРОВ ИСПОЛЬЗУЕТСЯ ЛИШЬ ЧАСТЬ БИТОВ (А «ЛИШНИЕ» КЛАДУТСЯ В РЕЗЕРВУАР), ТОГДА КАК ДЛЯ СЛОЖНЫХ ИСПОЛЬЗУЮТСЯ ВСЕ БИТЫ + РЕЗЕРВНЫЕ; ПОЭТОМУ ЗДЕСЬ МЫ ПОЛУЧАЕМ ЛУЧШЕЕ КАЧЕСТВО ИЗОБРАЖЕНИЯ ПРИ ЧУТЬ БОЛЬШИХ ЗАТРАТАХ РЕСУРСОВ. ЗДЕСЬ ЖЕ НАЧИНАЮТ ПРОЯВЛЯТЬ ИНТЕРЕСНЫЕ АРТЕФАКТЫ (ИЗ-ЗА ОГРАНИЧЕННОСТИ РАЗМЕРА РЕЗЕРВУАРА): КОНЕЦ СТАТИЧНЫХ СЦЕН ОКАЗЫВАЕТСЯ ВЫСШЕГО КАЧЕСТВА (ПОСКОЛЬКУ В РЕЗЕРВУАРЕ МНОГО ДОПОЛНИТЕЛЬНЫХ БИТ), А ДИНАМИЧЕСКИЕ СЦЕНЫ НАОБОРОТ «ПЛОХИЕ» ИЗ-ЗА ОТСУТСТВИЯ НУЖНЫХ БИТ.

— С ОДИНАКОВЫМ КАЧЕСТВОМ: РЕЖИМ, В КОТОРОМ ИСПОЛЬЗУЕТСЯ СЖАТИЕ КАДРОВ, ПО АНОЛОГИИ С АЛГОРИТМОМ JPEG, ПОЭТОМУ ПОЛУЧАЕМ НЕОДНОРОДНЫЙ БИТРЕЙТ, НО ОДИНАКОВОЕ КАЧЕСТВО. САМ ЖЕ КОЭФФИЦИЕНТ СЖАТИЯ МОЖНО МЕНЯТЬ, ЧТО БУДЕТ ВЛИЯТЬ НА ПИКСЕЛЬНОСТЬ КАРТИНКИ, ПРИЧЕМ ЭТОТ РЕЖИМ МАЛОТРЕБОВАТЕЛЕН К РЕСУРСАМ.

Двупроходный (2 pass) — довольно сложный для кодирующей системы, поскольку требует в два раза большего времени (первый проход — это оценка «сжимаемости» каждого кадра, а второй — собственно сжатие), также необходимо распределение различных фильтров и обработчиков по кадрам. Зато результат здесь значительно выше всех однопроходных вариантов, а требования к воспроизводящей системе малы.

➜ **битрейт.** Это одна из немаловажных характеристик как видео, так и аудиофайла, поскольку показывает количество бит, отведенных на одну секунду видео или звука. Соответственно, чем выше этот показатель, тем более качественный результат мы получаем, но здесь надо помнить, что возрастает и нагрузка на воспроизводящую систему, поскольку надо обеспечить обработку большего количества данных. Поэтому фрагменты в формате 6k-320 проигрывало малое количество плееров, так как некоторые из них попросту не смогли «переварить» такие файлы.

➜ **звук.** Рассмотрим аудиочасть, где чаще всего встречаются три следующих кодека:

[1] MP3 — КОДЕК, ПОЛУЧИВШИЙ ОГРОМНОЕ РАСПРОСТРАНЕНИЕ СРЕДИ АУДИОФАНАТОВ, ПОСКОЛЬКУ ПОЗВОЛЯЕТ ЗНАЧИТЕЛЬНО СНИЗИТЬ ОБЪЕМЫ МУЗЫКАЛЬНЫХ ПРОИЗВЕДЕНИЙ БЕЗ СИЛЬНЫХ ПОТЕРЬ В КАЧЕСТВЕ (ЗА СЧЕТ ИЗМЕНЕНИЯ БИТРЕЙТА), ПРИЧЕМ ПРИМЕНЯЮТСЯ СХЕМЫ С VBR И CBR.

[2] AC3 — ФОРМАТ МНОГОДОРОЖЕЧНОЙ ЗАПИСИ ЗВУКА ВЫСОКОГО КАЧЕСТВА (ВЫСОКОГО БИТРЕЙТА) ОТ DOLBY DIGITAL, ПОЗВОЛЯЕТ СОЗДАВАТЬ СЖАТЫЕ ФАЙЛЫ ДЛЯ ПРОСЛУШИВНИЯ НА 5.1 СИСТЕМАХ БЕЗ ОСОБЫХ ПОТЕРЬ В КАЧЕСТВЕ. ОБОЗНАЧЕНИЯ ЗДЕСЬ ТАК ЖЕ ПРОСТЫ ДЛЯ ПОНИМАНИЯ. НАПРИМЕР, «1XAC3-448» — ЭТО ОДНОДОРОЖЕЧНЫЙ ФАЙЛ СО ЗВУКОМ В ФОРМАТЕ AC3 И БИТРЕЙТОМ 448 KBPS.

[3] DIVXAUDIO — СПОСОБ КОДИРОВАНИЯ ЗВУКА, РАЗРАБОТАННЫЙ ТОЙ ЖЕ ГРУППОЙ, ЧТО СОЗДАЛА ВИДЕОКОДЕК.

Creative Zen Vision
($500) 8 баллов

ОБЪЕМ **30 Гб**

РАЗМЕР ЭКРАНА,: **3,7 дюйма**

ФОРМАТЫ АУДИО: **MP3, WMA, OGG, WAV**

ФОРМАТЫ ВИДЕО: **WMV9, MPEG1/2/4-SP, Motion-JPEG, DivX (4,5), XviD**

ФОРМАТЫ ФОТО: **BMP, JPEG**

ДОПОЛНИТЕЛЬНЫЕ ВОЗМОЖНОСТИ: **чтение карт CompactFlash, радио-тюнер**

ИНТЕРФЕЙС: **USB 2.0**

КОМПЛЕКТ ПОСТАВКИ: **Наушники, адаптер питания, USB-кабель, шнур для A/V-выхода, чехол, ПО Creative MediaSource, Creative Media Explorer, инструкция по установке и эксплуатации**

ВОЗМОЖНОСТЬ ОБНОВЛЕНИЯ ПО: **да**

РАЗМЕРЫ: **124.2x74.4x20 мм**

ВЕС: **239 г**

➜ **плюсы.** Это довольно увесистый девайс размером с ладонь. Он обладает большим экраном. Если это никому не мешает, то можешь слушать на нем музыку через динамики, а если рядом раздражительные люди, то через наушники из комплекта поставки (очень, кстати, хорошие, даром, что «капельки»). Меню и навигация по нему просты и удобны, разбираешься во всем сразу. Плеер работает со всем — музыка, видео, фото и тексты, так что большой цветной дисплей без работы не останется. Из дополнительных возможностей хочется отметить слот для карт CF, прикрытые крышечкой порты и встроенный микрофон. Девайс может получать питание по USB-шине.

➜ **минусы.** Закачать информацию на плеер можно только через процедуру синхронизации, запущенную в Windows Media Player'е. Это не совсем удобно. Из проводника можно записать информацию на плеер только в режиме его работы «Съемный диск». Агрегат несколько раз зависал при тестировании.

iRiver PMP-120
($500) 7 баллов

ОБЪЕМ: **20 Гб**

РАЗМЕР ЭКРАНА: **3,5 дюйма**

ФОРМАТЫ АУДИО: **MP3, WMA, WAV, ASF**

ФОРМАТЫ ВИДЕО: **AVI, MPEG4**

ФОРМАТЫ ФОТО: **JPEG, BMP**

ДОПОЛНИТЕЛЬНЫЕ ВОЗМОЖНОСТИ: **радио-тюнер, прямое кодирование в MP3, USB-хост, подключение к ТВ**

ИНТЕРФЕЙС: **USB 2.0**

КОМПЛЕКТ ПОСТАВКИ: **инструкция, утилиты, блок питания, интерфейсный кабель, наушники, необходимые соединительные провода, футляр для переноски**

ВОЗМОЖНОСТЬ ОБНОВЛЕНИЯ ПО: **да**

РАЗМЕРЫ: **139x84x32 мм**

ВЕС: **280 г**

➜ **плюсы.** Большой экран сразу заявляет о том, что на этом плеере можно не без удовольствия смотреть фильмы. Проверка показала, что это действительно так — дисплей качественный, звук из динамика льется, конечно, не Surround Sound, но вполне ничего. Кроме фильмов на этом плеере можно просматривать все остальное — фотки, музыку, тексты. Удобная конструкция корпуса позволяет ставить его на стол, а не держать в руках или на коленях. В комплект поставки входит все необходимое, даже футляр для транспортировки устройства.

Понравилось, что наш тестовый файл скопировался на жесткий диск плеера довольно быстро. Возможно использование в качестве USB-хоста, то есть подключаешь к плееру камеру и скидываешь фотки — компьютер не нужен.

➜ **минусы.** Хотя, например, открытие файлов — здесь процесс довольно неспешный. Средства управления очень запутаны, так что поначалу придется осваивать способы управления этим изделием. Цена его очень велика.

лучшая покупка
СПЕЦ

Samsung YH-J70
($380) 6 баллов

ОБЪЕМ, ГБ: **20 Гб**
РАЗМЕР ЭКРАНА, ДЮЙМЫ: **1,5 дюйма**
ФОРМАТЫ АУДИО: **MP3, WMA, OGG, WAV**
ФОРМАТЫ ВИДЕО: **MPEG4**
ФОРМАТЫ ФОТО: **JPG**
ДОПОЛНИТЕЛЬНЫЕ ВОЗМОЖНОСТИ: **встроенный микрофон, радио-тюнер**
ИНТЕРФЕЙС: **USB 2.0**
КОМПЛЕКТ ПОСТАВКИ: **адаптер питания, кабели, переходники, диск с ПО**
ВОЗМОЖНОСТЬ ОБНОВЛЕНИЯ ПО: **да**
РАЗМЕРЫ: **62x99,8x16,4 мм**
ВЕС: **135 г**

➔ **ПЛЮСЫ.** Очень компактный плеер, который идеально подойдет тем, кто ищет себе спутника в дорогу. Девайс сможет развлечь тебя и музыкой, и видеоклипом, и текстом, и фотографией. В общем, с ним не соскучишься. В комплекте поставки найдется все необходимое для работы — кабели, переходники, инструкции и так далее.

Показал очень большое время автономной работы, что подтверждает его ориентацию на мобильных пользователей.

Смог воспроизвести все файлы из тестового пакета, благодаря одной своей не очень приятной особенности.

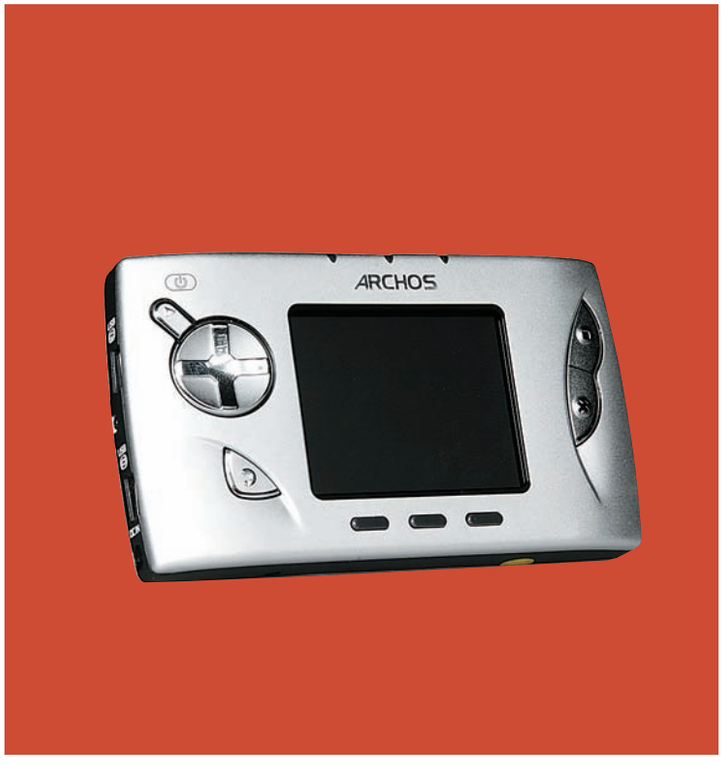
➔ **МИНУСЫ.** Работает только с видеофайлами своего формата, так что все фильмы и клипы придется предварительно в него конвертировать, а это занимает очень много времени (на тестовом компьютере 700 Мб преобразовывались целый час). Небольшие размеры, а значит экран тоже невелик. Наушники в комплекте среднего качества. Меню и навигация не так удобны, как у более габаритных конкурентов.

Epson P2000
($500) 8 баллов

ОБЪЕМ: **40 Гб**
РАЗМЕР ЭКРАНА: **3,8 дюйма**
ФОРМАТЫ АУДИО: **MP3, AAC**
ФОРМАТЫ ВИДЕО: **MPEG4, Motion JPEG**
ФОРМАТЫ ФОТО: **JPEG, TIFF, RAW**
ДОПОЛНИТЕЛЬНЫЕ ВОЗМОЖНОСТИ: **карты CompactFlash type II, карты SD, прямая печать на принтеры, подключение к ТВ**
ИНТЕРФЕЙС: **USB 2.0**
КОМПЛЕКТ ПОСТАВКИ: **аккумулятор, адаптер переменного тока, кабель USB, инструкция, полставка, футляр и ремешок для переноски, набор ПО**
ВОЗМОЖНОСТЬ ОБНОВЛЕНИЯ ПО: **да**
РАЗМЕРЫ: **147x84x31 мм**
ВЕС: **415 г**

➜ **плюсы.** Нашему вниманию представляется еще один плеер с большим экраном, большим жестким диском и большими возможностями по работе с различными видами файлов. Ну, на большом дисплее и фотки, и тексты смотрятся хорошо. Понравилось удобное и понятное меню, продуманная система управления. Файлы на плеер закидываются прямо из проводника безо всяких сторонних утилит. У этого устройства великое множество дополнительных функций. Работа с двумя типами флеш-карт, возможность передачи данных напрямую на принтер, без участия компьютера, а также опция подключения плеера к телевизору дает ему возможность стать не просто средством развлечения. Так что перед вами многофункциональный комбайн-помощник, а не банальная игрушка. Поразила близкая к рекордной скорость копирования с компьютера на жесткий диск плеера.

➜ **минусы.** Такая богатая функциональность самым негативным образом отразилась на размерах и весе устройства, которые очень велики. Очень слабая поддержка воспроизведения видеофайлов — из тестового комплекта запустилась едва ли третья часть. Возможно, дело можно будет поправить заливкой новой прошивки, хотя не факт.



Archos Gmini 402
($400) 7 баллов

ОБЪЕМ: **20 Гб**
РАЗМЕР ЭКРАНА: **2,2 дюйма**
ФОРМАТЫ АУДИО: **MP3, WMA, WAV**
ФОРМАТЫ ВИДЕО: **MPEG4, AVI**
ФОРМАТЫ ФОТО: **BMP, JPG**
ДОПОЛНИТЕЛЬНЫЕ ВОЗМОЖНОСТИ: **USB-хост, файловый менеджер, подключение к ТВ, игры**
ИНТЕРФЕЙС: **USB 2.0**
КОМПЛЕКТ ПОСТАВКИ: **наушники, USB-кабель, USB-host кабель, аудио/видео кабель и адаптер, зарядное устройство, чехол, инструкция по эксплуатации.**
ВОЗМОЖНОСТЬ ОБНОВЛЕНИЯ ПО: **да**
РАЗМЕРЫ: **106x60,3x17,4 мм**
ВЕС: **160 г**

➜ **плюсы.** Маленькая и очень удобная машинка, которая легко уместится в кармане. Несмотря на размеры, претендует на независимость от большого брата, так как обладает встроенным файловым менеджером, который позволяет без привлечения к этому делу ПК переименовывать файлы, создавать папки и так далее — в общем, нормальный такой файловый менеджер. Похожая штука есть и для упорядочивания твоей музыкальной коллекции по жанрам, именам и так далее.

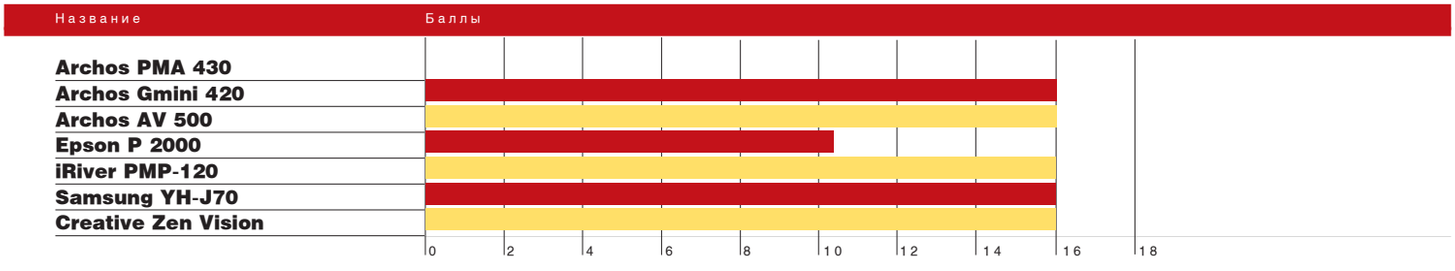
Как и другие участники нынешнего теста, этот малыш разбирается со всеми известными мировой науке видами файлов. Обладает встроенным микрофоном и возможностью вывода изображений на ТВ.

Система управления проста и довольно удобна. Несмотря на свои маленькие размеры, экран очень качественный.

➜ **минусы.** Время копирования тестового 700 Мб файла более чем ощутимо, ну это понятно — размеры не позволили поставить быстрый жесткий диск.

Запись мультимедийных данных для последующего прослушивания, проигрывания и просматривания возможна только через синхронизацию Windows Media Player'а. Через проводник можно записать файлы только как на съемный жесткий диск.

Разрешение в DivX 5



Поддержка различных разрешений плеерами. Здесь все файлы закодированы кодеком DivX 5.0.

выбор редакции
спец

Archos AV500
($670) 8 баллов

ОБЪЕМ: **30 Гб**

РАЗМЕР ЭКРАНА: **4 дюйма**

ФОРМАТЫ АУДИО: **MP3, WMA, WAV**

ФОРМАТЫ ВИДЕО: **MPEG4, AVI**

ФОРМАТЫ ФОТО: **BMP, JPG**

ДОПОЛНИТЕЛЬНЫЕ ВОЗМОЖНОСТИ: **USB-хост, файловый менеджер, подключение к ТВ, игры**

ИНТЕРФЕЙС: **USB 2.0**

КОМПЛЕКТ ПОСТАВКИ: **USB-кабель, хост-адаптер USB, AC-адаптер, наушники, защитный чехол, инструкция, ТВ-крэдл, пульт ДУ, аудио/видео кабели (SCART in и SCART out).**

ВОЗМОЖНОСТЬ ОБНОВЛЕНИЯ ПО: **да**

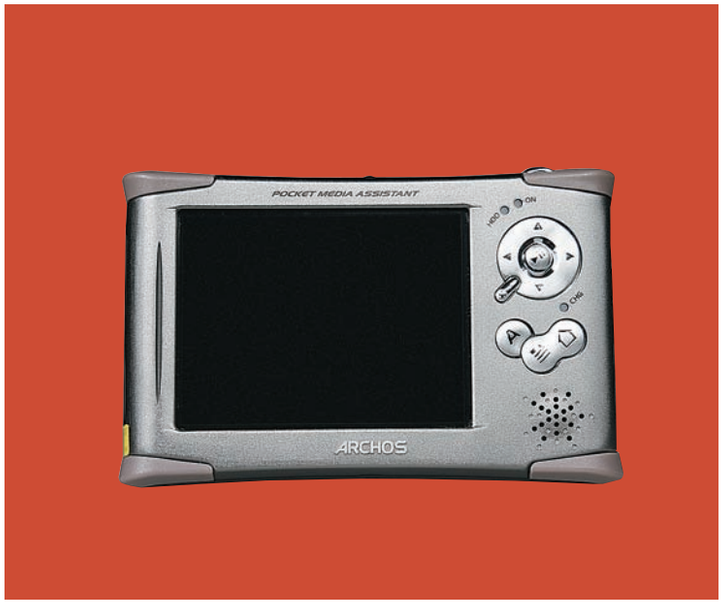
РАЗМЕРЫ: **76x124x1,8 мм**

ВЕС: **255 г**

→ **плюсы.** Серьезно усовершенствованная версия Archos Gmini 402 в измененном дизайне как снаружи, так и внутри. Изменен корпус, размещение портов и средств управления. Как и у Archos Gmini 402, интерфейс красочный и понятный. Со средствами управления разбираешься довольно быстро, система продуманная. Понравилось то, что в этой модели можно заливать любые файлы через проводник, не заморачиваясь ни на какие синхронизации.

Все плюсы, вроде качественного экрана, внутренних менеджеров и так далее, сохранились. Также был заменен жесткий диск, что самым положительным образом сказалось на скорости копирования.
И не забудем про отличный комплект поставки.

→ **минусы.** Есть проблемы с воспроизведением файлов из тестового комплекта — полностью не запустились фильмы, закодированные DivX 3. Обновление прошивки предусмотрено, но вряд ли это поможет.



Archos PMA430
($850) 9 баллов

ОБЪЕМ: **30 Гб**

РАЗМЕР ЭКРАНА: **4 дюйма**

ФОРМАТЫ АУДИО: **MP3, WAV, WMA**

ФОРМАТЫ ВИДЕО: **AVI, MPEG4**

ФОРМАТЫ ФОТО: **JPEG, PNG, GIF, BMP**

ДОПОЛНИТЕЛЬНЫЕ ВОЗМОЖНОСТИ: **USB-хост, Wi-Fi b, IR, органайзер, игры, сенсорный экран**

ИНТЕРФЕЙС: **USB 2.0**

КОМПЛЕКТ ПОСТАВКИ: **USB-кабель, AC-адаптер, наушники, защитный чехол, инструкция.**

ВОЗМОЖНОСТЬ ОБНОВЛЕНИЯ ПО: **да**

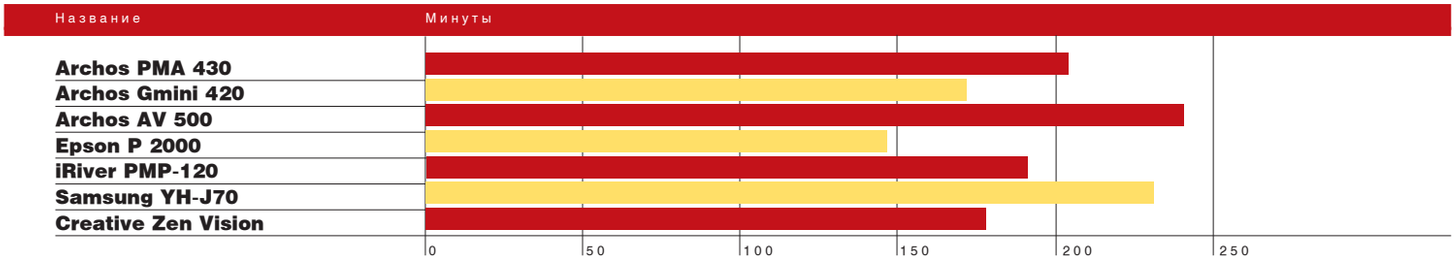
РАЗМЕРЫ: **125x78x20 мм**

ВЕС: **280 г**

➔ **плюсы.** Самый навороченный из сегодняшних участников. Этот плеер обладает собственной ОС — Linux Qutopia, под управлением которой находятся все дополнительные возможности этого устройства, а их немало. Это органайзер (адресная книга, калькулятор, календарь), игры, сенсорный экран, а также встроенный адаптер Wi-Fi, с помощью которого можно выйти в интернет. Неплохо для «плеера», правда? Естественно, он может просматривать любые типы данных, которые на него записываются просто из проводника. Имеется встроенный микрофон, что дает устройству функции диктофона. Несмотря на такое обилие функций, у него далеко не самые большие габариты и вес. В комплекте поставки есть все, что может пригодиться.

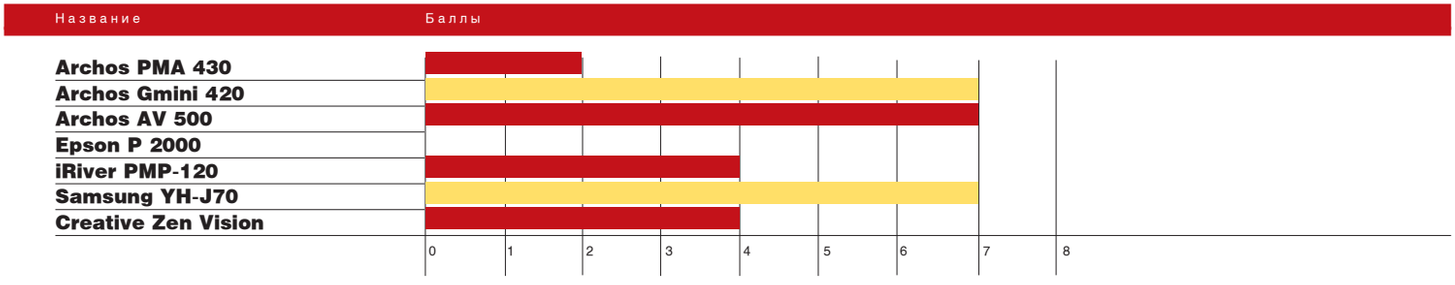
➔ **минусы.** Если ты по какой-то причине не любишь пользоваться сенсорным экраном, то у тебя могут возникнуть проблемы — обычная система управления не очень удобная, путанная. Файлы открываются довольно медленно.

Время автономной работы



Время автономной работы плеера — количество минут, которые ты сможешь без задействования внешней сети смотреть фильмы. Здесь большие (практически в два раза) разбросы наверняка вызваны разной емкостью аккумуляторов и аппетитами встроенных экранов и винчестеров.

Аудиодорожки



Наверняка не раз возникала такая ситуация, когда при запуске фильма присутствует изображение, а звука нет. Вероятность повторения этой неприятности с плеерами так же весьма велика. И если на компьютере ты просто ставил недостающий кодек, то здесь придется либо перепрошивать медиаплеер, что не всегда возможно, либо перекодировать фильм, что отнимет достаточно много времени. Выходом станет приобретение аппарата, поддерживающего большинство форматов — здесь больший балл означает лучшую совместимость.

➔ **выводы**. Покрутив плееры в руках, сразу понимаешь, что при прочих равных компактность приоритетнее всего. Samsung YH-J70 получает «Лучшую покупку» за малые размеры, длительное время работы, приемлемую цену и поддержку всех тестовых видеофайлов. Однако стоит брать его, только если ты обладатель мощного компьютера, на котором конвертер будет работать быстрее, а не по часу на фильм, как на слабенькой машине, участвующей в тесте.

Archos AV500 обладает большим экраном, пультом, возможностью подключения к телевизору, максимальным временем автономной работы и внушительным дисковым пространством. То есть на любую вечеринку ты попадаешь со своим мультимедиа-центром с многочасовой подборкой видеоприколов, музыки и фильмов. За это мы и решили дать Archos AV500 «выбор редакции».

Test_lab выражает благодарность за предоставленные на тестирование источники бесперебойного питания компаниям: ПИРИТ (т.(495) 974-3210, **www.pirit.ru**)

Однако стоит задуматься и произвести простейшие расчеты. За максимальное время автономной работы со включенным дисплеем (около 3,5 часа) можно посмотреть всего пару фильмов. А они вполне влезут на 2-гигабайтную флеш-карту (за $150), вставленную в КПК за $300. А по возможностям КПК пока на голову превосходят любые медиа-плееры, здорово выигрывая у них и в весе.

Правда, стоит отметить, что качество видео на КПК все же будет хуже, и слабенькие модели не смогут проиграть фильм, сжатый с очень хорошим качеством — процессор просто надорвется. Так что медиаплеер все-таки больше подходит прожженному тусовщику, которому непременно надо таскать с собой серьезную коллекцию и просматривать ее в хорошем качестве, а не тому, кто хочет изредка посмотреть пару фильмов в дороге

hard

тихий, но эффективный

ТЕСТИРУЕМ COOLERMASTER XDREAM K640 [RR-KIFL9E1-GP]

TEST_LAB

технические характеристики:

ПОДДЕРЖИВАЕМЫЕ РАЗЪЕМЫ: **Socket 754, 939, 940, AM2**
МАТЕРИАЛ РАДИАТОРА: **алюминий + медный сердечник**
СКОРОСТЬ: **800-2800 об/мин**
УРОВЕНЬ ШУМА ПРИ СРЕДНЕЙ НАГРУЗКЕ: **19,5 дб**
ВЕС: **397 г**
РАЗМЕРЫ КУЛЕРА: **90x90x40 мм**
РАЗМЕРЫ ВЕНТИЛЯТОРА: **92x25мм**
РАЗЪЕМ ДЛЯ ПОДКЛЮЧЕНИЯ, КОНТАКТОВ: **3**
МАКСИМАЛЬНАЯ ТЕМПЕРАТУРА С НАГРУЗКОЙ: **66 ° C**
МИНИМАЛЬНАЯ ТЕМПЕРАТУРА БЕЗ НАГРУЗКИ: **54 ° C**

Итак, начнем с малого. Попробуем разобраться с названием этого холодильника. Первая часть — XDream, наверное, имеется в виду Мечта X. Тот самый кулер, который ты так давно искал и хотел заполучить — кулер твоей мечты. С этим все хорошо, но вот что могут значить таинственные K640? Ни к процессорным сокетам, ни к количеству ребер это никакого отношения не имеет. Посему для нас вторая часть в названии осталась загадкой. Но не имя красит... Данный шедевр инженерной мысли предназначен только для процессоров AMD, и что самое главное, его можно ставить на самые новые CPU с разъемом AM2. Производитель также утверждает, что его творение сможет справиться даже с такими горячими парнями как FX51. Проверим...

Ко всему прочему, в описании сказано, что уровень шума равен 19,5 Дб на расстоянии одного метра при средней нагрузке. На практике кулер оказался действительно очень тихим, даже на максимальных оборотах.

Во внешности CoolerMaster XDream K640 нет ничего особенного: черный вентилятор и прямоугольный алюминиевый радиатор. А вот в конструкции есть несколько очень интересных особенностей. Во-первых, это слегка возвышающийся над основанием медный сердечник (чуть меньше одного миллиметра), который может соприкасаться только с 60% поверхности процессора. На наш взгляд, это не лучшим образом влияет на охлаждение, но результаты теста развеяли наш пессимизм.

Радиатор в верхней части где-то на 1 см шире с каждой из 4-х сторон. Далее, сами ребра имеют перекрестное сечение, то есть от центра в четыре стороны под углом в 90 градусов. Ну и последняя конструктивная особенность, сейчас уже достаточно распространенная — по бокам лопасти вентилятора не ограничены рамкой.

На кругляшок медного сердечника производителем нанесена термопаста белого цвета очень ровным и достаточно тонким слоем. Именно так ее надо мазать в идеале.

Памятуя о прошлом неудачном опыте установки кулеров, были опасения изрезать пальцы о ребра в процессе крепежа. Но совершенно зря: установка этого кулера предельно проста! Ура! Надеемся, это не исключение из правил, а закономерность для всех кулеров этой марки.

CPU в тестовом стенде был очень горячим AMD Athlon64 FX-57, и при этом в системе трудились еще два X1900XT, что явно не могло не нагревать воздух внутри корпуса до запредельных температур. В связи с этим, мы побоялись тестить все это с закрытой боковой крышкой и сняли ее. В простое температура оказалась равна 54 градусам, что не так мало, но для такого мощного тестового стенда нормально. На максимальной нагрузке (созданной утилитой S&M) в течение 15 минут температура повысилась до 66 и застыла на этой отметке. Восторг исключительный! Реальный XDream! Тихий и производительный. Единственное, что на такой горячий камень, да еще с двумя X1900XT мы бы все-таки не рекомендовали ставить его в закрытый корпус. Но во всех остальных случаях тебе хватит этого тихоходного аппарата за глаза.

тестовый стенд:

Материнская плата: **Asus A8R32-MVP Deluxe**
Процессор: **AMD Athlon 64 FX-57**
Видеокарта: **2xATI Radeon X1900XT Crossfire**
Память: **2x512 Мб DDR400 Hynix Original**
HDD: **WD1600JD, 160 Гб, 7200 об/мин**

видеорекордер от плекстор

PLEXTOR CONVERTX PX-TV402U

TEST_LAB

технические характеристики:

ТВ-ТЮНЕР:	**PAL/SECAM**
ВИДЕОВХОДЫ:	**S-Video, RCA**
АУДИОВХОДЫ:	**RCA (Stereo)**
TV-ВХОДЫ:	**RF/коаксиальный**
ПО В КОМПЛЕКТЕ:	**InterVideo WinDVR 5, InterVideo WinDVD Creator 2**
РАЗМЕРЫ:	**184x32,4x155 мм**
ВЕС:	**500 г**
ЦЕНА:	**$200**

С твоим зрением все в порядке: это видеорекордер, выпущенный под маркой Plextor. По сути, это очень продвинутое устройство видеозахвата. С обычными CD/DVD-драйвами эта штука не имеет ничего общего, кроме имени компании производителя. Оказалось, что это уже второй подобный девайс от Plextor. Полное название устройства — Plextor Personal Video Recorder ConvertX PVR PX-TV402U. В комплект поставки входит целая куча различных проводков. Есть кабель с блоком питания, состоящий из двух частей, длинною чуть более двух метров. Шнур USB (около метра). Имеются также кабели 2xRCA-2xRCA и RCA-RCA для подключения к видео/аудио выходам (оба чуть более метра), а также провод S-Video-RCA той же длинны. Еще в коробочке лежат переходник SCART-3xRCA, многофункциональный пульт ДУ и инфракрасный приемник для него. Подключение ConvertX PVR осуществляется проще некуда. Сначала надо установить драйверы с диска, а потом воткнуть устройство в USB-порт и подать питание. Обе программы с диска поставляются вместе с серийным ключом и полностью русифицированы. Это ПО для видеозахвата (InterVideo WinDVR 5), редактирования и записи захваченного видео на диск (InterVideo WinDVD Creator 2). Записывать можно как на CD, так и на DVD.

Сама коробочка конвертера — серебристого цвета с черной передней панелью — выглядит элегантно и сдержанно. На корпусе два индикатора: Power («питание») и Ready to record («готов к записи»). Его легко можно будет поставить как в строгий классический, так и в современный интерьер в стиле «техно».

Возможности у Plextor ConvertX PX-TV402U действительно очень большие. Его можно использовать как ТВ-тюнер, подключив антенну напрямую. Получается просто и удобно: Plextor смог поймать даже больше каналов, чем домашний телевизор марки Sharp. Управлять просмотром очень удобно, можно одновременно глядеть один канал и записывать другой. В окне предпростомтра (сканирования) каналов можно выводить, к примеру, только выбранные каналы, которым, к тому же, можно вручную дать названия, чтобы даже во время рекламы не гадать, что за канал смотришь. Но качество изображения все же немного хуже, чем при подключении к телевизору через видеоразъемы.

Подсоединиться можно к любому устройству, имеющему композитные или RCA-выходы. Причем аудио захватывается в режиме стерео. Удобна возможность легкого переключения между разными входами захвата. Например, включив антенну напрямую, а также подсоединившись с помощью тюльпанов к видеомагнитофону, а через композитный выход еще к чему-нибудь, между ними можно переключаться в два действия.

При этом во время обычного просмотра загрузка процессора составляет около 17%, а во время записи на хард от 24 до 30%. Записывать видео можно в различных форматах: на жесткий диск для последующего монтажа и сразу на DVD или CD в форматах MPEG 1,2,4, AVI (DivX) и других, если в компьютере есть CD/DVD-рекордер. Разрешение варьируется от 176x144 до 720x576. Качество захватываемого звука также регулируется.

С помощью этого видеоконверета можно легко и просто перегнать в «цифру» домашний видеоархив с кассет VHS, которые есть почти в любом доме.

Подводя итог, можно сказать, что, как и все обычные рекордеры Plextor, ConvertX PX-TV402U высочайшего качества. В данном случае можно с уверенность сказать, что своих немалых денег устройство стоит.

тестовый стенд:

МАТЕРИНСКАЯ ПЛАТА:	**Asus P5AD2-E Premium**
ПРОЦЕССОР:	**Intel Pentium 4 505 (2,66@3,2)**
КУЛЕР:	**Zalman CNPS7700 Cu**
ВИДЕОКАРТА:	**PowerColor X800GT 256 Mb**
ПАМЯТЬ:	**2x512 Мб Corsair PC5400UL**
HDD:	**WD2000JD, 200 Гб, 7200 об/мин**

Test_lab выражает благодарность за предоставленные на тестирование источники бесперебойного питания компаниям: ПИРИТ (т.(495) 974-3210, **www.pirit.ru**)

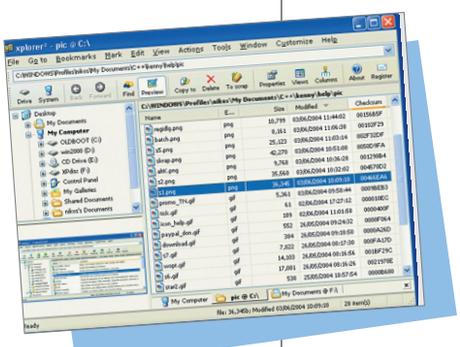
Soft

noname

НАИСВЕЖАЙШИЕ ПРОГРАММЫ ОТ NNM.RU
DOC@NNM.RU

Xplorer2 v.1.5.0.1

Xplorer2 — файловый менеджер, чем-то похожий на стандартный Проводник, но предоставляющий дополнительные возможности за счет своих многочисленных кнопок и панелей.
К примеру, Xplorer2 имеет не две, а три панели просмотра. В первой панели отображается древо каталогов, а две другие позволяют работать с файлами. Вдобавок, встроенные средства этого менеджера позволяют просматривать графику, предварительно прослушивать аудио- и просматривать видеофайлы, а также файлы форматов HTML, Text, RTF и Hex. Для работы с файлами и директориями на локальном PC тут имеются все необходимые опции (копирование, перемещение, удаление, поиск, фильтрация, просмотр по заданным параметрам и т.д.). Оригинальная возможность Xplorer2 — помещение файлов в специальный контейнер (Scrap Conteiner), который можно сравнить с виртуальной папкой. В ней могут храниться файлы, расположенные в разных местах. При этом они не перемещаются в контейнер, а на них просто создается ссылка. Поддерживается работа с сетевыми дисками, причем в подключенных сетевых дисках при необходимости происходит автоматическое обновление файлов. Xplorer2 может работать как с отдельно взятыми файлами, так и с файлами в пакетном режиме.



Portable Burning AIO by Friction Baby

Подборка лучших программ для копирования и записи CD и DVD дисков, которая найдет место на твоей флешке и всегда будет рядом! Для запуска приложений не нужно инсталляции, что очень удобно при ежедневной работе на разных компьютерах.
Состав:

1. ALCOHOL 120 1.9.5.3823
2. BLINDWRITE
3. CD-DVD DR
4. CLONE DVD 2
5. DEEP BURNER1
6. DVD REGION + CSS FREE 5.9
6. MICRO
7. PORT DVDFAB DECRYPTER
8. SMALL CD-WRITER
9. SILENTNIGHT MICRO CD BURNER

Image to Icon Converter v1.8

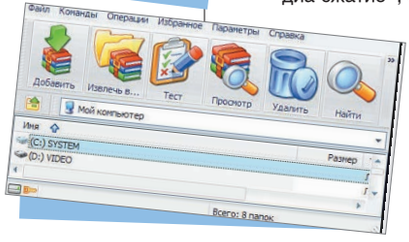
На портале **nnm.ru** хорошо расходятся иконки, но многих смущают их экзотические форматы, вроде PNG. Вот программка Image to Icon Converter, которая конвертирует любые изображения (BMP, DIB, GIF, JPG, JPE, JPEG, TIF, TIFF, CPT, WMF, EMF, PNG, PCX, JP2, JPC, J2K, TGA, RAS) в ICO.

Remote Installer v1.3.76

Remote Installer — инструмент, позволяющий инсталлировать и деинсталлировать программное обеспечение на удаленных компьютерах.

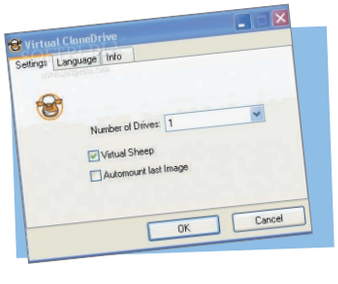
WinRAR v3.60 beta 4

Программа умеет создавать SFX-архивы с задаваемым текстом в окне и заголовке окна, паролить архивы, создавать многотомный архив, использовать «мультимедиа сжатие», с помощью которого можно добиться еще большей степени сжатия мультимедиа-файлов. WinRar удобно интегрируется в контекстное меню и прекрасно работает с архивами ZIP, CAB, ARJ, LZN, TAR, GZ, ACE, UUE, BZ2, JAR, ISO.



Virtual CloneDrive 5.1.4.5 Multilingual (Freeware)

Утилита, предназначенная для создания виртуальных дисков из образов, созданных программами CloneCD и CloneDVD.
После инсталляции Virtual CloneDrive и перезагрузки компьютера в системе создается виртуальный CD/DVD-ROM, в который и вставляются снятые образы.
При этом ты имеешь возможность пользоваться «клонами» CD/DVD дисков непосредственно с винчестера компьютера, без записи дисков на физические CD/DVD. Образы добавляются через контекстное меню созданного виртуального диска.



CloneDVD 2.8.9.9

Опять обновилась одна из лучших программ для клонирования DVD-дисков. Интуитивно понятный интерфейс делает эту программу привлекательной с точки зрения неискушенного пользователя. Для того, чтобы сделать клон диска, нужно лишь пройти несколько шагов диалога программы....

Можно скопировать только некоторые части DVD диска или сделать точную его копию, с меню навигации, субтитрами, всеми языками перевода. CloneDVD поддерживает работу практически со всеми современными DVD-приводами. Работать с такой программой — одно удовольствие как продвинутым пользователям, так и начинающим.

В этой версии добавлены новые опции, которые помогут улучшить качество видеокартинки, обновились языковые интерфейсы, исправлено несколько ошибок, внесены другие положительные изменения.

Audio Editor Gold 8.4.5

Audio Editor Gold — это отличный редактор аудио-файлов, который поддерживает все существующие форматы. Умеет конвертировать музыку из одного формата в другой, редактировать теги, обладает отличными встроенными эффектами и т.д. Имеет простой и удобный интерфейс, что, несомненно, является плюсом для начинающих пользователей.

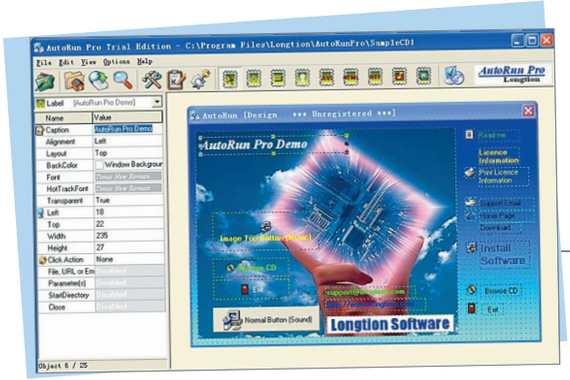
WinTools.NET Professional 7.4.1

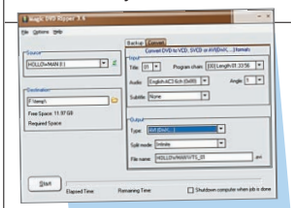
Набор инструментов, предназначенный для повышения производительности операционной системы MS Windows и поддержания производительности на высоком уровне на протяжение всего эксплуатационного периода. В состав программы входят следующие инструменты: Clean Uninstaller, Scan Files, Scan Registry, Start Up Manager, Tweak UI, Net Tweaker, The Privacy.

AutoRun Pro Enterprise 8.0.0.71

Мощный визуальный инструмент для создания интерфейсов автозагрузочных меню и презентаций профессионального уровня для CD/DVD.

Это самый простой способ создания и редактирования таких интерфейсов в среде WYSIWYG (получаешь то, что видишь) — клик, перемещение и просмотр результата. Вставка рисунков, кнопок, HTML, RTF, текстовых лейблов. На каждый объект можно назначить определенное действие. Объект может менять свое состояние при наведении или нажатии и т.д. Программа легко осваивается, присутствуют демонстрации и мастера работы с проектами.





Magic DVD Ripper v4.1 Beta

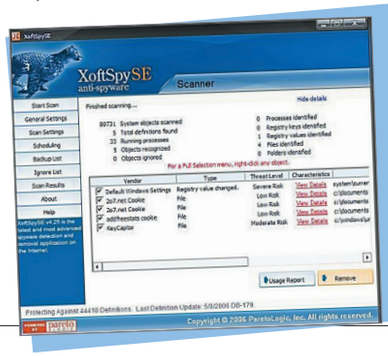
Мощная утилита для создания копий DVD-фильмов меньшего размера с настраиваемым качеством. Программа позволяет конвертировать файлы в форматы VCD (MPEG-1), SVCD (MPEG-2), DivX AVI и другие AVI.

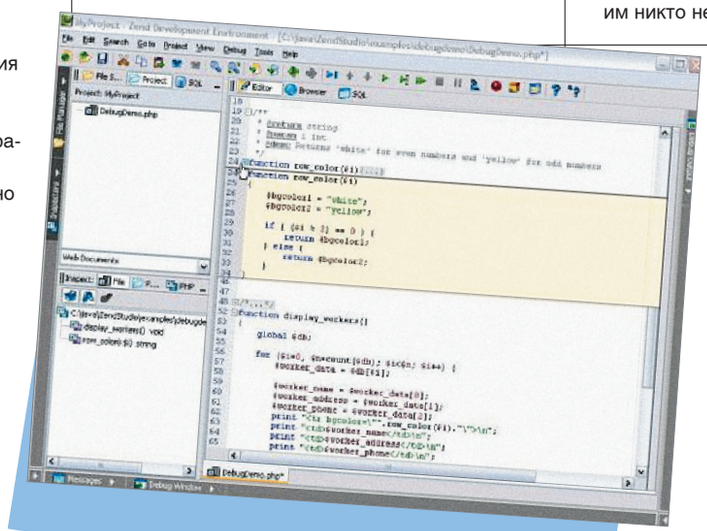
Winamp v5.22

Вышла новая версия самого известного аудиоплеера! (Ведь видео им никто не смотрит, надеюсь? :)

XoftSpySE 4.26.182

Программа предназначена для обнаружения и удаления Adware, Spyware, Spybots, Malware, Spy Pop-ups, Keyloggers, Unwanted Toolbars и других вредоносных программ. Она может полностью просканировать оперативную память и жесткий диск твоего компьютера на наличие там шпионского модуля. Громадная, постоянно обновляющаяся база данных этой программы позволит тебе быть надежно защищенными от вредоносных программ и не потерять свои конфиденциальные данные!





Zend Studio Enterprise Edition 5.2.0

Zend Studio 5 — это интегрируемая среда разработки (IDE), доступная для профессионалов, которая охватывает все компоненты разработки необходимых для полного применения и реализации возможностей PHP. Содержит максимальный набор инструментов разработчика для редактирования, отладки, анализа, оптимизации кода и баз данных.

admining

НАСТРОЙКА ДОМЕННОЙ ПОЛИТИКИ БЕЗОПАСНОСТИ.
ЧАСТЬ ТРЕТЬЯ — ЗАКЛЮЧИТЕЛЬНАЯ

АЛЕКСАНДР ПРИХОДЬКО
(SANPRIH@MAIL.RU)

Продолжая тему прошлого модуля, хотелось бы обратить внимание на возможности управления через GPO такими вещами на пользовательских компьютерах, как сервисы. Ты, изучив внимательно некоторые полезные ресурсы в интернете, журналах и мануалах, можешь заметить, что, при установке, Windows XP запускает целый сонм сервисов, которые тебе в повседневной жизни не нужны. Таким образом, садишься и прикидываешь, какие сервисы лишние, и на уровне доменной политики отключаешь их. Сейчас мы проделаем это на примере сервиса «Удаленный реестр». Данный параметр у нас активирован. Для просмотра запущенных сервисов очень удобно пользоваться продуктом «procexp» фирмы «sysinternals» — **www.sysinternals.com**. Данная прога позволяет посмотреть описание процесса, запущенного на машине. Посмотрим это на компе доменного пользователя Балаганова (рис. Диспетчер задач)

Мы видим, что служба «Удаленный реестр» запущена и работает. Теперь пристрелим ее. На контроллере домена создаем новый объект групповой политики и назовем его «Сервисы». Открываем на редактирование и начинаем издеваться над веткой «Computer Configuration» → «Windows Settings» → «Security Settings» → «System Services». Находим параметр «Remote Registry», активируем данный параметр проставлением галочки в «Define This policy Setting» и отключаем «Удаленный реестр» активированием «Disabled». Прикручиваем политику «Сервисы» на весь домен. Как обычно, перечитываем политику «gpupdate /force». Перегружаем машину Балаганова и смотрим, что получилось.

Таким образом, ты можешь увеличить производительность всех машин домена через применение GPO. Еще немного о применении GPO: если ты будешь разворачивать систему обновлений операционных систем и других приложений от Microsoft в домене, то GPO и здесь спасет отца русской демократии. Разворачиваешь где-нибудь WSUS, настраиваешь его на закачку апдейтов, а через GPO настраиваешь обновления на всех клиентских машинах: GPO «Сервисы» → «Computer Configuration» → «Administrative Templates» → «Windows Components» → «Windows Update». Да, еще рекомендуется настроить аудит на файлы, расположенные на сетевых ресурсах. Если какой-либо юзер удалит чужой файл на сетевом ресурсе, ты всегда сможешь найти, кто это сделал, и сдать его хозяину файла. А процесс разборки можно снять на видео и выложить в сеть для всеобщего обозрения. За аудит отвечает ветка GPO «Computer Configuration» → «Windows Settings» → «Security Settings» → «Local policies» → «Audit Policy» → «Audit object access». Отмечаем «Success» и «Failure».

Теперь для включения аудита осталось сделать следующее: правая кнопка мыши на сетевом ресурсе (расшаренной папке), «Properties» → «Security» → «Advanced» → закладка «Auditing» → кнопка «Add» → и выбираем «Domain Users». Открывается окно свойств аудита.

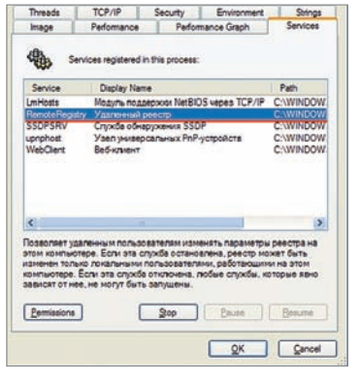
Отмечаем указанные на рисунке «Свойства аудита» чекбоксы. Аудит настроен. Теперь проверим, как он работает. Пользователем «Бендер» на диске «Обмен» создадим текстовый файл и удалим его под пользователем «Балаганов». Для контроля над процессом используем на контроллере домена «Event Viewer». Легко видеть, как Бендер создал свой файл, а Балаганов удалил чужой документ.

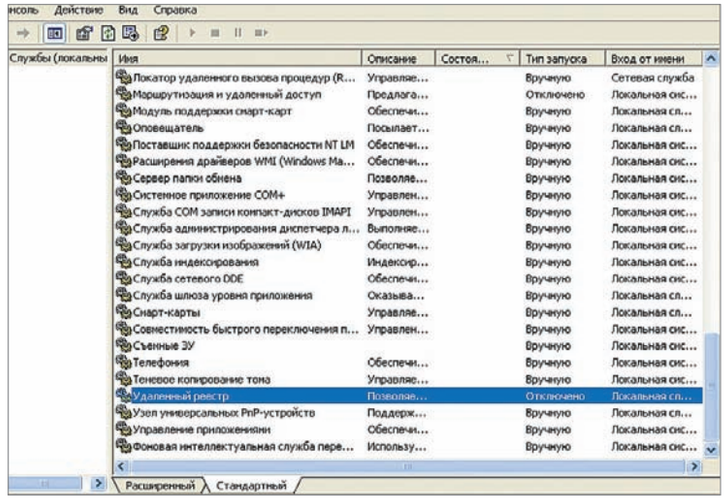
Теперь ты всегда можешь сказать пользователю, кто именно снес его годовой отчет, который он по ошибке выложил в папку «Обмен». Кстати, политику аудита настраивай на «Default Domain Policy».
И еще: для быстрого поиска нужных тебе событий в «Event Viewer» можно пользоваться фильтрами. Например, для поиска нужных событий по созданию-удалению файлов делаем следующее: правая кнопка мыши на ветке «Security» → «View» → «Filter». Далее в «Event Source» выбираем «Security», а в категории — «Object Access». Теперь ты увидишь только события, относящиеся к нужной тебе тематике.

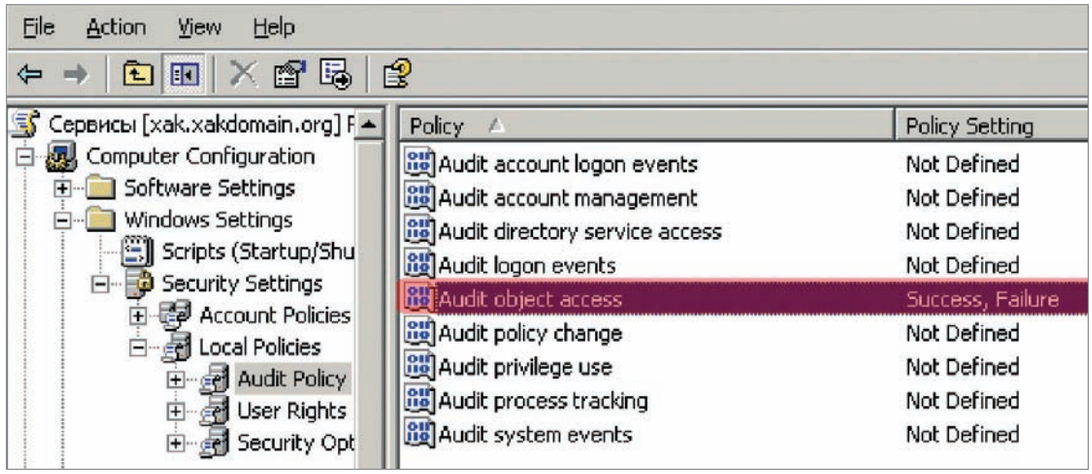
Используй для просмотра фильтры, и тогда твои глаза никогда не устанут.

Службы

Диспетчер задач







Аудит файлов

→ разворачиваем антивирусную защиту. Прежде, чем приступить к описанию построения защиты, хотелось бы сразу отметить, почему выбраны именно продукты от Лаборатории Касперского. Как обычно, отбрасывая религиозную составляющую, в определении продуктов оставим только функциональность и экономическую составляющую.

Посчитаем стоимость антивирусного ПО для сети из трех серверов и сорока клиентских машин. Почтовый сервер не считаем.

1 KASPERSKY ANTI-VIRUS BUSINESS OPTIMAL SUITE RUSSIAN EDITION. 40 WORKSTATION 1 YEAR BASE LICENCE — 740 У.Е.

2 KASPERSKY ANTI-VIRUS BUSINESS OPTIMAL FOR WINDOWS RUSSIAN EDITION.

3 FILESERVER 1 YEAR BASE LICENCE — 956 У.Е.

Итого: для Касперского Антивируса нужно — 1700 у.е.

посчитаем продукт от Symantec:

1 SYMANTEC ANTIVIRUS 10.0 WITH GROUPWARE PROTECTION BUSINESS PACK 25 USER IN GOLD MAINTENANCE 1YEAR RNW VALUE BAND S — 1689 У.Е.

2 SYMANTEC ANTIVIRUS 10.0 WITH GROUPWARE PROTECTION BUSINESS PACK 10 USER IN GOLD MAINTENANCE 1YEAR RNW VALUE BAND S — 784 У.Е.

3 SYMANTEC ANTIVIRUS 10.0 WITH GROUPWARE PROTECTION BUSINESS PACK 5 USER IN GOLD MAINTENANCE 1YEAR RNW VALUE BAND S — 421 У.Е.

Итого: 2894 у.е. Данные с сайта **www.symantec.com/small_business/products**.

теперь посмотрим на TrendMicro:

1 ENTERPRISE EDITION SUITE CLIENT SERVER SUITE ENTERPRISE EDITION 40 USERS — 2229 У.Е.

Антивирус NOD32 Enterprise Edition newsale for 40 User — 1340 у.е.

1 АНТИВИРУС DR.WEB ДЛЯ WINDOWS 95-XP, НА 12 МЕСЯЦЕВ 36..40 ПК (ДЛЯ КОНЕЧНОГО ПОЛЬЗОВАТЕЛЯ ЗА 1 ПК) — 830 У.Е.

2 АНТИВИРУС DR.WEB ДЛЯ ФАЙЛОВЫХ СЕРВЕРОВ, НА 12 МЕСЯЦЕВ 3 ПК (ЗА 1 СЕРВЕР ДЛЯ КОНЕЧНОГО ПОЛЬЗОВАТЕЛЯ) — 1125 У.Е.

Итого: Для Dr. WEB нужно 1955 у.е.

Все, больше искать инфу по антивирусам не буду. Если покупать лицензионный софт, то выходит, что продукты Лаборатории Касперского дешевле. Займемся разворачиванием Kaspersky Anti-Virus Business Optimal.

Считаем, что ключик у тебя в кармане и на сервер, и на клиентские машины. Если коробки с софтом у тебя нет, то качаем следующие модули: **www.kaspersky.ru/productupdates**. На этой странице выбираем «Антивирус Касперского Business Optimal» и на открывшейся странице выбираем «Антивирус Касперского для Widows Workstations», «Антивирус Касперского для Widows Files Servers», «Kaspersky Administration Kit». С сайта **www.microsoft.com** легко качаем бесплатный Microsoft SQL Server, из последних. Вот что по поводу SQL-сервера пишет Лаборатория Касперского:

«При установке «Сервера администрирования» должны быть непременно выполнены следующие системные требования: операционные системы: Microsoft Windows NT Server / Workstation 4.0 SP 6a и выше; Microsoft Windows 2000 Server / Professional SP1 и выше; Microsoft Windows XP Professional / Home SP1 и выше; Microsoft Windows Server 2003.

Сервер баз данных (может быть установлен на другой машине): Microsoft SQL Server 2005; Microsoft SQL Server 2000 SP 3 и выше; Microsoft SQL Server 2000 Desktop Engine (MSDE) SP 3 и выше (дистрибутив MSDE 2000 SP3 входит в комплект поставки Kaspersky Administration Kit и может быть установлен непосредственно с компакт диска Kaspersky Administration Kit)».

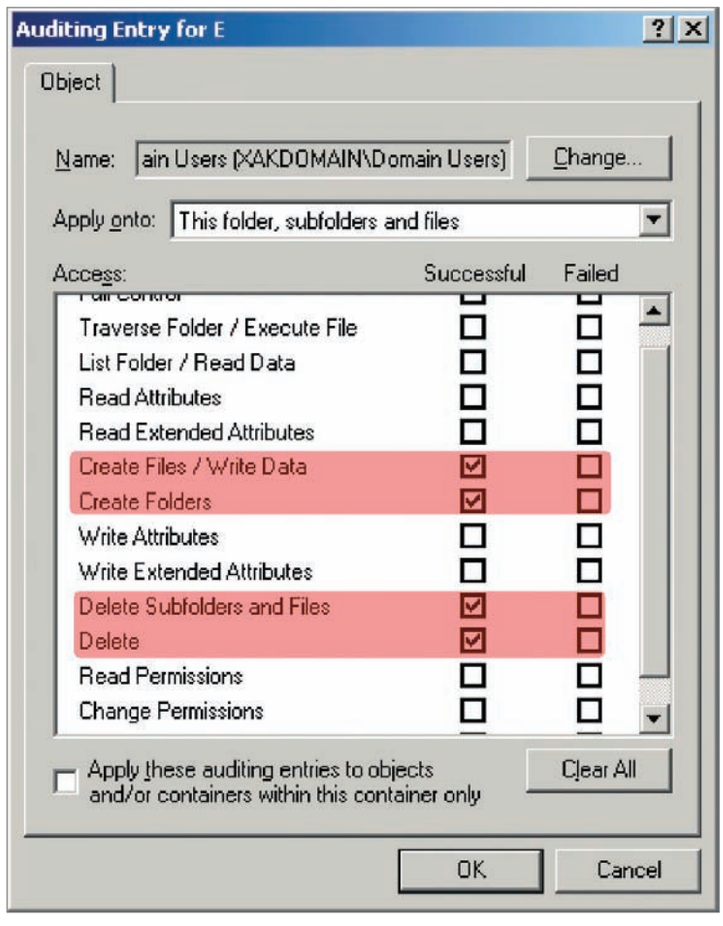
Теперь у тебя есть все необходимое для разворачивания антивирусной защиты. На своем самом любимом сервере, самом надежном (контроллере домена), развернем сначала «Microsoft SQL Server». Он будет держать базу пользователей. При установке «Microsoft SQL Server» везде просто нажимаем «Next» и ставим его со всеми параметрами по умолчанию. После установки перегрузим сервер, для того, чтобы сервис запустился.

Теперь установим «Антивирус Касперского для Widows Files Servers». Чтобы не было путаницы, сначала разберемся в назначении всех программ.

«Kaspersky Administration Kit» — это средство управления сетью антивирусной защиты. «Kaspersky Administration Kit» может быть установлен на любой машине сети и просто подключаться к Серверу администрирования. Сервер администрирования — это оболочка, которая и создает виртуальную сеть антивирусной защиты. Microsoft SQL Server — это хранилище базы данных сети антивирусной защиты.

Так как мы разворачиваем антивирусную защиту на сервере (контроллере домена), то получается, что на контроллере домена мы установим следующие приложения: «Microsoft SQL Server», «Антивирус Касперского для Widows Files

Свойства аудита



Servers» — антивирусная защита конкретной машины (контроллера домена), «Kaspersky Administration Kit» — средство управления антивирусной сетевой защитой, «Сервер Администрирования» — собственно, средство контроля за сетью. Устанавливаем «Антивирус Касперского для Widows Files Servers». Никаких сложностей с установкой нет, в нужный момент подсовываем лицензионный ключ. После установки даже не требуется перезагрузка компьютера. Первая особенность антивируса для операционной системы «Windows Server» — нет никаких графических оболочек для управления антивирусом. Теперь, чтобы контролировать состояние сервера, необходимо установить «Kaspersky Administration Kit». Вот первая особенность: так как мы разворачиваем «Админкит» на контроллере домена, где предполагается держать всю сеть, устанавливаем оба компонента.

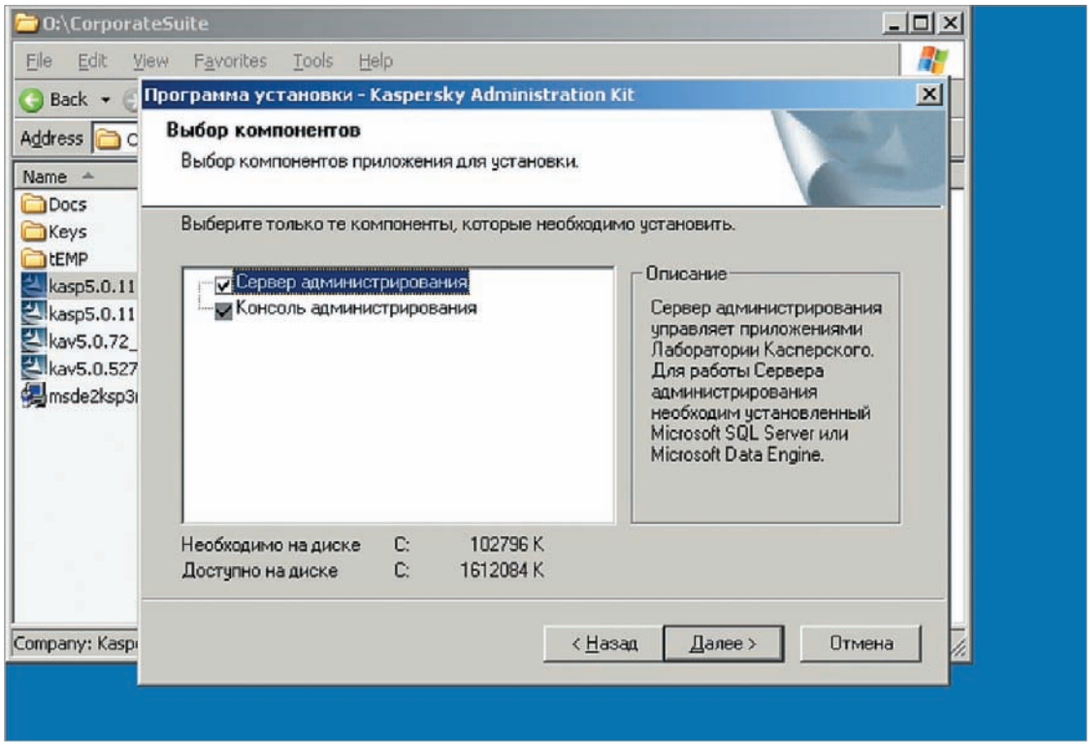
На странице «Свойства Сервера Администрирования» отмечаем «Учетная запись системы» и затем везде давим кнопку «Далее». После установки запускаем «Kaspersky Administration Kit».

Нажимаем на плюсик напротив «Сервер Администрирования — localhost». Разворачиваются настройки «Сервера Администрирования».

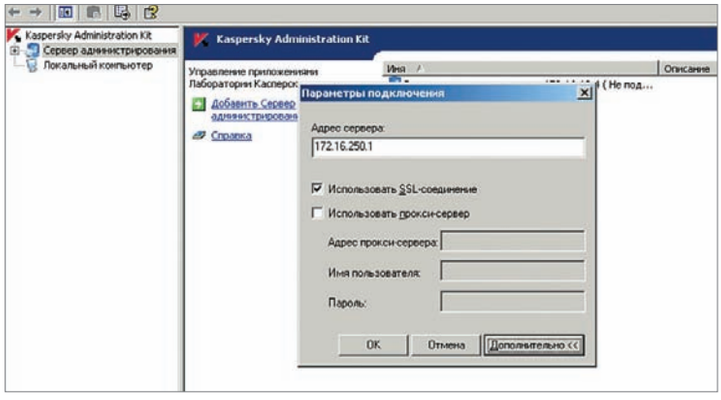
При первом запуске «Админкита» он предложит сформировать сеть администрирования на основе данных сети. Можно согласиться с этим, потом, если не понравится, поправим. Теперь, чтобы увидеть нашу сеть, нужно просто наступить на папочку «Группы». Мы получили всю нашу сеть.

Также хочу сказать следующее: управлять антивирусной сетью можно с любого компьютера сети. Для этого необходимо установить «Админкит», не устанавливая «Сервер администрирования». Теперь, для подключения к «Серверу Администрирования» необходимо в параметрах указать имя сервера (его ip-адрес) и знать учетную запись входа на сервер.

Теперь мы готовы настроить нашу антивирусную защиту на уровне компании. В следующий раз мы разберем, как автоматом разворачивать антивирусную защиту на рабочих станциях, не вставая с любимого кресла. Подробно рассмотрим назначение политик и задач. И ты начнешь жить спокойно, а вирусы жить перестанут ☻

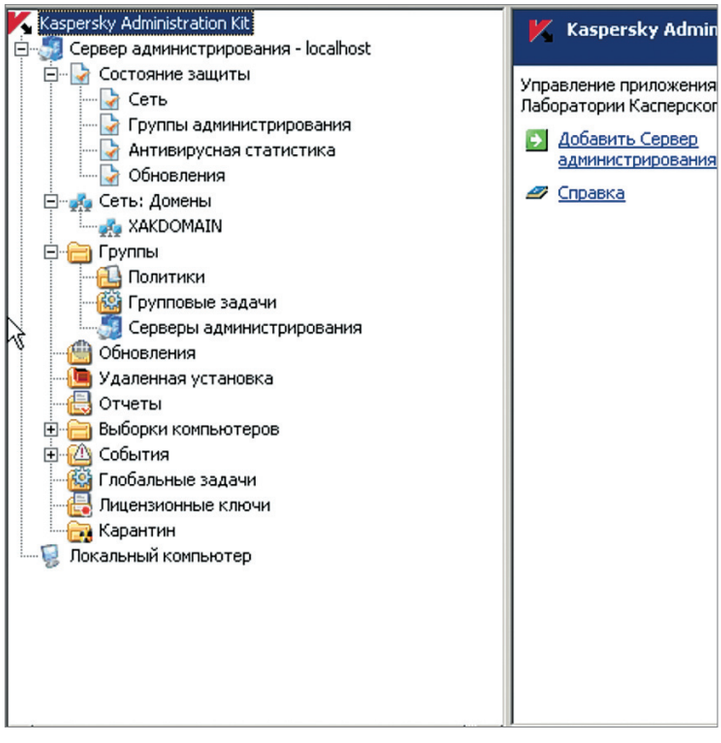


Установка «Админкита»

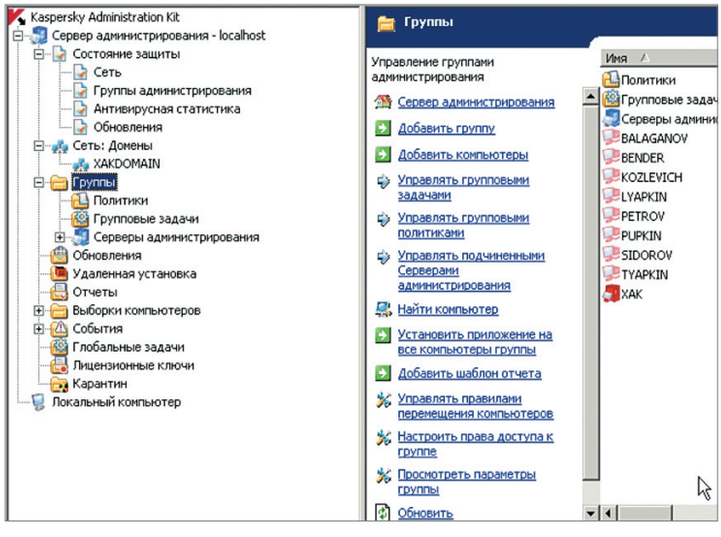


Подключение к серверу администрирования

Сеть администрирования



Вид компьютеров сети



анкета

ЕСЛИ ТЫ ХОЧЕШЬ ПОМОЧЬ НАМ ДЕЛАТЬ ЖУРНАЛ, ВСТУПАЙ В ФОКУС-ГРУППУ СПЕЦА! УЧАСТНИКИ ФОКУС-ГРУППЫ СМОГУТ ПЕРВЫМИ ОЦЕНИТЬ ПРЕДСТОЯЩИЕ НОВОВВЕДЕНИЯ, ВЫСКАЗЫВАТЬ СВОЕ МНЕНИЕ О КАЖДОМ НОМЕРЕ НАПРЯМУЮ РЕДАКЦИИ. ОТ ТЕБЯ ТРЕБУЕТСЯ НЕМНОГО: БЫТЬ В ОНЛАЙНЕ, ПЕРИОДИЧЕСКИ ОТВЕЧАТЬ НА ВОПРОСЫ РЕДАКЦИИ И, САМОЕ ГЛАВНОЕ, ЖЕЛАНИЕ. ЧТОБЫ ПОПАСТЬ В ФОКУС-ГРУППУ, НУЖНО ВСЕГО ЛИШЬ ЗАПОЛНИТЬ ЭТУ АНКЕТУ И ПРИСЛАТЬ ЕЕ НАМ. ЕСЛИ ТЫ НЕ ХОЧЕШЬ БЫТЬ В ТЕСТ-ГРУППЕ, ВСЕ РАВНО ПРИШЛИ АНКЕТУ — НАМ ЭТО ОЧЕНЬ ВАЖНО!

Заполненную анкету присылай по адресу:
101000, Москва, Главпочтампт, а/я 654, Хакер Спец,
с пометкой «Анкета» или на vote@real.xakep.ru.

Давно ли ты читаешь «Хакер Спец»?
- ◯ с первых номеров
- ◯ около года
- ◯ несколько последних номеров
- ◯ первый раз

Как ты считаешь, изменился ли «Хакер Спец» за последнее время?
- ◯ да, улучшился
- ◯ да, ухудшился
- ◯ нет, по-моему, не изменился

Какой из последних номеров тебе понравился больше всего?
- ◯ 10.05(59) — Мобильный взлом
- ◯ 11.05(60) — Скрытая угроза
- ◯ 12.05(61) — Электронные деньги
- ◯ 01.06(62) — Backup

Понравился ли тебе новый дизайн Спеца?
- ◯ да
- ◯ нет
- ◯ не обращаю внимания на дизайн

Хотелось бы тебе новых рубрик в ОФФТОПИКе?
- ◯ да
- ◯ нет

Достаточно ли объемна ТЕМА НОМЕРА?
- ◯ Вполне
- ◯ Ее нужно увеличить
- ◯ Слишком большая

Какие журналы ты читаешь, кроме Спеца?
- ☐ Хакер
- ☐ CHIP
- ☐ CHIP Special
- ☐ Компьютерра
- ☐ Upgrade
- ☐ Мир ПК
- ☐ Upgrade Special

Другой(ие) _____

Какой оптический привод в твоем компьютере?
- ◯ CD-ROM/CD-RW
- ◯ Combo CD-RW/DVD-ROM
- ◯ DVD-ROM/DVD-RW

Часто ли ты бываешь на xakep.ru?
- ◯ Постоянно
- ◯ Иногда
- ◯ Очень редко
- ◯ Никогда не был

Предложи тему для очередного номера:
_____

о себе

ФИО _____
Где ты живешь _____
E-mail _____
Сколько тебе лет _____
- ◯ меньше 17
- ◯ 18-20
- ◯ 21-23
- ◯ 24-27
- ◯ 28-30
- ◯ 30-33
- ◯ больше 33

Твое семейное положение
- ◯ холост
- ◯ женат

В каком вузе ты учишься (учился)
- ◯ техническом
- ◯ гуманитарном
- ◯ я не учусь в вузе

Связана ли твоя работа с ИТ?
- ◯ да
- ◯ да — планирую работать в ИТ
- ◯ нет
- ◯ я не работаю

Твой средний месячный доход?
- ◯ меньше $100
- ◯ $100-300
- ◯ $300-700
- ◯ больше $700

Сможешь ли ты сам собрать компьютер?
- ◯ с закрытыми глазами
- ◯ по книжке
- ◯ сомневаюсь

Какой у тебя канал в интернет?
- ◯ выделенка
- ◯ dial-up
- ◯ нет интернета

Чем ты пользуешься для общения в Сети?
- ☐ e-mail
- ☐ чаты
- ☐ ICQ и другие мессенджеры

другое _____

На каком языке ты пишешь?
- ☐ Assembler
- ☐ C/C++
- ☐ Pascal/Delphi
- ☐ Basic/VB
- ☐ Perl

другое _____
- ☐ я не программер

С какими платформами у тебя есть опыт работы?
- ☐ PC (Windows)
- ☐ *nix (Unix, Linux, BSD)
- ☐ Macintosh
- ☐ Palm OS
- ☐ Pocket PC (Windows CE)
- ☐ EPOC/Symbian

другое _____

Какие из перечисленных вещей у тебя есть?
- ☐ DVD-плеер
- ☐ DVD-ROM
- ☐ MP3-плеер
- ☐ ноутбук
- ☐ домашний кинотеатр
- ☐ мобильный телефон
- ☐ КПК (коммуникатор)
- ☐ цифровой фотоаппарат
- ☐ цифровая видеокамера
- ☐ GPS-навигатор
- ☐ **Да, я хочу в фокус-группу!**

Crew

e-mail

ПИШИТЕ ПИСЬМА! SPEC@REAL.XAKEP.RU
SKYWRITER

fox910@mail.ru
хороший дефрагментор

Здравствуйте, редакция спец-хакера.
В февральском номере была такая статья «Беспощадное повышение работоспособности NTFS». (Не удивляйтесь, что вопрос АЖ про февральский выпуск, просто читаю электронную версию :)).
В этой статье безжалостные оптимизаторы NTFS лихо расписывали преимущества программы «ПОЛНАЯ ВЕРСИЯ дефрагментатора», посылая стандартную в топку.

Дак что это за программа такая — «ПОЛНОВЕРСИОННЫЙ дефрагментатор»? Где можно взять такую чудо-прогу, дефрагментирующую все подряд? И как она называется?

Вот она, истинная суть!
Так находят предателей в нашем лагере. Мы стараемся, ищем качественных авторов, готовим материал, избавляем его от багов (по возможности, конечно), а некоторые товарищи даже отказываются его приобретать! Хотят пользоваться благами на халяву.
А ведь учитывая цену трафика (0,12$ за 1 Мб), стоимость скачанного PDF-файла приблизительно равна стоимости журнала! И как теперь мне, одолеваемому двойственными чувствами, ответить на вопросы такого человека? Это же ведь Иуда! Хуже — Брут (не путать с брутто и нетто), практически. Предатель! Причем столь же безжалостный, сколь безжалостны дефрагментаторы NTFS. Которые дефрагментируют свой диск, например, известной программой Disk Keeper, взяв ее, например, с сайта производителя. Стыдно, товарищ. Стыдно должно быть.

zombie80@yandex.ru
объявление

Перцы Челябинска! Ты хакер? Ты хочешь им стать? Тогда пиши, пол и возраст значения не имеют! Давай учиться вместе.
Мылить на: zombie80@yandex.ru

Да-да-да! Всегда приятно получать такие письма. Иногда ожидаешь их месяцами. И тем слаще оказывается приход:).

Сразу видно, человек — наш коллега по цеху. Хочет распространить такое известное явление, как хакерство, в массы. И начал он это делать самым что ни на есть хакерским способом — путем спама! Причем, почтовый адрес человека сразу заставляет вспомнить известного деятеля группы 29A и задуматься, а уж не он ли замышляет организовать новую команду настоящих хэккеров (так это слово было написано в одной старинной советской книге про программистов)?! И такому человеку, не тая, отвечу я — да, да, хочу стать хакером я!

azilan@mail.ru
Виктор Азовский
помощь

Отошлите мне что-нибудь, я настраиваю почтовый ящик!!!
Ответьте взаимностью!

Отправь слово «2$» на номер 1234 и потрать два бакса.
Ах, да, кстати, еще тебе может ответить взаимностью очаровательная пышногрудая блондинка. Но это если повезет, а везет редко.

Мы же (редакция) отвечаем взаимностью всем Вам! Даже когда вы, милые читатели, в столь безвыходном положении, как пишущий нам Виктор. Даже в этой ситуации мы поможем — ответим взаимностью, ящик Виктора обязательно заработает, и да пребудет мир во всем мире!
P.S. Отослали Виктору троянца.

marilynmanson48@mail.ru
bodya sipolonov
помогите разогнать 3 pentium

У меня древний pentium 3 866 Mhz. Мне его уже не хватает, а я страшный геймер, который хочет играть. Выходит много игр, а я не могу в них поиграть, потому что они жутко тормозят. Мне хотелось бы немного его разогнать. Хотя бы до 1000 Mhz. Помогите, пожалуйста, очень прошу. Вот параметры моего компа: Intel Pentium(r) 3 866, 512 MB ОЗУ (оперативка RAM), GeForce 6 6200 128mb, тип шины: AGP 2X. Заранее огромное спасибо!

Бодя? Так, кажется, тебя зовут? В общем, здравствуй, Боди (даже неловко как-то так тебя называть...)

Пентиум твой и правда древний, впрочем, не древнее моего Pentium II 350 MHz. Но не это главное. Главное, что, я абсолютно уверен, геймер ты не страшный, а очень даже симпатичный — не стоит комплексовать по этому поводу. Даже с учетом того, что геймер очень хочет играть. Но на этом хорошие новости закан-

чиваются, и начинается сплошной «отстой». Понимаешь, дело в том, что, даже если ты разгонишь свой PIII до 1000 и 1 МГц, это не сильно скажется на производительности в целом, а особенно — игр. Видишь ли, игры требовательны в основном к графической подсистеме, а она у тебя, как сам видишь, убога — 2X во времена PCI-E считаю непозволительным отставанием. Так что, лечи материнскую и видео-платы, а процессор не мучай — он и без тебя перегреется в жаркие летние деньки.
Заранее огромное не за что.

suv_iamm@mail.ru

Serghey Suvorov
RAID, Intel Matrix Storage

Коллеги, сами мы не местные, помогите, кто чем может!
У меня на плате ASUS P5GD1 Pro стоит Int.Matr.Storage контроллер. Два физических диска разбиты на C: (RAID 1) и D: (RAID 0). C: управляется контроллером и драйверами, D: — только драйверами. Как и чем провести полный backup системы?

Пока я вижу только один (неважнецкий) вариант. Проводится Windows-backup диска C:, после чего этот файл и диск D: сбрасываются в DVD-архив.

После краха системы устанавливаю Винду под RAID 1 на C:, готовлю RAID 0 на D:. Затем на D: сбрасываю архивы и из Backup.bkf, восстанавливаю старую Windows с опцией «заменять все файлы». Плохо то, что ВСЕ все равно не заменятся, и пролетят мои многочисленные обновления и т.п.

Не подскажете ли что-нибудь получше? (НЕ в порядке лести: читаю кучу комп. журналов, но лучше вашего ничего нет).
Ваш Сергей. Донецк, Украина.

Спасибо, Сергей, на добром слове. Не в порядке лести, но мы очень польщены. Что же до сути письма, то, честно говоря, прежде, чем вник, прочитал его 3-4 раза. И скажу сразу — ты молодец! Не много людей сейчас тратят денежки на настоящий RAID0. Прежде всего экономят на жестаках, а ты — не экономишь, и это радует. Родные документы важнее.

Что до схемы создания резервной копии, то мне видится все гораздо проще (все упоминания ОС Windows подразумевают версию XP):

1 ПРИ ПОМОЩИ УТИЛИТ РЕЗЕРВИРОВАНИЯ HDD (А-ЛЯ NORTON GHOST) СОХРАНЯЕШЬ ДИСК C: С ВИНДОЙ (ЗАГРУЗИВШИСЬ С ДИСКА ЭТОЙ ПРОГРАММЫ РЕЗЕРВИРОВАНИЯ, ИБО ЭТО ЕДВА ЛИ НЕ ЕДИНСТВЕННЫЙ СПОСОБ ЗАБЭКАПИТЬ ВСЮ ВИНДУ; РАБОЧУЮ КОПИЮ WINDOWS ОЧЕНЬ СЛОЖНО ПРОЧИТАТЬ ЦЕЛИКОМ С ЖЕСТАКА, А ЕЩЕ СЛОЖНЕЕ ЗАМЕНЯТЬ ВСЕ ФАЙЛЫ ПРИ ВОССТАНОВЛЕНИИ — РЕЕСТР ТЕБЕ НЕ ЗАМЕНИТЬ НА РАБОТАЮЩЕЙ ВИНДЕ НИКОГДА, РАВНО КАК И НЕ ПРОЧИТАТЬ).

2 ПОТОМ ПРОГРАММОЙ WINDOWS BACKUP РЕЗЕРВИРУЕШЬ ВСЕ ОСТАЛЬНОЕ (ДИСК D:).

После всего этого возникает резонный вопрос: зачем бэкапить Винду целиком? Почему бы не резервировать только свои файлы? Серьезно сэкономишь на носителях.

А что до обновлений, которые ты можешь потерять — тешь себя мыслью, что ты теряешь только обновления.
Ваши Спецы. Москва, Россия.

fillbill@rambler.ru

суперагентFillBill
Тема не указана

Здравствуйте!!!
У меня компьютер Pentium2 300 МГц, материнская плата Lucky Star 6LX2\6EX2 ver 1.1. Какой максимальный объем оперативной памяти SDRAM можно использовать для работы с этим процессором (на этой материнской плате)? Если можно, пришлите мне, пожалуйста, ответ на e-mail: FillBill@rambler.ru

Привет, суперагент Билл.
Тут уже шла речь об антиквариате, и в этом смысле я, наверное, повторюсь. Очень (ну, очень) советую потратить $$$ не на покупку SDRAM, а на покупку нового компа. Положа руку на сердце, скажу, что производительность от этого вырастет, как говорят наши зарубежные коллеги, драматически. А если данная информация просто является предметом споров, то отошлю тебя прямиком к документации к твоей материнской плате. Знаешь, к каждой M/B дается такая книжечка. Так вот, там написано, сколько и какой памяти способна принять каждая из них на борт. От себя же скажу, что для чипсетов LX обычным значением было 2 или 4 Гб.
Ответ присылаем тебе свежим номером прямо в киоск Союзпечати.

fillbill@rambler.ru

суперагентFillBill

Здравствуйте!!!
Переустановил Windows2000. На C-диске (объем 2 ГБ) была файловая система NTFS, на остальных локальных дисках была файловая система FAT32 (объем D — 3ГБ, E — 8ГБ, F — 8ГБ, G — 9ГБ). Для работы с файлами больше 4 Гб захотел сделать на всех дисках файловую систему NTFS.

Только собрался форматировать D-диск, вдруг вспомнил, что на нем остались незабэкапенные важные файлы. Перед этим сделал D-диск и E-диск неразмеченными для переназначения их размеров. Уменьшил объем D до 2 ГБ, а объем E увеличил до 9 ГБ. Оставив их неразмеченными, доустановил Windows2000 и начал работу. После установки уже через операционную систему произвел форматирование E-диска. После этого установил программу Partition Magic 8.0, чтобы попробовать восстановить данные, с ее помощью объединил два логических диска D и E в один, сделав D-диск каталогом E-диска. Но после данной операции папка с бывшим D-диском так и осталась пустой. Можно ли как-то мне еще восстановить данные? Если можно пришлите мне, пожалуйста, ответ на e-mail: FillBill@rambler.ru

Суперагент! Снова ты! Будто старого знакомого встречаю! Очень рад тебя видеть, слышать, читать.

Честно говоря, увидев второе письмо, мы сразу были весьма и весьма польщены... Столько доверия. В общем, тов. Аваланч (он же главный редактор нетленного сего издания) теперь назначен твоим личным консультантом по техническим вопросам — если что, обращайся напрямую к нему, он всегда рад помочь.

А пока вопрос от меня: может ли быть на жестком диске больше 24 логических? А если может, то как называется тот, что после «Z:»? Ждем от тебя ответа со снимком экрана в качестве доказательства.

P.S. Данные ты свои потерял, ибо многократно перезаписал таблицу разделов прежде чем слил диски. И максимум, чего бы ты мог достичь, это при помощи программы DiskEdit выковырять хоть какие-то самые важные данные. Впрочем, все это справедливо ровно до того момента, как ты записал что-то на свежесозданные диски...

zxz-zxz@mail.ru

Вася Пупкин
hello!!!

Alle!!!
Вы, ребята, конечно, молодцы, и журнал у вас — просто отпад, но ответьте мне на один вопрос: почему у вас сайт так долго грузится?

Я, конечно, понимаю, что у вас один сайт на два журнала, но это, сорри, не повод... То, что на нем загружается все сразу, конечно, хорошо, но не у всех ведь выделенка стоит! Улавливайте нужды народа:).
Ведь для кого-то лучше загрузить материал по частям, чтобы иметь возможность посмотреть хоть что-то, чем уйти с сайта, так и не дождавшись 5-минутной загрузки. Решайте вопрос, перцы:). GOOD LUCK!!

Василий! Прости дураков грешных! Говорил я Веб-мастеру, что не стоит делать сайт в виде несжатого интерактивного AVI-файла. Говорил ему, мол, он и на выделенке-то подтормаживает. Все равно не послушал он меня. Сделал. И вот результат.

Так что не переживай, видео убрали, теперь все должно грузиться просто мигом! C

Story

на далекой пангее

БОМБАРДИРОВЩИК ЗАХОДИЛ НА ЦЕЛЬ УЖЕ В ЧЕТВЕРТЫЙ РАЗ. ЛЕ РОЙ ПРОВОДИЛ ЕГО ВЗГЛЯДОМ ИЗ-ПОД ЛАДОНИ, ВОТКНУВ ЛОПАТУ В ЗЕМЛЮ

NIRO (NIRO@REAL.XAKEP.RU)

— Когда же это кончится... — процедил он сквозь зубы, глядя на жужжащий высоко в небе крестик. — Там, наверное, уже ничего не осталось.

Вчера самолеты посетили это место шесть раз. Бомбы сыпались густо, с противным свистом, и хотя до цели отсюда было около двух километров, надсадный вой — сначала падения, а потом разрывов — не давал спокойно работать ни Ле Рою, ни четверым его напарникам. Вот и сейчас — едва Ле Рой услышал гул моторов первого самолета, из туч над их головами вынырнули еще пять машин; совершив маневр, они выстроились зигзагом и открыли бомболюки.

Черные точки, поначалу летевшие рядом с самолетами, быстро теряли скорость и по дуге ныряли вниз.

— Ветер в нашу сторону, — сказал Педро. — Через полчаса нечем будет дышать.

Ле Рой согласно кивнул. Остальные молча достали респираторы и нацепили на лица, сразу став похожими на бульдогов с синими мордами. Гул взрывов долетел до них спустя некоторое время — Ле Рой сделал нехитрые вычисления и решил, что цель не изменилась. Те же самые два километра.

— Интересно, что там... — задумчиво спросил сам у себя Киринаикос. — Вчера шесть, сегодня четыре. Город?

— На такой равнине, грек, мы бы увидели город еще пять дней назад, — взявшись за лопату и не оборачиваясь, ответил Ле Рой. — Нет, там что-то другое...

— Города бывают разные, — ответил Киринаикос. — Там, откуда я родом...

— Заткнись, — угрюмо бросил Педро, достав из кармана маленький напильник. — Мы все откуда-нибудь родом. Копай!

Сам он несколько раз провел по острию лопаты напильником с противным скрежетом; все остальные машинально проверили лезвия своих орудий и решили повременить с заточкой.

Комья земли вновь полетели в стороны. Ров углублялся. Через двадцать пять минут (прогноз Педро сбывался) потянуло дымом. Сначала легко, практически незаметно — так, словно кто-то неподалеку развел маленький костерок, потом — явственно, противно. Дым оседал на языке и в глотке.

— Попали, — выдохнул Киринаикос. — Горит...

— Что? — спросил Ле Рой.

— Похоже, что лес.

— Нет, — вступил в разговор Олафсен. — Это не лес. Точнее, не совсем лес.

— Откуда ты знаешь, как горит лес, проклятый викинг? — возмутился Педро. — Живешь там, в своей Швеции, среди фьордов и мха... Да и когда ты там был в последний раз?!

Швед закрыл глаза — было видно, что он борется с собой; еще секунда — и он бы кинулся в драку.

— Не напоминай мне о фьордах, мой милый испанец...

— Мексиканец!

— Тем более, — вежливо кивнул Олафсен. — Тем более — потому что они очень дороги мне. И, судя по всему, я их больше никогда не увижу. Я знаю, как горит лес. Я знаю, как горят дома; я даже знаю, как горит море, когда на нем разлита нефть из тонущего торпедированного транспорта. Поэтому поверь мне — там горит не лес.

— А что? — не удержался Киринаикос.

— Джунгли.

— Там — джунгли? — скорчив жуткую гримасу, переспросил Педро.

— Там — джунгли? Ты выжил из ума, викинг! Посмотри под ноги — мы роем этот проклятый ров посреди пустыни!

— Что не мешает быть джунглям в двух километрах от нас, — сказал Олафсен. Да и пустыней это трудно назвать. Я бы сказал — прерия.

Ле Рой молча согласился со шведом. Дым принес с собой какие-то странные запахи; лес не мог так пахнуть. Сырость, испарения — то, что периодически прилетало к ним с ветром, сейчас было перемешано с гарью. «Странно, — подумалось Ле Рою. — Зачем кому-то бомбить джунгли? Чем они могли помешать?».

— Джунгли... — задумчиво произнес Киринаикос, поглядывая на тех парней, что работали молча со вчерашнего дня. — Прерия... Как это может сочетаться? Куда нас забросила эта поганая война?

— Черта, — замогильным голосом сказал Олафсен и провел рукой по горизонту. — Там черта. За чертой может быть все, что угодно. Я знаю. Я помню.

— Кто из нас оказался здесь первым? — внезапно спросил Педро. — Самым первым? Кто сделал первый удар лопатой, кто разметил направление этой чертовой канавы? И кто приказал ему это сделать?!

— Я, — поднял руку один из молчунов. — Я здесь уже восемь дней. Я делал расчеты. Я отвечаю за точность проекта. Мое имя Адольф.

ПОЧЕМУ ТЫ СРАЗУ НЕ СКАЗАЛ НАМ О ТОМ, ЧТО МЫ РАБОТАЕМ НА ЗАРАЖЕННОЙ ТЕРРИТОРИИ! СВОЛОЧЬ, ПОЧЕМУ ТЫ МОЛЧАЛ?! МЫ СХВАТИЛИ УЖЕ СТОЛЬКО РЕНТГЕН!


B
D

Приятно познакомиться со всеми вами — но лучше работать, а не молоть языком.

— Немцы, — пробурчал Киринаикос. — Ох уж эти немцы с их вечным стремлением к порядку... Хуже японцев — слава богу, что узкоглазых здесь нет. Вместе они бы достали тут кого угодно.

— Ты не ответил, кто приказал тебе, — Педро бросил лопату на землю и подошел к Адольфу. — Неужели ты сам пришел сюда и стал копать?

— Нет, не сам, — немец остановился, воткнул лопату и оперся на черенок. — Вряд ли я бы догадался даже о существовании этого места, — он обвел глазами окрестности с небогатой растительностью.

— Тогда кто?

— Я не знаю, — криво улыбнулся Адольф. — И никто не знает. Просто ты оказываешься здесь, и все. Никто из вас не чувствует во рту привкус крови?

Все моментально прислушались к своим ощущениям, после чего отрицательно покачали головами.

— Это хорошо, — улыбнулся Адольф. — Значит, я хорошо поработал до вашего прихода. Лично я избавился от него лишь пару часов назад.

— Ты о чем? — спросил Ле Рой. — Что за привкус? Если я правильно понял, здесь опасно находиться?

— Уже нет, — отрицательно покачал головой Адольф. — Прошу верить на слово и не отвлекаться на пустые разговоры. У нас слишком много работы.

— Много? — подошел поближе Олафсен, засунув руки в карманы. — Что-то я не понял, если можно — с этого места поподробнее. Не очень хочется много работать.

— Ничего не выйдет...— попытался улыбнуться Адольф, но сразу понял, что со шведом такой тон не пройдет. — К сожалению, от нас с вами это не зависит. Зря вы оставили лопату — если вы думаете, что за нами никто не наблюдает, вы ошибаетесь. Мы здесь как на ладони.

Олафсен резко обернулся. Его глаза шарили по горизонту — но безрезультатно. Он остановился, посмотрел себе под ноги, а когда поднял взгляд вновь, Адольф отступил на шаг.

ОН ВЗЯЛСЯ ЗА ДРУГОЙ КРАЙ И ВДРУГ ЗАМЕТИЛ, ЧТО В ГЛУБИНЕ БРОНЕВИКА ЧТО-ТО ШЕВЕЛИТСЯ. КАКОЙ-ТО ЧЕРНЫЙ МЕШОК ИЗДАВАЛ СТРАННЫЕ СТОНУЩИЕ ЗВУКИ

— Слышишь, немец, — процедил швед сквозь зубы, — или ты объяснишь мне, что мы здесь делаем... Или будет больно. И ты все равно скажешь. Кто-нибудь согласен со мной?

Несколько человек поддержали его. Всем — или почти всем — хотелось знать, что они здесь делают и как они здесь оказались. Адольф отступил еще на один шаг и постарался ответить всем сразу:

— Я прошу вас всех прислушаться к голосу разума. Надеюсь, никто не против это сделать? Так вот: я понятия не имею, откуда здесь я сам и все остальные. Я уже БЫЛ здесь, когда появились все остальные — был, и сам не знаю, почему. Вы появлялись по одному, реже — по два. Просто из воздуха. Появлялись, словно эфир со скоростью света ткал живую материю. Вроде никого нет — и вот еще одна фигура с лопатой стоит возле меня в грязной рубашке и широких штанах. Вы включались в работу молча и не спрашивли ничего — смотрите, сколько земли перекидали. Думаю, скоро можно закладывать фундамент...

— Не отвлекайся, — вновь надавил Олафсен. — Говори.

— Я ведь и говорю, — продолжил Адольф. — Мы работаем, и все тут. И я твердо убежден, что за нами наблюдают. Издалека, из укрытия... Может, в очень мощный бинокль. И я совершенно точно уверен — нам не стоит долго простаивать без дела, иначе нам напомнят о нашем предназначении. Причем напомнят так, что мы очень и очень пожалеем.

— Это угрозы? — поинтересовался Киринаикос. — Ты требуешь от нас подчинения? Ты здесь главный?

— Нет, я не главный. Я — первый. И если бы вы видели, что здесь было до вас — поверьте, вы сказали бы мне «спасибо».

Ле Рой в который раз осмотрелся и так и не смог понять, что же имел в виду немец. Никаких признаков того, что кто-то работал здесь до их появления, и уж тем более — что этот «кто-то» провернул здесь колоссальную работу, не было. Кроме их рва, постепенно заполняющегося грунтовыми водами — поначалу медленно, пропотевая, а дальше все быстрее и быстрее — здесь, в этой глуши, не было ничего. И тем глупее смотрелась тут группа парней с лопатами, ведущая этот ров по какому-то непонятному ориентиру, будто вбитому им в мозги.

— Я верю, — после паузы сказал он. — Но не понимаю. Поэтому мы все еще ждем объяснений. Что именно делал здесь ты, пока мы не пришли?

Адольф тяжело вздохнул.

— Я понимаю так же мало, как и вы, — махнул он рукой. — Мы ничем не отличаемся. Почему вы придаете такое значение моей персоне, мне непонятно — я же не требую от вас благодарности за то, что я разгреб здесь кучу радиоактивного мусора!

— Кучу чего? — напрягся грек.

— Да, вы не ослышались! — взмахнул обеими руками Адольф, словно это придавало его словам больший вес. — Когда я появился здесь, прямо передо мной на этой чертовой земле лежали сорок полуразвалившихся бочек с какой-то непонятной жидкостью, непрерывно подтекающей изо всех щелей! Едкой, мерзкой на вид жидкостью, которая еще вдобавок и светилась в сумерках, словно бочки были напичканы светлячками по самый верх!

— И где же она теперь? — спросил Киринаикос, глядя себе под ноги. Выражение его лица говорило о том, что он хочет немедленно отсюда уйти — и чем дальше, тем лучше. — Неужели ты выпил ее всю, проклятый немец?! Почему ты сразу не сказал нам о том, что мы работаем на зараженной территории! Сволочь, почему ты молчал?! Мы уже схватили столько рентген!

Он схватил свою лопату и, судя по всему, собирался раскроить Адольфу череп, но Ле Рой ему не позволил. Он ловким незаметным движением выставил ногу — и Киринаикос полетел головой в грязную коричневую жижу на дне канавы.

Швед и немец посмотрели на Ле Роя, как на человека, совершившего самый нелогичный поступок в своей жизни — причем Олафсен смотрел, как хищник, а Адольф — благодарно и восхищенно. Ле Рой сам не ожидал подобной смелости, поэтому едва сумел остановить себя не ринуться вниз, к барахтающемуся в дерьме греку, чтобы вытащить его на сухую землю. Он встретился взглядом поочередно с каждым заинтересованным лицом, после чего ткнул пальцем в Адольфа:

— Мало информации.

— Да вы меня все время перебиваете! — возмутился немец. — Кто следующий кинется на меня с лопатой?

— Успокойся, никто, — покачал головой Ле Рой. — Нам всем хочется знать, куда ты дел эти сорок бочек с радиоактивным дерьмом. Ведь ты же что-то с ними сделал, раз их здесь нет?

— Гениальная мысль, — пробурчал Адольф. — Конечно, я попытался что-то сделать, но уже через несколько минут у меня из носа пошла кровь. Во рту появился металлический привкус, зашумело в голове, короче — недолго бы мне осталось, но... На какое-то время, как я понимаю, я выпал из жизни: складывалось впечатление, что она проплывает мимо меня. Я уже приготовился умереть, но вдруг почувствовал себя лучше — не совсем, но настолько, чтобы выполнить приказ...

— Какой? — спросил Олафсен.

— Чей? — перестав отряхивать с себя грязь, спросил грек.

— Не знаю, — ответил Адольф Киринаикосу. — Он просто выстроился в моей голове, как доминанта, как директива... Я очнулся от своего радиоактивного транса и принялся переворачивать бочки, разливая светящееся дерьмо по земле. Они были тяжелыми, ржавыми, с массой зазубрин, неподатливые... Но я сумел выпотрошить больше половины из них, когда понял, что жидкость ушла в землю, не оставив и следа. Она просто исчезла — как и все мои ощущения. Я снова был здоров — и ни на секунду не сомневаюсь, что, столкнувшись с бочками, я заразился лучевой болезнью. И, осознав, что я все еще жив, я закончил работу вдвое быстрее, чем рассчитывал — будто кто вдохнул в меня силы. Вся эта урановая водичка исчезла, словно ее и не было. А потом стали появляться вы.

Он вдруг улыбнулся своим словам:
— Надеюсь, между ее исчезновением и вашим появлением нет прямой связи.

Ле Рой помолчал немного, потом усмехнулся и ответил:
— Будем надеяться...
— Может, стоит вернуться к работе? — спросил Адольф, закончив свой монолог. — Все-таки есть высокая вероятность того, что нас могут проверить.
— И что нас ждет? — поинтересовался Олафсен, сложив на груди руки.
— Не знаю, — отрицательно покачал головой Адольф. — Но думаю, что ничего хорошего. Мы ничего не делаем уже почти двадцать минут — а это много, по меркам того, кто наблюдает за нами.
— Есть ощущение, что ты знаком с этими людьми лично, — швед приблизился на пару шагов. — И сдается мне, что грек зря нырнул в дерьмо с головой, — последнее адресовалось уже Ле Рою. — Ты кто — француз? Шотландец?
— Канадец, — ответил Ле Рой. — И место Киринаикоса было именно в канаве — не думаю, что нам помешают лишние рабочие руки. Если бы сейчас на дне рва лежал Адольф с пробитой головой, мы бы — раз! — не узнали бы того, что он нам рассказал, и — два! — делали бы часть его работы.

Грек, сидя на краю рва, поднял глаза на Ле Роя и прищурился — бескомпромиссная ненависть сквозила в этом взгляде. Чувствовалось, что злобу он затаил всерьез и надолго, хотя всего лишь пару минут назад собирался убить совершенно другого человека. Ле Рой, почувствовав этот взгляд, ответил тем же.

И оба поняли, что не останутся без внимания.

Адольф посмотрел на них обоих, потом почесал в затылке и сказал:
— Не знаю, как вы, а я продолжу.

Он отмерил несколько шагов вдоль по ходу рва, сделал там отметку острием лопаты, вернулся и принялся отбрасывать землю в сторону. Те, что стояли по эту сторону рва, последовали его примеру; четверо оказавшихся по другую сторону переглянулись, перебросились парой слов и тоже вернулись к работе.

Тем временем на горизонте — там, откуда тянуло дымом — стало тихо. Хлопки далеких взрывов прекратились, крестики самолетов исчезли в вечернем небе.

Ле Рой считал, сколько раз он взрезал лопатой землю.
— Девятьсот тридцать два... Девятьсот тридцать три...

Когда счет перевалил за тысячу, он позволил себе осмотреться. На той стороне двое курили, свесив ноги с края канавы, другие копали, все медленнее и медленнее, поглядывая на бездельников с нескрываемой злобой и презрением. Ле Рой распрямил спину, смахнул пот со лба.
— Чушь какая-то, — пробурчал он себе под нос. — Зачем мы здесь? На много километров на все стороны света ни души, где-то далеко идет война — а мы появляемся из ниоткуда, роем эту чертову яму, смотрим, как она заполняется водой, плюем и мочимся в нее, рвем друг другу рубашки и ноздри, ненавидим, ругаемся, спорим, мы, люди из разных стран, разных религий и убеждений... Эй, Адольф!

Немец оторвался от работы, воткнул лопату в землю, потянулся и только потом отозвался:
— Что, канадец?
— Устал?
— Глупый вопрос. Да.
— Тогда почему не объявляешь перекур?
— Почему я? Вон те двое объявили его сами себе. Не преувеличивай мою роль, — немец отмахнулся от Ле Роя ладонью. — Ты что-то хотел спросить?
— Я спросил.
— Нет, не это. Я же чувствую — ты швырял землю, а сам думал, думал... Что не дает тебе покоя?

Ле Рой хотел удивиться проницательности немца, но подумал, что тут нет ничего такого сверхъестественного — скорее всего, об этом думали все. Ну, или почти все.
— Мне, как ты совершенно справедливо заметил, не дает покоя одна мысль. Одна, но зато какая!
— Продолжай, раз уж начал, — подбодрил немец. — И, раз уж мы отвлеклись от дела — перекур.
— Надолго? — спросил грек, практически падая на землю — просто удивительно, на чем он держался последние полчаса...
— Там увидим, — хитро посмотрел Адольф на него. — Смотря что мы сейчас будем обсуждать с канадцем.

Киринаикос кивнул, сделав это, как китайский болванчик — сил держать голову у него уже не осталось. Он лег на землю, после чего крикнул куда-то в небо:
— Господи, дайте кто-нибудь сигарету!!!

Швед подошел к нему, присел рядом, вытащил из кармана пачку папирос, закурил одну из них, после чего воткнул уже дымящуюся в рот греку и вытянулся рядом.

Адольф улыбнулся, глядя на это.
— Что ты хотел спросить?
— Кто твои родители, немец? — неожиданно для самого себя произнес Ле Рой.
— Но ты хотел спросить не это, — удивленно поднял брови Адольф. — Ты же думал о том, что...
— Стоп, — перебил его канадец. — Ты прав. Но ответь сначала на этот вопрос.

Немец задумался, глядя себе под ноги.
— Как бы дико это не прозвучало, Ле Рой, но мне нечего тебе сказать.
— Поясни.
— Нечего — это значит нечего, — развел руками Адольф. — Я только сейчас подумал о них — и вдруг понял, что никогда в жизни их не видел. Да были ли они у меня? Чертовщина какая-то!

Он сделал несколько шагов вдоль рва, пнул большой ком земли, проследил, как он упал в воду, разбрызгивая вокруг себя грязь.
— Родители... Да я не помню даже, откуда я родом! Постой, Ле Рой, неужели ты что-то понял?
— Пока нет, — пригладил мокрые волосы канадец. — Пока — нет... Сейчас бы дождь... Сильный, холодный, чтобы как в детстве... Как в детстве... Эй, Олафсен!
— Чего? — буркнул швед, не поднимая головы.
— Расскажи, ты любил в детстве дождь?
— Чего?
— А что тебя смутило? Слово «дождь» или слово «детство»?
— Его смутило слово «любил», — попытался рассмеяться грек, но у него плохо получилось. Он закашлялся, сел и оглянулся на Ле Роя. — Хочу, чтобы ты знал, канадец: не поворачивайся ко мне спиной. Никогда.
— Злопамятный? — не сводя глаз со шведа, спросил Ле Рой. — Не самое лучшее качество в жизни. Олафсен, я жду ответа — как там насчет своего детства? Есть какие-то отклики из глубин сознания?

Швед тоже поднялся, выпустил клуб дыма из своих больших легких и, наконец, соблаговолил ответить:
— Детство как детство. Плохо помню...
— Плохо? — подошел поближе Ле Рой, отметив краем глаза, что Киринаикос приблизил руку к черенку лопаты. — Или совсем не помнишь?
— Я тоже не помню, — вмешался в их разговор Адольф. Он подошел и встал так, что оказался точно между греком и канадцем, Киринаикос прикинул расстояние, разочарованно убрал руку и снова лег на землю.
— Просто до твоего вопроса о родителях я жил так, как будто они и не нужны вовсе, будто их и не было. Странно, правда?
— Ничего странного, — ответил Ле Рой. — Я тоже — ни мамы с папой, ни детства. Пустота. Хуже всего, что у меня складывается впечатление, что меня СДЕЛАЛИ, чтобы я рыл эту чертову канаву.
— Не все так плохо, — ответил Олафсен. — Я помню... Какие-то улицы, бараки... Люди, похожие на меня...
— Чем похожие? — поинтересовался Ле Рой.
— Одеждой, походкой, у кого-то в руках лопаты, у кого-то — оружие; и над всем этим — флаг. Шведский флаг... Какое-то большое здание в центре города, а на верхушке шпиль с флагом.
— Как ты оказался здесь? — спросил канадец, вспоминая свое прошлое — маленький кусочек, застрявший в памяти, как кусочек пищи между зубов. — Можно хоть какие-то подробности?
— Можно, отчего же... — Олафсен поднялся, отряхнул спецовку, отбросил в сторону окурок. — Пришли люди, вошли в город, приказали...

В этот момент он посмотрел на Адольфа и махнул в его сторону рукой:
— Вот эти.

Канадец не понял, посмотрел сначала на Адольфа, потом перевел взгляд на шведа:
— Поясни.
— Что толку пояснять?! — явно нервничая, крикнул Олафсен. — Теперь уже все равно. Нет у меня на них зла — а ведь должно быть, правда? Пожалуй, это единственное, что меня удивляет — почему я абсолютно равнодушен к случившемуся?

Адольф напряженно слушал все, о чем говорил Олафсен. Он либо очень хорошо скрывал какую-то правду, либо на самом деле был совершенно не информирован о том, что же случилось со шведом в тот момент, когда «вот эти люди» вошли в его город.
— Нельзя ли как-то уточнить — почему, зачем, когда? — настойчиво

спросил канадец. — И вообще — почему мне всегда приходится просить вас всех рассказывать поподробнее? У вас что, слов не хватает? Или речь не развита?
— Кто ты такой? — внезапно спросил со своего места Киринаикос. — Чего ты лезешь ко всем со своими расспросами? Кто уполномочил тебя проводить следствие? Начни с себя — и, может быть, тогда мы согласимся с тем, что у тебя есть право задавать вопросы. Хотя я вряд ли соглашусь. Помни о том, что я сказал.
— Резонно, — заметил швед. — Эй, парни! — крикнул он на ту сторону рва, где расположились на отдых остальные члены их коллектива. — Не хотите послушать слезливую историю жизни канадца Ле Роя?

Четверо до этой минуты неподвижно лежавших на земле, встали, подошли к краю рва, прикинули, смогут ли перепрыгнуть ту жижу, что уже накопилась внизу, переглянулись и поочередно прыгнули. Выбравшись наверх, они подошли поближе и присели на землю, образовав вместе с Киринаикосом и шведом полукруг, в центре которого оказались немец и Ле Рой. Адольф посмотрел вокруг и отошел в сторону, опустившись на землю возле грека.
— Значит так, да? — спросил канадец. — Решили сделать меня крайним? Один не помнит своих родителей, другой не знает, было ли у него детство, третий помнит шведский флаг над каким-то домом, но при этом равнодушно роет канаву вместе с немцем и греком? Решили, что ответит и внесет ясность именно канадец?
— Ну, примерно так, — ответил за всех Киринаикос, не глядя ему в глаза. — Внеси эту самую ясность. Да побыстрее — судя по словам Адольфа, у нас могут быть проблемы, если мы надолго перестанем копать.
— Это так, — кивнул Адольф. — Не сочтите меня за надсмотрщика, но он прав.
— Кто придет проверять — твои люди? — спросил канадец. — Немцы?

Адольф кивнул.
— Чушь какая-то, — кивнул канадец. — Получается, что в город Олафсена вошли немцы, заставили работать на себя, но при этом создали какую-то интернациональную бригаду и поставили присматривать и руководить процессом одного из своих. Мы работаем, работаем, а сами — я уверен, что у каждого в голове есть мысль, подобная моей — думаем о том, почему мы не можем бросить все и уйти. Понимаю, что стоя среди степи, сложно принять решение пуститься в бега — нет ни одного нормального ориентира, неизвестно, куда идти. Но ведь уйти возможно? Что нас держит?
— Ничего, — сказал швед, встал и пошел в ту сторону, откуда до них долетал звук бомбежки. — Посмотрим, что из этого выйдет...

Все провожали его взглядами. Спустя некоторое время фигурка шведа стала плохо различимой из-за марева, поднимающегося от земли.
— Он вернется, — вдруг сказал Адольф. Все вздрогнули и посмотрели на него. — Там ничего нет. В смысле, конечно, есть — но совсем не то, что он хотел бы там найти. И уж тем более там нет дороги домой.
— Рассказывай, чего тянуть, — сказал кто-то из подошедших с другой стороны. — Чего мы, зря перебирались сюда?

Ле Рой оглядел всех, вздохнул и сказал:
— Думаю, мы все похожи — настолько, насколько объяснял швед. Мы не помним ничего из своей жизни — ничего, кроме каких-то обрывков улиц, домов, людей с оружием. Я еще отметил про себя цокот копыт по булыжным мостовым...
— Было, — сказал кто-то. Канадец не разобрал, кто именно, но согласно кивнул.
— Вот видите, что-то общее есть практически у всех нас... — продолжил канадец, но грек перебил его.
— Я вспоминаю, — неожиданно вставил он, — что на улицах моего города было очень много людей с книгами в руках — просто невообразимое количество. Они сидели вдоль улиц на скамейках, их было видно в окнах домов, на набережной — да где они только не появлялись! Сам-то я читать так и не научился...
— Я такого не помню, — прокомментировал канадец. — Честно говоря, читать я тоже не умею: вот взглянул на клеймо на лопате, знаю, что это буквы, но слова из них сложить — не получается. Зато знаю много молитв — где-то на краю застряло такое количество божественной благодати, что просто не передать словами! Сложно связать это с детством, которого не было — разного рода псалмы и молитвы я заучивал наизусть с чьих-то слов, это вне всякого сомнения...

Мексиканец, до этого момента молчавший, словно набрав в рот воды, внезапно принялся бормотать себе под нос какие-то слова и истово креститься. Он закрыл глаза, мелко-мелко крестил себе лоб и раскачивался взад-вперед. Ле Рой уловил в его молитвах какие-то знакомые созвучия.
— Точно, — сказал он. — Мы тоже молились подобным образом — вот только крестились широко, стоя под сводами городского собора. Я помню свой город какими-то кусками: молитвы, чтение книг на каждом углу, гарцующие всадники, порт... Вот еще что: мой город стоял на берегу моря... Или реки... Сложно сказать.

Педро прекратил на пару секунд свою молитву, прислушиваясь к словам Ле Роя, потом продолжил. Киринаикос поднялся, оглядел горизонт.
— Там что-то движется, — ткнул он пальцем в ту сторону, куда ушел Олафсен. — Что-то большое — больше, чем швед. Какая-то машина.

Все встали и принялись вглядываться туда, куда указал грек. Действительно, что-то большое и быстрое приближалось к ним; скоро уже стал слышен гул, похожий на гудение бомбардировщика.
— Танк, — сказал из-за спин Педро. — Точно вам говорю. Их привел швед... Проклятый викинг!

Все молчали. Комментировать слова Педро было глупо — вряд ли швед ушел, чтобы привести сюда войска. Тем временем танк приближался.

Канадец машинально сжал крепче черенок лопаты — хотя, как он мог навредить танку при помощи лопаты? Однако стало чуть спокойнее: он заметил, что и другие подняли с земли орудия труда и сжали их в руках. Некоторое время спустя стало слышно, что звук разложился на два — один звук был более высокий, второй — низкий, тяжелый, пробиравший до мозга костей.

А через пару минут они подъехали: танк и впереди него — машина мотопехоты. Броневичок лихо развернулся в десятке метров от стоящих людей; они сделали пару шагов назад, чтобы не утонуть в облаке пыли, образовавшемся от разворота гусениц. Танк замер неподалеку, качнув стволом.
— Серьезные ребята, — сказал кто-то за спиной. — Что за знак на борту?
— Это мои, — ответил Адольф и вышел вперед, взмахнув рукой. Люк танка лязгнул и открылся. Наружу по пояс показался офицер в запыленной форме; он снял шлемофон, вытер пот со лба и крикнул:
— Привет, парни!

Ответом была тишина. Ле Рой заметил, что грек прикрывает лопатой грудь, и сделал то же самое. Адольф подошел поближе к танку, оставив броневик в стороне.
— Здравствуйте! — крикнул он в ответ. — Как добрались?
— Черт бы побрал эти степи! — сказал в ответ офицер, выбираясь на броню. — Пыль: ни кустика, ни колодца! Вы-то как? Вода еще есть?
— Ее и не было, — шепнул канадец и вдруг понял, что они не пили и не ели с того самого момента, как появились здесь. И тут же захотелось пить — язык, превратившийся в кусок наждачной бумаги, кричал о жажде, горло пересохло. Ле Рой огляделся и убедился в том, что воды нет — как будто она могла взяться из ниоткуда!
— Насчет воды — это вы здорово спросили, — рассмеялся Адольф. — Мы здесь уже скоро сутки, а ни грамма влаги не видели. Если не считать того дерьма, что постепенно копится на дне рва — а уж взять такую воду в рот не рискнет ни один нормальный человек.

Тем временем офицер спрыгнул на землю, оставив шлем на броне, одернул китель и подошел поближе, протянув руку Адольфу. Тот с видимым удовольствием пожал ее.
— У вас все в порядке? — поинтересовался командир танка. — Воду и продукты мы вам привезли, они в броневике. Должно хватить на первое время, а дальше — посмотрим... Но, как я понял, желающих работать становится меньше?

Он перевел глаза на стоявших неподалеку людей, пересчитал их, тихо шевеля губами.
— Не хватает, — сказал он Адольфу. — Одного не хватает.
— Знаю, — согласился тот. — Но я не стал останавливать — думаю, что он никуда не денется и вернется.
— Тут вы правы, — кивнул офицер. — Ганс! — крикнул он в сторону танка. Из люка показалась взъерошенная голова блондина.
— Доставай! — приказал офицер.
— Есть! — ответил Ганс, выскочил на башню и, наклонившись, потянул что-то изнутри. Канадец не удивился, когда увидел, что Ганс вытаскивает на броню Олафсена.
— Господи... — перекрестился Педро, увидев залитое кровью лицо шведа. — За что они его так?..

Действительно, глядя на Олафсена, не вспомнить Господа было нельзя. Он был не просто избит — похоже, он был изувечен, причем не случайно, а преднамеренно. Канадец обратил внимание, как дергался и гримасничал швед, когда его руки и ноги задевали за броню — похоже, у него осталось очень мало целых костей. Гансу помогал еще один человек — вдвоем они выволокли шведа на землю и уложили возле гусеницы.

Командир тем временем о чем-то переговорил с Адольфом, согласно кивнул и крикнул:

— Три человека пусть пока разгружают броневик. Продукты и воду в одну сторону, все остальное — ближе ко рву!

«Остальное — это, интересно, что? — подумал канадец, чувствуя, как Педро и грек недоверчиво смотрят на закрытые десантные люки броневика. — Что там может быть? И за что так избили шведа? Нам в назидание?».

Очень не хотелось приближаться к броневику. Вообще, не хотелось что-либо делать под дулом танка: было в этом что-то унизительное. Но парни, которые приехали на танке, решили иначе. Они подошли к стоящим на краю канавы людям, пристально взглянули в глаза каждому и ткнули пальцами в тех, кто, по их мнению, мог наиболее быстро и хорошо исполнить приказ. Этими троими оказались Ле Рой, Педро и еще один парень, что пришел с другой стороны.

Ганс достал из кобуры пистолет и махнул им в сторону броневика.

— Живо, разгружайте — если не хотите умереть с голоду! — приказал он. — А ты, Дитрих, присматривай за ними. И самое главное — проверяй мешки.

Танкист кивнул и подтолкнул Педро. Остальные, не дожидаясь тычка под ребра, пошли сами.

Дверцы десантных люков отворились на удивление тихо. Ле Рой посмотрел внутрь, увидел пару ящиков с надписью «Консервы», потом несколько упаковок минеральной воды и еще что-то в глубине, подошел, взял воду, прикинул, куда бы положить и определил местом складирования тот участок, где они только что отдыхали. Следом за ним принялся вытаскивать продукты Педро. Третий парень попытался взвалить на себя ящик с консервами, но ему это оказалось не под силу.

— Сейчас, помогу, — поставив воду на землю, сказал канадец. Вернувшись, он взялся за другой край и вдруг заметил, что в глубине броневика что-то шевелится. Какой-то черный мешок издавал странные стонущие звуки. Ле Рой решил не говорить пока об этом — скоро они все равно до него доберутся, тогда и станет ясно.

Они вытащили еду — ящики быстро кончились, их было не так уж много, потом выгрузили две большие палатки (Киринаикос и еще три человека быстро принялись устанавливать их, чтобы скрыть от палящего солнца воду). Все это время мешок в броневике потихоньку постанывал, а Адольф, усевшись на броню, о чем-то весело трепался с офицером. Вскоре до канадца долетели звуки губной гармошки. «Развлекаются, — зло подумал Ле Рой. — Встретил земляков... Вот только странно, почему они командуют нами? Почему они — главные? Дело в той войне, что идет неподалеку?».

В это время на очередное бомбометание прибыла эскадрилья бомбардировщиков. Офицер, дурачась, соскочил с брони, щелкнул каблуками и крикнул «Хайль!». Адольф поддержал его, выкрикнув то же самое. Они рассмеялись, офицер хлопнул его по плечу и предложил выпить из тонкой фляжки, которую вынул из-за пазухи. Адольф несколько раз отхлебнул, поморщился и, довольный, вернул флягу. Офицер тоже пару раз приложился к ней, глотнул с видимым наслаждением и подошел к Ле Рою и тем, кто вместе с ним разгружал броневик.

— Хорошо, — похвалил он, увидев, что процесс идет полным ходом. — Те мешки, что лежат в глубине десантного отсека, выгружайте поближе ко рву — потом поймете, почему.

Он к чему-то принюхался, потом посмотрел в сторону самолетов и произнес:

— Скоро нам праздновать... Там бригада Биндермана. Когда они войдут в город, мы узнаем это по красному зареву. Он обещал сжечь там все книги, добавив в огонь какую-то дрянь, что раскрашивает дым в ярко-красный цвет. Как только небо окрасится в розовые цвета — значит, мы вошли в город.

Он посмотрел в глаза Ле Рою и зло прищурился.

— Работать! — внезапно крикнул он. И куда только исчез тот милый офицер, который трепал всех по щекам и раздавал трофейный коньяк! Его место занял грубый солдафон-самодур, раздающий приказы направо и налево. — Мешки брать вдвоем и тащить ко рву! Быстро, я сказал!

Канадец ухватил первый мешок, который наощупь оказался то ли пластиковым, то ли еще каким-то синтетическим, никак не из ткани, как казалось в темноте десантного отсека. Потянул на себя — там что-то свободно болталось. Киринаикос, закончив ставить палатку и спрятав туда воду, подошел, ухватился за другой конец, шепнул канадцу:

— Я всегда буду рядом, сволочь... Не поворачивайся ко мне спиной, слышишь?

Ле Рой постарался не обращать внимания на его шипение, но совет грека принял на заметку. Вдвоем они вытащили мешок наружу и по его контурам поняли, что там человек.

Мертвый человек.

Встретившись взглядами, они машинально посмотрели внутрь броневика. Там были еще около двадцати таких мешков. Двадцать трупов. И один мешок продолжал шевелиться.

— Выполнять! — снова крикнул офицер и толкнул канадца в плечо. Ле Рой очнулся от своего забытья и быстро, в паре с греком, потащил мешок к канаве.

«Мы копали могилу, — подумал он. — Но она чересчур велика для двадцати покойников. Неужели скоро их будет намного больше? Остальных привезут из города?!».

Мешок они сложили рядом с большой кучей земли. Офицер подошел к ним, заглянул вниз, смачно плюнул, после чего толкнул мешок ногой. Тело покатилось по склону, пока его не остановила грязная жижа на дне. Оно бултыхнулось в грязь, несколько секунд полежало на поверхности, после чего стало медленно погружаться.

— Ганс! — крикнул он. — Оставь шведа, иди сюда!

Подчиненный быстро подбежал, оставив Олафсена валяться на земле.

— Первый — черт с ним! Но всех остальных — проверяй!

— Есть! — Ганс вытянулся в струну, отдал честь. Командир танка еще раз осмотрелся вокруг, взглянул в сторону города, надеясь увидеть красный дым, и вернулся к своей броне.

— Следующий! — крикнул Ганс. Второй мешок тащил Педро со своим напарником. Они также оставили его на краю. Ганс шевельнул его ногой, потом вытащил пистолет и выстрелил сквозь ткань в голову. Кроме выстрела, никто не услышал ни звука.

— Бросай!

Педро толкнул мешок с бруствера вниз. Он упал рядом с первым. К этому времени Ле Рой и грек подтащили третий...

Когда дошла очередь до шевелящегося и стонущего мешка, канадец прикусил губу. Там, внутри, был живой человек — и через минуту его застрелят.

Грек не обращал на это внимания. Он молча делал свое дело, ни на секунду не забывая о том, что Ганс может выпустить мозги не только тем, кто лежит в мешках, но и тем, кто эти мешки носит. Они положили мешок у ног танкиста, тот выстрелил...

А спустя секунду из мешка раздался ответный выстрел: Ганс схватился за грудь, покачнулся и упал в ров. Командир танка в этой ситуации не растерялся — несколько метких выстрелов из пистолета заставили человека в мешке умереть. Он подбежал к краю канавы, толкнул ногой мешок и заорал:

— Что смотрите, суки?! Работать!

Потом подбежал к открытым дверям, на ходу перезаряжая пистолет, и расстрелял все мешки внутри броневика.

— Сволочи! — орал он, выпуская пулю за пулей. — Всех... Всех!.. Расстрелять! Утопить! Стереть с лица земли!

Адольф подошел к нему со спины, прикоснулся к плечу, надеясь успокоить...

ГАНС ШЕВЕЛЬНУЛ ЕГО НОГОЙ, ПОТОМ ВЫТАЩИЛ ПИСТОЛЕТ И ВЫСТРЕЛИЛ СКВОЗЬ ТКАНЬ В ГОЛОВУ. КРОМЕ ВЫСТРЕЛА, НИКТО НЕ УСЛЫШАЛ НИ ЗВУКА

Офицер резко развернулся на каблуках и, не раздумывая, выстрелил в него. Адольф сложился пополам — пуля попала в живот — застонал и посмотрел на офицера так жалостливо и удивленно, что у канадца, который стоял в двух шагах в стороне, перехватило дыхание от ужаса и сострадания.

А через секунду он упал рядом с броневиком, несколько раз дернулся и затих. Смерть Адольфа несколько отрезвила командира танка. Он ненавидящим взглядом посмотрел на стоящих вокруг людей и произнес:

— Здесь нет своих и чужих... Здесь все меняется местами каждую секунду... Здесь нет любимчиков... Убью каждого, в ком увижу опасность для своей жизни. Работайте... И этого — тоже в канаву, — он перешагнул через труп Адольфа и пошел к танку.

АБСУРДОМ БЫЛО ВСЕ. И ОНИ САМИ, И ИХ РАБОТА, И ЭТА МОГИЛА С ТОННАМИ ГРЯЗНОЙ ВОНЮЧЕЙ ЖИЖИ НА ДНЕ, И ПРОПАВШИЕ БОЧКИ С РАДИОАКТИВНЫМ ДЕРЬМОМ, И ЛОВУШКА, ВСТРЕТИВШАЯ ШВЕДА... И ДАЖЕ ТАНК, КОТОРЫМ УПРАВЛЯЛ ЛЮБИТЕЛЬ КОНЬЯКА, ОЖИДАВШИЙ КРАСНОГО ЗАРЕВА НА ЗАКАТЕ.

Башня танка с противным шумом повернулась, направив дуло на работающих возле броневика людей. Это было немым приказом.

Грек и Ле Рой переглянулись снова, взяли немца за руки и ноги и скинули вниз, в ров. Адольф быстро исчез из виду: остальные простреленные мешки быстро скрыли его от глаз людей, оставшихся наверху. Когда броневик опустел, его водитель закрыл двери, мощно газанул, оставив после себя вонючее облако, и умчался в сторону бомбежки. Следом попятился танк.

— Я думал, мы делаем что-то полезное, — внезапно сказал Педро.

— А иначе — что же это за дьявольщина? Зачем мы здесь?

— Мы могильщики, — озвучил общую мысль Ле Рой. — Киринаикос, я думаю, нам нет смысла враждовать — тот, кого ты хотел убить, мертв. Да и оглядываясь на все то, что было здесь в последний час, ты должен признать, что я сделал правильно, свалив тебя в канаву...

— И почему же? — презрительно скорчив лицо, спросил грек.

— Потому что если бы экипаж танка не нашел Адольфа среди живых, думаю, нам всем нашлось бы место рядом с теми мешками. А вышло наоборот — сам немец лежит там, превращаясь в грязь.

Грек нахмурился, но признал правоту Ле Роя. Скорее всего, так и вышло бы — экипаж танка сровнял бы их бригаду с землей...

Тем временем Педро подошел к лежащему на земле Олафсену. Швед был без сознания.

— Дайте воды, — попросил мексиканец. Принесли бутылку, Педро плеснул немного на лицо избитого шведа. Тот вздрогнул и попытался защититься. Похоже, он думал, что кошмар продолжается. — Тихо, тихо, — успокоил его Педро, протер лицо от крови. — Ты слышишь меня, Олафсен?

Тот кивнул, но глаз не разомкнул. Его пальцы шарили по земле в поисках того, за что бы можно было зацепиться, он хотел приподняться. Подошел Ле Рой, помог мексиканцу отнести раненого в палатку.

Через пару минут Олафсен попросил пить. Ему влили немного воды сквозь распухшие губы.

— Уйти нельзя, — сказал он, не обращаясь ни к кому конкретно. — Там... Я не знаю, что там...

— За что они тебя так изуродовали? У тебя сломана левая рука, в крови все тело... — Педро ощупывал шведа и ориентировался на его стоны. — Надо будет сделать шину для предплечья, разломаем чью-нибудь лопату, прибинтуем.

— Это не они... — снова нашел в себе силы заговорить швед. — Это... Я не знаю, кто... Скорее, что... Какая-то сила. Я просто шел по степи... Километра два... И вдруг что-то меня швырнуло назад...

— Как? — не понял мексиканец. — Никого и ничего не было? Но ты...

— Швырнуло так, что мне показалось, будто меня сбила машина. Странно, но я не почувствовал удара, было другое ощущение... Дайте еще воды...

Мексиканец машинально вложил ему в сломанную руку бутылку с водой. Олафсен вскрикнул, уронил ее и разлил всю воду. Педро выругался, взял еще одну и напоил шведа сам.

— Ощущение, что меня дернули назад, — сказал Олафсен, отдышавшись и уняв боль. — Тогда я и сломал руку — упал неловко, покатился по своим же следам, рука подвернулась под грудь...

— Чушь какая-то, — сказал канадец. — Может, за тобой кто-то шел? Или сработала какая-то ловушка? Не может быть так, как ты рассказываешь! Все в мире имеет свою причину!

— Ты так думаешь? — ухмыльнулся Педро. — В чем причина нашего появления здесь? Кто мы? Думаю, на это у тебя ничуть не больше ответов, чем на историю Олафсена!

Канадец замолчал. Педро был прав на сто процентов — абсурдом было все. И они сами, и их работа, и эта могила с тоннами грязной вонючей жижи на дне, и пропавшие бочки с радиоактивным дерьмом, и ловушка, встретившая шведа... И даже танк, которым управлял любитель коньяка, ожидавший красного зарева на закате.

— Кстати, что там насчет пожара, который нам обещали немцы? — спросил сам себя Ле Рой и вышел из-под брезентового навеса. На горизонте по-прежнему что-то громыхало, по-прежнему тянуло дымком, но никакого намека на красный пожар не было. Канадец посмотрел на следы танковых гусениц и покачал головой.

— Уйти нельзя, остаться в живых сложно, работать противно... — сказал он, ни к кому конкретно не обращаясь. — Как же быть? Как поступить в этой ситуации? По сути дела мы никому не нужны — при этом я уверен, что кто-нибудь опять придет проверить нашу работу. И никто не сможет предсказать, в каком расположении духа будет этот «кто-нибудь».

— Маленькое уточнение, на которое никто почему-то не обратил внимания, — сказал Киринаикос. Он все это время стоял у входа в палатку и слушал, о чем говорил Олафсен. Рассуждения Ле Роя тоже не миновали его ушей.

— На что именно мы не обратили внимания? — спросил канадец, продолжая смотреть в сторону невидимого отсюда города, расположенного, если верить шведу, в джунглях.

— В одном из мешков осталось оружие, — грек улыбнулся заходящему солнцу. — Оно, конечно, могло испортиться в воде — но чем черт не шутит... А если в остальных мешках тоже что-нибудь затерялось?

— Считаешь, нам надо вооружиться? — повернулся к Киринаикосу Ле Рой. — Лично я чувствую, как внутри меня поднимается желание работать — и оно сильнее меня. Еще несколько минут, и я возьму лопату и пойду ковырять эту чертову землю, несмотря на то, что в канаве лежат расстрелянные люди.

— Ты не одинок, — сказал Педро. — Швед отключился, думаю, долго он не протянет. Надо срочно принимать какое-то решение.

— Ты не понял, мексиканец, — грек сложил руки на груди. — Похоже, мы не сможем ничего сделать — мы будем работать тут до тех пор, пока сами не окажемся на дне рва. Следом за Адольфом.

— Тупик? — переспросил Ле Рой.

— Тупик, — согласился Педро.

— Лучше бы они привезли вина, — мечтательно закатил к небу глаза Киринаикос. — Сейчас бы сидели в палатке, пили что-нибудь крас-

ное... Или белое... У нас вот много хорошего винограда. И голова потом не болит. А перед смертью зато как было бы спокойно и приятно на душе...
— Ты уже простился с жизнью? — нахмурил брови канадец. — Решил выпить кувшин вина, лечь и ждать пулю в лоб? Я полез за оружием.

Он стал спускаться к утопленным телам. Земля осыпалась под ногами, Ле Рой с трудом удерживался от того, чтобы не съехать в грязь на спине. Проклиная всех и вся, он остановился на краю, присел, подтянул к себе один из мешков, выволок себе под ноги. Разорвать его было делом трудным — зашито было поверху широкими стежками и толстой ниткой. Сверху сбросили лопату — дело пошло чуть быстрее, о ее острый край Ле Рой перерезал нить, раскрыл...

В этом мешке ничего не было. В смысле, не было оружия. Там был человек, убитый выстрелом в голову. На груди табличка — «Повстанец». Канадец угрюмо посмотрел в залитое кровью лицо, оттолкнул от себя мешок обратно в воду.

Вторым был тот самый простреленный мешок. Они, конечно, были простреляны почти все, но этот Ле Рой отличил сразу — у него было одно пулевое отверстие на уровне пояса, там, где несчастный повстанец берег припрятанный пистолет. Канадец взял его в руку, проверил наличие патронов в обойме — сделал это крайне неумело, едва не утопив ее.
— Бомбежка прекратилась, — сказал сверху грек. — И никакого красного дыма. А солнце уже заходит, поторопись.
— Не хочешь помочь? — зло спросил Ле Рой.
— Как представлю, что надо обыскивать грязные окровавленные трупы — тошнота к горлу подступает... И знаешь, мне почему-то все меньше и меньше хочется работать... Помнишь то зовущее ощущение, на уровне приказа?

Ле Рой поднялся, прислушался к своим ощущениям и кивнул, соглашаясь.
— В нас что-то изменилось? — спросил грек.
— Вряд ли, — ответил Ле Рой. — Думаю, что не в нас. Вокруг.
— Что ты имеешь в виду? — Киринаикос осмотрелся, словно хотел увидеть нечто зримое и вещественное — что-то, что указывало бы на изменения в их душах.
— Там, — канадец махнул рукой в сторону города, — что-то идет не так, как хотелось бы тем, кто приезжал сюда на танке. Думаю, все идет в противоположную сторону. Слышишь, грек, тут есть еще пистолет...

Ле Рой выбрался наружу и заметил, что Киринаикос и Педро смотрят куда-то в сторону горизонта. К ним приближалась колонна: столб пыли накрыл все пространство с наветренной стороны. Скоро они уже слышали шум моторов.
— Интересно, в чью пользу повернется сейчас, — спросил Ле Рой, пристраивая в руке пистолет, отдав второй греку.
— Адольфа уже нет, — сказал мексиканец. — Хотя, вдруг это кто-нибудь другой?

На этот раз колонна состояла не только из бронемашин — были в ее составе и несколько тягачей с пушками. Головной танк остановился в нескольких метрах, дыша горячим железом.

Люк открылся, показался человек с перепачканным лицом. Он быстро выскочил на броню, заглянул высока в отрытый ров, покачал головой и крикнул что-то в шлемофон.

Похоже, история повторялась. Несколько бронемашин обогнули колонну и приблизились ко рву, вот только помощи у рабочих они не попросили — солдаты сами быстро перекидали трупы, даже не упакованные в мешки, в братскую могилу и вернулись на свои места.
— Канадцы есть? — подошел поближе офицер из головного танка.

Ле Рой сделал шаг вперед, сжимая за спиной рукоять пистолета.
— Чудесно, — похлопал его по плечу танкист. — Пойдешь с нами. Работа в этом квадрате закончена. То, что эти идиоты считали мелиоративным процессом, подошло как нельзя лучше для больших могильников. Ты герой, парень. Поедешь с нами.
— А мы? — спросил грек, шагнув вперед. — Что мы здесь делаем? Куда идти нам? И зачем мы копали здесь могилу?
— Трофей? — улыбнувшись, кивнул в сторону грека танкист. — Понимаю. Да ты и сам, наверное, был чьим-то трофеем. Ну да ничего, мы поправили это положение. Под городом они подавились своей собственной костью... Мы положили всю бригаду этого мерзавца Биндермана. Теперь на этом участке фронта мы полностью доминируем.
— Я рад, — мало что понимая, ответил Ле Рой.
— Мало этому радоваться. Надо вдохнуть воздух свободы полной грудью. Иди, займи место в броневике.

Он повернулся к своему танку и сделал какой-то малопонятный жест.

Из танка через секунду ударил пулемет.

Палатку и всех, кто в ней находился, сбросило в ров, поверх свежих трупов. Олафсен, грек, Педро — все были убиты. Запах пороха быстро наполнил все вокруг и так же быстро улетучился на ветру.
— Они больше не нужны. Они — обуза, — сказал офицер из-за спины. — Вперед, парень, война еще не закончилась!

Ле Рой отвернулся от трупов. Ноги сами понесли его мимо колонны в сторону броневиков.

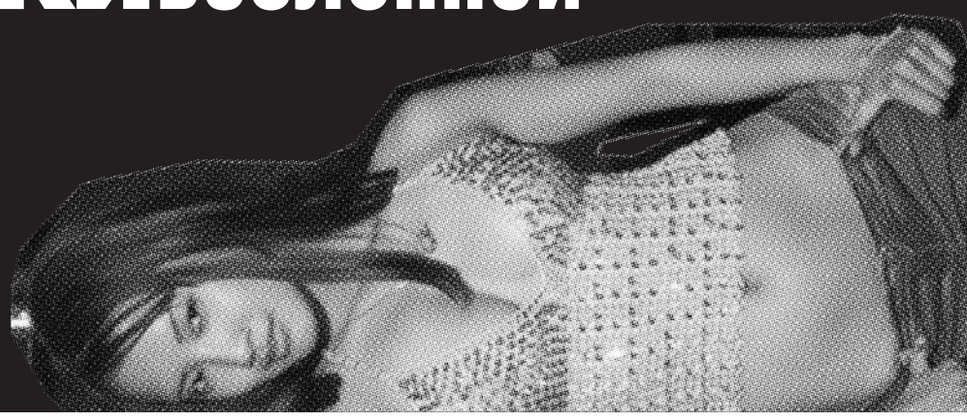
Вдруг он остановился. Он понял, что все это время ему не давал покоя один вопрос.
— Офицер... — решился он. — Ответьте, пожалуйста, если сможете...
— Что случилось?
— Вопрос... На него нет ответа... Ведь мы... Я из Канады, Педро из Мексики, Киринаикос из Афин... Да и остальные... Как мы понимали друг друга, на каком языке мы говорили?
— На русском, — улыбнулся танкист.
— Почему? — недоуменно спросил Ле Рой.
— Потому что русификатор очень хороший, — ответил офицер. Потом поднял глаза к небу, потянулся с наслаждением:
— Золотой век продолжается...

Через несколько минут колонна тронулась дальше, унося с собой Ле Роя. Сегодня канадцы оказались сильнее. Никто не знал, что будет завтра.

«Цивилизация» всегда была непредсказуема ●

ИСХОДНИКИ ВСЕЛЕННОЙ

КОЛОНКА КРИСА КАСПЕРСКИ



• КАК ХАКНУТЬ АЗИАТКУ

Восточными красавицами нынче «болеют» многие. Увлечение востоком — это просто эпидемия какая-то. Хакеры, живущие в глубине норы своего одиночества, отгородившиеся от мира четырьмя стенами и уткнувшиеся в монитор, обычно испытывают большие проблемы даже с обычными девушками, а уж тем более с азиатками. Как воплотить эту мечту в реальность?

Магическая притягательность узкого разреза глаз на самом деле обманчива. Обладание женщиной — это всегда мираж, призрак. Обольстительницы часто манят в свои сны сильных богатырей, но оттуда уже нет возврата. Восточные женщины при близком рассмотрении совсем не такие, как на расстоянии, тем более, что среди них всякие встречаются. Жить-то (если речь идет о супружестве) с человеком, с его менталитетом, а не с разрезом! Как говориться, опыт — это то, что получаешь, не получив того, что хотел, но с другой стороны — если мужчина просит руки женщины, значит ему надоела своя. Ладно, оставим все эти рассуждения в стороне и займемся практическими вопросами.

➔ **как не стоит знакомиться.** Жителям больших городов хорошо — вышел на рынок, там этих азиаток... ну просто туева хуча! Продают корейскую морковку, но по-корейски не знают ни слова, потому что все они из xUSSR. Так что не помешает предварительно выучить хотя бы нескольких слов на языке своей мечты (ссылки на on-line словари приведены во врезке), чтобы отличить некачественную подделку от оригинала.

То же самое относится к знакомству с проститутками, которые якобы из Азии, но на проверку — все это грим и косметика. Хотя настоящие азиатки среди проституток все-таки встречаются, однако, прежде чем предлагать такой руку и сердце, следует основательно подумать. Дело даже не в венерических болезнях (сейчас все лечат, кроме СПИДа, который является самым большим заговором XX века) и не в деформированной психике. Часто за проституткой тянется «хвост» стоящих за ней личностей, создающих очень большие проблемы.

Знакомства через интернет-службы наподобие **love.mail.ru**, как правило, обнаруживают только русских эмигранток. На **china.kulichki.com** в основном обитают самцы, а девушки в основном все те же иммигрантки, уже замужние или достаточно состоятельные для того, чтобы выбирать не первого попавшегося мужика. Все эти пути знакомства с вероятностью, близкой к единице, обречены на провал.

➔ **с чего следует начинать знакомство.** Достаточно часто приходится слышать утверждение, что знакомства с иностранками (особенно восточными) следует начинать с изучения истории, менталитета, обычаев и традиций их страны. Какая-то логика в этом есть, но... те традиции, что описываются в доступной литературе, главным образом относятся к ископаемым женщинам, а некрофилов среди нас, надеюсь, нет. Тем не менее, норм приличия и этикета никто не отменял, так что знакомство с ними просто необходимо. В частности, в ряде районов Индонезии (например, в Buginese) здороваться не то чтобы не принято, у них просто нет соответствующих конструкций в языке, и хотя можно сказать что-то вроде «pole tega ki» (где же тебя столько носило?), — это будет вопрос, предполагающий ответ, в то время как в английском «how do you do?» вовсе не означает, что спрашивающий всерьез интересуется вашими делами.

Поскольку восточных языков очень много, то первым делом нужно определиться с кем, собственно говоря, мы собираемся знакомиться. Знать язык своей пассии хотя бы на уровне разговорника для туристов — необходимо. Также следует свободно владеть английским, поскольку вероятность встретить русскоговорящую азиатку ничтожно мала.

➔ **знакомства — рецептурный справочник.**

вариант #1: заходим на бесплатный сайт международных знакомств, например, PEN PALS (**www.anglik.net/penpals.htm**), на котором достаточно много азиаток. Пишем (естественно, на английском) письма всем, кого только найдем и дальше заводим непринужденный разговор о прошлогоднем снеге или высоких технологиях. Предлагать руку и сердце с первых строк не стоит. Девушку сперва надо очаровать, вырастить у нее за спиной крылья, но и тогда не стоит рассчитывать, что она прилетит к вам, потому что те, кто переписываются через интернет, как правило, имеют виды на карьеру, живут в комфортабельных квартирах, и просто так оставлять свою страну не собираются, но познакомиться через них с обычными девушками, желающими иммигрировать — вполне можно. Кстати, то же самое относится и к мужчинам. На хакерских форумах достаточно высокий процент азиатских пацаков, с которыми можно списаться и подкатить с той же просьбой. Иногда их можно идентифицировать по мылу (что-то типа @students.itb.ac.id), но чаще они используют американские ящики и тогда приходится знакомимся со всеми форумовчанами. Только на быстрый успех здесь лучше не рассчитывать. Азиатские парни испытают с девушками те же самые проблемы, что и мы.

вариант #2: на **www.oriental.com** или форуме русско-китайской дружбы (**http://cpcfriend.com/**) достаточно много русскоговорящих восточных красавиц. Это просто клад для тех, кто не знает ни английского, ни китайского, ни японского... словом, никаких других языков, кроме русского. Достаточно многие из них уже находятся в России или хотят приехать в ближайшее время, но, например, не имеют денег. Аферисток среди них, как ни странно, очень мало. Лично я не встретил ни одной, хотя встречался (за свой счет) со многими, но возможно, мне просто до сих пор везло, хотя постоянное везение — это уже закономерность.

вариант #3: садимся на самолет и летим на отдых в далекую восточную страну. Со знанием местного языка найти спутницу жизни — плевое дело. Английский уже накладывает существенные ограничения, но шансы по-прежнему остаются велики. С одним лишь русским поиски пассии рискуют затянуться на всю оставшуюся жизнь.

Когда ваши мечты сбываются — это хорошо. Плохо — когда они сбываются у других. В общем, учите мат. часть и удачных вам поисков! **C**

Попробуйте подписаться в редакции, позвоните нам.

(это удобнее, чем принято думать :)

SYNC

Лучшие цифровые камеры


Хакер

Хакер Спец

Железо

Страна Игр

PC Игры

Мобильные компьютеры

Maxi Tuning

Total DVD

DVD Эксперт

Total Football

Onboard

Mountain Bike Action

Хулиган

Свой бизнес

- Для подписчиков в Москве курьерская доставка **БЕСПЛАТНО** в день выхода журнала
- Дешевле, чем в розницу
- Гарантия доставки и замены в случае потери
- Специальные предложения для подписчиков
- Первый номер подписки высылается по звонку вместе с заполненной квитанцией для оплаты

8-495-780-88-29 (для Москвы)
8-800-200-3-999 (для России)
ВСЕ ЗВОНКИ БЕСПЛАТНЫЕ
Мы работаем с 9 до 18 по рабочим дням

(game)land

“ФУТБОЛЬНЫЙ МЕНЕДЖЕР”!

СОЗДАЙ СВОЮ КОМАНДУ ИЗ РЕАЛЬНЫХ ИГРОКОВ И ПРИВЕДИ ЕЕ К ПОБЕДЕ

ТЫ ПОЛУЧАЕШЬ $135 МИЛЛИОНОВ
на приобретение игроков российской премьер-лиги при регистрации на сайте www.total-football.ru.
Подробности на сайте **www.total-football.ru**

ГЛАВНЫЙ ПРИЗ – ПОЕЗДКА НА ФИНАЛ ЛИГИ ЧЕМПИОНОВ 2006/07

Стартовал Футбольный менеджер посвященный Чемпионату мира 2006
Призы от компании **adidas**. Подробности на **adidas.total-footbal.ru**