

Hacking in a Foreign Language: A Network Security Guide to Russia



Kenneth Geers
Black Hat
Amsterdam 2005

Briefing Outline

1. Russia as a threat
2. Russia as a resource
3. Crossing International Borders
4. The International Political Scene



Russia as a Threat



Hacking: Russian Perspective

- Excellent technical education
- Understanding of networks, programming
- 1980's: hacked American software in order to make programs work in USSR
- Now: many skilled people, too few jobs
- Russian police have higher priorities!



Hacking: Russian Perspective 2

- Desire for Internet access, but it is expensive
 - Cheaper to steal access and services!
- Legit MS Office = 2 months' salary
- CD burner = two weeks' salary
- Russian outdoor markets:
 - MS Operating System a few dollars
- Hacking: more social approval?
 - Communal sharing culture



Russia and Cybercrime

- Russian hackers love financial crimes: banks, investment companies, fraud, piracy
- Russian citizen Igor Kovalyev: "Here hacking is a good job, one of the few good jobs left."
- Vladimir Levin: in 1994-95 illegally transferred \$10 million from Citibank
 - FBI NYC and Russian Telecoms traced activity to Levin's St Petersburg employer
- October 2000: Microsoft traced attack to IP address in St. Petersburg, Russia



Russia and Cybercrime 2

- High profits bring more investment
 - New techniques, new revenue
- FBI: in 2001, millions of credit card numbers stolen by organized hacking groups in Russia and the Ukraine
- Novarg/MyDoom worm: whole world impact
- Russian MVD: cyber crime doubled in 2003: 11,000 reported cases
- Arrests in 2004:
 - International gambling extortion ring
 - Russian student fined for spamming



<http://www.drinkordie.com>

Drink Or Die

a dod entertainment productions



- The international warez movement
- DoD: SW piracy group founded in Russia 1993
- Expanded internationally in the 1990's
- 1998-2001, over \$50 million in warez
- 20 “candy store” FTP sites (“Godcomplex”)
- Sophisticated security includes encryption
- Operation Buccaneer
- “Bandido” and “thesaint” arrested

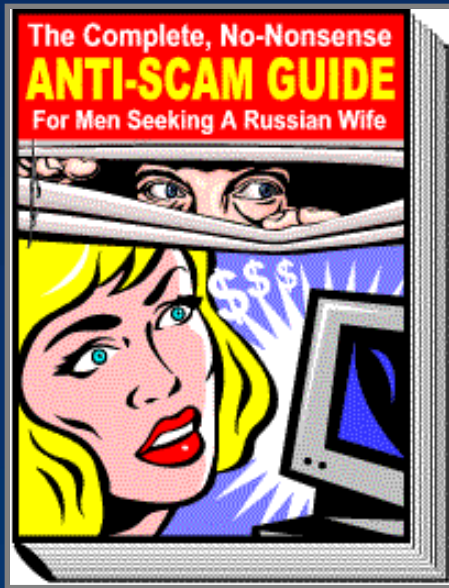
Drink Or Di

Dmitry Sklyarov

- Black Hat / DefCon connection
- First Indictment under Digital Millennium Copyright Act
- Advanced eBook Processor "AEBPR"
- Five Adobe copyright violations
- Dmitry: computer programmer and cryptanalyst
- Long confession on FBI site
- Cooperated in prosecuting Elcomsoft
- Company acquitted
- Victory for the EFF!



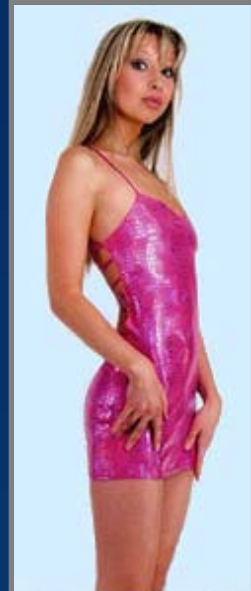
Social Engineering... Russian Style



Russian Brides Cyber Guide

Black List: Alphabetical Archive

- ◆ **NEW!** [Scam-free search - GUARANTEED!](#) - We do the job for you.
- ◆ **NEW!** [Last month updates to the Black List](#)
- ◆ **Must read!** [ANTI-SCAM GUIDE](#) - Read how to r
- ◆ **Must read!** [ARRESTS!](#) - Scammers arrested in
- ◆ **Must read!** [Soviet Unions](#) - How successful are



Name: Elena

EM®

Looking for a partner
Age to 100

ID: 017097
Name: Maria

Confirmed profile ✓

EM®

Age	32
Height	173 cm / 5' 8"
Weight	60 kg / 132 lbs
Eye Color	Grey
Hair Color	Light brown
Hair Length	Long
Marital status	Widow
Children	no kids
Personality	serious, romantic, tidy, sense of humor, caring, economical
Interests	videos, gardening, chess, listening to music, travel

Want her email address?

It's only
\$10

Elena's Models®
Meet The Love of Your Life



Russkii Virii

- Internet access in Russia growing
- As is Russian malicious code!
- Bagel, Mydoom, Netsky
- Motive: money, which...
- Fuels other crime: smuggling, prostitution
- Keyloggers and Ebay
- Coreflood and Joe Lopez



IIS Annihilation

- Sophisticated HangUP Web attack
- Compromises Microsoft IIS, Internet Explorer
- Appends malicious JavaScript onto each webpage on the infected site
- Web surfers who viewed infected pages were invisibly redirected to a Russian hacker site
- The Russian server (217.107.218.147) loaded backdoor and key logger onto victim
- Snatched authentication info:
 - eBay, PayPal, EarthLink, Juno, and Yahoo



Russian Hacktivism

- CHC (Chaos Hackers Crew)
 - Hit NATO in response to bombings in Yugoslavia with virus-infected email
 - “Protest actions” against White House and Department of Defense servers
- RAF (Russian Antifascist Frontier)
- Hacking your political adversary’s sites: morally justifiable?



Info War and Espionage

- State-sponsored computer network operations
- Robert Hanssen
 - veteran FBI CI agent, C programmer
 - Created a FBI field office teletype system
 - Hacked FBI superior's account
 - Mid-1980's: encrypted BBS messages for handler
 - Offered Russians wireless encryption via Palm VII
 - Highly classified info for \$ and diamonds
 - Internal searches: "hanssen dead drop washington"
- National critical infrastructure protection



Russia as a Resource



Russian Hacker Sites

HAKEP.RU

ХАКЕРУ.РУ

PORTAL OF RUSSIAN HACKERS



MaZaFaKa.Ru

поиск:

Меню:

- Взлом программы
- Наши релизы
- Наши программы
- Документация
- Инструменты
- Форум команды
- Гостевая книга
- Партнерам
- Наши друзья
- Обратная связь
- О команде

Geek.RU

CRACKL@B

ТНМ.2001



Сайты Хакера: Hacker Sites

<http://thm.h1.ru/>

<http://ahteam.org/>

<http://cracklab.narod.ru/>

<http://www.geekru.narod.ru/>

<http://hangup.da.ru/>

<http://www.xakep.ru/>

<http://www.xakepxp.by.ru/>

<http://www.kibus1.narod.ru/>

<http://www.hacker.dax.ru/>

<http://hscool.net/>

<http://www.xakepy.ru/>

<http://www.cyberhack.ru/>

<http://www.mazafaka.ru/>

<http://madalf.ru/>

<http://tehnofil.ru/>

<http://forum.web-hack.ru/>





Civil Hackers' School Гражданская Школа Хэкеров



[news](#)
новости



[levels](#)
уровни



[online education](#)
обучение online



[about school](#)
о школе



[students](#)
ученики



[links](#)
ссылки



[entrance exams](#)
вступительные экзамены



[hacker groups](#)
хэкерские группы



[classes](#)
классы

[about Founder](#) | [about webmaster](#) | [good stuff](#) | [journal](#) | [conference](#) |
[site map](#) | [spryg extra](#) | [hacking run](#) | [attestation](#) | [entrance exam](#) |
[actions](#) | [ideas about site](#) | [how to donate money](#) | [sponsors](#) | [banners](#)

об Основателе | о вебмастере | хорошие вещи | журнал |
конференция | карта сайта | спрыг extra | хэкинг ран |
аттестация | вступительный экзамен | акции |
отзывы о сайте | как пожертвовать денег | спонсоры |
баннеры

School Founder

[Ilya Vladimirovich aka Arvi the Hacker](#) - founder of our *school*. The date of our school foundation is - 9 dec 1996. Since this moment Ilya Vladimirovich rules the school, constantly update methodics of teaching and criteria of [levels](#) etc.



Основатель Школы

[Илья Владимирович ака Арви Хэкер](#) - основатель Школы. Дата основания школы - 9 декабря 1996 года. Начиная с того далёкого времени Илья Владимирович руководит школой, постоянно совершенствуя методики обучения, критерии прохождения на следующий [уровень](#) etc.



Cyber-Hack portal

Our strength in our mind

System Loaded...Searching Database...Startup...85...

Раздел

Все разделы

Зона регистрации | Ваш аккаунт | Статьи | Софт | Форум | Обучение ✓ | Февраль 28, 2005

Навигация

- Главная
 - Главная страница
 - В избранное
 - Обучение
- Новости
 - О проекте
 - Добавить статью
 - Архив статей
- Аккаунт
 - Управление аккаунтом
 - Личные сообщения
 - Сообщения с пейджера
- Ресурсы
 - Зона Download
 - Статьи
 - Система поиска
 - Магазин
 - Аукцион
- Дискуссии
 - Форум
 - [-] Дневники
 - Обратная связь
 - Рекомендовать портал
- Хакерские утилиты
 - Сканнер портов
 - Анонимная почта
 - DNS-Информер

=[Добро пожаловать на CyberHack - портал!]=

Вы находитесь в кибер-хакерской зоне рунета. На этом ресурсе присутствуют закрытые материалы и секретные сведения. Доступ на сервер строго ограничен.

- Получение доступа: Перейти в зону регистрации
- Центральный вход в аккаунт: Пройти аутентификацию
- Вход в административную зону: Панель администратора

Тематика сайта: взлом, защита, хакерство, программирование, вирусология.

На сайте Вас ждёт: софт, компоненты для программирования, статьи, халва (ICQ - шестизначки, семизначки и т.д.), форум по хакерству, книги, материалы для вебдизайна, вебмастеров и многое другое.

Тут Вы можете познакомиться с хакерами, как членами нашей команды, так и с огромным числом зарегистрированных пользователей. Портал полностью легальный, так что здесь Вы можете даже найти работу или, наоборот, оставить вакансию на работу для наших специалистов.

Наш опрос

Текущий опрос:
Кодинг

***Лучшее средство разработки это:**

- Delphi
- CBuilder
- Visual C
- Visual Studio
- Assembler
- KDevelop
- Другое

Я умею программировать на:

- Pascal
- C
- Assembler
- PHP
- Java
- Perl
- HTML
- Другое

Результаты
Ответов :299

[Список всех опросов](#)

Новости портала

Последние сообщения на форуме

Тема	Поместил	Прос.	Отв.	Последний
Почему в заголовках один и тот же текст ?	Romero	25	6	Rondo 28/02/2005
Как стать хакером?	Rondo	144	31	Rondo 28/02/2005
что можно реально сделать хакеру-новичку по ip?	suslik89	32	8	Rondo 28/02/2005
Кому надо-пользуйтесь	yurik	184	35	Rondo 28/02/2005
Обмен ссылками	Romero	47	13	Rondo 28/02/2005
Железо	Rondo	68	16	Rondo 28/02/2005
Вопросы по курсам	holod	789	41	sjm 28/02/2005



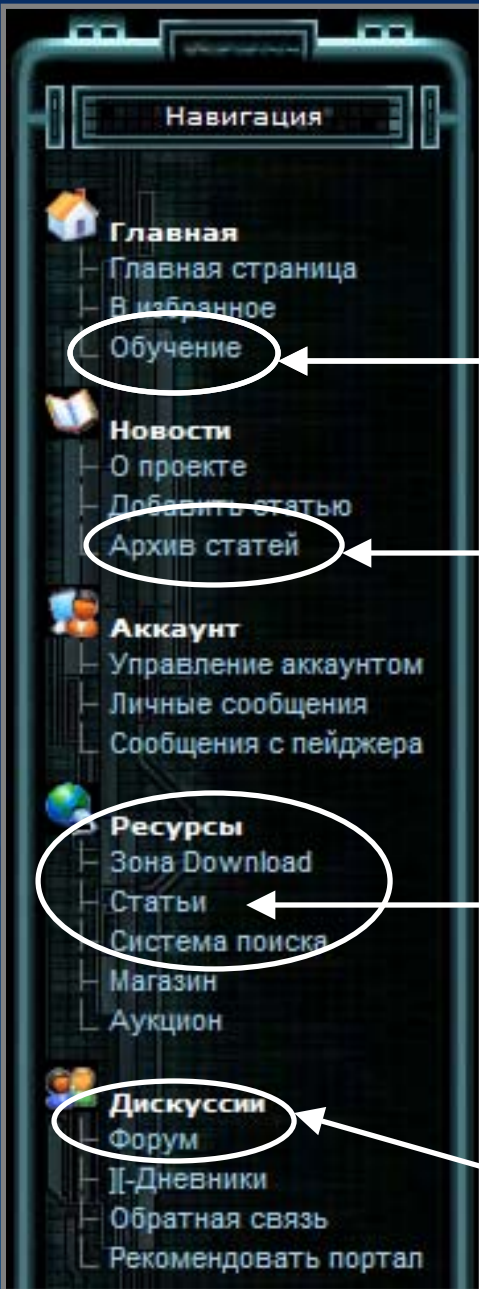
www.cyberhack.ru motto

“Хакеры, Взлом, Защита, Программирование, Исходники, Халява, Софт, Проги”

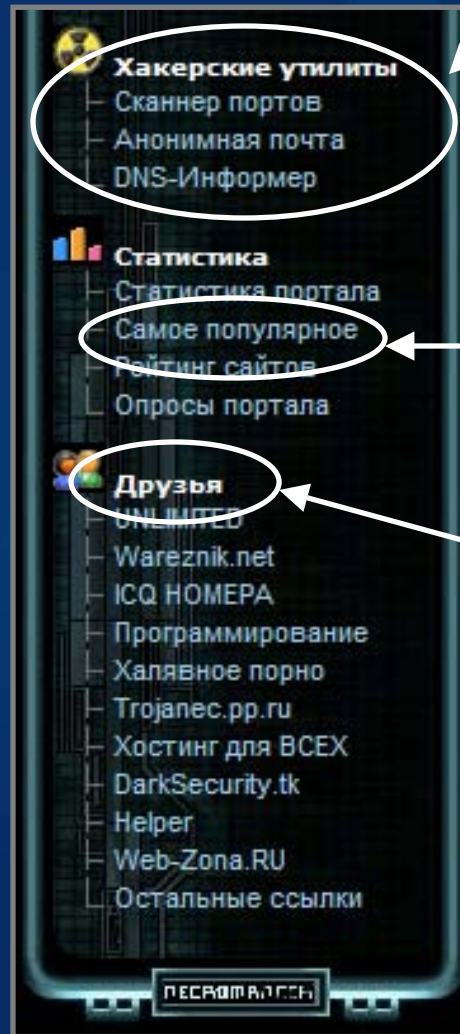
Хакеры:	Hackers
Взлом:	Attack
Защита:	Defense
Программирование:	Programming
Исходники:	Beginners
Халява	<u>Warez</u>
Софт:	Software
Проги:	Programs



Site Map



- Main
 - Training
- News
 - Archive
- Resources
 - Download
 - Articles
 - Search
- Discussions
 - Forum



- Hacker Tools
 - Port Scanner
 - Anonymous Email
 - DNS Informer
- Statistics
 - Most Popular
- Friends
 - Resources...
 - Free Stuff...



Articles by Topic

Хакерство



Программирование



Защита



Системы



Халява



Вирусология



Внедрение



Хакерство:

Hacking

Программирование:

Programming

Защита:

Defense

Системы:

Systems

Халява:

Warez

Вирусология:

Virology

Внедрение:

Intrusion



Архив Статей: Archive of Articles

Архив статей

CyberHack.RU - хакеры, взлом, защита, программирование, исходники, халява, софт, проги: Все статьи

Статьи	Комментарии	раз прочтено	Баллы	Дата	Действия
• Захвата ламмерских каналов на IRC	0	10	0	2005-03-17	 
• <i>Новости:</i> Хакер - бди!	1	20	5	2005-03-16	 
• Халявный инет	1	59	4.5	2005-03-13	 
• TOP 10 самых разыскиваемых хакеров в истории.	2	30	4.66	2005-03-13	 
• Советы начинающим хакерам.	2	43	0	2005-03-12	 
• Главное в деле - конспирация	1	31	5	2005-03-10	 
• Самые знаменитые компьютерные вирусы	0	19	0	2005-03-10	 
• Угоняем красивые аси.	9	89	5	2005-03-09	 
• Учим пользоваться Brutus AET2	0	56	4	2005-03-07	 
• Бесплатный Интернет	0	53	0	2005-03-05	 
• Взлом провайдера	0	51	5	2005-03-04	 
• Windows XP специально	0	200	3.5	2005-02-27	 
• Как записать на болванку больше 700мб	0	95	4.33	2005-02-27	 
• Новый безопасный интернет-протокол	0	30	5	2005-02-22	 
• Семья Гамбино сделала в интернете 650 млн. долларов	0	30	5	2005-02-21	 

Загрузки: Downloads

• Безопасность

Шифровщики данных and etc.

• E-mail

Бомберы, спаммеры и много полезного.

• Пароли

Различные программы для генерации и подбора паролей от разного софта

• ICQ

В данной категории находятся файлы, необходимые для защиты, угона Аськи. Патчи, версии и т.д.

• Прочее

В данной категории находятся файлы, которые не вошли в остальные разделы сайта.

• Трояны и

BackDoor'ы

Самые популярные трояны

• Защита

В данной категории находятся файлы, необходимые для защиты данных от хакерских атак.

• Литература

В данной категории находятся книги по программированию и хаку. Программирование, Хакерская литература, Художественная фантастика

• Нападение

В данной категории находятся программы, необходимые хакеру для нападения.

• Программирование

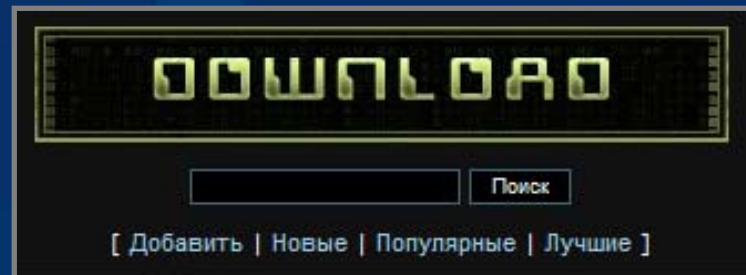
В данном разделе находятся ресурсы для программирования различного софта. Компиляторы, Компоненты, Исходники

• Сканеры

В данной категории находятся ссылки на различные сканеры (сетевой безопасности, IP, портов и пр.)

• Проху

Всё что нужно для анонимного присутствия в Инете.



Безопасность: Security

Пароли: Passwords

Прочее: Miscellaneous

Трояны: Trojans

Защита: Defense

Литература: Literature

Нападение: Attack

Программирование:
Programming

Сканеры:
Scanners



Top Ten Downloads







10 самые загружаемые файлы

- 1: Retina The Network Security Scanner 5.0.15 (Категория: Нападение) - (294 раз скачано)
- 2: NetBus (Категория: Трояны и BackDoor`ы) - (189 раз скачано)
- 3: Anonymity 4 Proxu (Категория: Proxu) - (159 раз скачано)
- 4: 007 Spy Software (Категория: Трояны и BackDoor`ы) - (144 раз скачано)
- 5: STC 4.0 (Категория: Нападение) - (140 раз скачано)
- 6: Advanced ICQ IP Sniffer (Категория: ICQ) - (106 раз скачано)
- 7: Sp-finall (Категория: ICQ) - (100 раз скачано)
- 8: Отомсти Ламеру v.1.3 (Категория: E-mail) - (89 раз скачано)
- 9: ICQ PAGER (Категория: ICQ) - (88 раз скачано)
- 10: CrazyPostman (Категория: Нападение) - (78 раз скачано)

The only tool above (same name) currently on the www.insecure.org *Top 75 Network Security Tools* is the Retina Scanner, at #21 on 3/20/2005.



Discussion Forums

Форум	Темы	Сообщения	Последнее сообщение
Как взломать? How to hack?			
 Взлом сетевых ресурсов Форум на тему взлома сетевых ресурсов Модераторы: hold, sim, Rondo, Модераторы, Администраторы	60	477	Пн Мар 21, 2005 5:49 am CherViak
Как защитить? How to defend?			
 Защита сетевых ресурсов Форум на тему защиты сетевых ресурсов	2	29	Вс Мар 20, 2005 10:30 pm
Социальная инженерия Social Engineering			
 Личный опыт Описание приёмов социальной инженерии из личного опыта можете			Пн Мар 21, 2005 2:11 am
Фрикинг Phreaking			
 Средства радио-шпионажа В данном форуме предлагается обсудить работу со средствами			Вс Мар 20, 2005 2:04 am
Программирование Programming			
 Delphi В этом форуме предлагается обсуждение вопросов, связанных с			Вс Мар 20, 2005 1:39 am
Операционные системы Operating Systems			
 *nix В данном форуме предлагается обсудить *nix системы	8	40	Пн Мар 21, 2005 1:36 am
Оффтопик Off Topic			
 Не в тему Все левые сообщения (если хочется оставить, но не знаешь где) можно постить тут	44	645	Пн Мар 21, 2005 6:23 am vurik
Обратная связь Contact Info			
 Предложения по расширению В данном форуме Вебмастера портала выслушают ваши предложения по расширению сайта, либо по изменению его разделов и структуры.	5	65	Пн Мар 07, 2005 6:38 pm yurik
People People: White/Black Lists			
 White list Проверенные люди, которым можно доверять!	0	0	Нет сообщений
Делишки Trinkets: Buy and Sell			
 Продажа			



Хакерские Утилиты

Сканер TCP-портов

*Хост (без http://www.) или IP: *От: *До:

Рекомендуется сканировать только один какой-либо порт (21,25,80,110 и пр.). Иначе сканирование может занять несколько минут...

Сканер TCP-портов

Результаты сканирования: kremlin.ru с 80 до 80 порта.

Порт: 80 открыт. | Сервис | HTTP.

Старший брат всегда смотрит за тобой, не забывай это ;)

Анонимная отправка E-Mail

Получатель	<input type="text"/>
Отправитель	<input type="text"/>
Тема письма	<input type="text"/>
Сообщение	<input type="text"/>

Results for
kremlin.ru:

Port: 80 Open
Service: HTTP

DNS - информер

Занят ли домен? Домен (без зоны): Зона:

Кому принадлежит IP-адрес? IP-адрес: Страна:

Какой IP у домена? Домен (с зоной):

Какой домен у IP? IP-адрес:

Hacker Tools:
TCP Port Scanner
Anonymous E-mail
DNS Informer

“Big brother is always watching over you, don't forget ;)”



Administrators and Contact

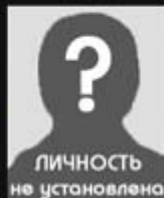
О проекте Cyberhack.RU

Данный проект создан с целью создания единого хакерского портала, сбора информации по взломам, программированию, новостям хака, а также для объединения хакеров Интернета - обеспечения их взаимного знакомства, общения, обмена софтом, разработками и информацией. Если Вы обладаете знаниями в данной области, присоединяйтесь к нашему проекту. Для этого Вам необходимо зарегистрироваться и подписаться на рассылку наших новостей. В этом случае Вы всегда будете иметь доступ к самой свежей информации и программам по хакерству.

Организаторы портала:

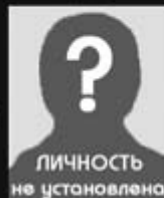
Администратор
портала HoLoD:

E-Mail:
holod@cyberhack.ru



Администратор
портала Dark:

E-Mail:
dark@cyberhack.ru



На данный момент в проекте принимают участие:

4 администратора
4 модератора форума
1494 зарегистрированных пользователей
За последние сутки зарегистрировано 9 пользователей

На сайте опубликовано:

101 статей
101 файлов
27 ссылок
219 сообщений на форуме
2 опросов
80 комментариев к статьям, ссылкам, опросам, файлам

Administrators:

holod@cyberhack.ru

dark@cyberhack.ru



REALCODING.NET

ПРОГРАММИРОВАНИЕ ДЛЯ ВСЕХ

Главное меню

- Главная
- Е-Книги
- Обзоры книг
- Проекты
- Партнеры
- Гостевая книга
- Контакты
- Настройки
- О нас пишут
- Реклама на сайте

.NET

- ADO .NET
- Создание отчетов
- Понимание SOAP
- Веб сервисы
- БД в Asp.NET
- Visual Basic 7.NET
- .NETFramework
- Visual C# .NET
- DNS в .NET
- COM компоненты
- COM+ компоненты
- Assemblies (сборки)
- Remoting в .NET
- ASP.NET в примерах
- Windows Forms
- XML в .NET
- Visual Studio.NET
- XAML
- .NET Framework FAQ

Главная страница

Последнее на форуме

- **В каком формате лучше сканировать?** >> Электронные книги. EBooks Скачать
- **Подскажите как конвертнуть ...** >> Курилка
- **Udp, Buffer Size и потоки...** >> Вопросы по сетям
- **Установка Trial компонента** >> Общие вопросы
- **типы переменных** >> Borland C++ Builder
- **Tmemorystream, Timage и Jpeg...** >> Мультимедиа
- **Помогите** >> PHP
- **Просьба ко всем!** >> Базарная площадь
- **Установка Asp.net** >> ASP.NET
- **Тег типа <p></p> умеющий делать отступление** >> Для веб мастера

Последние статьи

- **Формы пользовательского интерфейса**
- **SQL Server 2005: версии, лицензии и стоимость**
- **Программная сортировка DataGridView**
- **PHP. Использование удалённых/remote файлов**
- **Хранение XML данных (Storing XML Data)**

Последние файлы

- **VBto Converter 1.0**
- **Instrumentation Model Kit 1.0**
- **Oracle9i. Программирование на языке PL/SQL**
- **.NET Framework 2.0 SDK Beta 1 x86**
- **Wrox - Professional C++**

Последние новости

Программист обвиняет ряд коммерческих компаний в нарушении GPL

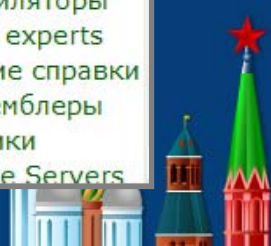
Харальд Вельте, программист, занимающийся разработкой программ с открытым кодом, обвиняет Motorola и ещё 12 других компаний в нелегальном использовании Linux. Точнее, в том, что те используют открытую ОС с нарушением лицензии GPL, по которой она и распространяется. Подробнее..

Разделы форума

- Delphi,Pascal
- C/C++, среды
- WEB dev · Java
- VB, VBscript
- DirectX, OpenGL
- Assembler
- .NET Framework
- Алгоритмы
- ОС (Win, Unix)
- Интернет, сети
- Дизайн и графика
- Разговоры
- Сертификация
- PowerBuilder
- Microsoft Office
- Железо

Софт

- Распространение
- Компиляторы
- Упаковщики
- profilers & testers
- Редакторы кода
- Реестр
- Декомпиляторы
- addons, experts
- Создание справки
- Дизассемблеры
- Отладчики
- Database Servers



Free Translation Services

- www.word2word.com
- www.google.com/language_tools
 - non-Euro: Japanese, Korean, Chinese
- www.babelfish.altavista.com
 - up to 150 words or a webpage
- www.translate.ru (Russian site)
- www.freetranslation.com
- www.translation2.paralink.com
- www.foreignword.com/Tools/transnow.htm
 - 1600 language pairs



Commercial Translation Software

- www.lingvo.ru (Russian site)
- www.worldlingo.com
- www.tranexp.com
- www.babylon.com
 - free trial version download
- www.allvirtualware.com
- www.systransoft.com
- www.languageweaver.com
 - several prestigious awards



Software and Translation

- **Natural Language Processing (NLP)**: the subfield of artificial intelligence and linguistics that studies the processing of NL (English, Dutch, Russian, etc)
 - Devoted to making computers "understand" human languages
- **Machine translation (MT)**: computer translation of texts from one natural language to another
 - Considers grammatical structure
 - Renders up to 80% accuracy
 - Draft-quality, not for literature or legal texts
 - Humans still need to pre- and post-edit (proof-read)
 - Goal is no human intervention



Translation Software at Work 1

Smashing The Stack For Fun And Profit

by Aleph One

aleph1@underground.org

`smash the stack` [C programming] n. On many C implementations it is possible to corrupt the execution stack by writing past the end of an array declared auto in a routine. Code that does this is said to smash the stack, and can cause return from the routine to jump to a random address. This can produce some of the most insidious data-dependent bugs known to mankind. Variants include trash the stack, scribble the stack, mangle the stack; the term mung the stack is not used, as this is never done intentionally. See spam; see also alias bug, fandango on core, memory leak, precedence lossage, overrun screw.



Translation Software at Work 2

Ломать Стог Для Потехи И Профита:

Алеплю одним,

smash ` aleph1@underground.org. stack`

[ч программируя] н. На много вставк ч по возможности коррумпировать стог исполнения путем писание за концом автомобиля объявленного блоком в режиме. Закопируйте делает это сказаны, что ломает стог, и может причинить возвращение от режима к скачке к случайно адресу. Это может произвести некоторые из самых злокозненных данн-zavisimux черепашок знанных к mankind. Варианты вклюают погань стог, scribble стог, мангль стог; термина tung стог не использована, как это никогда не сделано преднамеренно. См. spat; см. также alias черепашку, fandango на сердечнике, утечке памяти, lossage предшествования, винте заскока.

Babel Fish Translation



Translation Software at Work 3

To break Stack For The fun I of the profit:
To alepyu one,
smash `aleph1@underground.org. stack`

[h programming] n. na many vstavk h as far as possible to korrumpirovat' the stack of the performance by way writing after the end of the automobile of that declared by block in the regime. Code makes this they are said, which breaks stack, and it can cause return from the regime to the gallop to randomly the address. This can produce some of the most insidious it is given - .zavisimyx cherepashok znannykh to mankind. Versions vklyuayut trash stack, scribble stack, mangle stack; term mung stack it is not used, as this is never done prednamerenno. See spam; see also alias bug, fandango on the core, the leakage of memory, lossage precedence, the screw of overrun.



Russified Software

RUSSIAN
APACHE



English version

Русский

- koi8-r
- windows
- cp-866
- iso

Russian Apache	Как это работает	Рекомендации	Где взять	Как установить	Как настроить	Статус и поддержка
Краткий обзор	ЧаВО [FAQ]	Список рассылки	Благодарности	Поиск по серверу	Powered by Russian Apache	



Crossing International Borders in Cyberspace

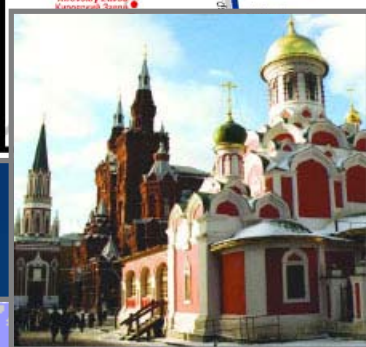
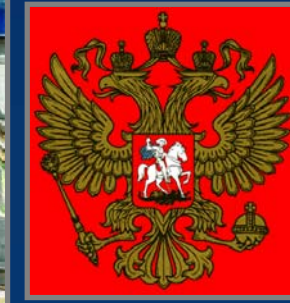
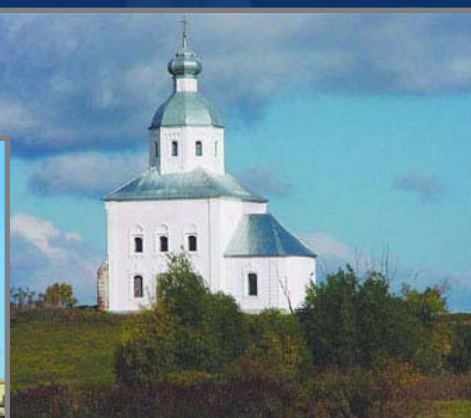


Four T Plan

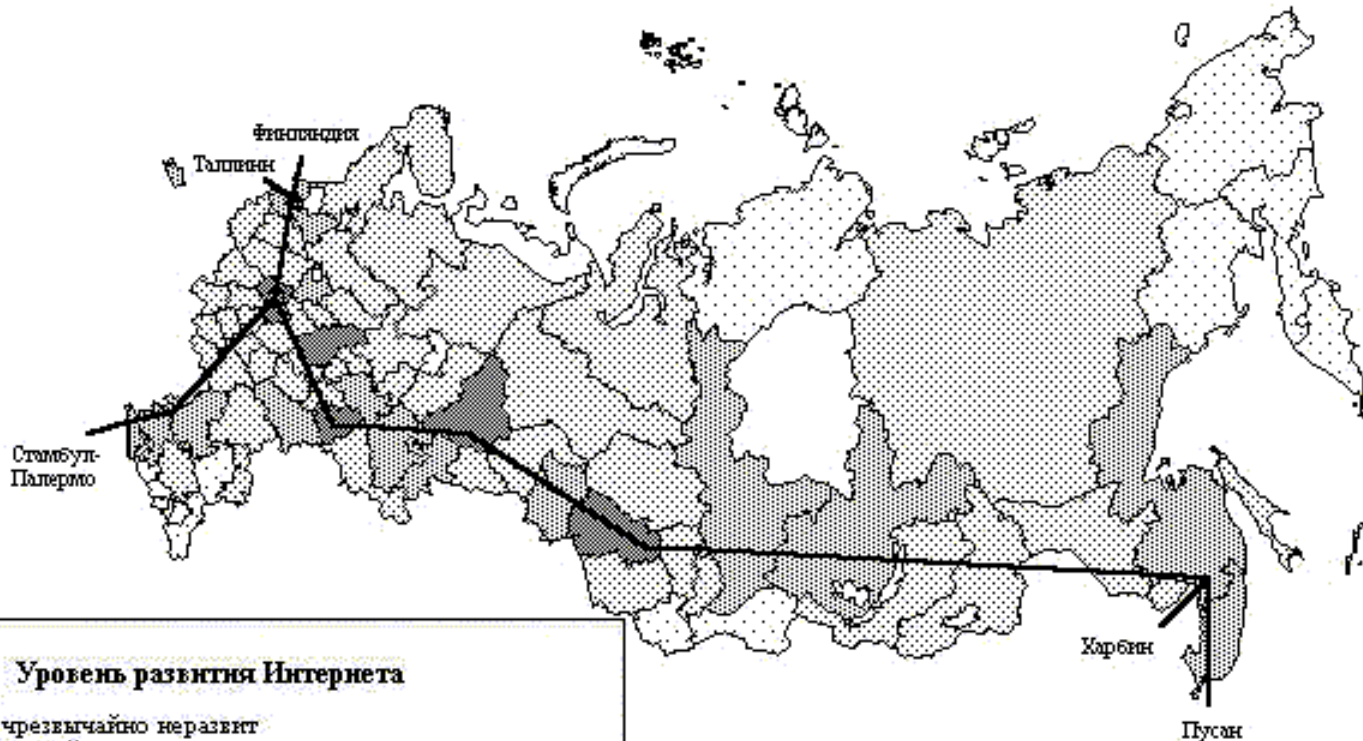
- Tribes
 - Anthropological: history, culture, law
- Terrain
 - Infrastructure: publications, traceroutes
- Techniques
 - Hacker sites, groups, news, malware
- Translation
 - Leveling the playing field



Russia



Rostelecom



Russian Telecommunications

- Internet country codes: .ru, .su
- Internet hosts: 600,000, Users: 6 million
- Telephones: 35.5 mil, Cell: 17.5 mil
 - digital trunk lines: Saint Petersburg to Khabarovsk, Moscow to Novorossiysk
- International connections:
 - three undersea fiber-optic cables
 - 50,000 digital call switches
 - satellite: Intelsat, Intersputnik, Eutelsat, Inmarsat, Orbita
 - International Country Code: 7

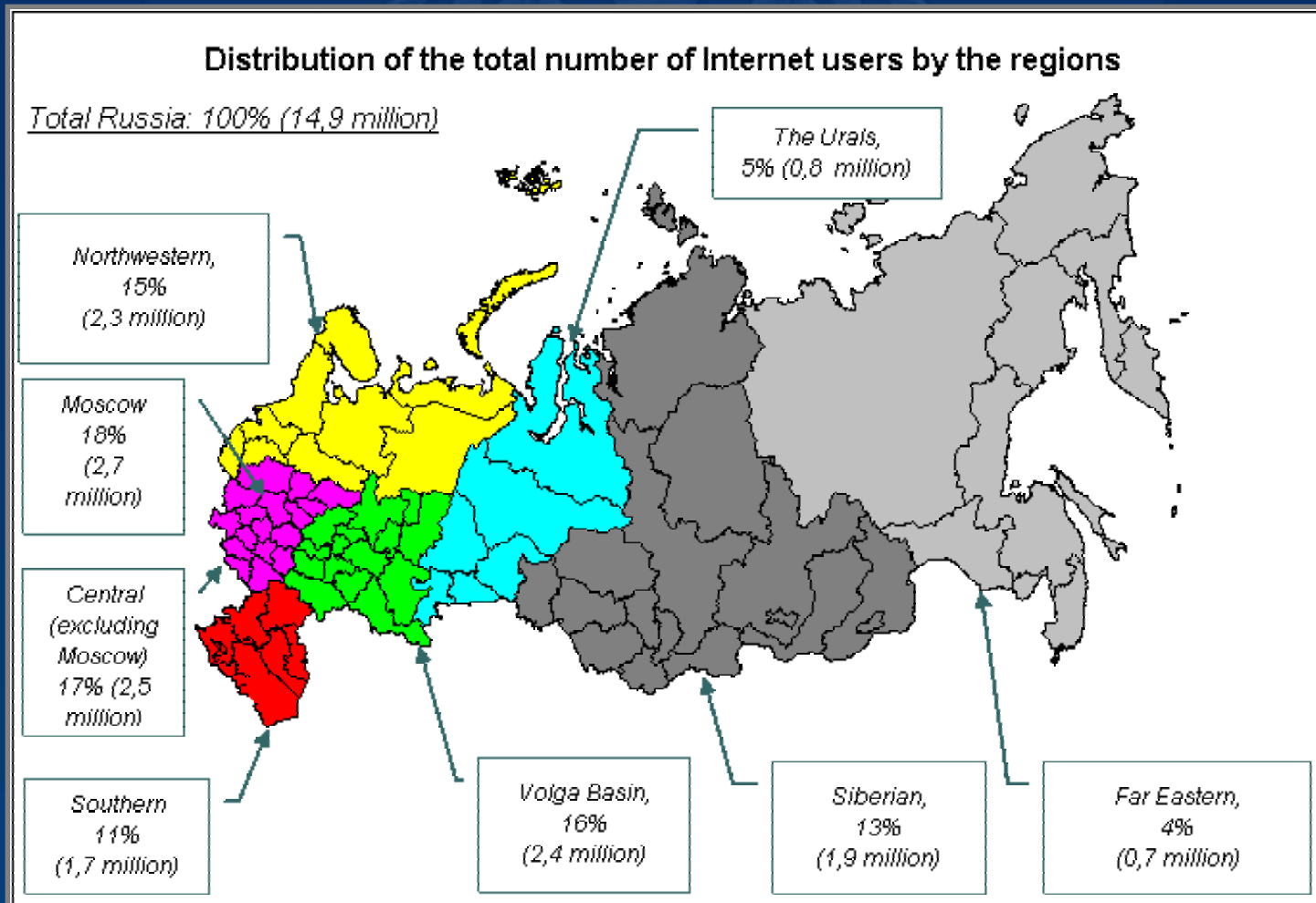


РУНЕТ

- RUNET, or Russian Net
- Russian cyberspace
- Everything Russian AND Internet
- All online content generated in Russian inside Russia
- Aimed at Russian community worldwide
- Includes not just the hackers, but the 'stupid users' as well: чайник and олень (donkey)

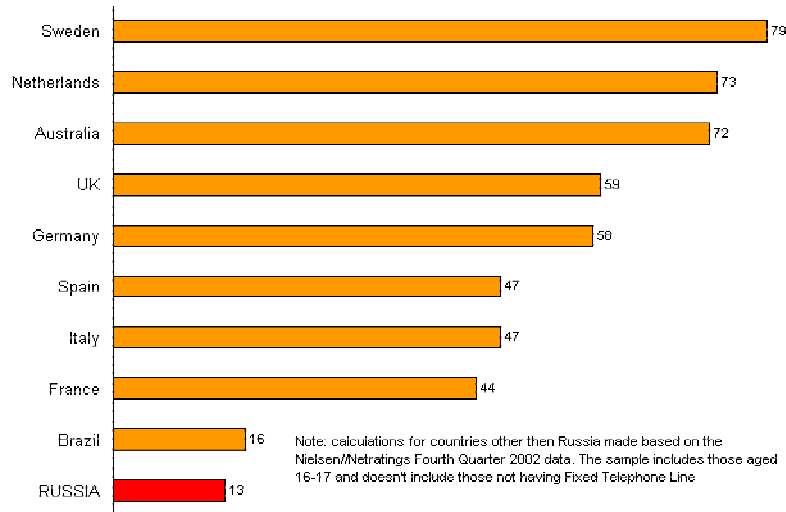


Internet Usage in Russia

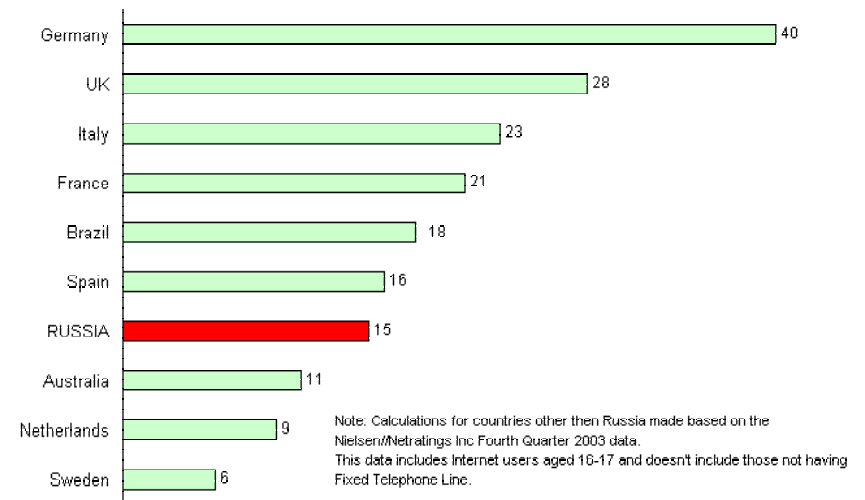


Internet Usage by Country

Percentage of Internet users in the following countries,
% of population



Number of Internet users in the following countries, millions



Rostelecom

Магистральная цифровая сеть ОАО "Ростелеком" на период до 2005 год



Golden Telecom

GOLDEN TELECOM NETWORK TOPOLOGY CIS

SensitRehbidPartners

www.goldentelecom.ru

● All channels ● Terrestrial channels ● Satellite channels ● IP channels



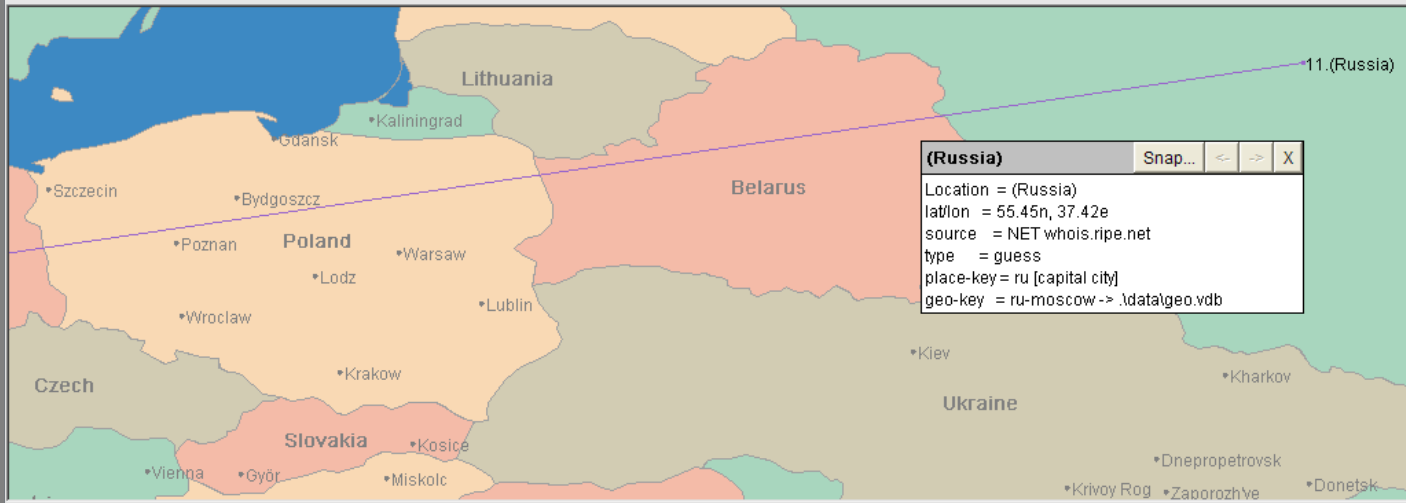
Learning to Fish: Traceroutes

- Maps the routes data travels across networks
- Gives physical locations of Web servers and routers
- Possible to plot these on a map
- Determines connectivity and efficiency of data flow
- Possible to determine who owns the network
- Possible to trace unwanted activity like spam
- Can help in finding contact information
- Can report type of remote computer running



Tracerouting Russia

Report for www.kremlin.ru [194.226.82.50]



IP Address	Node Name	Location	Tzone	Network
192.168.0.3	Bbox37	...		(private use)
65.79.128.1	-	New Castle, DE		Lamont Digital Systems, Inc. LDS
12.124.235.137	-	Middletown, NJ, USA		AT&T Worldnet Services ATTSVI-12-124-154-0-1
12.123.9.42	gbr1-a90s14.wswdc.ip.att.net	Washington, DC, USA	-05:00	AT&T Worldnet Services ATTSVI-12-122-0-0
12.122.11.177	tbr2-p013402.wswdc.ip.att.net	Washington, DC, USA	-05:00	AT&T Worldnet Services ATTSVI-12-122-0-0
12.123.9.117	ggr2-p3120.wswdc.ip.att.net	Washington, DC, USA	-05:00	AT&T Worldnet Services ATTSVI-12-122-0-0
213.248.88.33	ash-bb1-pos2-2-0.telia.net	...		Telia International Carrier
213.248.80.137	nyk-bb2-pos0-3-0.telia.net	...		Telia International Carrier
213.248.64.33	kbn-bb2-pos1-3-0.telia.net	...		Telia International Carrier
213.248.65.30	s-bb2-pos7-0-0.telia.net	...		Telia International Carrier
213.248.65.42	mow-b1-pos1-1.telia.net	...		Telia International Carrier
213.248.99.90	rtcomm-104928-mow-b1.c.telia.net	...		Telia International Carrier
217.106.7.226	msk-dsr0-ge1-0-0-0.rt-comm.ru	(Russia)		RTComm.RU
195.161.2.134				Rostelecom Internet Center
194.226.82.50	www.kremlin.ru	(Russia)		RUSSIAN STATE INTERNET NETWORK

Roundtrip time to 217.106.7.226, average = 152ms, min = 146ms, max = 172ms -- 23.03.2005 22:29:22

[\(Collapse Table\)](#)



TraceReport.bat

```
tracert 303.shkola.spb.ru >tracerpt.txt
```

```
tracert acorn-sb.narod.ru >>tracerpt.txt
```

```
tracert adcom.net.ru >>tracerpt.txt
```

```
tracert admin.smolensk.ru >>tracerpt.txt
```

```
tracert agentvolk.narod.ru >>tracerpt.txt
```

```
tracert alfatelex.tver.ru >>tracerpt.txt
```

```
tracert anarchy1.narod.ru >>tracerpt.txt
```



Traceroute Map of Russia



New York

Stockholm

Kaliningrad



Arkhangelsk

Sakhalin

- 12.123.3.x att.net New York > 193.10.68.x nordu.net Stockholm, Sweden > 193.10.252.x RUN.net Moscow, Russia > 193.232.80.x spb-gw.runnet.ru Federal Center for University Network > 194.106.194.x univ.kern.ru Kaliningrad, Russia (Kaliningrad State University)
- 62.84.193.x Sweden SE-COLT-PROVIDER > 217.150.40.x transtelecom.net Russia > 213.24.60.x artelecom.ru Russia > 80.82.177.x dvinaland.atnet.ru Arkhangelsk, Russia > 80.82.178.x www.dvinaland.ru Arkhangelsk, Russia
- 213.248.101.x telia.net Telia International Carrier > 217.106.5.x RTComm.RU Russia > 195.72.224.x sakhalin.ru Sakhalin, Russia, UBTS, Yuzhno-Sakhalinsk > 195.72.226.x www.adm.sakhalin.ru Sakhalin, Russia (Regional Admin of Sakhalin Island and Kuril's)

Major Russian IP ranges

- 193 .124 .0 .0 – 193 .124 .0 .255 EUnet/RELCOM; Moscow
- 193 .125 .0 .0 – 193 .125 .0 .255 Novosibirsk State Technical University
- 193 .233 .0 .0 – 193 .233 .0 .255 FREEnet NetworkOperations Center
- 194 .67 .0 .0 – 194 .67 .0 .255 Sovam Teleport; Moscow, Russia
- 195 .161 .0 .0 – 195 .161 .0 .255 Rostelecom/Internet Center
- 195 .209 .0 .0 – 195 .209 .15 .255 Russian Backbone Net
- 195 .54 .0 .0 – 195 .54 .0 .255 Chelyabinsk Ctr Scientific and Tech Info
- 212 .122 .0 .0 – 212 .122 .1 .255 Vladivostok Long Dist and Int'l Telephone
- 212 .16 .0 .0 – 212 .16 .1 .255 Moscow State University
- 212 .41 .0 .48 – 212 .41 .0 .63 Siberian Institute of Information Tech
- 212 .6 .0 .0 – 212 .6 .0 .255 WAN and Dial Up interfaces
- 213 .158 .0 .0 – 213 .158 .0 .255 Saint Petersburg Telegraph
- 213 .221 .0 .80 – 213 .221 .0 .83 SOVINTEL SHH NET, Moscow
- 217 .114 .0 .0 – 217 .114 .1 .255 RU SKYNET



Offensive Russian IP Ranges

- Bob's Block List (BBL):
 - Spammers: mail.ru, ufanet.ru, hotmail.ru, nsc.ru, id.ru, all banner.relcom.ru
- www.spamcop.net
 - no Russian IPs listed!
- The Spamhaus Project



Russian Government Portal



ОФИЦИАЛЬНАЯ
РОССИЯ



СЕРВЕР ОРГАНОВ ГОСУДАРСТВЕННОЙ ВЛАСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

03.02.2005

ENGLISH



ПРЕЗИДЕНТ
РОССИЙСКОЙ
ФЕДЕРАЦИИ



ФЕДЕРАЛЬНЫЕ
ОРГАНЫ
ИСПОЛНИТЕЛЬНОЙ
ВЛАСТИ



ФЕДЕРАЛЬНОЕ
СОБРАНИЕ
РОССИЙСКОЙ
ФЕДЕРАЦИИ



СУДЕБНАЯ
ВЛАСТЬ
РОССИЙСКОЙ
ФЕДЕРАЦИИ



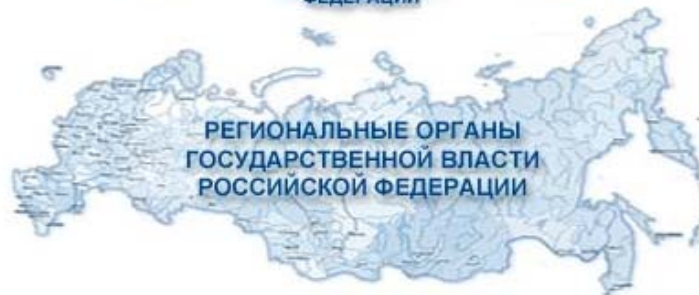
СОВЕТ
БЕЗОПАСНОСТИ
РОССИЙСКОЙ
ФЕДЕРАЦИИ



ЦЕНТРАЛЬНАЯ
ИЗБИРАТЕЛЬНАЯ
КОМИССИЯ
РОССИЙСКОЙ
ФЕДЕРАЦИИ



СЧЁТНАЯ
ПАЛАТА
РОССИЙСКОЙ
ФЕДЕРАЦИИ



www.kremlin.ru

The image shows two overlapping browser windows displaying the website of the President of Russia. The top window is in Russian, titled "Президент России - Mozilla Firefox", and shows the main page with a navigation menu on the left and a central content area. The bottom window is in English, titled "President of Russia - Mozilla Firefox", and shows a similar layout with a navigation menu on the left and a central content area. The English version includes a "direct speech" section with a quote from President Putin and a "news" section with several articles. The Russian version includes a "на сайте" section with news about the 60th anniversary of the victory in the Great Patriotic War and a "тема" section with a photo album and updates.

Президент России - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://president.kremlin.ru/mainpage.shtml
Getting Started Latest Headlines
Сегодня четверг, 3 февраля | Поиск | Карта сайта | English version

Президент России

СОБЫТИЯ
ВЫСТУПЛЕНИЯ
ДОКУМЕНТЫ
ПРИОРИТЕТЫ
ПРЕЗИДЕНТ
ИНСТИТУТЫ
АТРИБУТЫ
ПЕРВОЕ ЛИЦО
ПИСЬМА
К СВЕДЕНИЮ СМИ

Главное
Новости
График Президента
Совещания, заседания, встречи
Внешнеполитические мероприятия
Пресс-конференции, встречи с прессой
Досье событий

на сайте

28 января
Выступление на заседании Совета Безопасности >

28 января
Об обращении граждан на тему замены натуральных льгот денежными выплатами >

>>> Все обновления

тема

DISCOVERING THE KREMLIN

PHOTO ALBUM

THE PRESIDENT-TO SCHOOL-AGE CITIZENS

updates

January 27
Speech at the Memorial Ceremony Dedicated to the 60th Anniversary of the Liberation of the Nazi Concentration Camp of Auschwitz-Birkenau >

January 17
Speech at a Meeting with the Government >

>>> All updates

President of Russia - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://president.kremlin.ru/eng/
Getting Started Latest Headlines
Today is February 3, Thursday | Search | Site map | Russian version

President of Russia

February 2, 2005, Moscow, Kremlin.
"The central event in our relations this year will be the visit by Mr Hu Jintao to Russia. We are expecting him to visit for the 60th anniversary of Victory in the Great Patriotic War."
Meeting with member of the State Council of China Tan Jiaxuan
>>> All speeches

in the spotlight

February 2, 2005 14:00
Vladimir Putin met with a member of the State Council of China, Tan Jiaxuan. >

February 2, 2005 13:30
At the Emergency Ministry, the President held a meeting on the liquidation of the consequences of the tsunami in South-East Asia. >

February 1, 2005 16:40
President Vladimir Putin met with Director of the Federal Service for Military-Technical Cooperation Mikhail Dmitriyev. >

>>> All news

news

February 2, 2005
The consequences of the tsunami in South-East Asia make it necessary to think about how to organise work in predicting such catastrophes in Russia. >

views

The 60th Anniversary of the Allied Landing in Normandy >

events files

January 27 - 28, 2005
Krakow, Poland
The 60th Anniversary of the Liberation of Auschwitz >



Russian Cyber Crime Office

CYBERNETIC POLICE
Компьютерная преступность и борьба с нею

Наберите номер телефона !

Understanding C. Crime
Понятие и классификация компьютерных преступлений

Information Protection Laws
Законодательство в сфере информации, информатизации и защиты информации

Information Security in Russia
Система защиты информации в России

Send an E-mail
Почтовая служба "Киберпола"

Forum
Форум

Library
Библиотека публикаций

SORM
Понятие и назначение "СОПМ"

C. Crime Units
Подразделения по борьбе с компьютерными преступлениями в России

Computer Criminals
Всё о компьютерных правонарушителях

Anthology
Антология компьютерных преступлений в России

Новости борьбы с киберпреступностью

"Справочная служба"

(C) CyberCop, 2004

10338
Sp ioG
20
1

“Cybernetic Police”: <http://www.cyberpol.ru/>
cybercop@cyberpol.ru



Киберполиции: Cybernetic Police



Official Russian Designations



кардеры (от английского слова "**card**") - лица, специализирующиеся на незаконной деятельности в сфере оборота пластиковых карт - документов на машинном носителе и их электронных реквизитов.

фрэкеры (от английского слова "**phreaker**") - лица, специализирующиеся на совершении преступлений в области электросвязи с использованием конфиденциальной компьютерной информации и специальных технических средств разработанных (приспособленных, запрограммированных) для негласного получения информации с технических каналов

крэкеры (от английского слова "**cracker**") - лица, занимающиеся "взломом" (модификацией, блокированием, уничтожением) программно - аппаратных средств защиты компьютерной информации, охраняемых законом



C. Crime: Statistics to 1982!



ОФИЦИАЛЬНАЯ СТАТИСТИКА КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ,
СОВЕРШЕННЫХ В РОССИЙСКОЙ ФЕДЕРАЦИИ

(по данным ГИЦ МВД России)

АНТОЛОГИЯ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ,
СОВЕРШЕННЫХ В РОССИЙСКОЙ ФЕДЕРАЦИИ

1982	1983	1985	1988	1991	1992	1993	1994
1995	1996	1997	1998	1999	2000	2001	2002
2003	2004	2005	2006				



Russian Cyber Crime Fighter

Ф.И.О.: Вехов Виталий Борисович

Ученая степень и звание: кандидат юридических наук, доцент, подполковник милиции.

Место работы: Волгоградская Академия МВД России, факультет повышения квалификации, кафедра организации следственной работы.

Тема кандидатской диссертации: Криминалистическая характеристика и совершенствование практики расследования и предупреждения преступлений, совершаемых с использованием средств компьютерной техники. – Волгоград., 1995.

Область научных интересов: методика выявления, раскрытия, расследования и предупреждения компьютерных преступлений; криминалистическое компьютероведение; использование компьютерных технологий в деятельности органов предварительного расследования; защита информации; техническая разведка; радио-электронная борьба.

Научные труды: более 40 опубликованных работ. В том числе 2 монографии, 2 учебно-практических и 4 учебно-методических пособия, 3 примерных методических программ для вузов МВД, главы в учебниках (список [опубликованных работ](#)).

E-mail: Vehov@avtlg.ru

Web: www.cyberpol.ru - автор проекта





Dialogue with Top Cyber Cop

Здравствуйте, уважаемый Kenneth Geers!

Можем дать следующие ответы на Ваши вопросы.

Вопрос: Получали ли вы в прошлом запросы об информации из-за рубежа?

Ответ: Да. Каждый день 89 подразделений Национального центрального бюро Интерпола России (89 divisions of a National central bureau of Interpol of Russia) по E-mail получают и обрабатывают много поручений и запросов от правоохранительных организаций стран - членов Международной организации уголовной полиции Interpol.

Вопрос: Что мешает улучшению международного сотрудничества?

Ответ: Разные правовые нормы в действующих национальных законодательствах. Требуется их частичная унификация.

Вопрос: Вы думаете было-бы трудно найти общую почву чтобы поделиться информацией?

Ответ: По международным соглашениям мы без особых проблем обмениваемся разведывательной и иной информацией о преступлениях и правонарушениях со специальными службами зарубежных государств. В последнее время часто проходят совместные совещания, семинары и конференции наших сотрудников с сотрудниками FBI (USA).

Вопрос: Вы думаете что боязнь утери национального суверенитета –непреодолимое препятствие?

Ответ: Обмен информацией на основе двухстороннего или многостороннего Договора (юридического акта) не опасен для национального суверенитета.

Спасибо за вопросы. Были рады Вам помочь.

Кем (по какой специальности) Вы работаете?

С уважением,

Виталий Вехов



Несколько Вопросов

К кому я могу обратиться по поводу гарантии информации?

To whom should I direct questions on information assurance?

Каким образом я должен доложить о подозрительных действиях в сети?

How should I send you suspicious network information?

Это представляет угрозу Windows/Linux/Solaris?

Does this pose a threat to Windows/Linux/Solaris?

Когда последний раз вы сделали дубликаты своих данных?

When is the last time you backed up your data?

Вы сможете нарисовать мне диаграмму/карту вашей сети?

Can you draw me a diagram of your network?

Вы думаете что эта угроза была направлена лично против меня?

Do you think this threat was directed at me personally?



Киберполиции: Regional Offices

http://ndki.narod.ru/links/MVD_online.html



Республики:

Отдел "Р" МВД Республики Горный Алтай: [Altay](#)

Отдел "К" МВД Республики Мордовия: [Mordoviya](#)

МВД Республики Татарстан: [Tatarstan](#)

Отдел "К" МВД Республики Чувашия: [Chuvashiya](#)

Края:

Отдел "К" УСТМ ГУВД Алтайского края: [Altay](#)

Отдел "К" ГУВД Красноярского края: [Krasnoyarsk](#)

Отдел "К" УВД Приморского края: [Primorskiy](#)

Отдел "К" УВД Ставропольского края: [Stavropol](#)

Области:

Отдел "К" УВД Архангельской области: [Arkhangel'sk](#)

Отдел "Р" УВД Владимирской области: [Vladimir](#)

УФСБ России по Воронежской области: [Voronezh](#)

Отдел "Р" УВД Кировской области: [Kirov](#)

Отдел "К" УВД Костромской области: [Kostroma](#)

Отдел "К" УВД Липецкой области: [Lipetsk](#)

Отдел "К" ГУВД Нижегородской области: [Nizhniy](#)

Отдел "Р" УВД Новгородской области: [Novgorod](#)

Отдел "К" УВД Оренбургской области: [Orenburg](#)

Отдел "К" ГУВД Самарской области: [Samara](#)

Отдел "Р" УВД Тамбовской области: [Tambov](#)

Отдел "Р" УВД Тульской области: [Tula](#)

Отдел "Р" УВД Ульяновской области: [Ul'yanovsk](#)

Отдел "К" УВД Читинской области: [Chita](#)

Автономные округа:

Отдел "К" УВД Ханты-Мансийского АО: [Khanty-Mansi](#)

International Law Enforcement

Links at Cyber Criminals Most Wanted Website (www.ccmmostwanted.com) for 67 countries (* = cybercrime laws in place):

Andorra, Argentina*, Australia*, Austria*, Belgium*, Brazil*, Brunei, Canada*, Chile*, China*, Czech Republic*, Denmark*, Fiji, Finland*, France*, Georgia, Germany*, Greece*, Guam, Hong Kong, Hungary*, Iceland*, India*, Indonesia, Iran, Ireland*, Israel*, Italy*, Jamaica, Japan*, Jordan, Korea - North*, Korea - South*, Latvia*, Lebanon, Liechtenstein, Luxembourg*, Malaysia*, Malta*, Mexico*, Netherlands*, Nigeria, New Zealand*, Norway*, Pakistan, Peru, Philippines*, Poland*, Portugal*, Puerto Rico, Russia*, Singapore*, Scotland, Slovenia, South Africa*, Spain*, Sweden*, Switzerland*, Taiwan, Thailand, Trinidad, Turkey*, Uganda, Ukraine, United Kingdom*, United States*, Uruguay, Yugoslavia

Links to UK websites include:

[Child Pornography](#)

[Consumer Protection](#)

[Cramming](#)

[Cyber Rights & Civil Liberties](#)

[Financial Services Authority](#)

[Harmful or illegal website content](#)

[Internet Police](#)

[Internet Watch Foundation](#)

[Missing Kids](#)

[National Crime Squad](#)

[Specialist Crime OCU Fraud Squad](#)

[National Criminal Intelligence Service](#)

[National High-Tech Crime Unit](#)

[Nigerian Scams](#)

[Pedophile Activity - Newsgroup](#)

[Pedophile Activity - Website](#)

[Pyramid Schemes](#)

[Serious Fraud Office](#)

[Victim Support](#)



Russian Malware



Kaspersky Labs



- Highly respected anti-virus lab
- 15+ years anti-virus and spyware R&D
- Accuracy and frequency of updates (hourly!) well-regarded
- Former Soviet military researcher
- Say “criminal elements” now responsible for 90% of malicious code
- Says more cyber crime from Brazil than Russia...
- The most hated man by Russian hackers...
- Connections to law enforcement?



www.antispam.ru

ANTISPAM.RU

[О спаме](#) [Пользователям](#) [Специалистам](#) [Статьи](#)
[Программы](#) [Ссылки](#) [Поиск на сервере](#) [О проекте](#)

"Reading Email Headers"

www.samspade.org

cyberpolice.ru

netlaw.ru

www.nospam.spb.ru

www.jmls.edu/cyber/cases/spam.html

www.ezhe.com/ses/index.html

Документ, в котором очень подробно и грамотно

рассказывается

интересная сис

генерации отчет

Если Вы устали от спама и спамеров - эта

статья поможет Вам

Здесь можно отправить нам новость для

размещения на АНТИСПАМ.РУ

Подписаться на рассылку новостей

(правила)

Ваш email

Подписаться!

Сетевое законод

У сервера есть

этой тематике

Спам в России

Неплохая попытка сделать актуальными русскоязычными

проект о борьбе со спамом

Судебные дела против спамеров (на англ. языке)

Большое количество описаний реальных судебных дел,

размещенное на сервере Юридической Школы Джона

Маршалла (США).

Спамэпидемстанция

ANTISPAM.RU

[О спаме](#) [Пользователям](#) [Специалистам](#) [Статьи](#)
[Программы](#) [Ссылки](#) [Поиск на сервере](#) [О проекте](#)

Если Вы устали от спама и спамеров - эта
статья поможет Вам

Здесь можно отправить нам новость для
размещения на АНТИСПАМ.РУ

Подписаться на рассылку новостей
(правила)

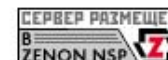
Ваш email

Подписаться!

Поиск на сайте

Что ищем?..

Искать!



Посетителей:
345582



English-Russian Hacker Lexicon

<u>English</u>	<u>Русский</u>	<u>Pronunciation</u>
account	<u>аккаунт, акк</u>	account
banner	<u>баннер</u>	banner
blog	<u>блог</u>	blog
browser	<u>браузер</u>	browser
cash, cache	<u>кеш</u>	cash
chat	<u>чат</u>	chat
domain	<u>домен</u>	domain
e-mail	<u>электронная почта</u>	<u>elektronaya pochta</u>
flame	<u>флэйм, флейм</u>	flame
host, hosting	<u>хост, хостинг</u>	host, hosting
java, javascript	<u>жаба, жабаскрипт</u>	<u>zhaba, zhabascript</u>
hacker	<u>хакер, хэкер</u>	hacker
Internet	<u>интернет</u>	internet



English-Russian Hacker Lexicon

<u>English</u>	<u>Русский</u>	<u>Pronunciation</u>
login	ЛОГИН	logeen
nick	НИК	neek
patch	ПАТЧ	patch
programme	программа, прога	programa, proga
screenshot	скриншот	screenshot
server	сервер	server
site	сайт	site
spam	СПАМ	spam
tools	тулза	toolza
user	юзер	user
warez	варез	vaarez
web	веб	veb
zip	ЗИП	zeep



Local Cyber News

- Reading the local newspapers
 - <http://www.gazeta.ru>
 - <http://www.lenta.ru>
 - <http://www.kommersant.ru>
 - <http://www.itogi.ru>
 - <http://www.izvestia.ru>
 - <http://www.mn.ru>
 - <http://www.mk.ru>
 - “...Putin keen to set up IT park...efforts underway to identify site...potential for much cooperation with India...”



One Word

English, German, Italian, Portuguese,
and Norwegian: Hacker

Russian: хакер

Dutch: De computerkraker, hakker

Arabic: El Qursan ('Pirate')

Hebrew: האקר

Chinese: 电脑黑客

Spanish: pirata informático

Korean: 해커

Japanese: ハッカー

Greek: χάκερ

French: Fouineur, bidouilleur



The International Political Scene



International Law

- Currently ill-suited for cybercrime
- Internet a borderless medium
 - Cannot apply nation-state style borders
- Definitions of cybercrime vary
 - Likewise the punishments
- Extradition of criminals
 - Difficult on many levels
- Bounty hunting: Microsoft
- Tapping fan-base: Half-Life 2



Extra-Territoriality and Cybercrime

- Impossible to examine all foreign packets
- High level of anonymity on the Web
- Scarcity of good log data (and expertise)
- Digital information can be destroyed quickly
- Evidence should be secured ASAP
- Cultural, linguistic, and political barriers
- Traceback involves time lags



The FBI Sting

- 2000: FBI learns hackers cracking banks, ISPs, and other firms in U.S.
- Activity traced to Russia
- Failed to acquire Russian assistance
- Took unilateral action with U.S. search warrant
- Invited two Russians to Seattle for interviews
- Sniffed keystrokes for usernames/passwords
- FBI officials never left their offices in U.S.
- First FBI extra-territorial seizure



European Cybercrime Convention

- Global cybercrime task force like Interpol?
- Opposition concerns:
 - Civil liberties (abuse of data sharing)
 - Poor relations between certain countries
 - Big obligations on ISPs
 - No cross-border searches, even in hot pursuit
 - Need to consult with local officials
 - Universal consent (safe havens)



Remote Search and Seizure

- Inconsistent with international law?
- Reconnaissance often uses universal media for observation in other countries
 - Binoculars, telescopes, surveillance aircraft, commercial satellites
 - personal interviews, mass media
- Network recon any different?
 - No physical entry
- Invasion or picture taking?



International Law: The Future

Voluntary participants need three things:

- Technological capability
- Legal authority
 - Territorial Sovereignty
- Willingness to Cooperate
 - Including ability: language, cultural political barriers
 - PRC CERT: One person, and he only speaks Chinese?!?



Спасибо



ARTWORK by
Len Gostinsky:
len@bitstream.net

References

- Aleph One. "Smashing The Stack For Fun And Profit." *Phrack 49*, Volume Seven, Issue Forty-Nine, File 14 of 16. Available: <http://www.insecure.org/stf/smashstack.txt>.
- Banisar, David. "Cybercrime treaty still horrible." *SecurityFocus*. December 14, 2000 8:00PM. Available: <http://www.securityfocus.com/news/124>.
- Billo, Charles and Welton Chang. *Cyber Warfare: An Analysis of The Means And Motivations of Selected Nation States*. Institute For Security Technology Studies, Dartmouth College. Revised. December 2004.
- Blau, John. "Viruses: From Russia, With Love?" IDG News Service, Friday, May 28, 2004. Available: <http://www.pcworld.com/news/article/0,aid,116304,pg,2,00.asp>
- Brunker, Mike. "FBI agent charged with hacking, Russia alleges agent broke law by downloading evidence." *MSNBC*. August 15, 2004. Available: <http://www.msnbc.com/news/563379.asp?cp1=1>.
- Delio, Michelle. "Inside Russia's Hacking Culture." March 12, 2001. Available: <http://www.wired.com/news/culture/0,1284,42346,00.html>.
- Federal Bureau of Investigation. "FBI Says Web 'Spoofing' Scams are a Growing Problem." Press Release. July 21, 2003. Available: <http://www.fbi.gov/pressrel/pressrel03/spoofing072103.htm>.
- Freeh, Louis J. "Before 9/11 -- and After." Op-Ed. *Wall Street Journal*. April 12, 2004. Available: http://ctstudies.com/Document/Freeh_WSJ_OPED_12APR04.html.
- Gebhardt, Bruce. Deputy Director, FBI. Speech to the International Security Management Association, Scottsdale, Arizona, January 12, 2004. Available: <http://www.fbi.gov/pressrel/speeches/gebhardt011204.htm>.
- Goldsmith, Jack. "The Internet and the Legitimacy of Remote Cross-Border Searches." *Public Law And Legal Theory Working Paper No. 16*, The Law School, University of Chicago. Available: <http://www.law.uchicago.edu/academics/publiclaw/resources/16.JG.Internet.pdf>.
- Ilett, Dan: "Russia's cybercrime-fighting Bond villain." *ZDNet UK*. January 13, 2005. Available: <http://www.zdnet.com.au/insight/security/0,39023764,39177092,00.htm>.
- "Key-loggers rip off eBay users." *ContractorUK*. January 18, 2005. Available: <http://www.contractoruk.com/news/001903.html>.
- Kvarnström, Håkan. "Attitudes toward computer hacking in Russia." Lecture notes in Information Warfare in *CyberCrime*, September 3, 2001. Available: http://www.cs.kau.se/~stefan/IW/CC_4-5.pdf.
- Legelis, Kim. "Combating Online Fraud: An Update." Symantec Corporation. Available: <http://information-integrity.com/article.cfm?articleid=100>.
- Leyden, John. "Chinese puzzle hampers banks' phishing fight." *The Register*. November 3, 2004, 8:58AM. Available: <http://www.securityfocus.com/news/9849>.
- Leyden, John. "Four charged in landmark UK phishing case." *The Register*. October 15, 2004 7:54AM. Available: <http://www.securityfocus.com/news/9731>.



Leyden, John. "Gone Phishin'," *The Register*. October 30, 2003, 8:36AM. Available: <http://www.securityfocus.com/news/7331>.

Leyden, John. "IE patch 'imminent'." *The Register*. July 30, 2004, 7:41AM. Available: <http://www.securityfocus.com/news/9245>.

Leyden, John. "US credit card firm fights DDoS attack." *The Register*. September 23, 2004, 8:00AM. Available: <http://www.securityfocus.com/news/9570>.

Mosnews. "Russian Anti-Virus Maker Kaspersky Lab Launches into U.S. Market." (Feb 2, 2005) Available: <http://www.mosnews.com/money/2005/02/08/kaspersky.shtml>.

"Most Web Users Safe As Major Net Attack Slows." Available: Available: <http://www.crn.com/sections/breakingnews/dailyarchives.jhtml?articleId=22102320>.

O'Flynn, Kevin. "Canadian Helps Bust Bride Scam." March 5, 2005. Available: <http://www.themoscowtimes.com/stories/2005/03/05/012.html>

Orlowski, Andrew. "Elcomsoft not guilty - DoJ retreats from Moscow." *The Register*. December 18, 2002 6:51AM. Available: <http://www.securityfocus.com/news/1867>.

Poulsen, Kevin. "Spy suspect had skillz." *SecurityFocus*. February 22, 2001. Available: <http://www.securityfocus.com/news/157>.

Rocich.ru. "Картирование Рунета." Available: <http://rocich.ru/article/5>.

"Rostelecom," Russia Today: Business and Economy. Available: http://www.russiatoday.ru/en/biz/business/lead_com/3181.html.

Russian Apache. Available: <http://www.web.ru/Resource/>.

Saytarly, Timofey. "Russia: cyber crime doubled in 2003." Computer Crime Research Center. January 30, 2004. Available: <http://www.crime-research.org/news/2004/01/Mess3004.html>.

Sherriff, Lucy. "Spam villains: named and shamed." *The Register*. February 27, 2004, 8:21AM. Available: <http://www.securityfocus.com/news/8143>.

Srinivasan, Arun. "Combating Cyberterrorism: How to avoid the scourge of a denial-of-service (DOS) attack." *Line 56*. February 01, 2005. Available: <http://www.line56.com/articles/default.asp?ArticleID=6315>.

Srinivasan, Arun. "Combating Cyberterrorism: How to avoid the scourge of a denial-of-service (DOS) attack." *Line 56*. February 01, 2005. Available: <http://www.line56.com/articles/default.asp?ArticleID=6315>.

"The Internet in Russia." The Public Opinion Foundation Database. 7th Release, Spring 2004. Available: <http://bd.english.fom.ru/report/map/eo040701>.

U.S. Congress. Senate Committee on Appropriations. "Cybercrime." Testimony by Louis J. Freeh, Director, FBI. February 16, 2000.



- U.S. Congress. Senate Judiciary Committee and House Judiciary Committee. "Cybercrime." al Testimony by Michael A. Vatis, Director, National Infrastructure Protection Center, FBI. February 29, 2000.
- U.S. Congress. Senate Judiciary Committee. "Cybercrime." Testimony by Louis J. Freeh, Director, FBI. March 28, 2000.
- U.S. Congress. Senate Judiciary Committee. "NIPC Cyber Threat Assessment, October 1999." Testimony by Michael A. Vatis, Director, National Infrastructure Protection Center, FBI. October 6, 1999.
- U.S. Department of Justice. "Defendant Indicted in Connection with Operating Illegal Internet Software Piracy Group." Press Release. March 12, 2003. Available: <http://www.cybercrime.gov/griffithsIndict.htm>.
- U.S. Department of Justice. "Russian National Enters into Agreement with the United States on First Digital Millennium Copyright Act Case." Press Release. December 13, 2001. Available: <http://www.cybercrime.gov/sklyarovAgree.htm>.
- U.S. Department of Justice. "First Indictment Under Digital Millennium Copyright Act Returned Against Russian National, Company, in San Jose, California." August 28, 2001. Available: <http://www.cybercrime.gov/Sklyarovindictment.htm>.
- U.S. Department of Justice. "Operation Buccaneer: Illegal 'warez' organizations and Internet piracy." Last updated July 19, 2002. Available: <http://www.cybercrime.gov/ob/OBorg&pr.htm>.
- U.S. Department of Justice. "Valley Man Indicted in International Software Piracy Scheme." Press Release. November 26, 2003. Available: <http://www.cybercrime.gov/stjohnIndict.htm>.
- "Volga to Ganga." *The Times of India*. January 28, 2005. Available: <http://timesofindia.indiatimes.com/articleshow/1002829.cms>.
- Справочная служба русского языка. Available: <http://www.rusyaz.ru/is/ns/>.





National Security Archive,
Suite 701, Gelman Library, The George Washington University,
2130 H Street, NW, Washington, D.C., 20037,
Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu