Антивирусная защита

Автор: Русинов А.С.
Сайт: rusinov.net
Версия: 1.5

Что могут сделать вирусы?

- Удалить все файлы
- Отсылать с вашего компьютера знакомым письма с вирусами
- Украсть важную информацию (ваши логины и пароли от посещаемых вами сайтов, номера кредитных карт и др. информацию)
- Ваш компьютер может стать участников атаки злоумышленников на другие компьютеры
- Замедлить или нарушить работу Windows
- И многое другое

Способы распространения

Через сеть-Интернет

- При посещении сайтов
- Рассылка через социальные сети (вконтакте, одноклассники, facebook)
- Присланные через почту, icq,skype … файлы, которые сам запускает пользователь
- При загрузки вируса на ваш компьютер без вашего ведома

Передача зараженных носителей

- Присоединение зараженного диска, флешки и др. к вашему компьютеру

Способы распространения. Через сеть-Интернет

Статистика заражения в сети-интернет

- Google - Каждая десятая страница, содержит программы-вирусы (2007 год)
- McAfee – 10.1% зараженных сайтов в зоне .ru (по сравнению с 2009 годом, в 2010 году количество зараженных сайтов увеличилось на 116,7 процентов)

Способы распространения. Через сеть-Интернет

Официальные зараженные сайты

- Википедия, 2006 год
- Microsoft (на сайте зараженная программа Windows Live Messenger), 2007 год
- ESET NOD32 Russia, 2009 год
- Департамент культуры города Москвы, 2010 год
- Федеральное агенство морского и речного транспорта (повторные заражения: 178 раз), 2010 год
- Организации объединенных наций (ООН), 2010 год
- Департамент казначейства США, 2010 год
- …

Here comes your

Способы распространения. Передача носителей.

Известные случаи

- iRiver – продажа зараженных плееров (2004 год)
- Seagate – партия внешних жестких дисков (1800 штук) заражена вирусом Virus.Win32.AutoRun.ah (2007 год)
- IBM – раздала зараженные флешки на конференции по безопасности IBM AusCERT (2010 год)

Популярные вирусы

2010 год

Примеры вирусов. Ложные архивы.

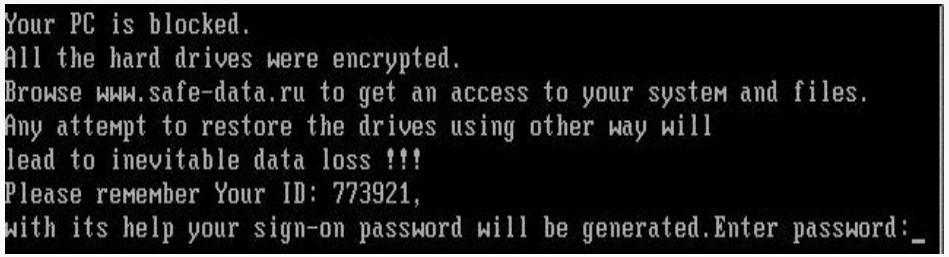
Ложные архивы

- Часто встречаются в сети-интернет
- Реальная стоимость sms от 250 до 360 рублей
- Пользователь после оплы ты не получает желаемой информации
- Как правило при запуске происходит заражение компьютера вирусом

Here comes your

Примеры вирусов. Загрузочные блокировщики.

Загрузочные блокировщики

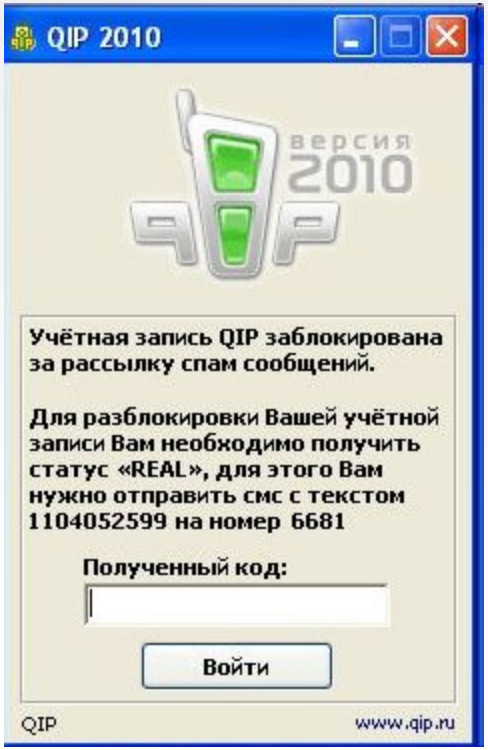


- Загружается до загрузки операционной системы
- Для разблокировки требуют от 50 у. е. и выше

Here comes your

Примеры вирусов. Блокировщики запуска IM – клиентов.

Блокировщики запуска IM-клиентов

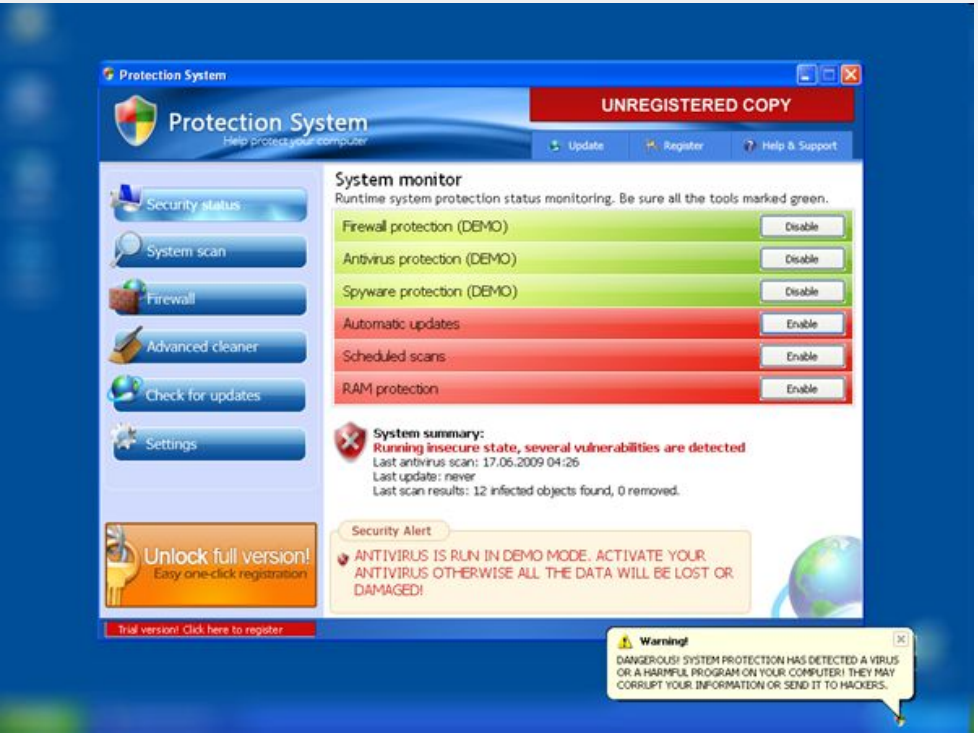


- Заражаются клиенты ICQ, QIP и Skype
- При запуске открывается похожая программа (вирус) и просит отослать платную sms

Here comes your

Примеры вирусов. Лжеантивирусы.

Лжеантивирусы

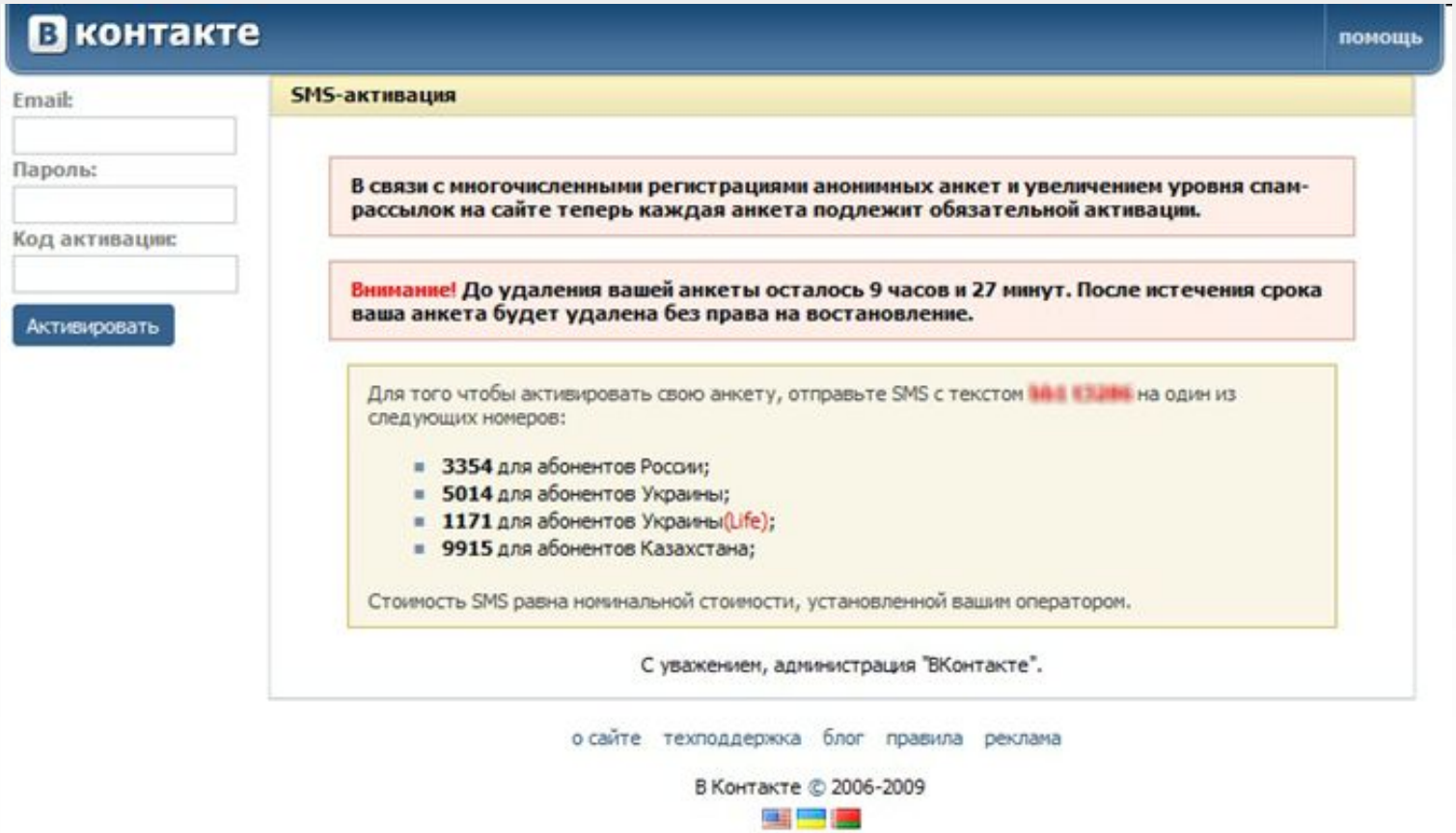


- Внешне похожи на антивирусное ПО
- «Антивирусы» сразу же сообщают о том, что система якобы заражена
- «Антивирусы» просят приобрести профессиональную версию “антивируса”
- Иногда угрожают уничтожением информации с жесткого диска

Here comes your

Примеры вирусов. Редиректоры.

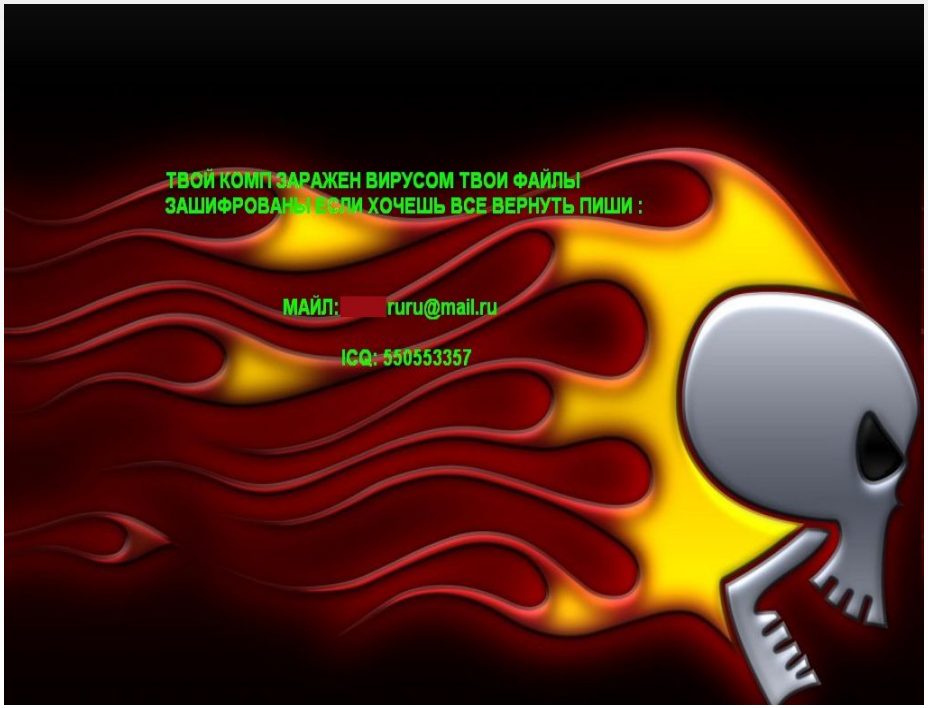
Редиректоры на вредоносные и мошеннические сайты



Here comes your

Примеры вирусов. Шифровальщики данных.

Шифровальщики данных



- Шифрует данные на компьютере
- Пользователь не имеет доступа к данным
- За расшифровку требуют от 50 у.е. и выше

Here comes your

Примеры вирусов. Блокировщики Windows.

Блокировщики Windows

- Пользователь лишается возможности работать за компьютером
- Требуют оплатить сумму под любым предлогом
- Реальная стоимость sms от 250 до 360 рублей
- Замечено: некоторые вирусы удаляются сами после 2 и более часов (максимальный срок был 2 недели)

Основные способы защиты

Основные способы защиты

Что необходимо сделать для защиты?

1. Установить антивирус
2. Установить фаервол (брандмауэр, межсетевой экран)
3. Отключить автозапуск
4. Создать ограниченную пользовательскую учетную запись и работать под ней
5. Использовать безопасный браузер
6. Соблюдать простые правила безопасности

Установка антивируса и фаервола

Установка и настройка COMODO Internet Security.

1. ПросмотретьПросмотреть видео установки
2. Просмотреть видео начальной настройки

Here comes your

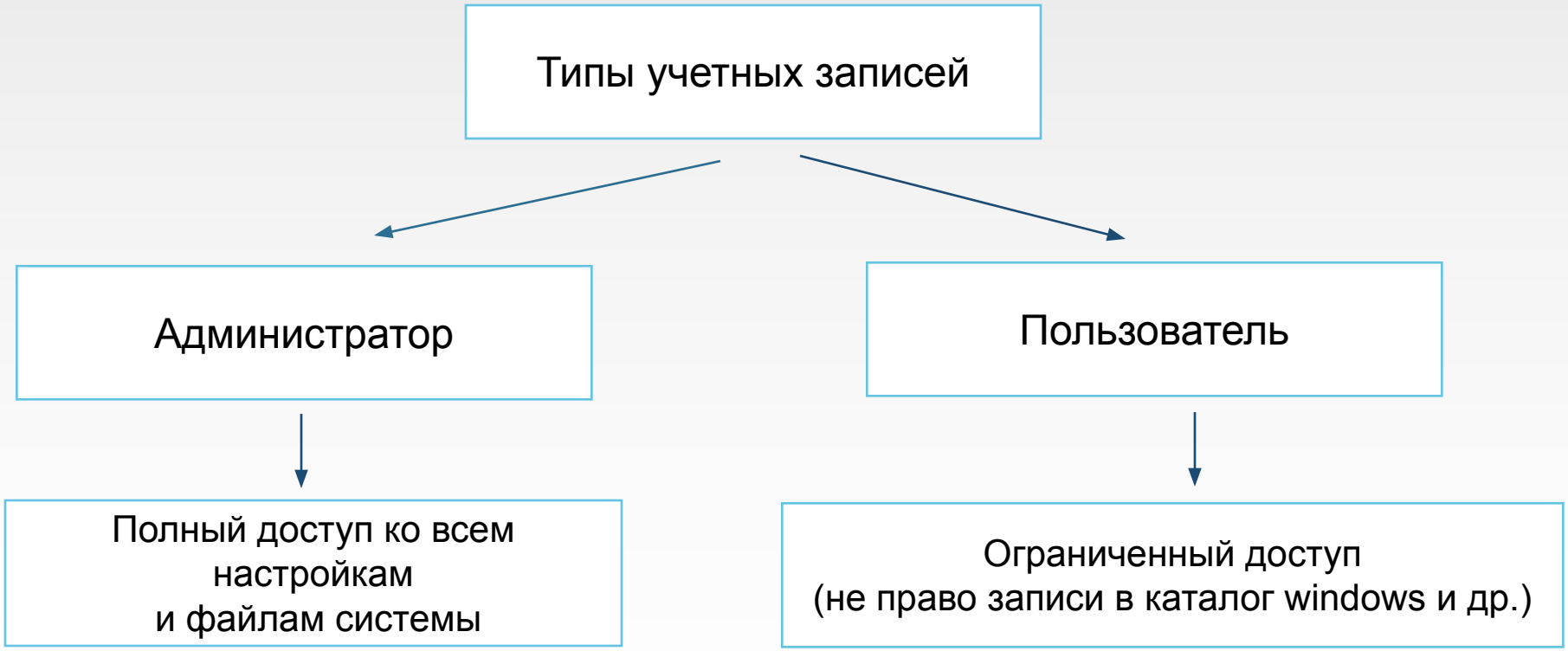
Защита флешек

Отключение автозапуска флешек:

- Скачать и установить Panda USB and AutoRun Vaccine
- После установки нажмите кнопку “Vaccinate computer”.

Here comes your

Создание ограниченной пользовательской учетной записи

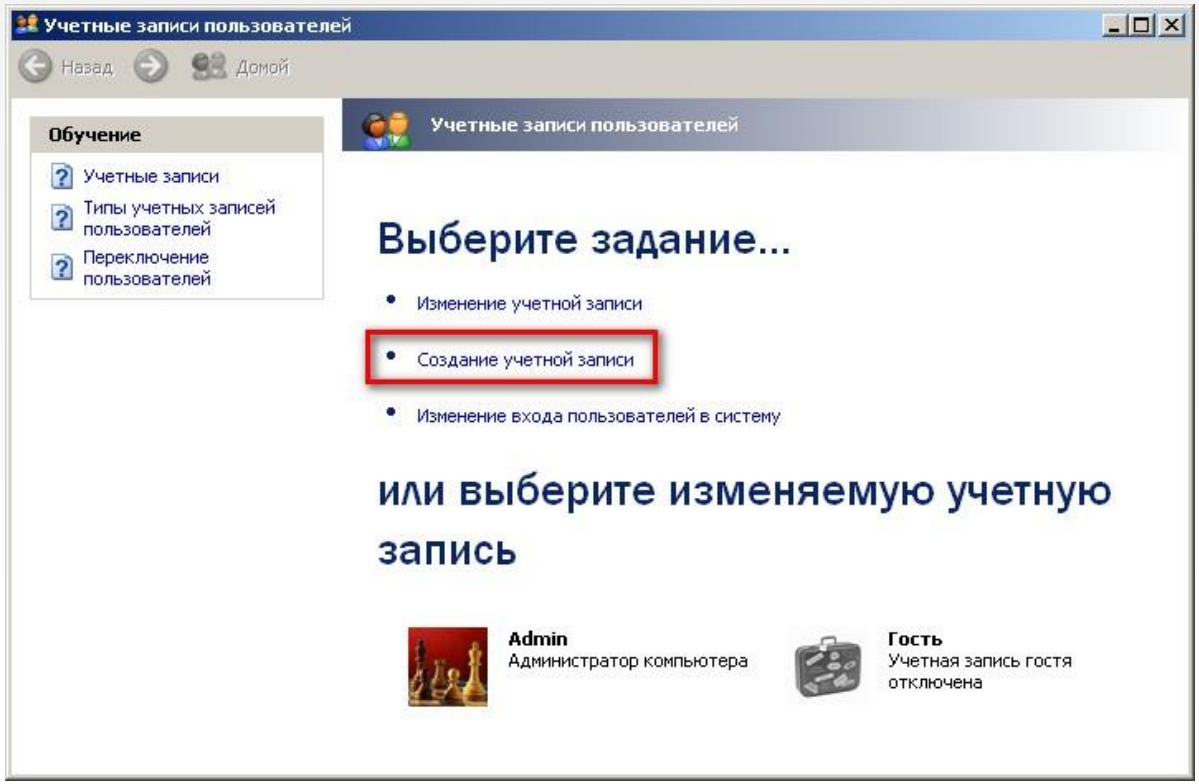


Работа в ограниченной учетной записи не позволит вирусу завладеть всей вашей системой!!!

Here comes your

Создание ограниченной пользовательской учетной записи

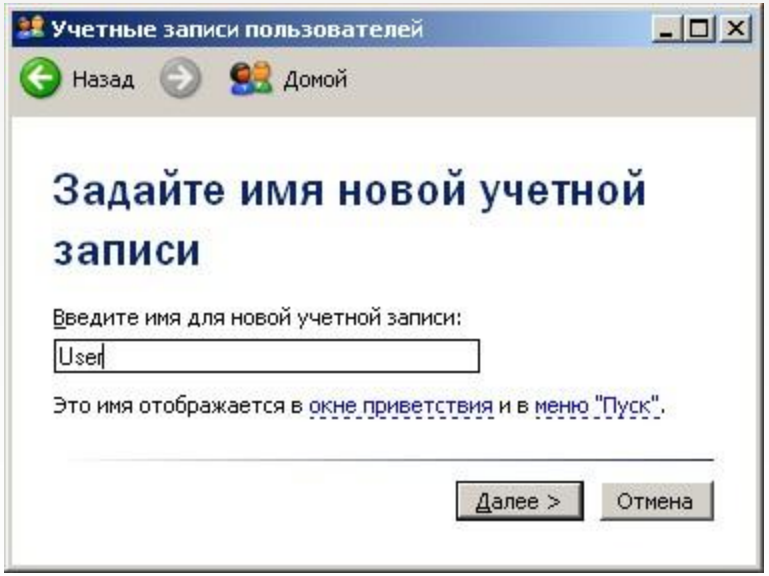
- Нажать кнопку “Пуск” □ “Настройка” □ “Панель управления” □ “учетные записи пользователей” (или “Пуск” □ “Панель управления” □ “учетные записи пользователей”)
- Нажать на ссылку “Создание учетной записи”



Here comes your

Создание ограниченной пользовательской учетной записи

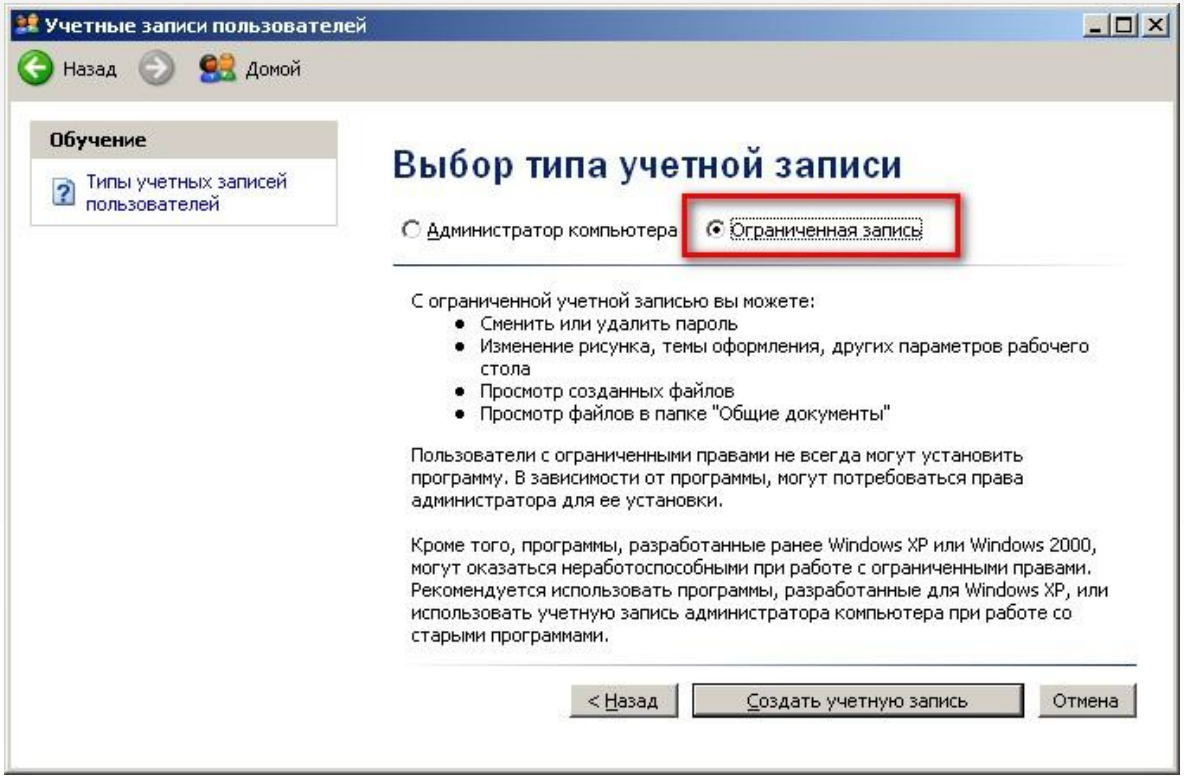
- Ввести имя учетной записи (латинскими буквами)



Here comes your

Создание ограниченной пользовательской учетной записи

- Выбрать тип учетной записи “ограниченная запись”
- Нажать кнопку “создать учетную запись”



Here comes your

Создание ограниченной пользовательской учетной записи

Создание ограниченной учетной записи не позволит вирусу завладеть всей вашей системой. Для этого необходимо:

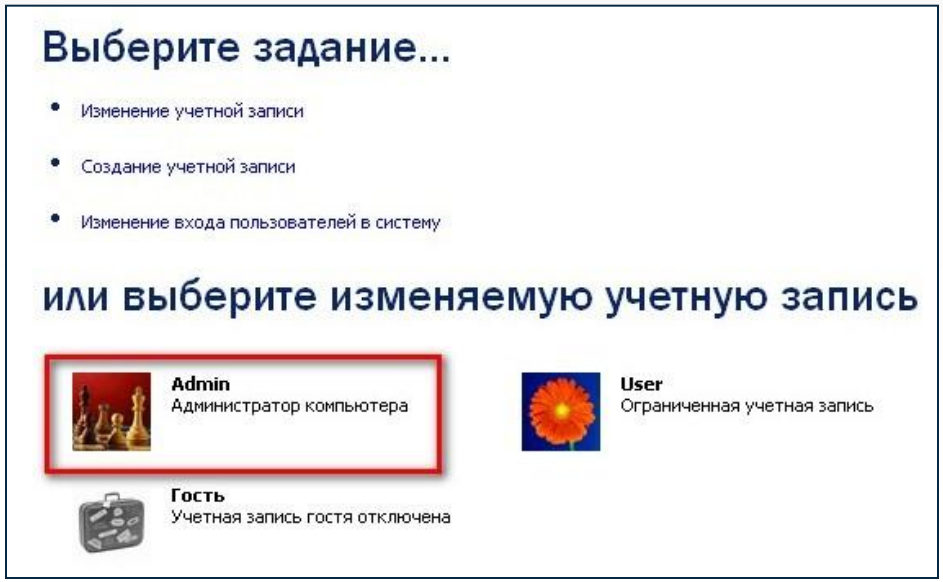
1. Нажать кнопку “Пуск” □ “Настройка” □ “Панель управления” □ “учетные записи пользователей” (или “Пуск” □ “Панель управления” □ “учетные записи пользователей”)
2. Нажать на ссылку “Создание учетной записи”
3. Ввести имя учетной записи (латинскими буквами)
4. Выбрать тип учетной записи “ограниченная запись”
5. Нажать кнопку “создать учетную запись”

Устанавливать программы нужно в учетной записи администратора. А работать только в ограниченной учетной записи.

Учетная запись. Установка пароля.

Всегда устанавливаете на учетную запись администратора пароль!!! Для этого необходимо:

- Нажать кнопку “Пуск” □ “Настройка” □ “Панель управления” □ “учетные записи пользователей” (или “Пуск” □ “Панель управления” □ “учетные записи пользователей”)
- Выбрать учетную запись администратора компьютера



Here comes your

Учетная запись. Установка пароля.

Всегда устанавливаете на учетную запись администратора пароль!!! Для этого необходимо:

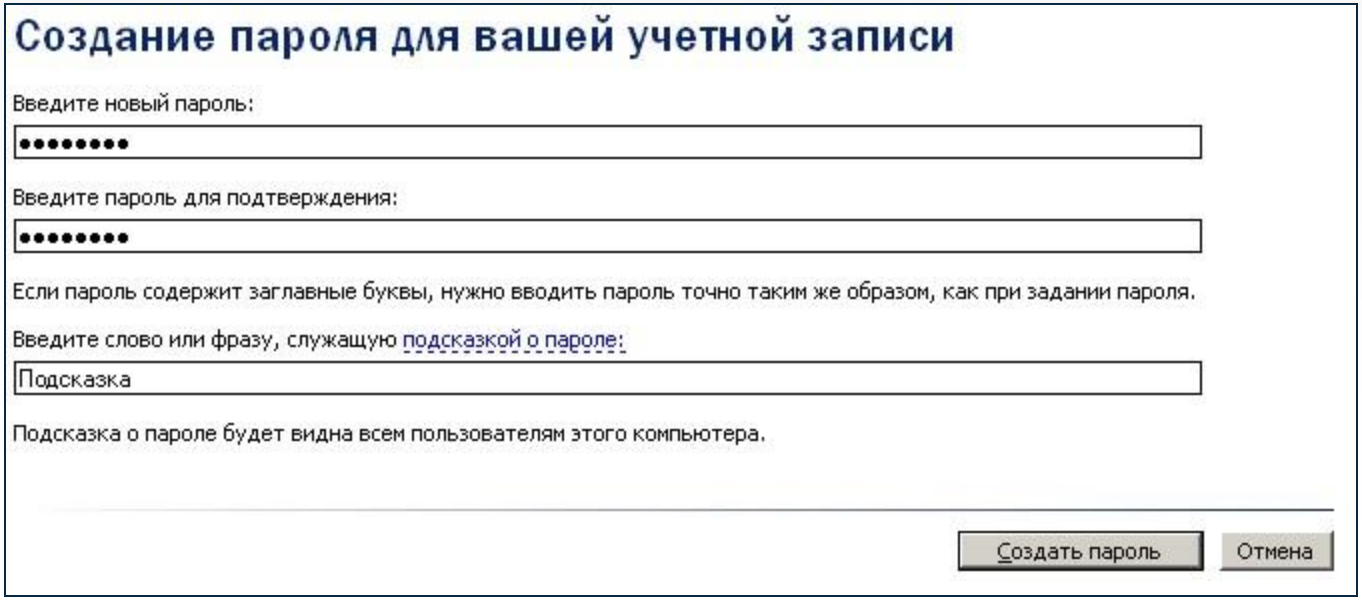
1. Нажать на ссылку “Создание пароля”

Here comes your

Учетная запись. Установка пароля.

Всегда устанавливаете на учетную запись администратора пароль!!! Для этого необходимо:

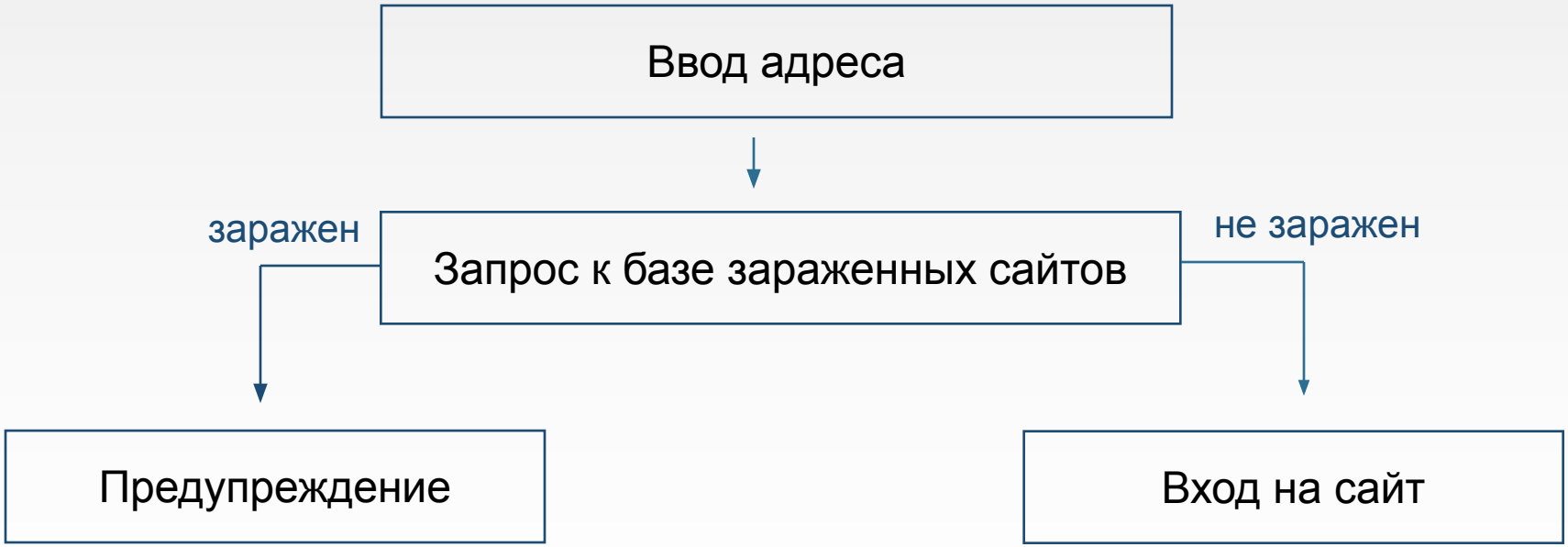
- Введите два раза новый пароль
- При необходимости напишите подсказку
- Нажмите кнопку “Создать пароль”, далее сделайте ваши файлы личными



Here comes your

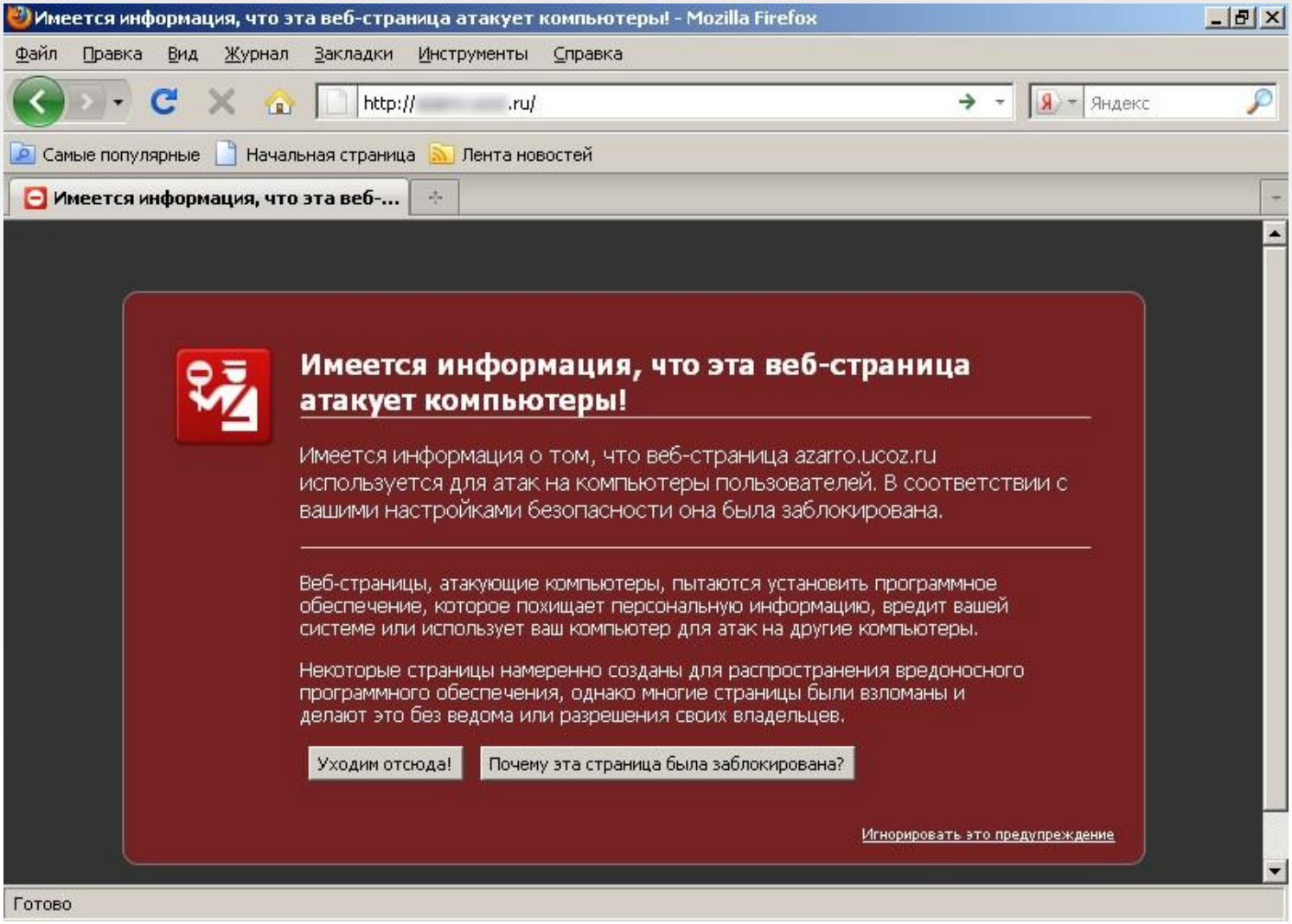
Безопасный браузер

Принцип проверки сайтов браузерами (например, mozila firefox или google chrome):



Here comes your

Безопасный браузер. Предупреждение.

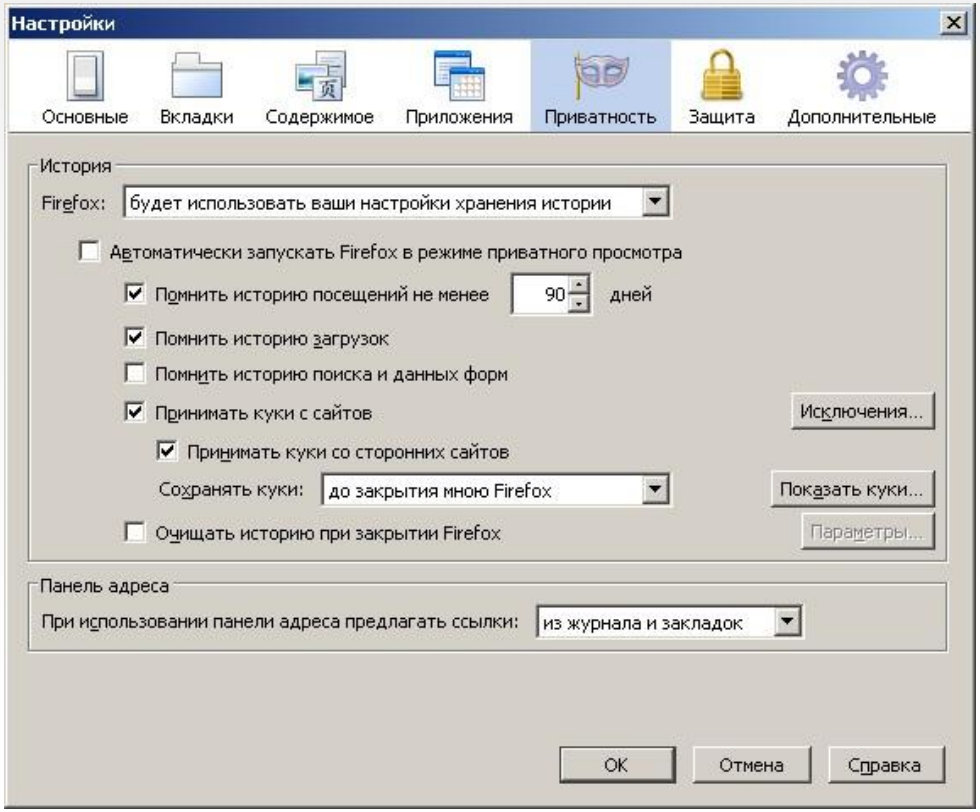


Here comes your

Безопасный браузер

Для безопасного входа на сайты необходимо сменить браузер. Например, установим и настроим firefox:

- Зайдите на сайт www.firefox.com и загрузите firefox.
- Выключить сохранение различной информации с помощью верхнего ниспадающего меню “инструменты” □ “настройки” □ “приватность” (см. рисунок)

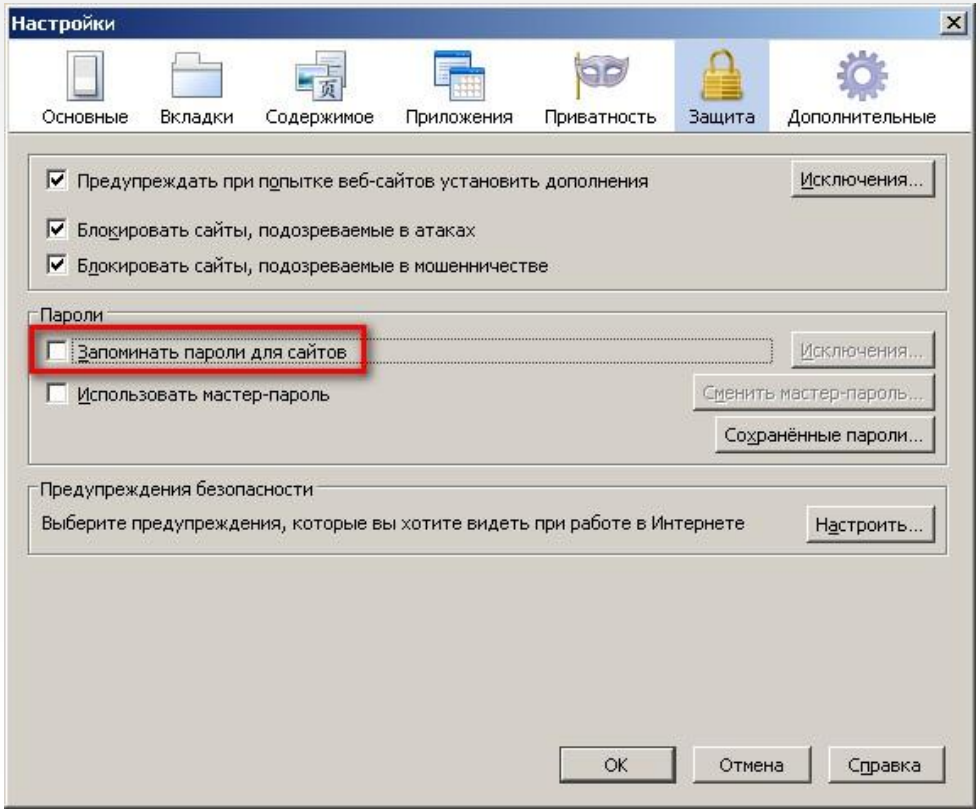


Here comes your

Безопасный браузер

Для безопасного входа на сайты необходимо сменить браузер. Например, установим и настроим firefox:

- Выключить сохранение паролей с помощью верхнего ниспадающего меню “инструменты” □ “настройки” □ “защита” (см. рисунок)



Here comes your

Безопасный браузер

Для дополнительной защиты от вирусов (а так же и отключить рекламму на сайтах) необходимо установить дополнения.

- Установите дополненияе NoScript (https://addons.mozilla.org/ru/firefox/addon/noscript/)
- Зайдите на сайт https://addons.mozilla.org/ru/firefox/addon/adblock-plus/ и установите расширение Adblock Plus
- Перезапустите браузер
- Зайдите на сайт http://code.google.com/p/ruadlist/
- Подпишитесь на все подписки (основная подписка, против счетчиков, BitBlock, анти-порно подписка)

Основные способы защиты. Правила.

Правила

- Следить за обновлениями программ (антивируса, фаервола, браузера и операционной системы…)
- Работать в системе под правами пользователя
- Следить какой файл вы запускаете
- Использовать безопасный пароль
- Сохраняйте пароль в тайне
- Регулярно делать копии важных файлов на внешние носители

Ответы на вопросы

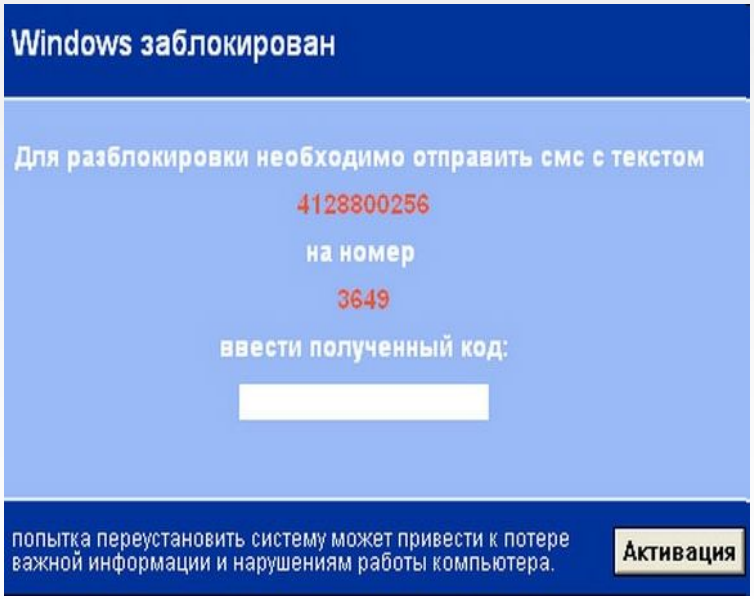
Защита флешек

Для защиты от передачи вирусов с помощью флешек необходимо:

- поставить патч KB950582 - http://support.microsoft.com/kb/953252 (только для Windows XP)
- Скачать и установить Panda USB and AutoRun Vaccine (и с помощью программы выбрать флешку и нажать на кнопку “Vaccinate USB”).
- Для технически подготовленных пользователей рекомендую заглянуть сюда.

Ответы на вопросы

Заразился вирусом “блокировщик Windows”, что делать?



- Зайти на специальную страничку DrWebЗайти на специальную страничку DrWeb или KasperskyЗайти на специальную страничку DrWeb или Kaspersky, или NOD.
- Выберите похожее изображение, которое блокирует ваш экран или введите в соответствующие поля номер телефона и текст с картинки
- Введите полученный код

Here comes your

Ответы на вопросы

Какой антивирус лучше?

Один из самых популярных вопросов, определенного ответа на этот вопрос нет, я предпочитаю DrWeb.

Если говорить о бесплатных антивирусах, то лучшими можно назвать:

- AVG Antivirus FREE
- Avast! Free Antivirus
- И др. (подробнее на моем сайте: http://rusinov.net/2011/01/09/sravenie-besplatnyx-antivirusov/)

Ответы на вопросы

Мой компьютер заражен, антивирус не помогает.

Ситуация стандартная, если вы не выполняли всех рекомендаций данных выше. Для лечения компьютера необходимо загрузиться с незараженной операционной системы и проверить ваш диск. Проще всего это сделать с помощью livecd (с этого диска загрузиться операционная система и можно произвести лечение компьютера). Наиболее популярные livecd:

- Drweb - http://www.freedrweb.com/download+cureit/
- Kaspersky Rescue Disk - http://support.kaspersky.com/viruses/rescuedisk

Ответы на вопросы

В Linux действительно нет вирусов?

Нет, это не так. В linux есть вирусы вот некоторые их них:

- Lion Worm
- Linux.Diesel Virus
- Linux.Vit.4096.
- Ramen virus
- Winux Virus
- *nix malware

Но стоит отметить, что из-за незначительной распространенности Linux среди домашних пользователей интерес к этим системам со стороны вирусописателей небольшой. Отсюда и малое количество вирусов для этих операционных систем (на 2009 год, официально выявлено всего 1898 вирусов).

Более подробно можно прочитать здесь - http://www.securelist.com/ru/analysis/208050538/Vredonosnye_programmy_dlya_alternativnykh_OS

Русинов А.С.

www.rusinov.net

Данная презентация находится на сайте автора.

Here comes your