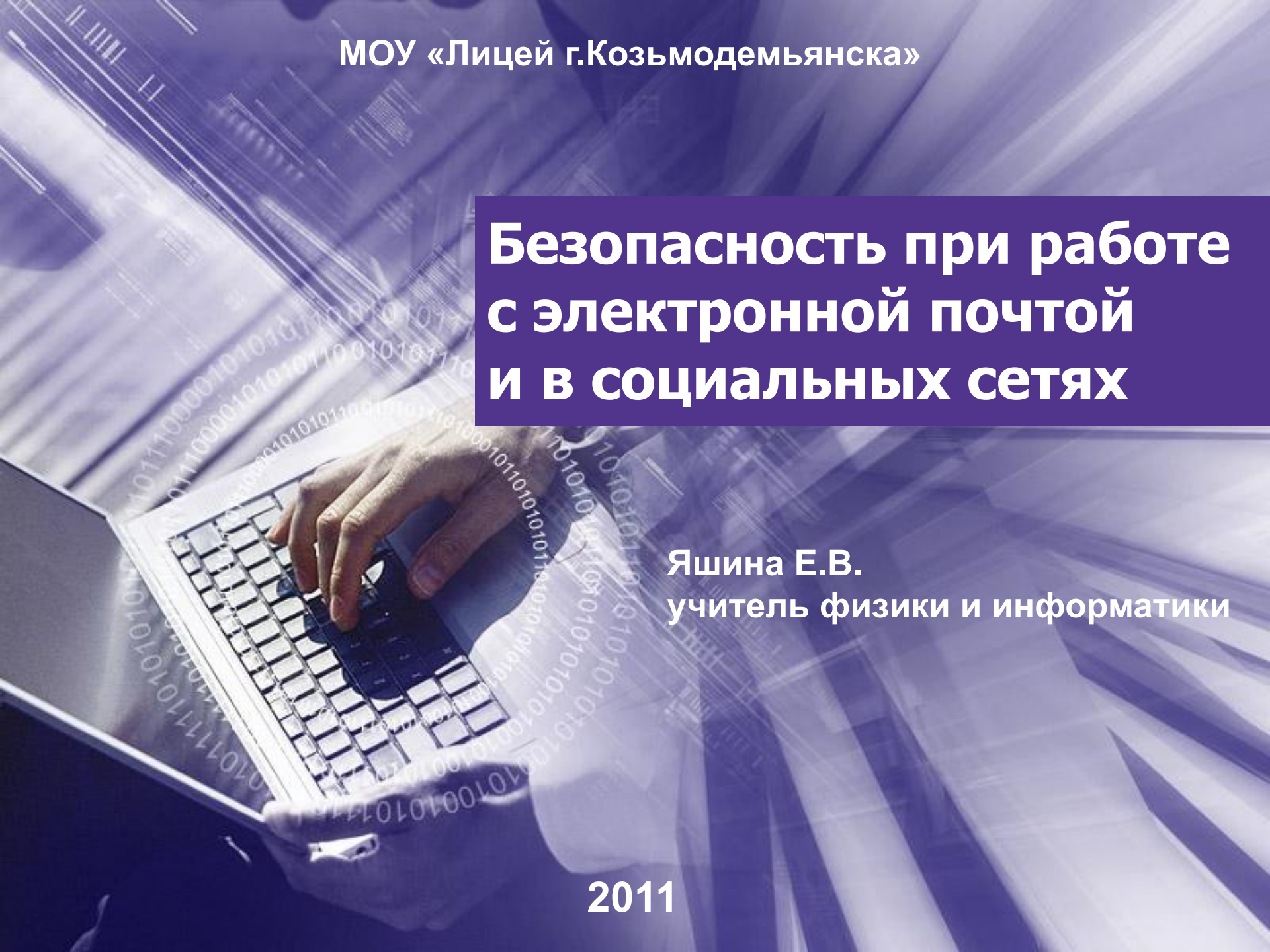
МОУ «Лицей г.Козьмодемьянска»

Безопасность при работе с электронной почтой и в социальных сетях



Яшина Е.В.
учитель физики и информатики

2011

Надёжная защита домашнего компьютера

- **технические меры**
  - установка брандмауэра
  - установка антивируса
- **информация**
  - о существующих угрозах
  - о методах противодействия

Основные источники угроз

Вредоносные программы

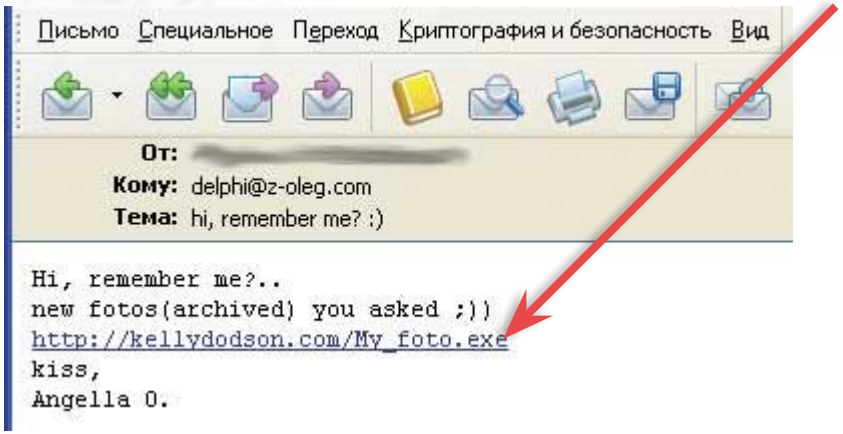
- любой исполняемый код, который тем или иным путем наносит вред операционной системе, прикладным программам и данным пользователя, похищает некоторую конфиденциальную информацию или использует ПК пользователя для организации атак на другие ПК в Интернете, рассылки спама и иной подобной деятельности

Мошенничество

- нетехнические подходы, базирующиеся на приемах и методах социальной инженерии (фишинг, финансовые пирамиды, различные методики сбора персональных данных и прочие способы мошенничества в сфере высоких технологий)

Прямая ссылка

1. ***Прямая ссылка на вредоносную программу в теле письма***:



С точки зрения пользователя, он загружает нечто, по виду напоминающее картинку. Распознать подобную ситуацию несложно: в данном случае расширение файла ****.exe*** позволяет понять, что речь идет именно об исполняемом файле, а не об изображении

Косвенные ссылки

2. ***Более сложные случаи***:

a) применение двойных расширений

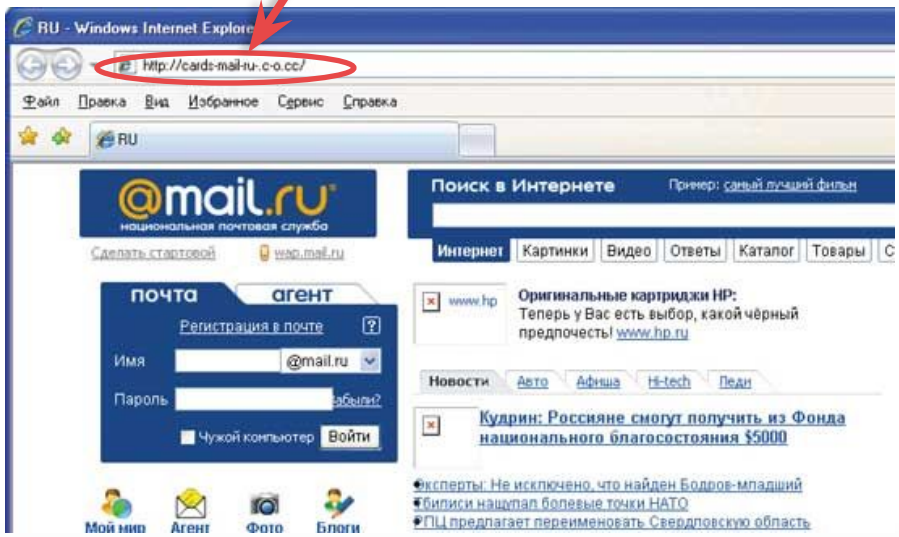
b) использование расширений, отличных от *.exe, но допускающих запуск: ****.com***, ****.cmd***, ****.pif*** и ****.scr***

c) создание письма в формате HTML и использование особенности тэга <A>, предназначенного для вставки ссылок в HTML. (*Данный тэг позволяет задавать ссылку и текст, который отображается для пользователя*). В результате пользователь думает, что в теле письма отображается ссылка, по которой произойдет переход при нажатии на нее, а переход происходит по совершенно ***иной*** ссылке. (***При наведении курсора на ссылку в теле письма почтовая программа отображает реальную ссылку при помощи всплывающей подсказки***)

Фишинг

3. Пользователю присылается письмо, убеждающее его перейти по имеющейся в письме ссылке на сайт якобы почтовой службы, банка или на иной сайт, предполагающий авторизацию. Ссылка или ведет на сайт с похожим URL (от настоящего URL он может отличаться всего одной буквой), или производится маскировка URL описанными выше методами

Пример поддельного, фишингового сайта

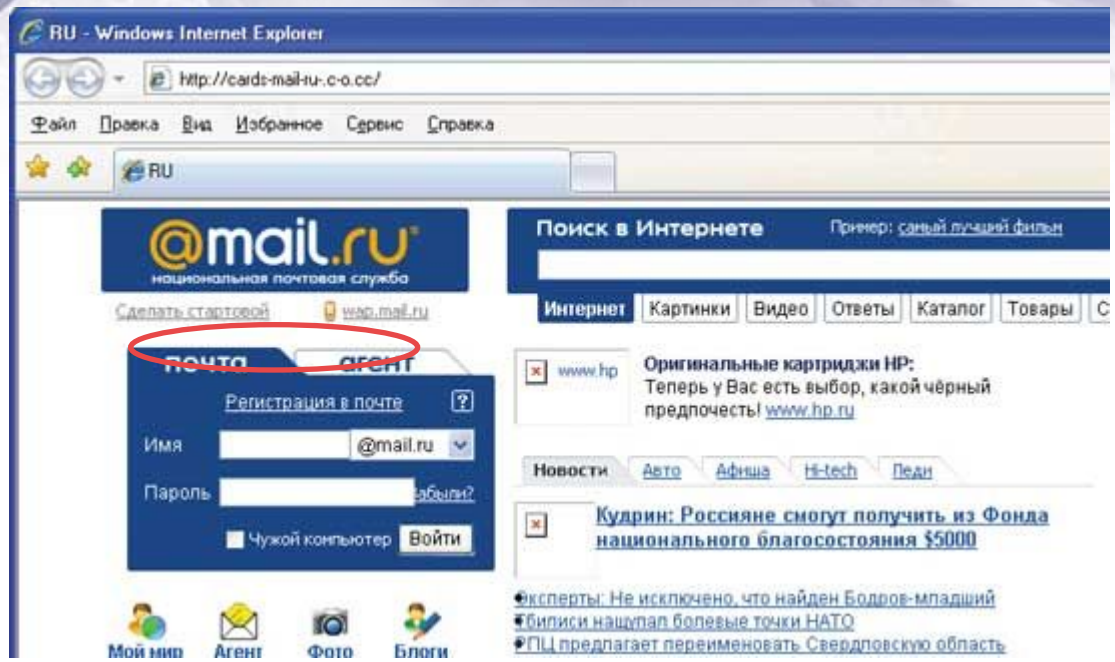


Признаки фишингового сайта

1) *URL содержит знакомые пользователям ключевые слова «cards» и «mail.ru», но URL совершенно иной*

2) *некоторые элементы странички накладываются друг на друга*

3) *часть картинок не отображается*



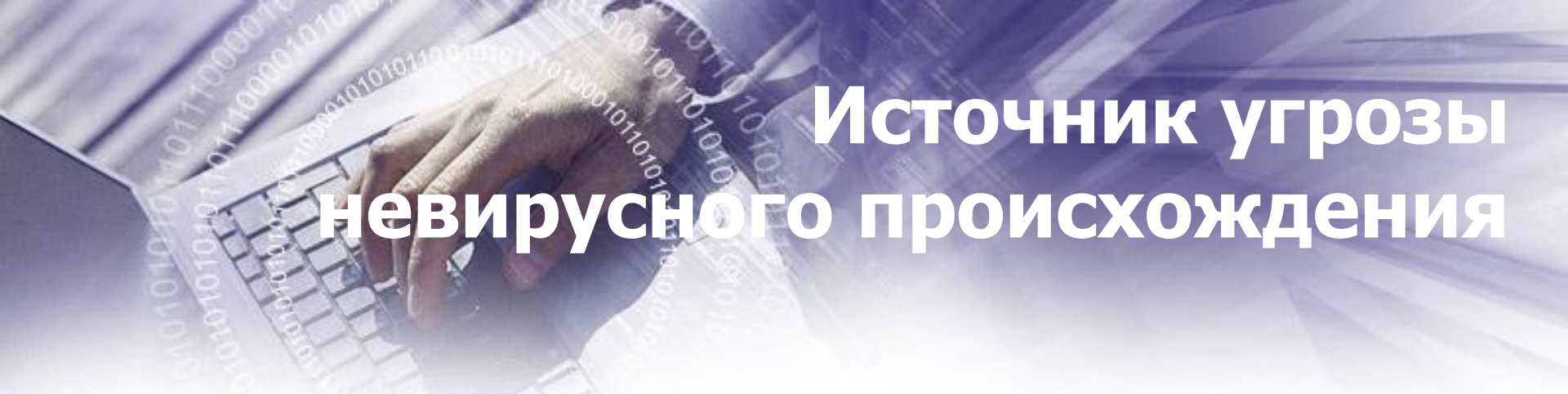
В случае ввода логина и пароля на подобном поддельном сайте они станут достоянием злоумышленников!

Использование вложений

1. вложением письма является вредоносный файл в чистом виде, без всякой маскировки
2. вложение содержит элементы маскировки реального имени и расширения
3. вредоносный объект находится в архивем (*архив нередко защищен паролем, который приложен к письму в текстовом или графическом виде*)
4. письмо содержит ***документ-эксплойт***, который сам по себе исполняемым файлом не является, но при его открытии выполняется некий вредоносный код, обычно осуществляющий загрузку и запуск вредоносного программного обеспечения. (*Таким документом, к примеру, может быть специальным образом сфабрикованное изображение или PDF-документ)*

Использование вложений

Имя вложенного файла маскируется под адрес электронной почты



Источник угрозы невирусного происхождения

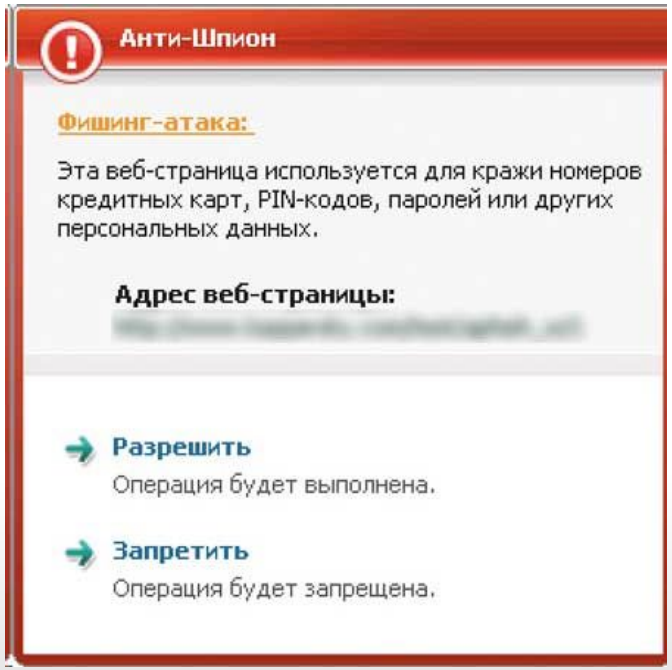
- Пользователю приходит письмо, в котором ему предлагается выслать авторам письма некую персональную информацию: отсканированные листы ***паспорта*** и иных документов, например ***водительских прав*** или ***карточки пенсионного страхования***, ***данные о месте работы*** и т.п.
- Предлог может быть любым — например ***предложение выгодного трудоустройства***, ***оформление льготных кредитов***, ***выплата неких выигрышей*** и т.п.
- Персональная информация, к примеру, ***может быть использована для получения кредита***

  Встречаются и более интересные предложения, например выслать отсканированное изображение кредитной карты с двух

Способы защиты

1. ***Технические средства:***

   при помощи антивируса *(желательно работающего совместно с почтовой программой или оснащенного функцией перехвата и проверки почтового трафика)*, обеспечивающего комплексную защиту, которая включает антифишинговые и антишпионские средства



Способы защиты

2. *Правила безопасности :*

a) не переходить по ссылкам, содержащимся в письмах. Даже если письмо пришло от знакомого адресата, следует учитывать, что его адрес может быть подделан или почтовый ящик известного вам абонента может быть взломан. Если переход по ссылке необходим, следует убедиться, что ссылка подлинная, после чего скопировать ее в буфер обмена и вставить в адресную строку браузера

b) перед открытием вложений следует сохранить их на диске и проверить антивирусом. Перед открытием желательно убедиться в том, что у файла реальное, а не двойное расширение. Для этого в проводнике следует включить отображение расширений известных файлов (меню ***Сервис→Свойства папки***, закладка ***Вид***, где следует снять галочку ***Скрывать расширения для зарегистрированных типов файлов***) или вместо проводника использовать альтернативный менеджер файлов, например ***FAR*** либо ***Total Commander***

Способы защиты

2. *Правила безопасности :*

c) банки, провайдеры Интернета, службы электронной почты и т.п. ***не рассылают писем с просьбой переслать им пароли или иную конфиденциальную информацию***. В любом случае, если письмо кажется похожим на правду, можно посетить их сайт (не по ссылке из письма!) и проверить, действительно ли требуется выполнение указанных в письме операций. Более того, можно обратиться в службу техподдержки и выяснить, посылали ли они подобный запрос

d) своевременно устанавливать обновления операционной системы, что снизит вероятность успешного применения эксплойтов

e) письмо может быть перехвачено третьими лицами или похищено с компьютера получателя. Поэтому не следует пересылать по электронной почте отсканированные листы паспорта и иные значимые документы, параметры доступа к кредитным картам и другие персональные данные

f) ***не работать*** с электронной почтой под учетной записью администратора

Социальные сети

«плюсы»

- расширяют круг общения
- помогают людям в поиске одноклассников, сокурсников, сослуживцев и т.п.

«минусы»

- пользователи таких сетей добровольно публикуют массу персональной информации о себе

Чем больше пользователь публикует персональной информации о себе и своей жизни, тем уязвимее он для мошенников

При разговоре по телефону или личной встрече обман можно распознать, а вот при общении в сети выявить обман намного сложнее

Источники

1. Презентация выполнена по материалам статьи ***Олега Зайцева*** «***Вредоносное ПО и домашний компьютер»:*** ***http://www.compress.ru/article.aspx?id=19575&iid=905#begin***

2. Помощь Почта@Mail.Ru «***Почта — частые вопросы и проблемы»:*** ***http://help.mail.ru/mail-help***

3. Безопасность систем электронной почты: ***http://www.nestor.minsk.by/sr/2003/09/30909.html***