

Тема урока:

**«Киберугрозы
современности:
главные правила их
распознавания
и предотвращения»**

Киберугроза что это?



**Киберугроза – это
незаконное проникновение
или угроза вредоносного
проникновения на
компьютер**



Интернет представляет собой
важный способ личного и
профессионального общения.



**Но он может также
ИСПОЛЬЗОВАТЬСЯ СО ЗЛЫМ
УМЫСЛОМ.**



МОЖЕТ ИСХОДИТЬ

1. Социальные сети. ОПАСНОСТЬ?

2. В последнее время стали распространены атаки на компьютер через мобильные устройства памяти (Flash-память).



Опасности!!!

- Вирусы, сетевые черви
- Спам в Интернете
- Фишинговые атаки.

Компьютерный вирус –

специально созданная вредоносная программа, обладающая способностью к «размножению» (самокопированию).



Зачем создаются эти вредоносные программы?

- Создание помех работе пользователя.
 - Уничтожение данных пользователя.
 - Шпионаж за пользователем.
 - Похищение данных, представляющих ценность или тайну.
 - Использование ресурсов заражённого компьютера в преступных целях.
- И т.д.



Тро́йнская программа (троянец) —

вредоносная программа,

которая выполняет несанкционированные пользователем передачу управления компьютером удаленному пользователю, а также действия по удалению, модификации, сбору и передачи информации третьим лицам.

Осуществить внедрение такого вредоносного ПО обычно гораздо проще не через интернет, а с помощью записанных на флэшках «**ТРОЯНОВ**».

Флэшки могут подбрасываться как в здание, где располагается организация, так и размещаться, скажем, на парковке рядом с ним, где их наверняка найдёт именно сотрудник нужной организации.

Поэтому если вы нашли на улице или в здании флэшку, не торопитесь радостно вставлять её в свой компьютер .



СПРАВОЧНАЯ ИНФОРМАЦИЯ

- **«Лаборатория Каспёрского»** — российская — российская компания, специализирующаяся на разработке систем защиты от компьютерных вирусов — российская компания, специализирующаяся на разработке систем защиты от компьютерных вирусов, спама — российская компания, специализирующаяся на разработке систем защиты от компьютерных вирусов, спама, хакерских атак и прочих **киберугроз**. Компания ведёт свою деятельность более чем в 200 странах и

СПРАВОЧНАЯ ИНФОРМАЦИЯ



Данные «Лаборатории
Касперского»

За последний год **91%** компаний, представители которых приняли участие в опросе, сталкивались с угрозами информационной безопасности.

**В России этот показатель еще выше –
96%.**



Сетевые черви представляют собой опасные программы, которые могут распространяться через **электронную почту** или **веб-страницы**.

Вирусы могут повредить файлы или программное обеспечение, хранящиеся на компьютере



Защитите свой компьютер

ОСНОВНЫЕ ПРАВИЛА

относительно электронной почты:

- 1. Никогда** не открывайте подозрительные сообщения или вложения электронной почты, полученные от незнакомых людей. Вместо этого сразу **удалите их**.
- 2. Никогда** не отвечайте на спам.

Защитите свой компьютер



3. **Создайте новый** или используйте семейный адрес электронной почты для Интернет-запросов, дискуссионных форумов и т.д.

4. **Никогда не пересылайте «письма счастья».**

Вместо этого сразу удаляйте их.

Спам в Интернете

Массовая рассылка нежелательных сообщений электронной почты известна как спам.

- Он приводит к перегрузке систем электронной почты.
- Может заблокировать почтовые ящики.

«Нигерийские письма»

Одной из разновидностей спама являются «Нигерийские письма» или другое название «Угроза 419». «Нигерийские письма» - вид мошенничества, получивший наибольшее развитие с появлением спама. Называется так потому, что письма особое распространение получили в Нигерии, причем еще до распространения Интернета они распространялись по обычной почте, начиная с середины 1980 годов.

С появлением интернета «Нигерийские письма» стали нарицательным понятием.

Как правило, у получателя письма просят помощь в многомиллионных операциях, обещая солидные проценты с сумм. Если получатель согласится, у него выманиваются всё большие суммы денег на сборы, взятки и т. д.

Мошенничество профессионально организовано: у мошенников есть офисы, работающий факс, часто мошенники связаны с правительственными организациями. Разумеется, обещанных денег жертва в любом случае не получает: их просто не существует.



Фишинг — вид интернет-мошенничества, целью которого является получение идентификационных данных пользователей.

Организаторы фишинг-атак используют массовые рассылки электронных писем от имени популярных брендов.

В эти письма они вставляют ссылки на фальшивые сайты, являющиеся точной копией настоящих. Оказавшись на таком сайте, пользователь может сообщить преступникам ценную информацию (имя пользователя и пароль для доступа или, даже, номер своей кредитной карты).



ОСТОРОЖНО,
МОШЕННИКИ!!!

Остерегайтесь мошенничества

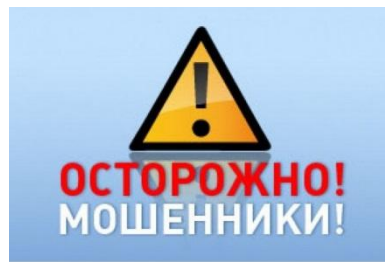
Думайте о том, с кем разговариваете.
В Интернете легко скрыть свою личность.
Рекомендуется проверять личность человека, с которым происходит общение.
Никогда не разглашайте в Интернете личную информацию, за исключением людей, которым вы доверяете.

Защитите свой компьютер



Закрывайте сомнительные всплывающие окна

Всплывающие окна — это небольшие окна с содержимым, побуждающим к переходу по ссылке. При отображении такого окна самым безопасным способом его закрытия является нажатие значка **X**



Проверьте!

**Всегда удостоверьтесь в том,
что вам известно, кому
предоставляется информация,
и вы понимаете, в каких целях
она будет использоваться.**



Помните!
В Интернете не вся
информация надежна
и не все
пользователи откровенны.



П о м н и т е !!!

**После публикации
информации в
Интернете ее больше
невозможно будет
контролировать и удалять
каждую ее копию.**

Думайте о других пользователях



- **Закону необходимо подчиняться даже в Интернете.**
- **При работе в Интернете будьте вежливы с другими пользователями Сети.**
- **Имена друзей, знакомых, их фотографии и другая личная информация не может публиковаться на веб-сайте без их согласия или согласия их родителей.**

Разрешается копирование материала из Интернета для личного использования, но присвоение авторства этого материала запрещено.

Передача и использование незаконных материалов (например, пиратские копии фильмов или музыкальных произведений, программное обеспечение с надорванными защитными кодами и т.д.) является противозаконным.

Копирование программного обеспечения или баз данных, для которых требуется лицензия, запрещено даже в целях личного использования.

Используемая литература и Интернет-ресурсы:

- Методические рекомендации на сайте ФГАОУ «Академия повышения квалификации и профессиональной переподготовки работников образования», в разделе «Рекомендуем» <http://www.apkpro.ru/content/blogcategory/34/113/>.
- Вопросы обеспечения информационной безопасности от компании Microsoft <http://www.microsoft.com/rus/protect/default.mspx#>
- Портал Сети творческих учителей.
http://www.it-n.ru/communities.aspx?cat_no=71586&tmpl=com
- http://www.youtube.com/watch?v=9uvNVZMdelk&feature=player_embedded Видеоролик.
- <http://www.saferinternet.ru/> Безопасный интернет.
-