УВАЖАЕМЫЕ СТУДЕНТЫ!

Изучите и законспектируйте новый теоретический материал тезисно по плану лекции,.

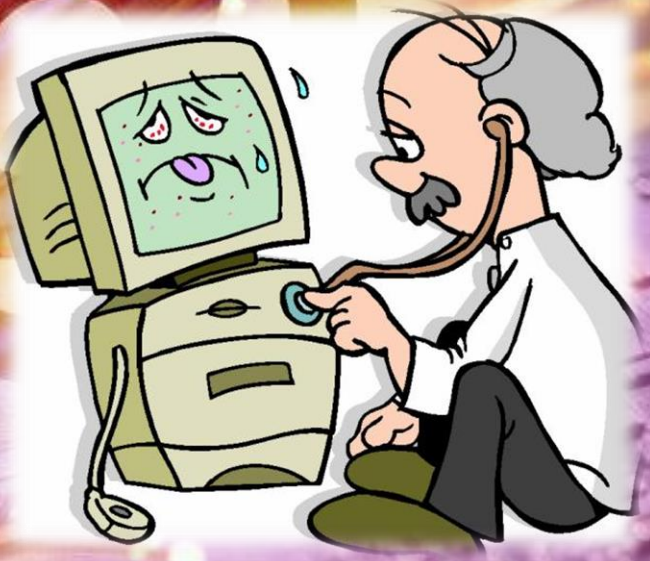
Результаты работы, фотоотчет, предоставить преподавателю на e-mail: xvsviv@rambler.ru в трехдневный срок с момента получения задания.

При возникновении вопросов по приведенному материалу обращаться по следующим номерам телефонов:072-138-93-11.

ВНИМАНИЕ!!! При отправке работы, не забывайте указывать ФИО студента, наименование дисциплины, дата проведения занятия (по расписанию).

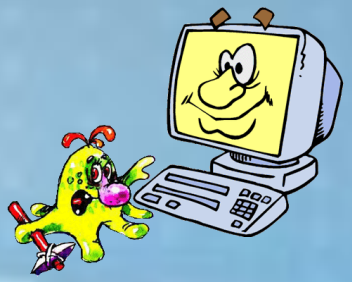
Лекция на тему: «Основные правила поиска вирусов с помощью антивирусной программы»

Компьютерные вирусы и антивирусные средства.
Работа в среде антивирусной программы.
Правила профилактики заражения компьютера вирусами.



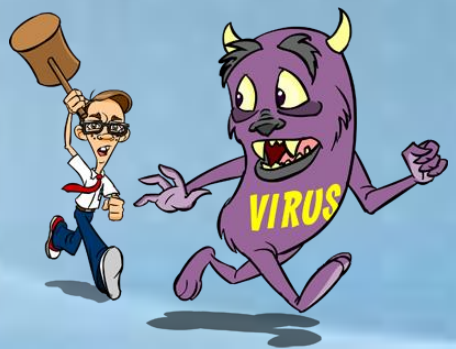
Компьютерные вирусы

Компьютерный вирус – разновидность компьютерных программ, отличительной особенностью которых является **способность к размножению** (саморепликация). В дополнение к этому вирусы могут без ведома пользователя выполнять прочие произвольные действия, в том числе наносящие вред пользователю и/или компьютеру. По этой причине вирусы относят к вредоносным программам.



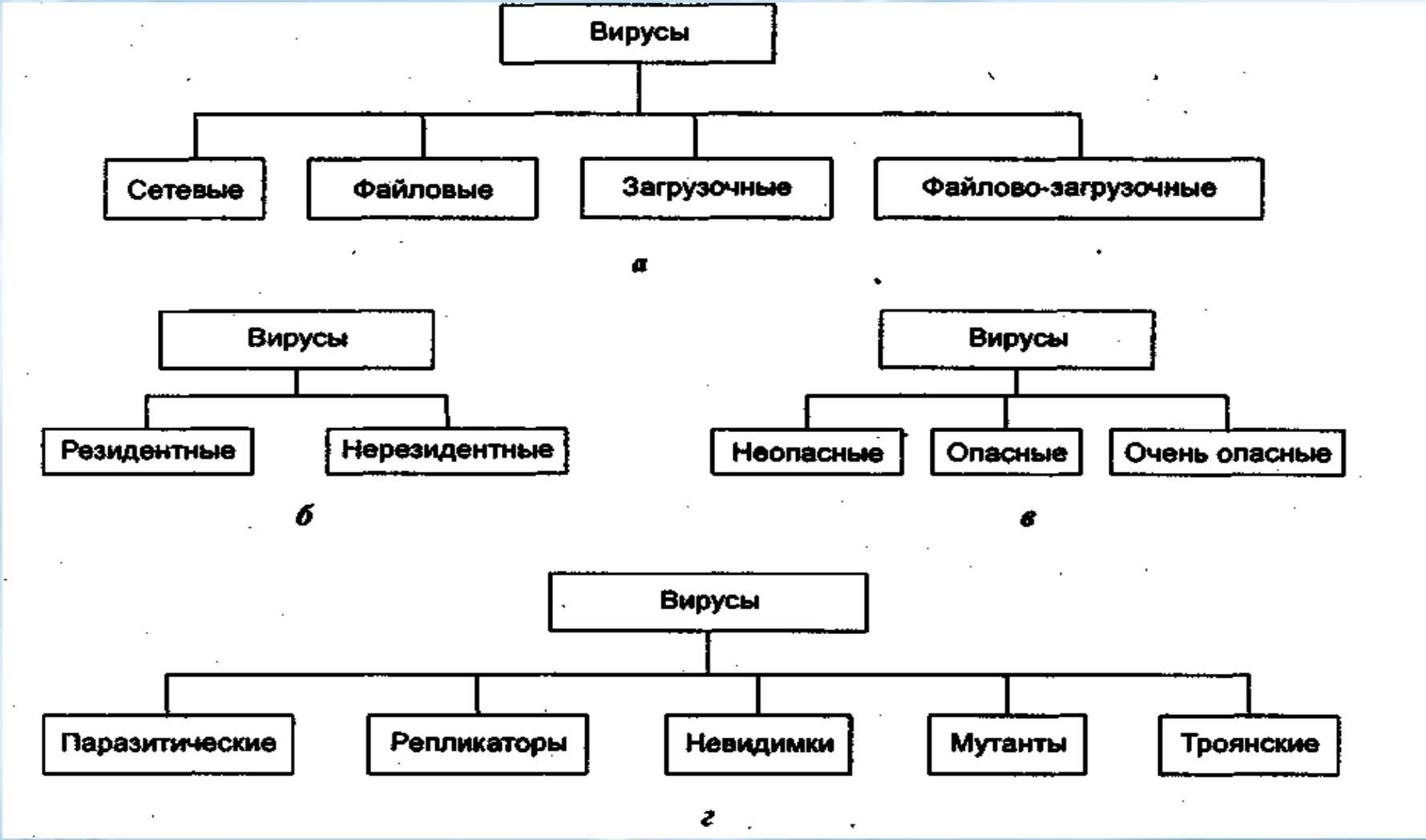
Основные признаки проявления вирусов

- Прекращение работы или неправильная работа ранее успешно функционировавших программ
- Медленная работа компьютера
- Невозможность загрузки операционной системы
- Исчезновение файлов и каталогов или искажение их содержимого
- Изменение даты и времени модификации файлов
- Изменение размеров файлов
- Частые зависания и сбои в работе компьютера
- Неожиданное значительное увеличение количества файлов на диске
- Существенное уменьшение размера свободной оперативной памяти
- Вывод на экран непредусмотренных сообщений или изображений
- Подача непредусмотренных звуковых сигналов



Классификация компьютерных вирусов

а - по среде обитания; б - по способу заражения;
в - по степени воздействия; г - по особенностям алгоритмов



По среде обитания:

Сетевые вирусы используют для своего распространения протоколы или команды компьютерных сетей и электронной почты.

Файловые вирусы либо различными способами внедряются в выполняемые файлы (наиболее распространенный тип вирусов), либо создают файлы-двойники (компаньон-вирусы), либо используют особенности организации файловой системы (link-вирусы)

Загрузочные вирусы записывают себя либо в загрузочный сектор диска (boot-сектор), либо в сектор, содержащий системный загрузчик винчестера (Master Boot Record), либо меняют указатель на активный boot-сектор.

По способу заражения:

Резидентные (такой вирус при инфицировании ПК оставляет в оперативной памяти свою резидентную часть, которая потом перехватывает обращение ОС к объектам заражения и поражает их. Резидентные вирусы живут до первой перезагрузки ПК)

Нерезидентные (не заражают оперативную память и могут быть активными ограниченное время)

По степени воздействия:

Неопасные (как правило эти вирусы забивают память компьютера путем своего размножения и могут организовывать мелкие пакости – проигрывать заложенную в них мелодию или показывать картинку);

Опасные (эти вирусы способны создать некоторые нарушения в функционировании ПК – сбои, перезагрузки, глюки, медленная работа компьютера и т.д.);

Очень опасные (опасные вирусы могут уничтожить программы, стереть важные данные, убить загрузочные и системные области жесткого диска, который потом можно выбросить)

По особенностям алгоритма:

Паразитические (меняют содержимое файлов и секторов диска. Такие вирусы легко вычисляются и удаляются);

Мутанты (их очень тяжело обнаружить из-за применения в них алгоритмов шифрования. Каждая следующая копия размножающегося вируса не будет похожа на предыдущую);

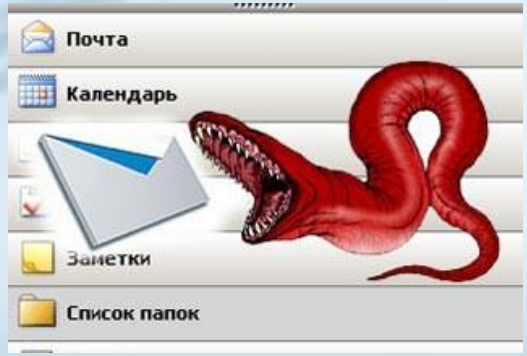
Репликаторы (вирусы-репликаторы, они же сетевые черви, проникают через компьютерные сети, они находят адреса компьютеров в сети и заражают их);

Троянский конь (один из самых опасных вирусов, так как трояны не размножаются, а воруют ценную (порой очень дорогую) информацию – пароли, банковские счета, электронные деньги и т.д.);

Невидимки (это трудно обнаружимые вирусы, которые перехватывают обращения ОС к зараженным файлам и секторам дисков и подставляют вместо своего незараженные участки.

Пути проникновения вирусов

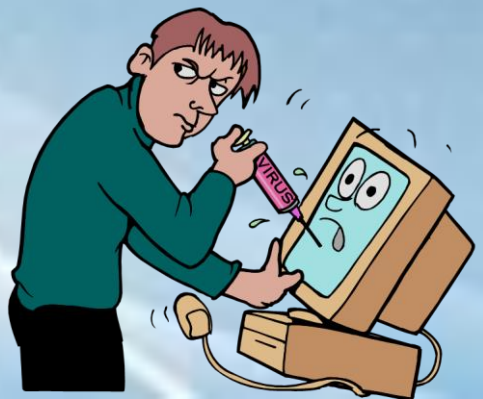
- Глобальная сеть Internet
- Электронная почта
- Локальная сеть
- Компьютеры «Общего назначения»
- Пиратское программное обеспечение
- Ремонтные службы
- Съемные накопители



Очень опасный вирус

Троянский конь - это вредоносное программное обеспечение, которое, без ведома владельца персонального компьютера может предоставить доступ к его данным или по определенному адресу выслать вашу персональную информацию. Кроме этого, вы даже себе и подумать не можете, что эта программа является "трояном", так как программы подобного рода законспирированы под нужные и безопасные приложения.

Trojan.Winlock (Винлокер) — семейство вредоносных программ блокирующих или затрудняющих работу с операционной системой, и требующих перечисление денег злоумышленникам за восстановление работоспособности компьютера. Впервые появились в конце 2007 года. Широкое распространение вирусы-вымогатели получили зимой 2009—2010 года, по некоторым данным оказались заражены миллионы компьютеров, преимущественно среди пользователей русскоязычного Интернета. Второй всплеск активности такого вредоносного ПО пришелся на май 2010 года.



Windows заблокирован!

Microsoft Security обнаружил нарушения использования сети интернет.
Причина: Просмотр нелицензионного ГЕЙ и ДЕТСКОГО порно.

Для разблокировки Windows необходимо:
Пополнить номер абонента Киевстар: +380976674804 на сумму 100 грн.
Оплатить можно через терминал для оплаты сотовой связи.
После оплаты, на выданном терминалом чеке, Вы найдёте Ваш персональный код разблокировки, который необходимо ввести ниже.

0 1 2 3 4 5 6 7 8 9 очистить

Ваш код:

ВХОД В СИСТЕМУ

Если в течении 12 часов с момента появления данного сообщения, не будет введён код, все данные, включая Windows и bios будут БЕЗВОЗВРАТНО УДАЛЕНЫ! Попытка переустановить систему приведёт к нарушениям работы компьютера. Microsoft Corporation.

КОМПЬЮТЕР ЗАБЛОКИРОВАН!

Ваш компьютер заблокирован за просмотр, копирование и тиражирование видеоматериалов содержащих элементы педофилии и насилия над детьми. Для снятия блокировки Вам необходимо оплатить штраф в размере 500 рублей на номер Билайн 8-965-347-15-40. В случае оплаты суммы равной штрафу либо превышающей ее на фискальном чеке терминала будет напечатан код разблокировки. Его нужно ввести в поле в нижней части окна и нажать кнопку "Разблокировать". После снятия блокировки Вы должны удалить все материалы содержащие элементы насилия и педофилии. Если в течение 12 часов штраф не будет оплачен, все данные на Вашем персональном компьютере будут безвозвратно удалены, а дело будет передано в суд для разбирательства по статье 242 ч.1 УК РФ.

Перезагрузка или выключение компьютера приведет к незамедлительному удалению ВСЕХ данных, включая код операционной системы и BIOS, с невозможностью дальнейшего восстановления.

Разблокировать

Статья 242.1. Изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних.
Изготовление, хранение или перемещение через Государственную границу Российской Федерации в целях распространения, публичной демонстрации или рекламирования либо распространение, публичная демонстрация или рекламирование материалов или предметов с порнографическими изображениями несовершеннолетних, а равно привлечение несовершеннолетних в качестве исполнителей для участия в зрелищных мероприятиях порнографического характера лицом, достигшим восемнадцатилетнего возраста, - наказываются лишением свободы на срок от двух до восьми лет с ограничением свободы на срок до одного года либо без такового.

Windows заблокирован

Для разблокировки необходимо отправить смс с текстом

t7580620000 на номер 3649

введите полученный код

Активация

для разблокировки у вас есть

02:59:41

*Попытка переустановить систему может привести к потере важной информации и нарушениям работы компьютера.

Trojan.Winlock условно можно разделить на 3 типа, в зависимости от того, насколько они затрудняют работу для пользователя.

1 тип — это баннеры или порноинформеры, появляющиеся только в окне браузера. Наиболее легко удаляемый тип. Обычно они выдают себя за дополнительные плагины или надстройки для браузера.

2 тип — это баннеры, которые остаются на рабочем столе после закрытия браузера и при этом закрывают большую его часть. Но у пользователей обычно остаётся возможность открывать другие программы, в том числе диспетчер задач и редактор реестра.

3 тип — это наиболее трудноудаляемый тип баннеров, которые закрывают практически весь рабочий стол, блокируют запуск диспетчера задач, редактора реестра, а также загрузку в безопасном режиме. Некоторые разновидности полностью блокируют клавиатуру, предоставляя пользователю лишь цифровые клавиши из своего «интерфейса», и рабочую мышь для ввода кода.

Методы защиты

Как защититься от вирусов

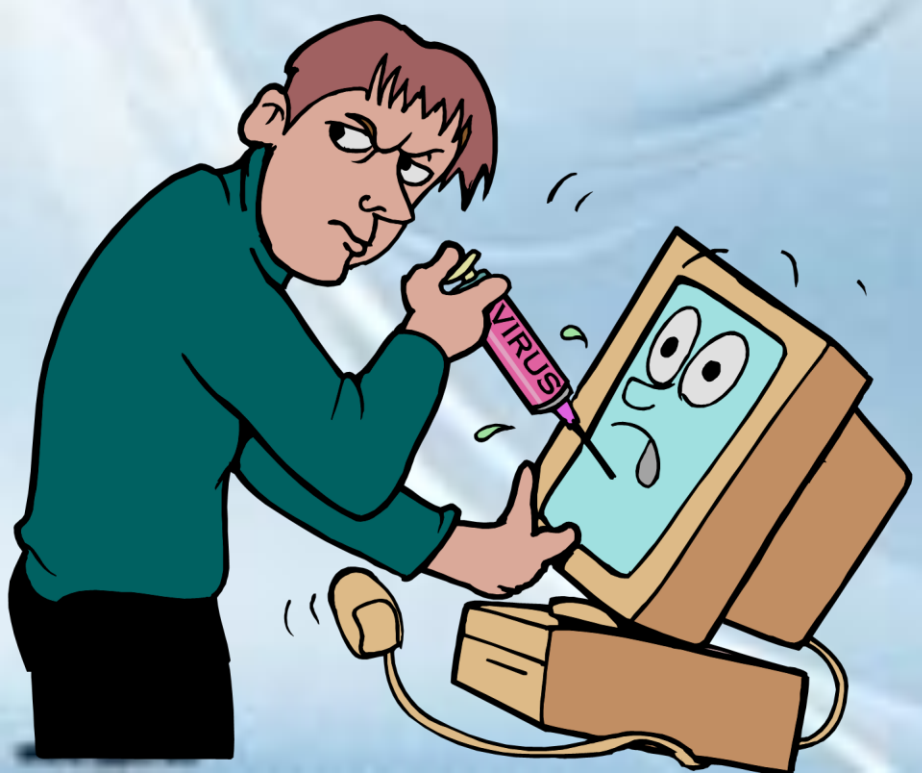
1. установите на свой ПК современную антивирусную программу.
2. перед просмотром информации принесенной на флэш-карте (дискете) с другого компьютера проверьте носитель антивирусом;
3. после разархивирования архивных файлов сразу проверьте их на вирусы (не все антивирусные программы могут искать вредоносный код в архивах или могут делать это не корректно);
4. периодически проверяйте компьютер на вирусы (если активно пользуетесь Интернетом – запускайте раз в неделю, а то и чаще);
5. как можно чаще делайте резервные копии важной информации (backup);
6. используйте совместно с антивирусной программой файервол (firewall) если компьютер подключен к Интернет;
7. настройте браузер (программа просмотра Интернет страниц – IE, Opera и т.д.) для запрета запуска активного содержимого html-страниц.

Антивирусные программы

Критерии выбора антивирусных программ

- Надежность и удобство в работе
- Качество обнаружения вирусов
- Существование версий под все популярные платформы
- Скорость работы
- Наличие дополнительных функций и возможностей

ПРОЦЕСС ЗАРАЖЕНИЯ ВИРУСОМ И ЛЕЧЕНИЯ ФАЙЛА



Компьютерный вирус → Незаражённая программа

↓

Заражённый файл | Компьютерный вирус

Антивирусная программа → ✂

Вылеченный файл

АНТИВИРУСНЫЕ ПРОГРАММЫ

СКАНЕРЫ
(фаги, полифаги)

- Универсальные
- Специализированные
- Резидентные
- Нерезидентные

CRC-СКАНЕРЫ
(ревизоры)

Блокировщики

Иммунизаторы

Рынок антивирусных программ очень разнообразен


АНТИВИРУС
КАСПЕРСКОГО

Возможности программы Антивирус Касперского

- защита от вирусов, троянских программ и червей;
- защита от шпионских, рекламных и других потенциально опасных программ;
- проверка файлов, почты и интернет-трафика в реальном времени;
- проактивная защита от новых и неизвестных угроз;
- антивирусная проверка данных на любых типах съемных носителей;
- проверка и лечение архивированных файлов;
- контроль выполнения опасных макрокоманд в документах Microsoft Office;
- средства создания диска аварийного восстановления системы.

Антивирус Касперского 6.0 для Windows Workstations

Kaspersky Anti-Virus

Настройка

Справка

Защита

Анти-Спам

Поиск вирусов

Сервис

Обновление

Файлы данных

Аварийный диск

Поддержка

Сервис

Информация о программе

Версия:	6.0.3.837
Срочное обновление:	b.c.d.e
Дата выпуска сигнатур:	17.12.2008 12:59:56
Количество сигнатур:	1468877

Информация о системе

Операционная система:	Microsoft Windows XP Professional Service Pack 3 (build 2600)

Информация о лицензии

Владелец:	ОУсредняя ОШ 3 "Образовательный центр" Мартынова Ольга Владимировна Россия пр-т Гагарина
Номер:	0B2C-0003F4-03CA22F7
Тип:	Коммерческая на 89 компьютеров
Дата окончания:	03.01.2011 2:59:59

kaspersky.ru viruslist.ru

Домашнее задание

Читать стр. 140-145,

Выполнить стр. 147, №2 (вопросы для размышления)

Написать в тетради краткий конспект по данной презентации.

По всем возникающим вопросам обращаться на электронный адрес учителя:
anastasiya.aldos@mail.ru

Желаю успехов!