КОМПЬЮТЕРНЫЕ ВИРУСЫ.

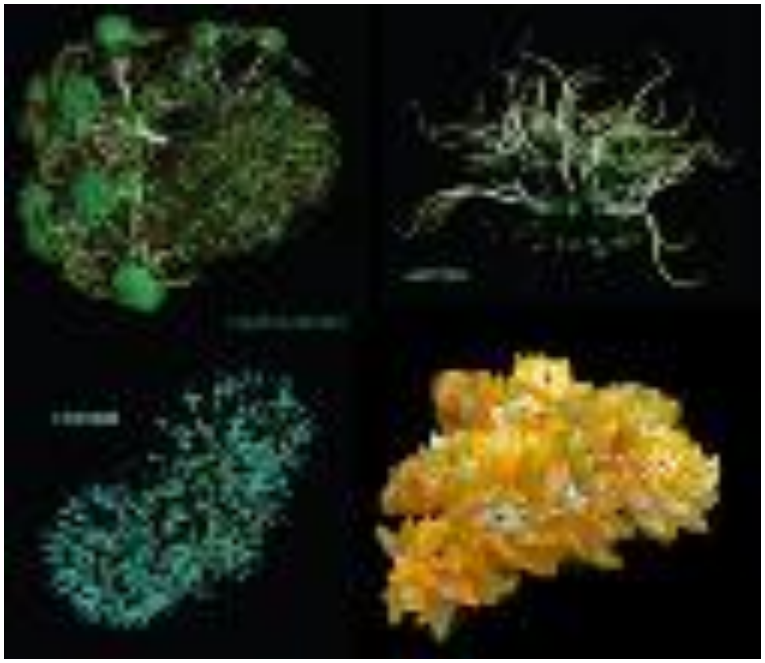
Основные вопросы:

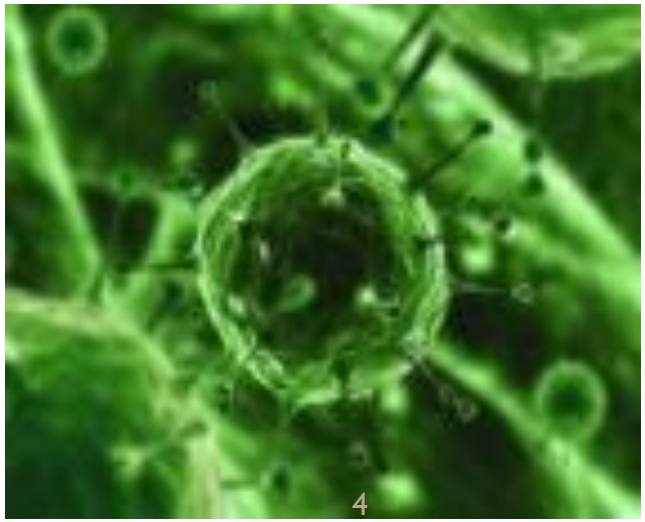
- *Понятие компьютерного вируса, их виды.*
- *Виды антивирусных программ.*

Что же такое вирус? И чем *биологический вирус* отличается от *компьютерного*?

Вирус – мельчайшая неклеточная частица, размножающаяся в живых клетках, возбудитель инфекционного заболевания.

Толковый словарь русского языка С. И. Ожегова и Н. Ю. Шведовой





Компьютерный вирус – специально созданная небольшая программа, способная к саморазмножению, засорению компьютера и выполнению других нежелательных действий.

Энциклопедия вирусов
«Лаборатории Касперского
http://www.viruslist.com/ru/viruses/encyclopedia

ЧТО ЖЕ ОБЩЕГО МЕЖДУ БИОЛОГИЧЕСКИМ И КОМПЬЮТЕРНЫМ ВИРУСАМИ?

1. ***Способность к размножению.***
2. ***Вред для здоровья человека и нежелательные действия для компьютера.***
3. ***Скрытность, т.к. вирусы имеют инкубационный период.***

ИСТОРИЯ КОМПЬЮТЕРНЫХ ВИРУСОВ

Первая «эпидемия» компьютерного вируса произошла в 1986 году, когда вирус по имени Brain (англ. «мозг») «заражал» дискеты персональных компьютеров. В настоящее время известно несколько десятков тысяч вирусов, заражающих компьютеры и распространяющихся по компьютерным сетям.

Признаки заражения

- общее замедление работы компьютера и уменьшение размера свободной оперативной памяти;

- некоторые программы перестают
- работать или появляются различные ошибки в программах;
- на экран выводятся посторонние символы и сообщения, появляются различные звуковые и видеоэффекты;
- размер некоторых исполнимых файлов и время их создания изменяются;
- некоторые файлы и диски оказываются испорченными;
- компьютер перестает загружаться с жесткого диска.

КЛАССИФИКАЦИЯ КОМПЬЮТЕРНЫХ ВИРУСОВ

ПРИЗНАКИ КЛАССИФИКАЦИИ

- Среда обитания
- Способ заражения
- Особенности алгоритма работы
- Степень воздействия

КЛАССИФИКАЦИЯ ВИРУСОВ

Среде обитания:

- ЗАГРУЗОЧНЫЕ
- ФАЙЛОВЫЕ
- МАКРО-ВИРУСЫ
- СКРИПТ-ВИРУСЫ
- СЕТЕВЫЕ-ВИРУСЫ

ЗАГРУЗОЧНЫЕ ВИРУСЫ

Загрузочные вирусы заражают загрузочный сектор гибкого или жесткого диска.

При заражении дисков загрузочные вирусы «подставляют» свой код вместо программы, получающей управление при загрузке системы, и отдают управление не оригинальному коду загрузчика, а коду вируса.

Профилактическая защита от таких вирусов состоит в отказе загрузки операционной системы с гибких дисков и установке в BIOS компьютера защиты загрузочного сектора от изменений.

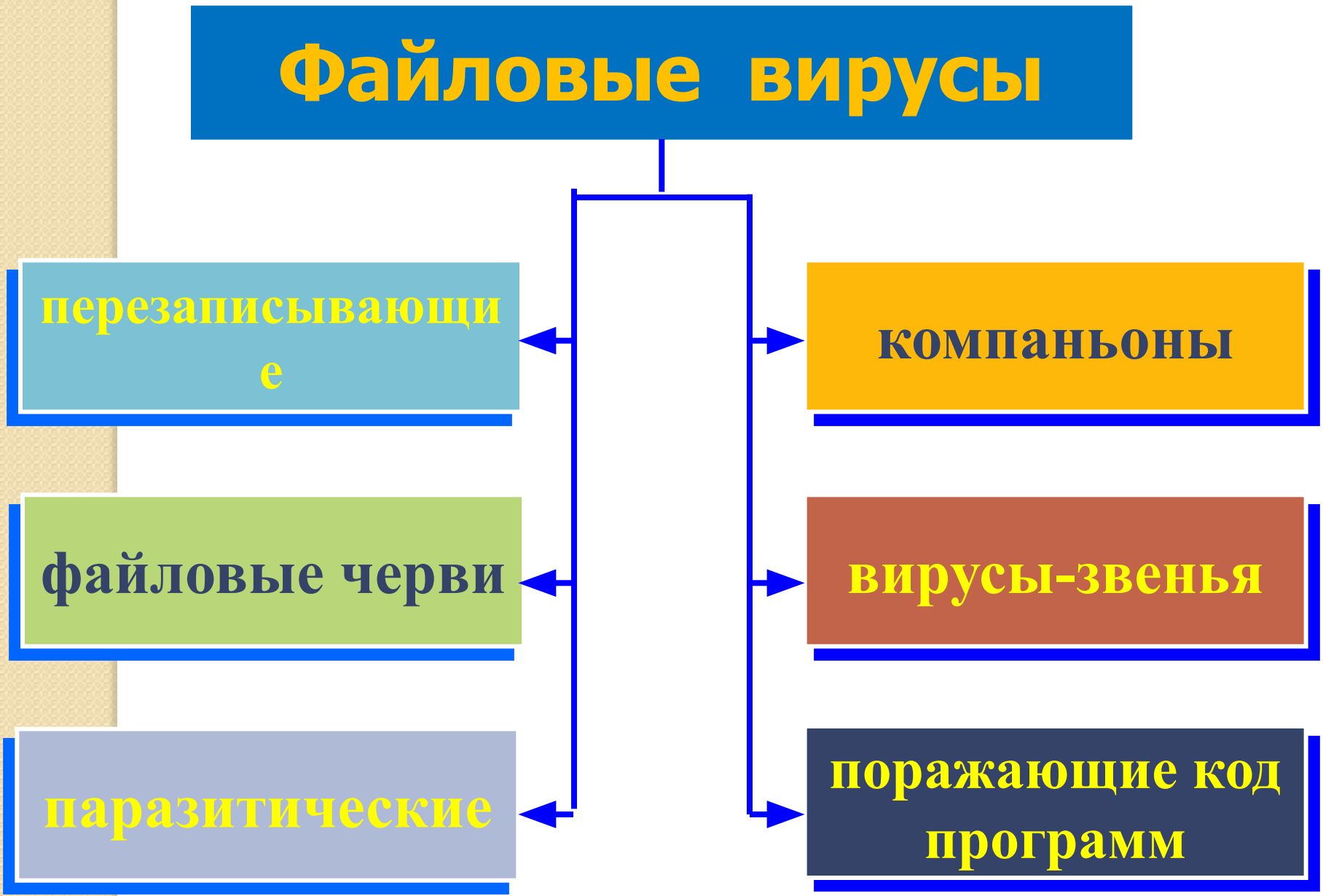
ФАЙЛОВЫЕ ВИРУСЫ

Файловые вирусы внедряются в исполняемые файлы (командные файлы *.bat, программы *.exe, системные файлы *.com и *.sys, программные библиотеки *.dll и др.) и обычно активируются при их

После запуска зараженного файла вирус находится в оперативной памяти компьютера и является активным (т.е. может заражать другие файлы) вплоть до момента выключения компьютера или перезагрузки операционной системы.

По способу заражения файловые вирусы разделяют на ***перезаписывающие вирусы***, ***вирусы-компаньоны*** и ***паразитические вирусы***.

Профилактическая защита от файловых вирусов состоит в том, что не рекомендуется запускать на исполнение файлы, полученные из сомнительного источника и предварительно не проверенные антивирусными программами.


Файловые вирусы
перезаписывающие
компаньоны
файловые черви
вирусы-звенья
паразитические
поражающие код программ

По способу заражения файловые вирусы разделяются на:

1. ***Перезаписывающие вирусы***. Записывают свое тело вместо кода программы, не изменяя название исполняемого файла, вследствие чего программа перестает запускаться.
2. ***Вирусы-компаньоны.*** Создают свою копию на месте заражаемой программы, но не уничтожают оригинальный файл, а переименовывают его или перемещают. При запуске программы вначале выполняется код вируса, а затем управление передается оригинальной программе.
3. ***Файловые черви*** создают собственные копии с привлекательными для пользователя названиями в надежде, что он их запустит.
4. ***Вирусы-звенья*** не изменяют код программы, а заставляют ОС выполнить свой код, изменяя адрес местоположения на диске зараженной программы, на собственный адрес.

По способу заражения файловые вирусы разделяются на:

5. ***Паразитические вирусы*** изменяют содержимое файла, добавляя в него свой код. При этом зараженная программа сохраняет полную или частичную работоспособность. Код может внедряться в начало, середину или конец программы.
6. ***Вирусы, поражающие исходный код программы***. Вирусы данного типа поражают исходный код программы или ее компоненты (.OBJ, .LIB, .DCU). После компиляции программы оказываются встроенными в неё.

МАКРО-ВИРУСЫ

Макро-вирусы заражают документы, созданные в офисных приложениях (заражают файлы документов, например текстовых).

Макро-вирусы являются макрокомандами (макросами) на встроенном языке программирования Visual Basic for Applications (VBA), которые помещаются в документ.

Макро-вирусы являются ***ограниченно-резидентными***, т.е. они находятся в оперативной памяти и заражают документ, пока он открыт.

Макро-вирусы заражают шаблоны документов.

Профилактическая защита от макро-вирусов состоит в предотвращении запуска вируса (запрете на загрузку макроса).

СКРИПТ-ВИРУСЫ

Скрипт-вирусы – активные элементы (программы) на языках JavaScript или VBScript, которые могут содержаться в файлах Web-страниц.

Заражение локального компьютера происходит при их передаче по Всемирной паутине с серверов Интернета в браузер локального компьютера.

В ***1998*** году появился первый скрипт-вирус VBScript.Rabbit, заражающий скрипты Web-страниц, а в мае ***2000*** года грянула глобальная эпидемия скрипт-вируса «LoveLetter».

Профилактическая защита от скрипт-вирусов состоит в том, что в браузере можно запретить получение активных элементов на локальный компьютер.

КЛАССИФИКАЦИЯ ВИРУСОВ

По степени воздействия:

НЕОПАСНЫЕ

(последствия действия вирусов - уменьшение свободной памяти на диске, графические и звуковые эффекты)

ОПАСНЫЕ

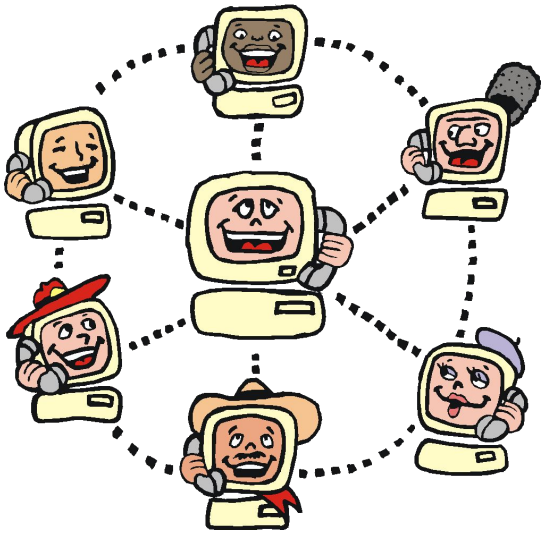
(последствия действия вирусов - сбои и «зависания» при работе компьютера)

ОЧЕНЬ ОПАСНЫЕ

(последствия действия вирусов - потеря программ и данных форматирование винчестера и т.д.)

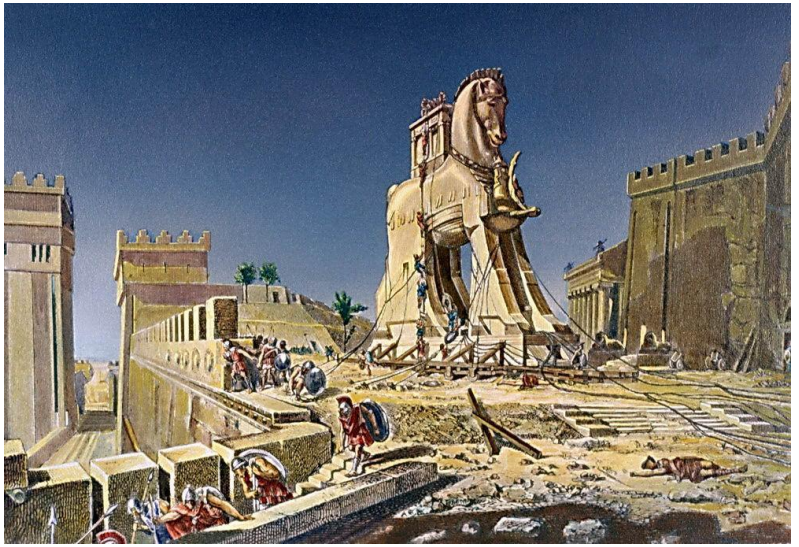
СЕТЕВЫЕ ВИРУСЫ

Могут передавать по компьютерным сетям свой программный код и запускать его на компьютерах, подключённых к этой сети. Заражение сетевым вирусом может произойти при работе с ***электронной почтой*** или при «***путешествиях***» по Всемирной паутине.



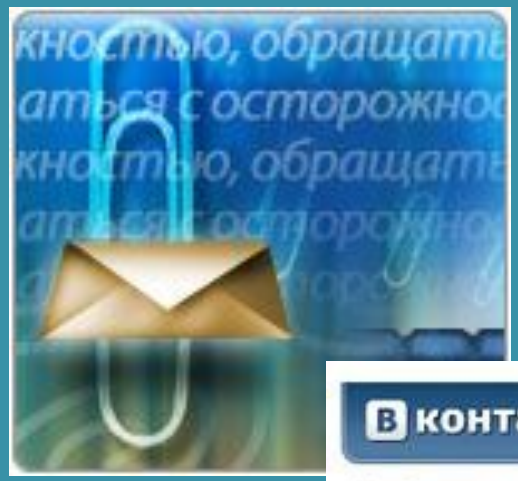
Сетевые вирусы

- сетевые черви
- троянские программы
- хакерские утилиты



СЕТЕВЫЕ ЧЕРВИ

Сетевые черви - это вредоносные программы, которые проникают на компьютер, используя сервисы компьютерных сетей: Всемирную паутину, электронную почту, интерактивное общение, файлообменные сети и т.д.

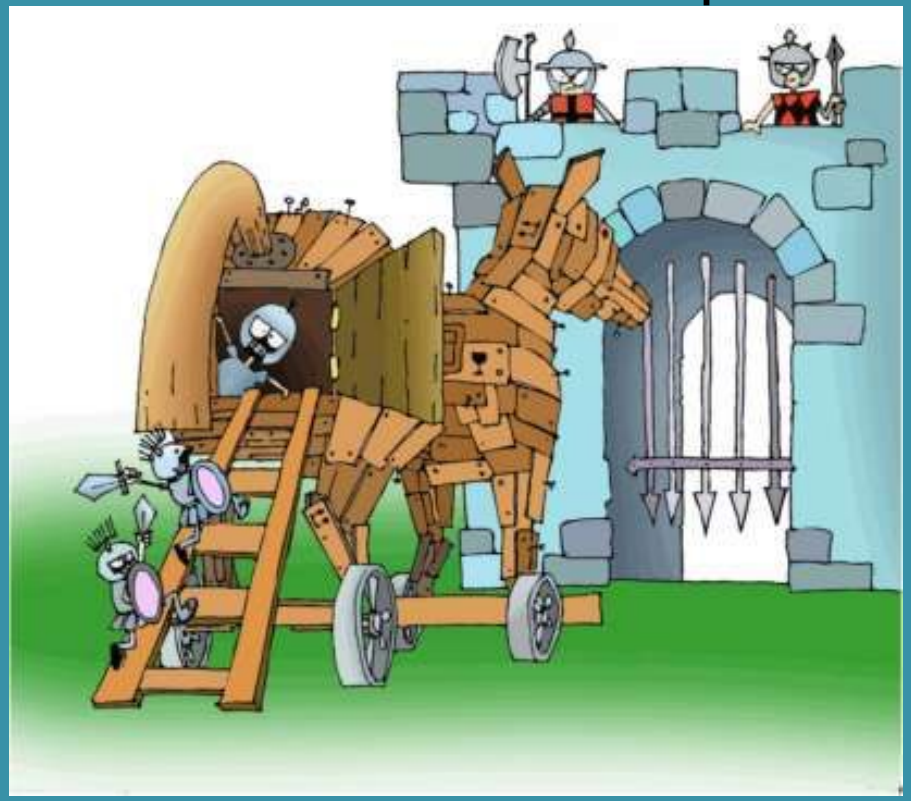


Многие сетевые черви используют более одного способа распространения своих копий по компьютерам локальных и глобальных сетей.

Активация сетевого червя может вызывать уничтожение программ и данных, а также похищение персональных данных пользователя.

ТРОЯНСКИЕ ПРОГРАММЫ

Троянская программа, троянец (от англ. trojan) – вредоносная программа, которая выполняет несанкционированную пользователем передачу управления компьютером удаленному пользователю, а также действия по удалению, модификации, сбору и пересылке информации третьим лицам.



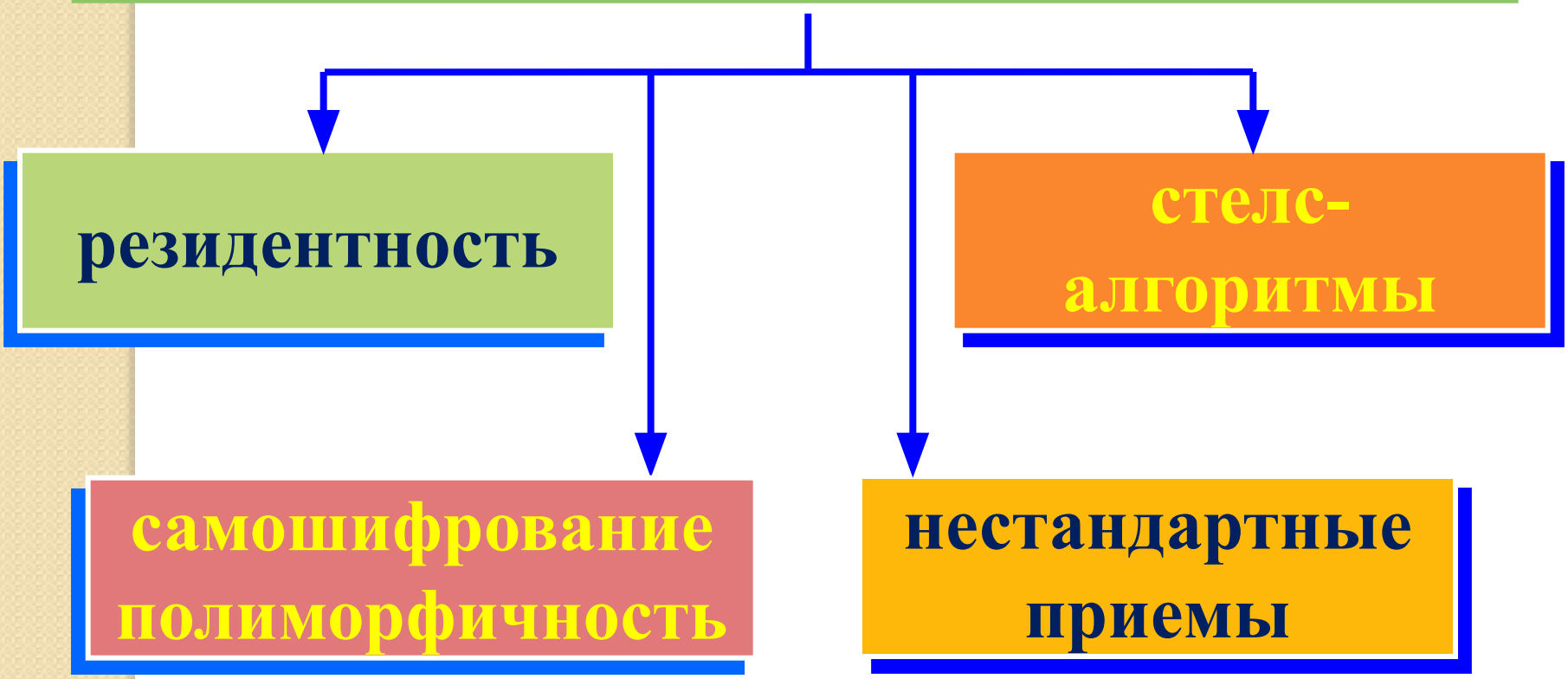
Троянские программы обычно проникают на компьютер как сетевые черви, а различаются между собой по тем действиям, которые они производят на зараженном компьютере.

Хакерские утилиты и прочие вредоносные программы.

К данной категории относятся:

- **утилиты автоматизации создания вирусов, червей и троянских программ;**
- **программные библиотеки, разработанные для создания вредоносного ПО;**
- **хакерские утилиты скрытия кода зараженных файлов от антивирусной проверки;**
- **программы, сообщающие пользователю заведомо ложную информацию о своих действиях в системе;**
- **прочие программы, тем или иным способом намеренно наносящие прямой или косвенный ущерб данному или удаленным компьютерам.**

ОСОБЕННОСТИ АЛГОРИТМА РАБОТЫ



ОСОБЕННОСТИ АЛГОРИТМА РАБОТЫ

Резидентный вирус при инфицировании компьютера оставляет в оперативной памяти свою резидентную часть, которая затем перехватывает обращения операционной системы к объектам заражения и внедряется в них. Резидентные вирусы находятся в памяти и являются активными вплоть до выключения компьютера или перезагрузки операционной системы.

Нерезидентные вирусы не заражают память компьютера и сохраняют активность ограниченное время. Резидентными можно считать макро-вирусы, поскольку они постоянно присутствуют в памяти компьютера на все время работы зараженного редактора.

Использование ***стел-алгоритмов*** позволяет вирусам полностью или частично скрыть себя в системе. Наиболее распространенным стелс-алгоритмом является перехват запросов ОС на чтение/запись зараженных объектов. Стелс-вирусы при этом либо временно лечат их, либо «подставляют» вместо себя незараженные участки информации.

ОСОБЕННОСТИ АЛГОРИТМА РАБОТЫ

Самошифрование и полиморфичность используются практически всеми типами вирусов для того, чтобы максимально усложнить процедуру детектирования вируса. ***Полиморфик-вирусы*** - это достаточно труднообнаружимые вирусы, не имеющие сигнатур, т.е. не содержащие ни одного постоянного участка кода. В большинстве случаев два образца одного и того же полиморфик-вируса не будут иметь ни одного совпадения. Это достигается шифрованием основного тела вируса и модификациями программы-расшифровщика.

Различные ***нестандартные приемы*** часто используются в вирусах для того, чтобы как можно глубже спрятать себя в ядре ОС, защитить от обнаружения свою резидентную копию, затруднить лечение от вируса и т.д.

Физкульминутка

Упражнение первое:

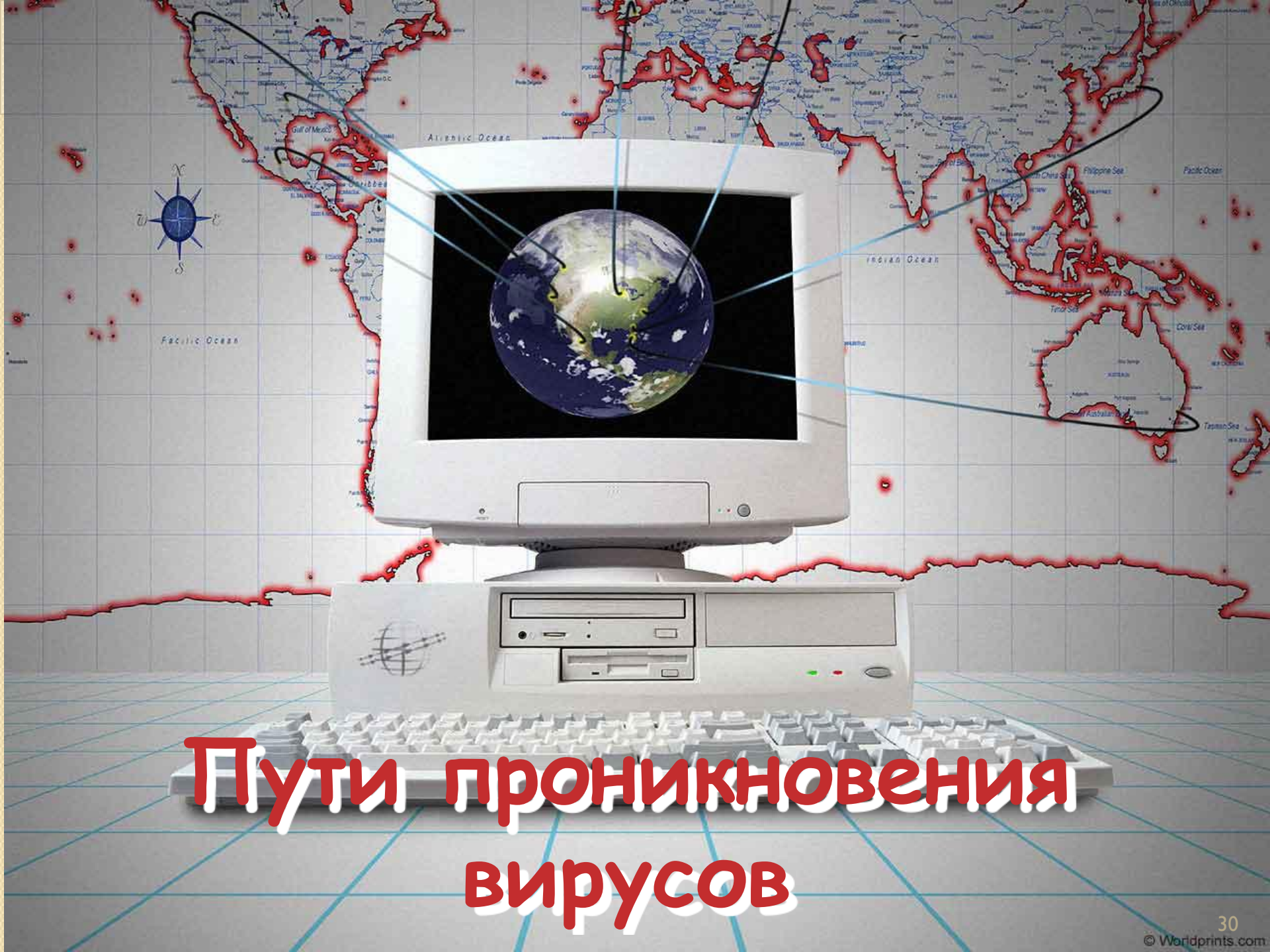
резко зажмурить глаза на 2-3 секунды: и широко открыть на 2-3 секунды, повторить упражнение 10 раз.

Упражнение второе:

часто-часто моргать глазами, повторить 10 раз.

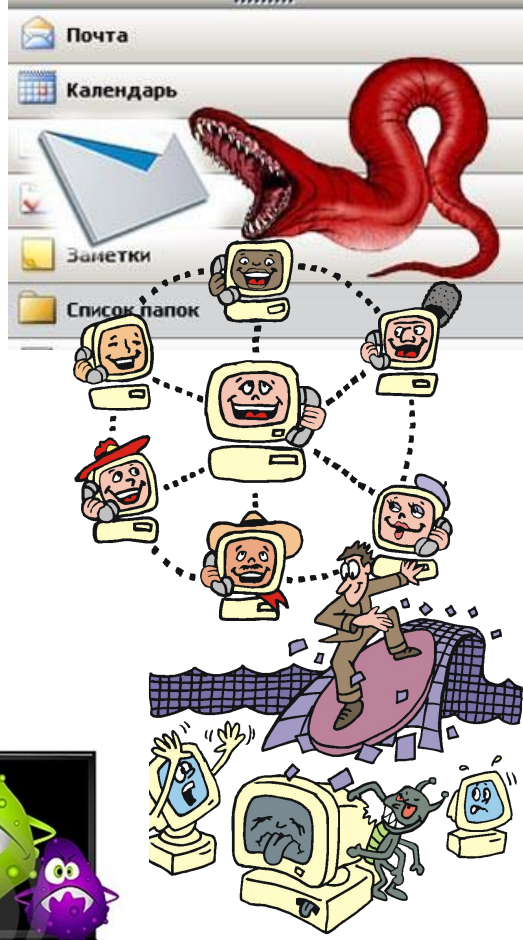
Упражнение третье:

поднять глаза вверх, при этом голова остается в одном положении, задержать взгляд на 2-3 секунды, затем опустить глаза вниз и задержать взгляд на 2-3 секунды повторить упражнение 10 раз .



Пути проникновения вирусов

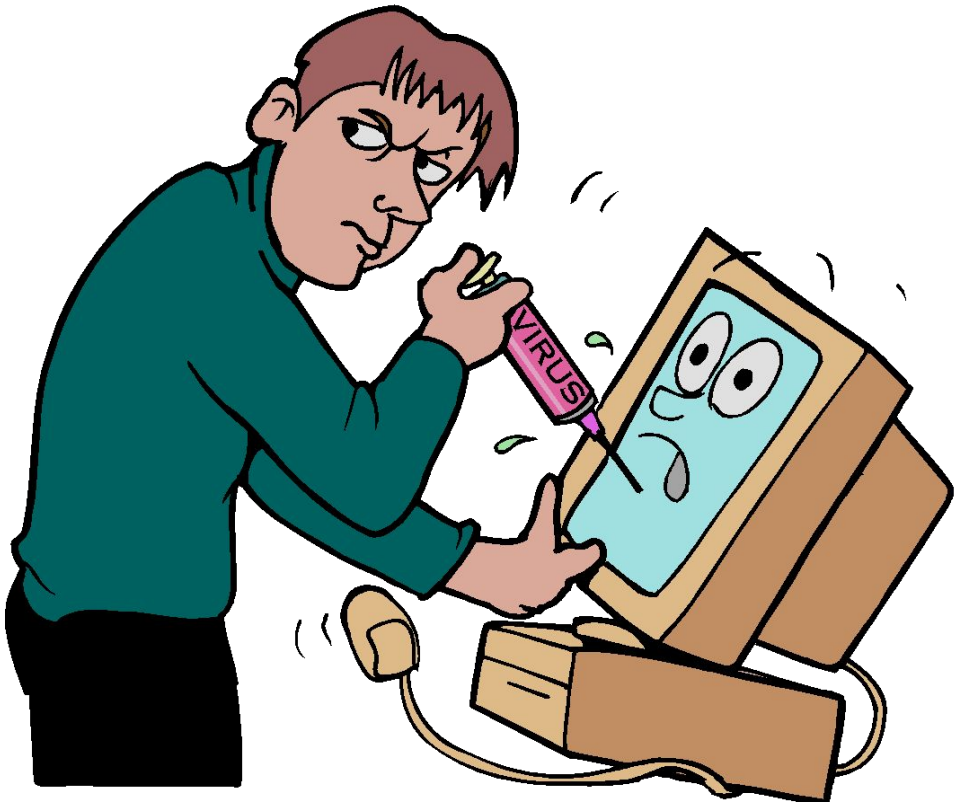
- Глобальная сеть Internet
- Электронная почта
- Локальная сеть
- Компьютеры «Общего назначения»
- Пиратское программное обеспечение
- Ремонтные службы
- Съемные накопители



Методы защиты

- Защита локальных сетей
- Использование дистрибутивного ПО
- Резервное копирование информации
- Использование антивирусных программ
- Не запускать непроверенные файлы

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**

Антивирусные программы

- Программы детекторы;
- программы-доктора или фаги;
- программы-ревизоры;
- программы-фильтры;
- программы-вакцины или иммунизаторы.

Программы-детекторы

Назначение – обнаружить вирусы.

Принцип работы антивирусных сканеров основан на проверке файлов, секторов и системной памяти и поиске в них вирусов

Программы-доктора

не только находят зараженные вирусами файлы, но и «лечат» их, то есть удаляют из файла тело программы-вируса, возвращая файлы в исходное состояние

Принцип работы антивирусных сканеров основан на проверке файлов, секторов и системной памяти и поиске в них вирусов

Программы-ревизоры

Принцип их работы состоит в подсчете контрольных сумм для присутствующих на диске файлов/системных секторов.

Эти суммы затем сохраняются в базе данных антивируса, как, впрочем, и некоторая другая информация: длины файлов, даты их последней модификации и т.д. При последующем запуске CRC-сканеры сверяют данные, содержащиеся в базе данных, с реально подсчитанными значениями.

Если информация о файле, записанная в базе данных, не совпадает с реальными значениями, то CRC-сканеры сигнализируют о том, что файл был изменен или заражен вирусом.

Программы-фильтры

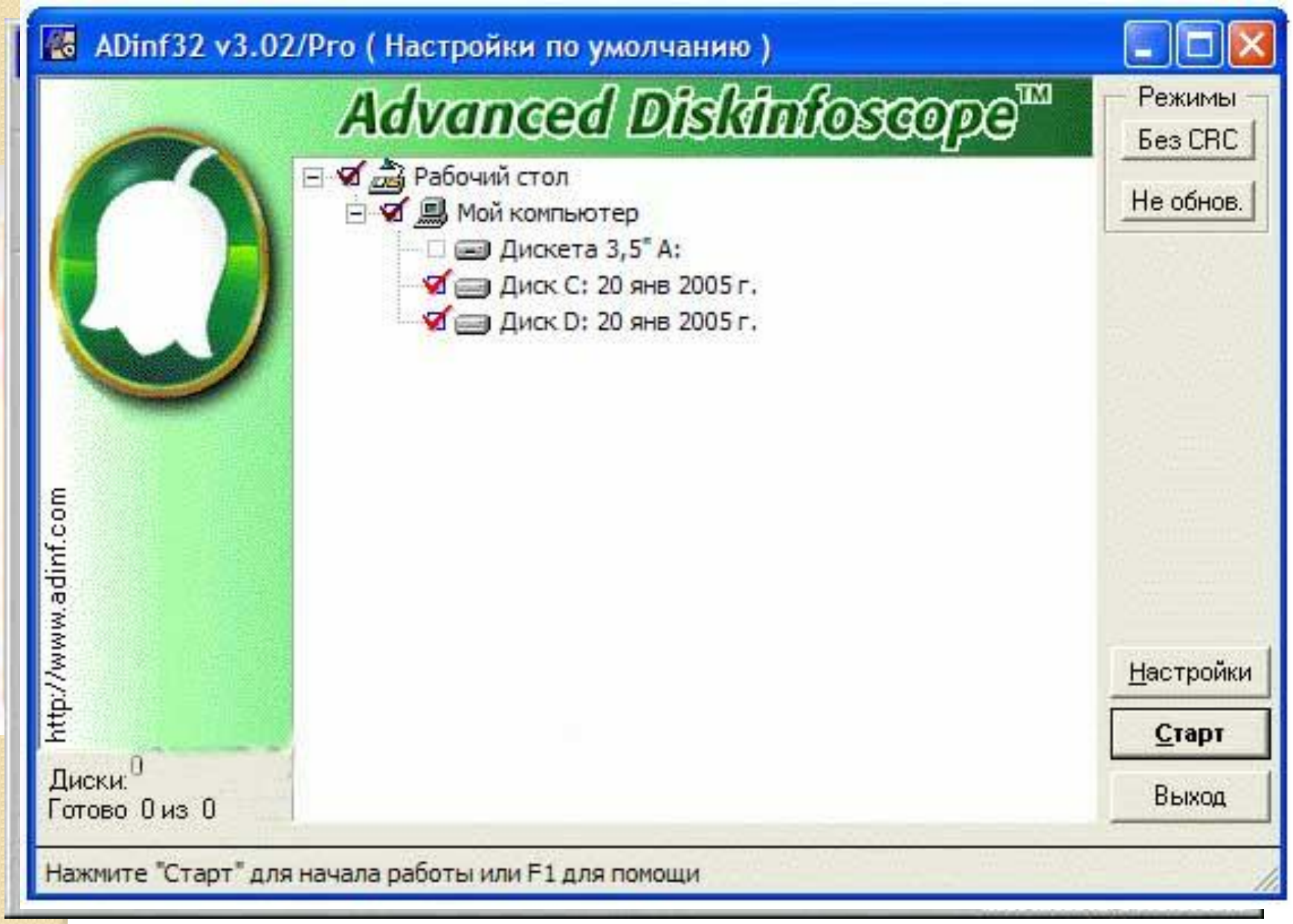
Это резидентные программы, перехватывающие «вирусо-опасные» ситуации и сообщающие об этом пользователю.

К «вирусо-опасным» относятся вызовы на открытие для записи в выполняемые файлы, запись в boot-сектора дисков или винчестера, попытки программ остаться резидентно и т.д., то есть вызовы, которые характерны для вирусов в моменты из размножения.

Программы-вакцины

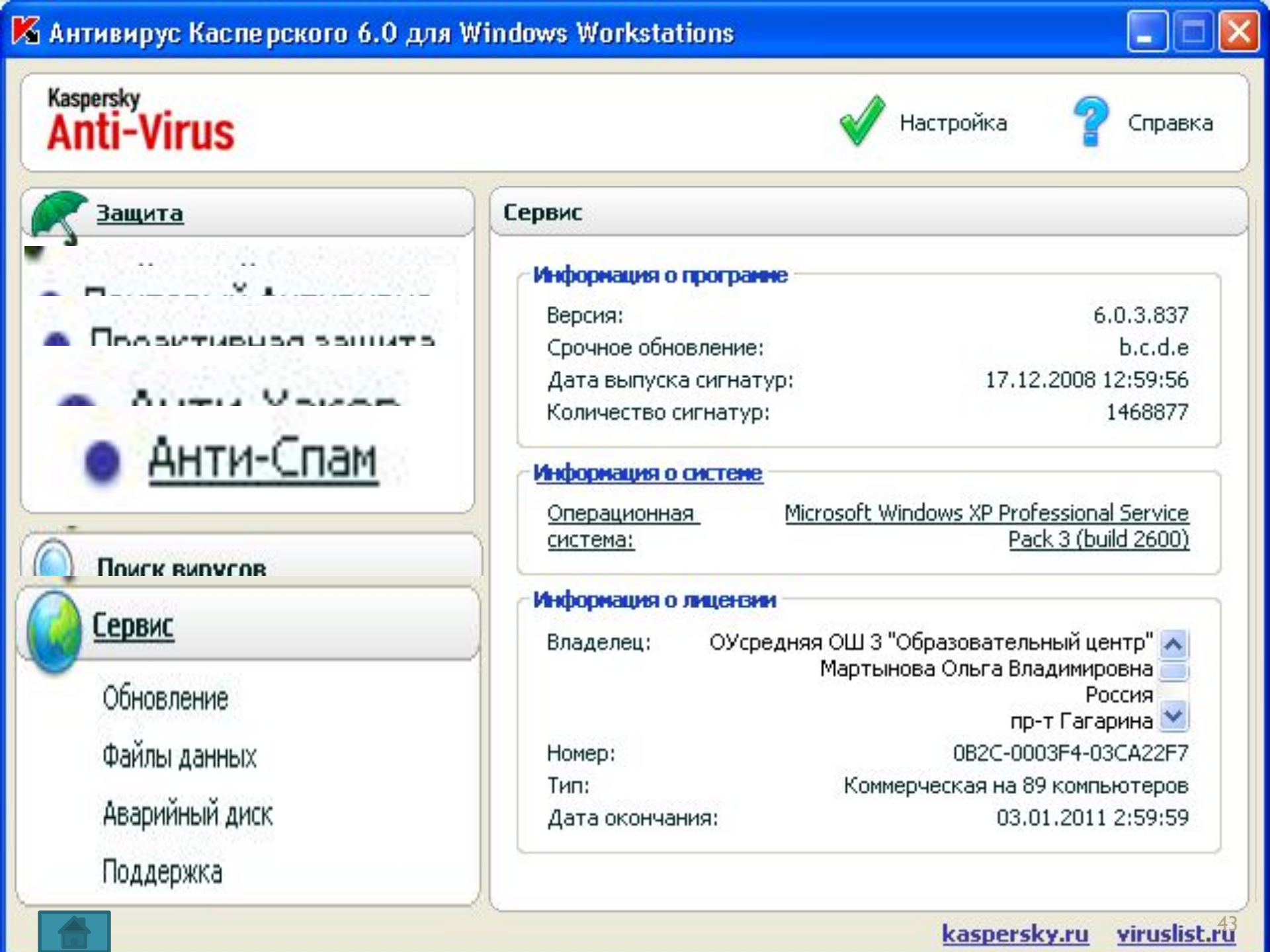
***Вакцины* или *иммунизаторы* - это резидентные программы, предотвращающие заражение файлов.**

Иммунизаторы делятся на два типа: иммунизаторы, сообщающие о заражении, и иммунизаторы, блокирующие заражение каким-либо типом вируса.


ADinf32 v3.02/Pro (Настройки по умолчанию)
Advanced Diskinfoscope™
Режимы
Без CRC
Не обнов.
Рабочий стол
Мой компьютер
Дискета 3,5" A:
Диск C: 20 янв 2005 г.
Диск D: 20 янв 2005 г.
http://www.adinf.com
Диски: 0
Готово 0 из 0
Настройки
Старт
Выход
Нажмите "Старт" для начала работы или F1 для помощи

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

СРЕДСТВА ЗАЩИТЫ ПЕРСОНАЛЬНОЙ ИНФОРМАЦИИ

- *антивирусные программы*
- *брандмауэры или файрволы*
- *антишпионы*

Функции файрвола

- информирует пользователя о попытках извне получить несанкционированный доступ к ресурсам данного компьютера, а также блокирует эти попытки;
- предотвращает попытки несанкционированно передать в сеть информацию с вашего компьютера (хищение паролей и конфиденциальной информации);
- отслеживает любые изменения в размерах выполняемых файлов, которые могут быть свидетельством заражения вирусом;
- блокирует рекламные окна на интернетовских сайтах;

Функции файрвола

- предупреждает, когда одна программа пытается запустить другую программу (это тоже может быть следствием работы вируса);
- закрывает от возможного доступа определенные сетевые порты компьютера;
- предупреждает о так называемом сканировании портов вашего компьютера, так как это может быть предвестником хакерской атаки;
- блокирует выполнение различных шпионских программ;
- предотвращает деструктивные действия троянских программ.

Пути проникновения рекламных шпионов

- **скачивание бесплатного программного обеспечения;**
- **вирусы и трояны;**
- **сайты сомнительного содержания.**

ПАМЯТКА
безопасности для пользователя домашнего компьютера

- Ограничить физический доступ к компьютеру, установить пароль на вход в систему и отключать доступ в Интернет, когда он не нужен;
- подписаться на информационные бюллетени Microsoft и регулярно обновлять операционную систему;
- отключить все неиспользуемые службы и закрыть порты, через которые могут осуществляться атаки;
- тщательно настроить все программы, работающие с Интернет, начиная с браузера — например, запретить использование Java и ActiveX;
- установить и обновлять антивирусную программу;

Домашнее задание:

- Подготовить сообщения: **«Виды компьютерных вирусов»**