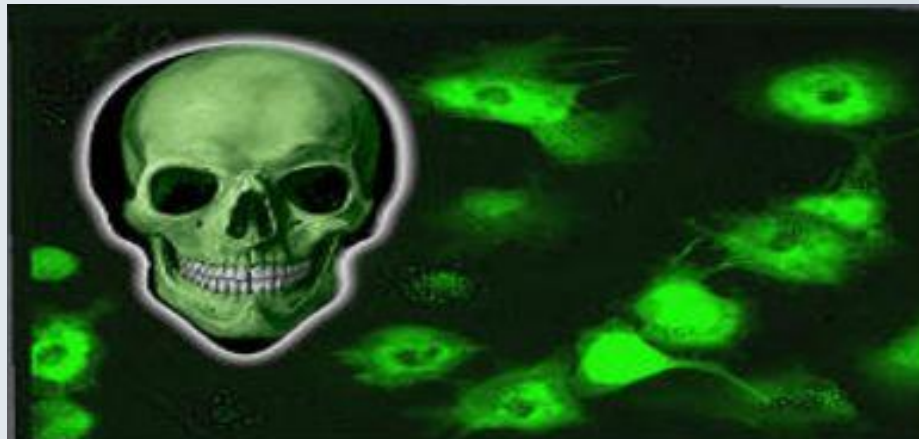


# Компьютерные вирусы и защита от них.



# Что такое компьютерный вирус?

■ Компьютерный вирус – это специально написанная небольшая по размерам программа, которая может «приписывать» себя к другим программам, а также выполнять различные нежелательные действия на компьютере. Программа, внутри которой находится вирус, называется «зараженной». Когда такая программа начинает работу, то сначала управление получает вирус. Вирус находит и «заражает» другие программы, а также выполняет какие-нибудь вредные действия (например, портит файлы или таблицу размещения файлов на диске, «засоряет» оперативную память и т.д.).

■ **Вирус** – это программа, обладающая способностью к самовоспроизведению. Такая способность является единственным свойством, присущим всем типам вирусов. Вирус не может существовать в «полной изоляции». Это означает, что сегодня нельзя представить себе вирус, который бы так или иначе не использовал код других программ, информацию о файловой структуре или даже просто имена других программ. Причина этого довольно понятна: вирус должен каким-нибудь способом обеспечить передачу себе управления.



- В настоящее время известно более 5000 программных вирусов, их можно классифицировать по следующим признакам:

1) среде обитания

2) способу заражения

3) механизму

4) особенностям алгоритма

# Классификация вирусов



В зависимости от среды обитания вирусы можно разделить на:

- **Сетевые вирусы** распространяются по различным компьютерным сетям.
- **Файловые вирусы** внедряются главным образом в исполняемые модули, т. е. в файлы, имеющие расширения COM и EXE. Файловые вирусы могут внедряться и в другие типы файлов, но, как правило, записанные в таких файлах, они никогда не получают управление и, следовательно, теряют способность к размножению.
- **Загрузочные вирусы** внедряются в загрузочный сектор диска (Boot-сектор) или в сектор, содержащий программу загрузки системного диска (Master Boot Record).
- **Файлово-загрузочные вирусы** заражают как файлы, так и загрузочные сектора дисков.



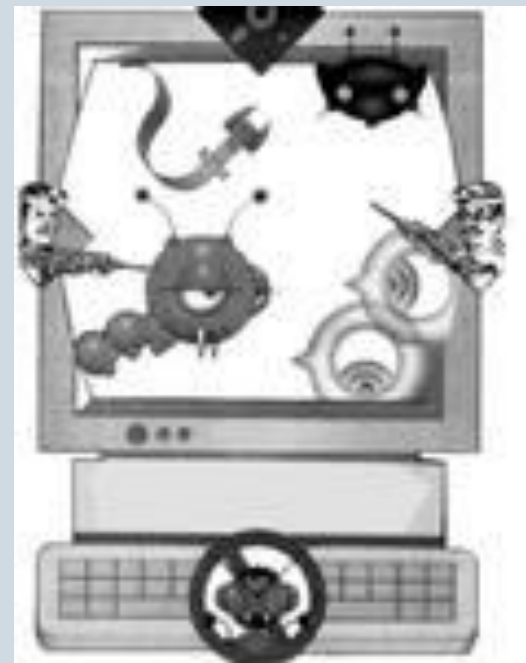
# По способу заражения вирусы делятся на:

- **Резидентные вирусы** при заражении компьютера оставляют в оперативной памяти свою резидентную часть, которая потом перехватывает обращение операционной системы к объектам заражения (файлам, загрузочным секторам дисков и т. п.) и внедряется в них. Резидентные вирусы находятся в памяти и являются активными вплоть до выключения или перезагрузки компьютера.
- **Нерезидентные вирусы** не заражают память компьютера и являются активными ограниченное время.



# По степени воздействия вирусы можно разделить на следующие виды:

- **Неопасные**, не мешающие работе компьютера, но уменьшающие объем свободной оперативной памяти и памяти на дисках, действия таких вирусов проявляются в каких-либо графических или звуковых эффектах.
- **Опасные**, которые могут привести к различным нарушениям в работе компьютера.
- **Очень опасные**, воздействие которых может привести к потере программ, уничтожению данных, стиранию информации в системных областях диска.



# По особенностям алгоритма вирусы трудно классифицировать из-за большого разнообразия.

- Простейшие вирусы - паразитические, они изменяют содержимое файлов и секторов диска и могут быть достаточно легко обнаружены и уничтожены.
- Вирусы-репликаторы(черви)- распространяются по компьютерным сетям, вычисляют адреса сетевых компьютеров и записывают по этим адресам свои копии.



- **Вирусы-невидимки (стелс-вирусы)** - очень трудно обнаружить и обезвредить, так как они перехватывают обращения операционной системы к пораженным файлам и секторам дисков и подставляют вместо своего тела незараженные участки диска.
- **Вирусы-мутанты** - содержат алгоритмы шифровки-расшифровки, благодаря которым копии одного и того же вируса не имеют ни одной повторяющейся цепочки байтов.
- **Квазивирусные или «тройные» программы** - хотя они и не способны к самораспространению, но очень опасны, так как, маскируясь под полезную программу, разрушают загрузочный сектор и файловую систему дисков.



## Для защиты от вирусов можно использовать:

- Общие средства защиты информации, которые полезны также и как страховка от физической порчи дисков, неправильно работающих программ или ошибочных действий пользователя;
- Профилактические меры, позволяющие уменьшить вероятность заражения вирусом;
- Специализированные программы для защиты от вирусов.





# Программы-детекторы

позволяют обнаруживать файлы, зараженные одним из нескольких известных вирусов. Эти программы проверяют, имеется ли в файлах на указанном пользователем диске специфическая для данного вируса комбинация байтов. При ее обнаружении в каком-либо файле на экран выводится соответствующее сообщение. Многие детекторы имеют режимы лечения или уничтожения зараженных файлов. Следует подчеркнуть, что программы-детекторы могут обнаружить вирусы, которые ей "известны".



# Программы-ревизоры

- имеют две стадии работы. Сначала они запоминают сведения о состоянии программ и системных областей дисков (загрузочного сектора и сектора с таблицей разбиения жесткого диска). Предполагается, что в этот момент программы и системные области дисков не заражены. После этого с помощью программы-ревизора можно в любой момент сравнить состояние программ и системных областей дисков с исходным. О выявленных несоответствиях сообщается пользователю.

# Программы-фильтры

- располагаются резидентно в оперативной памяти компьютера и перехватывают те обращения к операционной системе, которые используются вирусами для размножения и нанесения вреда, и сообщают о них пользователя. Пользователь может разрешить или запретить выполнение соответствующей операции.

Некоторые программы-фильтры не "ловят" подозрительные действия, а проверяют вызываемые на выполнение программы на наличие вирусов. Это вызывает замедление работы компьютера.

Однако преимущества использования программ-фильтров весьма значительны – они позволяют обнаружить многие вирусы на самой ранней стадии, когда вирус еще не успел размножиться и что-либо испортить. Тем самым можно свести убытки от вируса к минимуму.

# Программы-вакцины (Иммунизаторы)

- модифицируют программы и диски таким образом, что это не отражается на работе программ, но тот вирус, от которого производится вакцинация, считает эти программы или диски уже зараженными. Эти программы крайне неэффективны.



# AIDSTEST

## Антивирусные программы

В нашей стране, особую популярность

Украине практически на каждом IBM-совместимом персональном компьютере есть одна из версий этой программы. Одна из последних версия обнаруживает более 8000 вирусов.

# DOCTOR WEB

- В последнее время стремительно растет популярность другой антивирусной программы - Doctor Web. Dr.Web так же, как и Aidstest относится к классу детекторов - докторов, но в отличие от последнего, имеет так называемый "эвристический анализатор" - алгоритм, позволяющий обнаруживать неизвестные вирусы. "Лечебная паутина", как переводится с английского название программы, стала ответом отечественных программистов на нашествие самомодифицирующихся вирусов-мутантов. Последние при размножении модифицируют свое тело так, что не остается ни одной характерной цепочки байт, присутствовавшей в исходной версии вируса. Dr.Web можно назвать антивирусом нового поколения по сравнению с Aidstest и его аналогами.



## Dr.Web + ключ

Версия продукта: v.5.0

Инструкция: присутствует

Язык интерфейса: русский

Платформа: Windows 95 – XP, Vista

Функциональность: полная

# Microsoft Antivirus

- В состав современных версий MS-DOS (например, 7.10) входит антивирусная программа Microsoft Antivirus (MSAV). Этот антивирус может работать в режимах детектора-доктора и ревизора.

- Avast!Antivirus



**Avast AntiVirus + лицензия**

Версия продукта: *все версии*  
Инструкция: *4.8.1169 prof. edition*  
Язык интерфейса: *русский, english*  
Платформа: *Windows 95 – Vista*  
Функциональность: *полная*



**Avast AntiVirus + лицензия**

Версия продукта: *все версии*  
Инструкция: *4.8.1169 prof. edition*  
Язык интерфейса: *русский, english*  
Платформа: *Windows 95 – Vista*  
Функциональность: *полная*



# ADINF(Advanced DiskinfoScope)

- ADinf относится к классу программ-ревизоров. Антивирус имеет высокую скорость работы, способен с успехом противостоять вирусам, находящимся в памяти. Он позволяет контролировать диск, читая его по секторам через BIOS и не используя системные прерывания DOS, которые может перехватить вирус.





## Ключи Касперского + программы

### для поиска ключей

Версия продукта: *все версии*  
Инструкция: *присутствует*  
Язык интерфейса: *русский*  
Платформа: *Win 2000, XP, Vista*  
Функциональность: *полная*



## Kaspersky Antivirus + ключи

Версия продукта: *2009*  
Инструкция: *присутствует*  
Язык интерфейса: *русский*  
Платформа: *Windows XP, Vista*  
Функциональность: *полная*



## **NOD32 + ключи**

**+ автопоиск ключей**

Версия продукта: v3.0.672

Инструкция: *присутствует*

Язык интерфейса: *русский*

Платформа: *Windows XP, Vista*

Функциональность: *полная*



## **NOD 32**

**(ключи не требуются)**

Версия продукта: v2.7

Инструкция: *присутствует*

Язык интерфейса: *русский*

Платформа: *Windows NT/2000/XP*

Функциональность: *полная*