

Компьютерная презентация на тему: «Компьютерные вирусы и антивирусные программы»

**Автор: Ученика 6 «Б» класса
Гимназия № 7 (полного дня)
Кучер Ивана
ПРЕПОДАВАТЕЛЬ:
Сквалецкая Татьяна Юрьевна г.
Оренбург**

Содержание

- ❖ Введение
- ❖ Понятие компьютерного вируса
- ❖ Признаки заражения компьютера
- ❖ История возникновения вирусов
- ❖ Классификаций компьютерных вирусов
- ❖ Пути проникновения вирусов на компьютер
- ❖ Методы защиты от компьютерных вирусов
- ❖ Антивирусные программы

Введение



Персональный компьютер играет в жизни современного человека важную роль, поскольку он помогает ему почти во всех областях его деятельности. Современное общество все больше вовлекается в виртуальный мир Интернета. Но с активным развитием глобальных сетей актуальным является вопрос информационной безопасности, так как проникающие их сети вирусы могут нарушить целостность и сохранность вашей информации.

Защита компьютера от вирусов – это та задача, решать которую приходится всем пользователям, и особенно тем, кто активно пользуется Интернетом или работает в локальной сети.

Понятие компьютерного вируса

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

*Энциклопедия вирусов
«Лаборатории Касперского»*



Общее 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.

Признаки заражения компьютера:

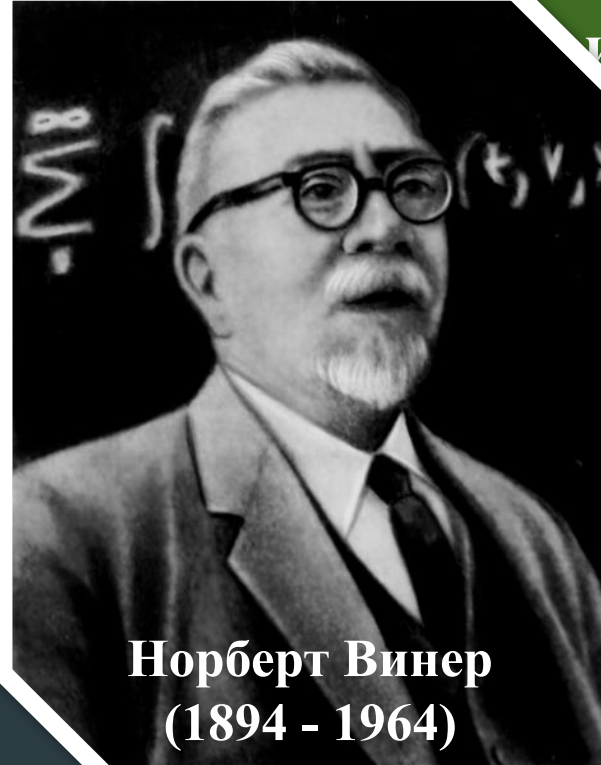
- некоторые программы перестают работать или работают с ошибками;
- размер некоторых исполнимых файлов и время их создания изменяются. В первую очередь это происходит с командным процессором, его размер увеличивается на величину размера вируса;
- на экран выводятся посторонние символы и сообщения, появляются странные видео и звуковые эффекты;
- работа компьютера замедляется и уменьшается размер свободной оперативной памяти;
- некоторые файлы и диски оказываются испорченными (иногда необратимо, если вирус отформатирует диск);
- компьютер перестает загружаться с жесткого диска.

История возникновения вирусов

Первые вирусы появились давно, еще на заре эпохи ЭВМ, и не всегда были вредоносными. Например, в конце 60-х в лаборатории Хероха была создана специальная



Джон фон Нейман
(1903 - 1957)

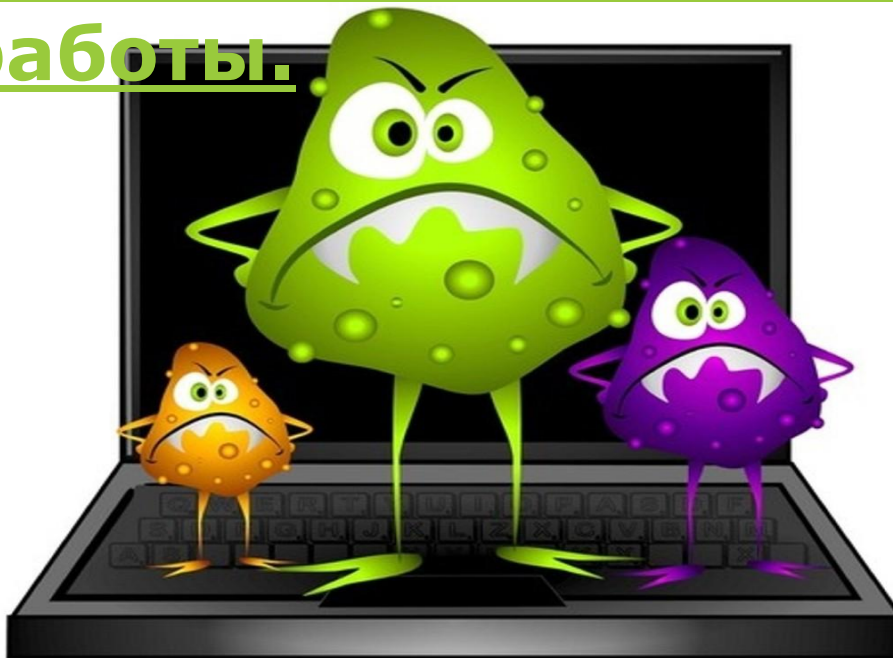


Норберт Винер
(1894 - 1964)

прообра вирусов, кото путеш льной выч и про бность вклю ств. про стали разр им умы , что неко спе овали ком в, чтобы онить за н строя их темы. П ования щихся искусственных конструкций проводилась в середине прошлого столетия учеными Джоном фон Нейманом и Норбинтом Винером.

Классификаций компьютерных вирусов:

1. по среде их обитания;
2. по способу заражения;
3. по степени воздействия;
4. по особенностям алгоритма работы.



1. по среде их обитания:

Компьютерный вирус

```
graph TD; A[Компьютерный вирус] --> B[Программные (файловые)]; A --> C[Загрузочные]; A --> D[Макровирусы]; A --> E[Сетевые вирусы];
```

Программные (файловые)

Это блоки программного кода, внедренные внутрь других прикладных программ.

Вирусный код запускается при запуске программы.

Загрузочные

Вирусы, которые располагаются в служебных секторах носителей данных на (гибких и жестких дисках).

Заражение происходит при загрузке данных с зараженного носителя.

Макровирусы

Поражают документы, выполненные в некоторых прикладных программах (например, Word).

Заражение происходит при открытии файла документа в окне программы.

Сетевые вирусы

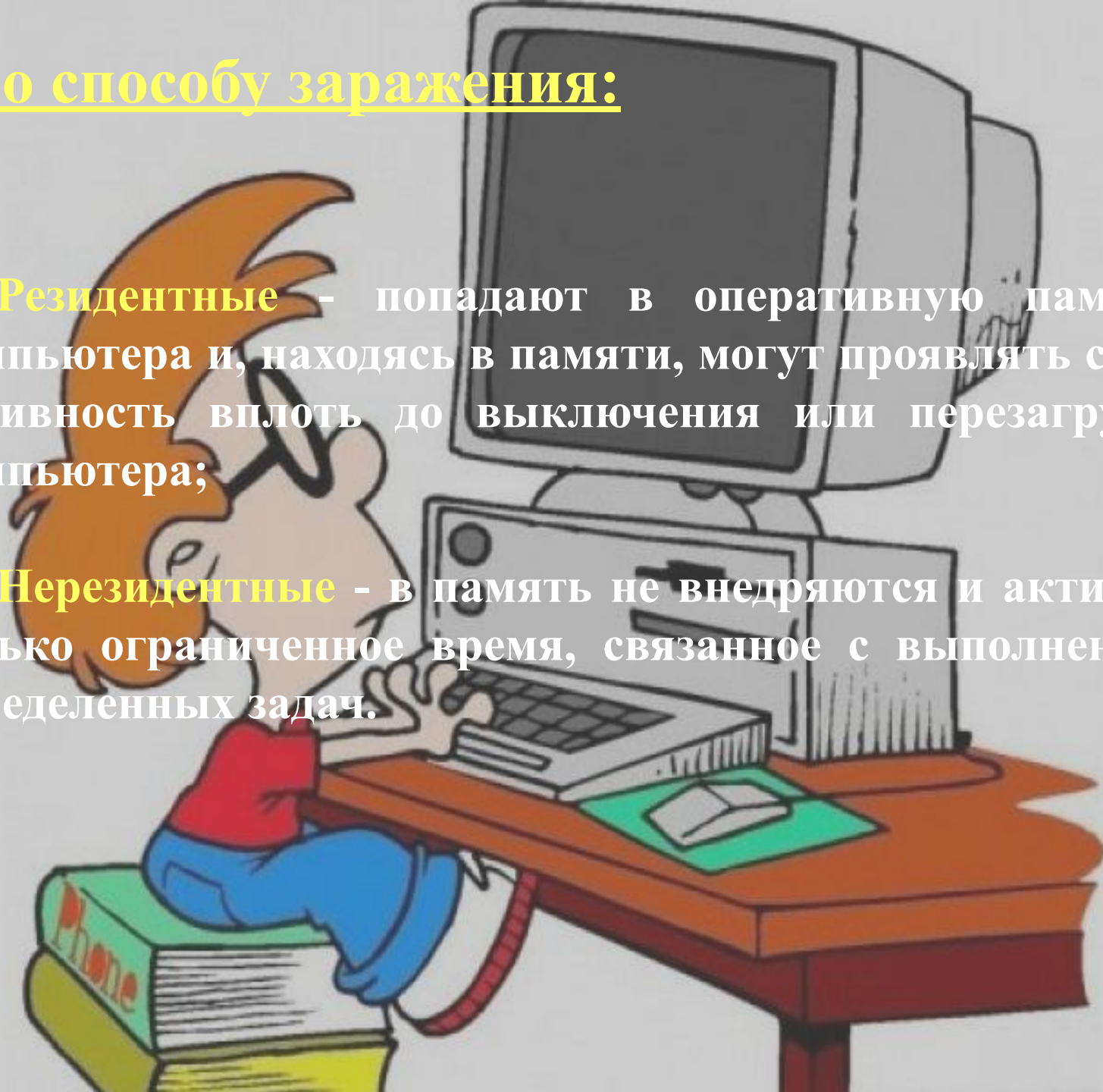
Вирусы, обитающие в оперативной памяти компьютера и не могут располагаться на дискетках.

На отдельных компьютерах, которые не соединены сетью, они существовать не могут.

2. по способу заражения:

Резидентные - попадают в оперативную память компьютера и, находясь в памяти, могут проявлять свою активность вплоть до выключения или перезагрузки компьютера;

Нерезидентные - в память не внедряются и активны только ограниченное время, связанное с выполнением определенных задач.



3. по степени воздействия:

Компьютерный вирус

```
graph TD; A[Компьютерный вирус] --> B[Безвредные]; A --> C[Неопасные]; A --> D[Опасные]; A --> E[Очень опасные];
```

Безвредные

никак не влияющие на работу компьютера (кроме уменьшения свободной памяти на диске в результате своего распространения).

Неопасные

не мешают работе компьютера, но уменьшают объем свободной оперативной памяти и памяти на дисках, действия таких вирусов проявляются в каких-либо графических или звуковых эффектах.

Опасные

могут привести к различным нарушениям в работе компьютера.

Очень опасные

воздействие этих вирусов может привести к потере программ, уничтожению данных, стиранию информации в системных областях диска.

4. по особенностям алгоритма работы:

- **Простейшие** - 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** - содержащие алгоритмы шифровки-расшифровки, благодаря которым копии одного и того же вируса не имеют ни одной повторяющейся цепочки байтов;
- **Квазивирусные («тройные» программы)** - не способны к самораспространению, но очень опасны, так как, маскируясь под полезную программу, разрушают загрузочный сектор и файловую систему дисков.

Пути проникновения вирусов на компьютер:

- ◆ Глобальная сеть Internet .
- ◆ Электронная почта.
- ◆ Локальная сеть.
- ◆ Компьютеры «Общего назначения».
- ◆ Пиратское программное обеспечение.
- ◆ Ремонтные службы.
- ◆ Съёмные накопители, на которых находятся заражённые вирусом файлы.
- ◆ Жёсткий диск, на который попал вирус.
- ◆ Вирус, оставшийся в оперативной памяти после предшествующего пользователя.

Методы защиты от компьютерных вирусов

- Установите на свой персональный компьютер современную антивирусную программу.
- Перед просмотром информации принесенной на флэш-карте (дискете) с другого компьютера проверьте носитель антивирусом.
- 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).
- Периодически проверяйте компьютер на вирусы (если активно пользуетесь Интернетом – запускайте раз в неделю, а то и чаще).
- Как можно чаще делайте резервные копии важной информации (backup).
- Используйте совместно с антивирусной программой файервол (firewall) если компьютер подключен к Интернет.
- Настройте браузер (программа просмотра Интернет страниц – IE, Opera и т.д.) для запрета запуска активного содержимого html-страниц.

Антивирусные программы

предназначены для предотвращения заражения компьютера вирусом и ликвидации последствий заражения.



В зависимости от назначения и принципа действия различают следующие антивирусные программы:

Сторожа или детекторы – предназначены для обнаружения файлов зараженных известными вирусами, или признаков указывающих на возможность заражения.

Доктора – предназначены для обнаружения и устранения известных им вирусов, удаляя их из тела программы и возвращая ее в исходное состояние. Наиболее известными представителями являются Dr.Web, AidsTest, Norton Anti Virus.

Ревизоры – они контролируют уязвимые и поэтому наиболее атакуемые компоненты компьютера, запоминают состояние служебных областей и файлов, а в случае обнаружения изменений сообщают пользователю.

Резидентные мониторы или фильтры – постоянно находятся в памяти компьютера для обнаружения попыток выполнить несанкционированные действия. В случае обнаружения подозрительного действия выводят запрос пользователю на подтверждение операций.

Вакцины – имитируют заражение файлов вирусами. Вирус будет воспринимать их зараженными и не будет внедряться. Чаще всего используются Aidstest Лозинского, Drweb, Dr.Solomon.