

# Компьютерные вирусы и антивирусные программы.

The image features the Microsoft Windows 95 logo, which is a stylized flag with four colored panes (red, green, blue, yellow) on a black background. The logo is set against a blue sky with white clouds. The word "Microsoft" is written in a light grey font above the logo, and "Windows 95" is written in a large, bold, black font below it.

Microsoft  
Windows 95

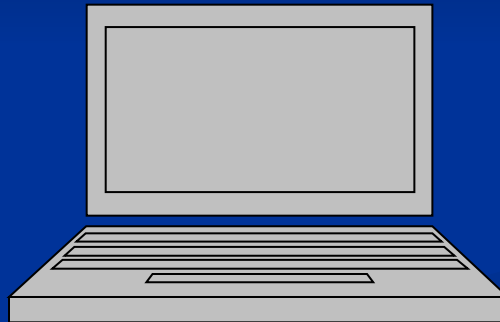
Презентация подготовлена для  
конкурса «Интернешка»

<http://interneshka.org>

Выполнил:  
Чернов Иван  
ученик 9-го класса  
МБОУ школа №4  
г. Кинешма,  
Ивановская область



Что такое?



Что такое?

Какие они бывают

происхождение

Как появились

Профилактика вирусов

# Что делать, если заражение уже произошло

- Отключиться о сети «Интернет».
- Отключить питание компьютера, тем самым прекратить распространение вируса.
- Запустить программу-антивирус с внешнего носителя.



■ Компьютерный вирус — вид вредоносного программного обеспечения, способного создавать копии самого себя и внедряться в код других программ, системные области памяти, загрузочные секторы, а также распространять свои копии по разнообразным каналам связи.



- Как правило, целью вируса является нарушение работы программно-аппаратных комплексов: удаление файлов, приведение в негодность структур размещения данных, блокирование работы пользователей или же приведение в негодность аппаратных комплексов компьютера и т. п. Даже если автор вируса не запрограммировал вредоносных эффектов, вирус может приводить к сбоям компьютера из-за ошибок, неучтённых тонкостей взаимодействия операционной системой и другими программами. Кроме того, вирусы, как правило, занимают место на накопителях информации и потребляют некоторые другие ресурсы системы.



# Что такое **антивирус**?

Программа направленная на обнаружение и уничтожение вирусов, восстановление повреждённых файлов.

Наиболее распространенные антивирусы:

Касперский

Avira

ESET NOD 32

Dr.Web

Avast





# Компьютерные вирусы

бывают

следующих типов:



- 1.Файловые вирусы.
- 2.Загрузочные вирусы.
- 3.Вирусы поражающие драйверы.
- 4.Невидимые или СТЕЛС-вирусы.
- 5.Самомодифицирующиеся вирусы.
  - 6.Сетевые вирусы.
  - сетевые черви (червь Морриса, 1987).
    - «тройанские кони» (AIDS1989).
  - полиморфные вирусы (Chameleon, 1990),



# История компьютерных вирусов

- Основы теории самовоспроизводящихся механизмов заложил американец венгерского происхождения Джон фон Нейман, который в 1951 году предложил метод создания таких механизмов. С 1961 года известны рабочие примеры таких программ.
- Первыми известными вирусами являются **Virus 1,2,3** и **Elk Cloner** для ПК **Apple II**, появившиеся в 1981 году
- Первые вирусные эпидемии относятся к 1986-1989 годам
- Вирус **Brain.A** (распространялся в загрузочных секторах дискет, вызвал крупнейшую эпидемию)
- Вирус **червь Морриса** (свыше 6200 компьютеров, большинство сетей вышло из строя на срок до пяти суток)
- Вирус **DATA CRIME** (около 100 тысяч зараженных ПЭВМ только в Нидерландах).
- В 1996 году появился первый вирус для **WINDOWS 95** — **Win95.Boza**, а в декабре того же года — первый резидентный вирус для неё — **Win95.Punch**.



# История компьютерных антивирусов

- В начале 1985 года Ги Вонг (англ. Gee Wong) написал программу **DPROTECT** — первый резидентный антивирус.
- В 1990 году появляются специализированная «Маленькая чёрная книжка о компьютерных вирусах» Марка Людвига, первый коммерческий антивирус **Symantec Norton AntiVirus**.
- .





# Профилактика

- Не работать под привилегированными учётными записями без крайней необходимости. (Учётная запись администратора в Windows)
- Не запускать незнакомые программы из сомнительных источников.
- Стараться блокировать возможность несанкционированного изменения системных файлов.
- Отключать потенциально опасную функциональность системы (например, autorun-носителей в MS Windows, сокрытие файлов, их расширений и пр.).
- Не заходить на подозрительные сайты, обращать внимание на адрес в адресной строке обозревателя.
- Пользоваться только доверенными дистрибутивами.
- Постоянно делать резервные копии важных данных, желательно на носители, которые не стираются (например, BD-R) и иметь образ системы со всеми настройками для быстрого развёртывания.
- Выполнять регулярные обновления часто используемых программ, особенно тех, которые обеспечивают безопасность системы.

