# ВИРУСЫ. АНТИВИРУСНЫЕ ПРОГРАММЫ

**Компьютерный вирус – это программа способная к самораспространению и выполняющая какие-либо нежелательные действия.**

**Обычно целью компьютерных вирусов является повреждение информаций пользователя и в худшем случае вывод операционной системы из строя.**

**Вирусы распространяются, внедряя себя в исполняемый код других программ или же заменяя собой другие программы.**

# ВИРУСЫ. АНТИВИРУСНЫЕ ПРОГРАММЫ

## Происхождение термина

**Компьютерный вирус был назван по аналогии с вирусами биологическими. По всей видимости, впервые слово вирус по отношению к программе было употреблено Грегори Бенфордом в фантастическом рассказе «Человек в шрамах», опубликованном в журнале Venture в мае 1970 года.**

**Термин «компьютерный вирус» впоследствии не раз открывался и переоткрывался — так, переменная в программе PERVADE, от значения которой зависело, будет ли программа ANIMAL распространяться по диску, называлась VIRUS.**

# ВИРУСЫ. АНТИВИРУСНЫЕ ПРОГРАММЫ

## Классификация

**1. По признаку операционная система**

- Вирусы для ос семейства windows
- Вирусы для ос UNIX-подобных систем

**2. По среде обитания**

- Загрзочные (заражают boot-сектора жестких дисков)
- Файловые
- Файлово-загрузочные

# ВИРУСЫ. АНТИВИРУСНЫЕ ПРОГРАММЫ

**3. По деструктивным возможностям**

- Безвредные (вирусы, вышедшие из строя по каким-то причинам)
- Неопасные (вирусы, не ведущие к потере информаций)
- Опасные (вирусы способные повредить информацию)

**4. По алгоритму работы**

- Трояны
- Черви
- Полиморфы

# ВИРУСЫ. АНТИВИРУСНЫЕ ПРОГРАММЫ

**«Троян» – это вирус, целью которого являются шпионские действия и информация пользователя. «Трояны» не имеют собственного механизма распространения, и этим отличаются от вирусов, которые распространяются, прикрепляя себя к безобидному ПО или документам.**

# ВИРУСЫ. АНТИВИРУСНЫЕ ПРОГРАММЫ

**«Червь» — разновидность самовоспроизводящихся компьютерных программ, распространяющихся в локальных и глобальных компьютерных сетях. В отличие от других типов компьютерных вирусов червь является самостоятельной программой. Черви могут использовать различные механизмы распространения. Некоторые черви требуют определенного действия пользователя для распространения (например, открытия инфицированного сообщения в клиенте электронной почты). Другие черви могут распространяться автономно, выбирая и атакуя компьютеры в полностью автоматическом режиме.**

# ВИРУСЫ. АНТИВИРУСНЫЕ ПРОГРАММЫ

**«Полиморф» - это вирус способный к самомодификации. Две версии одной программы могут не совпадать ни в одном байте.**

**Обычно свойство полиморфизма в чистом виде у компьютерных вирусов не встречается и идет в комплексе с другими.**

# ВИРУСЫ. АНТИВИРУСНЫЕ ПРОГРАММЫ

## Способы распространения

1. Накопители информации
2. Электронная почта
3. Компьютерная сеть
4. Web-страницы

# ВИРУСЫ. АНТИВИРУСНЫЕ ПРОГРАММЫ

**Антивирусные программы**

- это программы против вирусов.

# ВИРУСЫ. АНТИВИРУСНЫЕ ПРОГРАММЫ

## Классификация

**1. Программы-сканеры: определяют наличие вируса по базе сигнатур, хранящей сигнатуры (или их контрольные суммы) вирусов. Их эффективность определяется актуальностью вирусной базы и наличием эвристического анализатора**

**2. Программы-вакцины: изменяют прививаемый файл таким образом, чтобы вирус, против которого делается прививка, уже считал файл заражѐнным**

# ВИРУСЫ. АНТИВИРУСНЫЕ ПРОГРАММЫ

**3. Программы-ревизоры: запоминают состояние файловой системы, что делает в дальнейшем возможным анализ изменений.**

**4. Программы-сторожа: отслеживают потенциально опасные операции, выдавая пользователю соответствующий запрос на разрешение/запрещение операции.**

# ВИРУСЫ. АНТИВИРУСНЫЕ ПРОГРАММЫ

## Способы защиты

1. **Сигнатурный метод. Основан на антивирусных базах. Сигнатура – это совокупность черт однозначно определяющих наличие вируса в файле.**
2. **Эвристический анализ. Методика эвристического анализа позволяет обнаруживать ранее неизвестные инфекции.**

# ВИРУСЫ. АНТИВИРУСНЫЕ ПРОГРАММЫ

**Примеры антивирусных программ**

- **KAVP – антивирус Касперского (Россия)**
- **NOD32 – антивирус компании ESET (Словакия)**
- **PandaAntivirus – антивирус компаний Panda Software (Испания)**
- **McAfee – антивирус McAfee (США)**
- **Dr.Web – антивирус (Россия)**
- **AVZ – программа без резидентной защиты (Россия)**

**Резидентность – свойство программы, постоянно находиться в ОП.**