КОМПЬЮТЕРНЫЕ ВИРУСЫ, ТИПЫ ВИРУСОВ, МЕТОДЫ БОРЬБЫ С ВИРУСАМИ

Компьютерным вирусом называется программа, способная создавать свои копии (не обязательно полностью совпадающие с оригиналом) и внедрять их в различные объекты или ресурсы компьютерных систем, сетей и так далее без ведома пользователя.

6 основных типов вирусов:

- - файловые,
- - загрузочные,
- - призраки (полиморфные),
- - невидимки,
- - скрипт-вирусы,
- - макро-вирусы.

Вредоносные коды

Интернет-черви

«Троянские кони».

Основные симптомы вирусного поражения:

- - замедление работы некоторых программ,
- - увеличение размеров файлов (особенно выполняемых),
- - появление не существовавших ранее подозрительных файлов,
- - уменьшение объема доступной оперативной памяти (по сравнению с обычным режимом работы),
- - внезапно возникающие разнообразные видео и звуковые эффекты.

Основными путями проникновения вирусов в компьютер являются съемные электронные носители, а также компьютерные сети.

Классификация вирусов по деструктивным возможностям

- 1. Базовые, т.е. никак не влияющие на работу компьютера (кроме уменьшения свободной памяти на диске в результате своего распространения).
- 2. Неопасные, влияние которых ограничивается уменьшением свободной памяти на диске и графически и пр. эффектами.
- 3. Опасные вирусы, которые могут привести к серьезным ошибкам и сбоям в работе .
- 4. Очень опасные, которые могут привести к потере программ, уничтожить данные, стереть необходимую для работы компьютера информацию, записанную в системных областях памяти.

АНТИВИРУСНЫЕ ПРОГРАММЫ

можно классифицировать по пяти основным группам:

- - фильтры,
- - детекторы,
- - ревизоры,
- - доктора,
- - вакцинаторы.

Ни один тип антивирусных программ по отдельности не дает полной защиты от вирусов.

Лучшей **стратегией защиты** от вирусов является **многоуровневая**, "эшелонированная" **оборона**.

Средствам разведки в "обороне" от вирусов соответствуют

программы-детекторы,

позволяющие проверять вновь полученное программное обеспечение на наличие вирусов.

На переднем крае обороны находятся

программы-фильтры.

Эти программы могут первыми сообщить о работе вируса и предотвратить заражение программ и дисков.

Второй эшелон обороны составляют

программы-ревизоры, программы-доктора и доктора-ревизоры.

Самый глубокий эшелон обороны - это

средства разграничения доступа.

Они не позволяют вирусам и неверно работающим программам, даже если они проникли в компьютер, испортить важные данные.