

Компьютерные вирусы и борьба с ними

Учитесь работать безопасно и
аккуратно

Введение

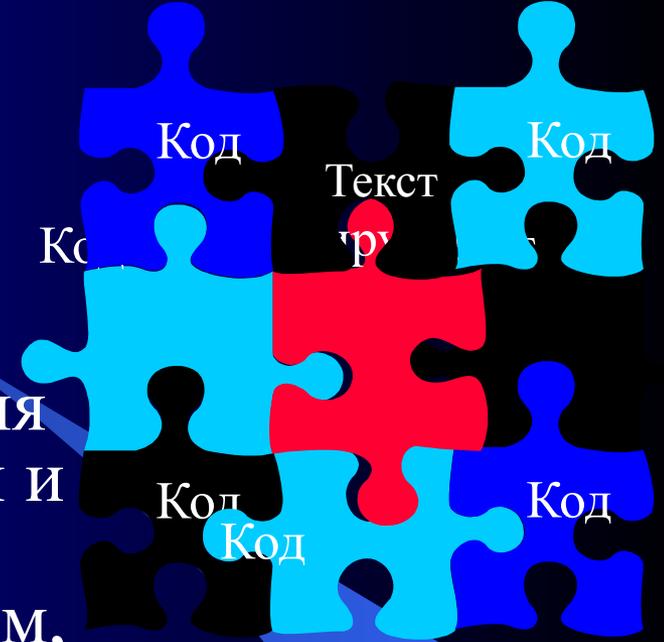
- Компьютерный вирус - это специально составленная небольшая по размерам программа, которая может "приписывать" себя к другим программам, файлам (т.е. "заражать" их) , а также выполнять различные нежелательные действия на компьютере (выдавать нежелательные сообщения, портить данные на дисках, "засорять" память компьютера, размножаться и т.д.). Сформулируйте тему для аудитории

Последствия

- Программа, внутри которой находится вирус, называется "зараженной". Когда такая программа начинает работу, то сначала управление получает вирус. Он 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.).

Последствия

- Для маскировки вируса действия по заражению других программ и нанесению вреда могут выполняться не всегда, а, скажем, при выполнении определенных условий. После того, как вирус выполнит нужные ему действия, он передает управление той программе, в которой он находится, и она работает также, как обычно. Тем самым внешне работа зараженной программы выглядит также, как и незараженной.



Основные методы защиты от компьютерных вирусов.

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 пользователей; профилактические меры, позволяющие уменьшить вероятность заражения вирусом;
- ❑ специализированные программы для защиты от вирусов.

- Общие средства защиты информации полезны не только для защиты от вируса. Имеются две основные разновидности этих средств:

Защита

- ❑ копирование информации - создание копий файлов и системных областей дисков;
- ❑ разграничение доступа предотвращает несанкционированное использование информации, в частности, защиту от изменений программ и данных вирусами, неправильно работающими программами и ошибочными действиями пользователей.

Несмотря на то, что общие средства защиты информации очень важны для защиты от вирусов, все же их одних недостаточно. Необходимо и применение специализированных программ для защиты от вирусов.

Эти программы можно разделить на несколько

ВИДОВ:

- Программы-детекторы позволяют обнаруживать файлы, зараженные одним из нескольких известных вирусов.
- Программы-доктора, или "фаги", "лечат" зараженные программы или диски, "выкусывая" из зараженных программ тело вируса, т.е. восстанавливая программу в том состоянии, в котором она находилась до заражения вирусом.
- Доктора-ревизоры - это гибриды ревизоров и докторов, т.е. программы, которые не только обнаруживают изменения в файлах и системных областях дисков, но и могут в случае изменений автоматически вернуть их в исходное состояние.

Эти программы можно разделить на несколько

ВИДОВ:

- 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 пользователю. Пользователь может разрешить или запретить выполнение соответствующей операции.