Методы и средства защиты от компьютерных вирусов

900igr.net

Программно-технические методы обнаружения вирусов

Основным средством борьбы с вирусами были и остаются антивирусные программы. Можно использовать антивирусные программы (антивирусы), не имея представления о том, как они устроены. Однако без понимания принципов устройства антивирусов, знания типов вирусов, а также способов их распространения, нельзя организовать надежную защиту компьютера. Как результат, компьютер может быть заражен, даже если на нем установлены антивирусы.

Основные методики обнаружения и защиты от вирусов:

- сканирование;
- эвристический анализ;
- использование антивирусных мониторов;
- обнаружение изменений;
- использование антивирусов, встроенных в BIOS компьютера.

Сканирование

- Самая простая методика поиска вирусов заключается в том, что антивирусная программа последовательно просматривает проверяемые файлы в поиске сигнатур известных вирусов.

Эвристический анализ

- Эвристический анализ позволяет обнаруживать ранее неизвестные вирусы. Антивирусные программы, реализующие метод эвристического анализа, проверяют программы и загрузочные секторы дисков и дискет, пытаясь обнаружить в них код, характерный для вирусов.

Антивирусные мониторы

- Целый класс антивирусных программ, которые постоянно находятся в памяти компьютера, и отслеживают все подозрительные действия, выполняемые другими программами. Монитор автоматически проверяет все запускаемые программы, создаваемые, открываемые и сохраняемые документы, файлы программ и документов, полученные через Интернет или скопированные на жесткий диск с дискеты и компакт диска. Антивирусный монитор сообщит пользователю, если какая-либо программа попытается выполнить потенциально опасное действие.

Обнаружение изменений

- Антивирусные программы, называемые ревизорами диска, не выполняют поиск вирусов по сигнатурам. Они запоминают предварительно характеристики всех областей диска, которые подвергаются нападению вируса, а затем периодически проверяют их (отсюда происходит название программы-ревизоры). Ревизор может найти изменения, сделанные известным или неизвестным вирусом

Защита, встроенная в BIOS компьютера

- В системные платы компьютеров тоже встраивают простейшие средства защиты от вирусов. Эти средства позволяют контролировать все обращения к главной загрузочной записи жестких дисков, а также к загрузочным секторам дисков и дискет. Если какая-либо программа попытается изменить содержимое загрузочных секторов, срабатывает защита и пользователь получает соответствующее предупреждение.