Компьютерные вирусы. Антивирусные программы.

Презентация подготовлена для конкурса «Интернешка» http://interneshka.org/»

Компьютерный вирус — вредоносное программное обеспечение. Способен создавать копии самого себя и внедрятся в код других программ, системные области памяти, загрузочные секторы, а также распространяться по разнообразным каналам связи.

- Основные классы двоичных вирусов: сетевые черви (червь Морриса, 1987), троянские кони (AIDS, 1989), полиморфные вирусы (Chameleon, 1990), стелс-вирусы (Frodo, Whale, 2-я половина 1990).

вирусов

- Вирусы копируют свое тело и обеспечивают последующее исполнение: внедрение себя в исполняемый код других программ, заменяя собой другие программы, прописываясь в автозапуск.
- Вирусом или его носителем может быть не только программа, содержащая машинный код, но и любая информация, содержащая автоматически исполняемые команды

Меры предосторожности:

- Не работать под привилегированными учётными записями без крайней необходимости.
- Не запускать незнакомые программы из сомнительных источников.
- Стараться блокировать возможность несанкционированного изменения системных файлов.
- Отключать потенциально опасную функциональность системы.
- Не заходить на подозрительные сайты, не обращать внимание на адрес в адресной строке обозревателя.
- Пользоваться только доверенными дистрибутивами.
- Постоянно делать резервные копии важных данных.
- Выполнять регулярные обновления часто используемых программ.

Антивирусная программа (антивирус) — специализированная программа для обнаружения компьютерных вирусов, а также нежелательных (считающихся вредоносными) программ и восстановления заражённых такими программами файлов, а также для профилактики — предотвращения заражения файлов или операционной системы вредоносным кодом.

- Их можно поделить на 3 типа:

  1)Серверный

  2)Скрипт или компонент CMS

  3)SAAS сервис

Лжеантивирус — программное обеспечение, не являющегося антивирусным (то есть не имеющего реальной функциональности для противодействия вредоносным программам), но выдающим себя за таковое.

- По сути, лжеантивирусы являются программами для обмана пользователей и получения прибыли в виде платежей за «лечение системы от вирусов», так и обычным вредоносным программным обеспечением. В настоящий момент это распространение приостановлено.

Обычно антивирус действует по схеме:

- Поиск в базе данных антивирусного ПО сигнатур вирусов.
- Если найден инфицированный код в памяти (оперативной и/или постоянной), запускается процесс «карантина», и процесс блокируется.
- Зарегистрированная программа обычно удаляет вирус. Незарегистрированная просит регистрации и оставляет систему уязвимой.

Пока!