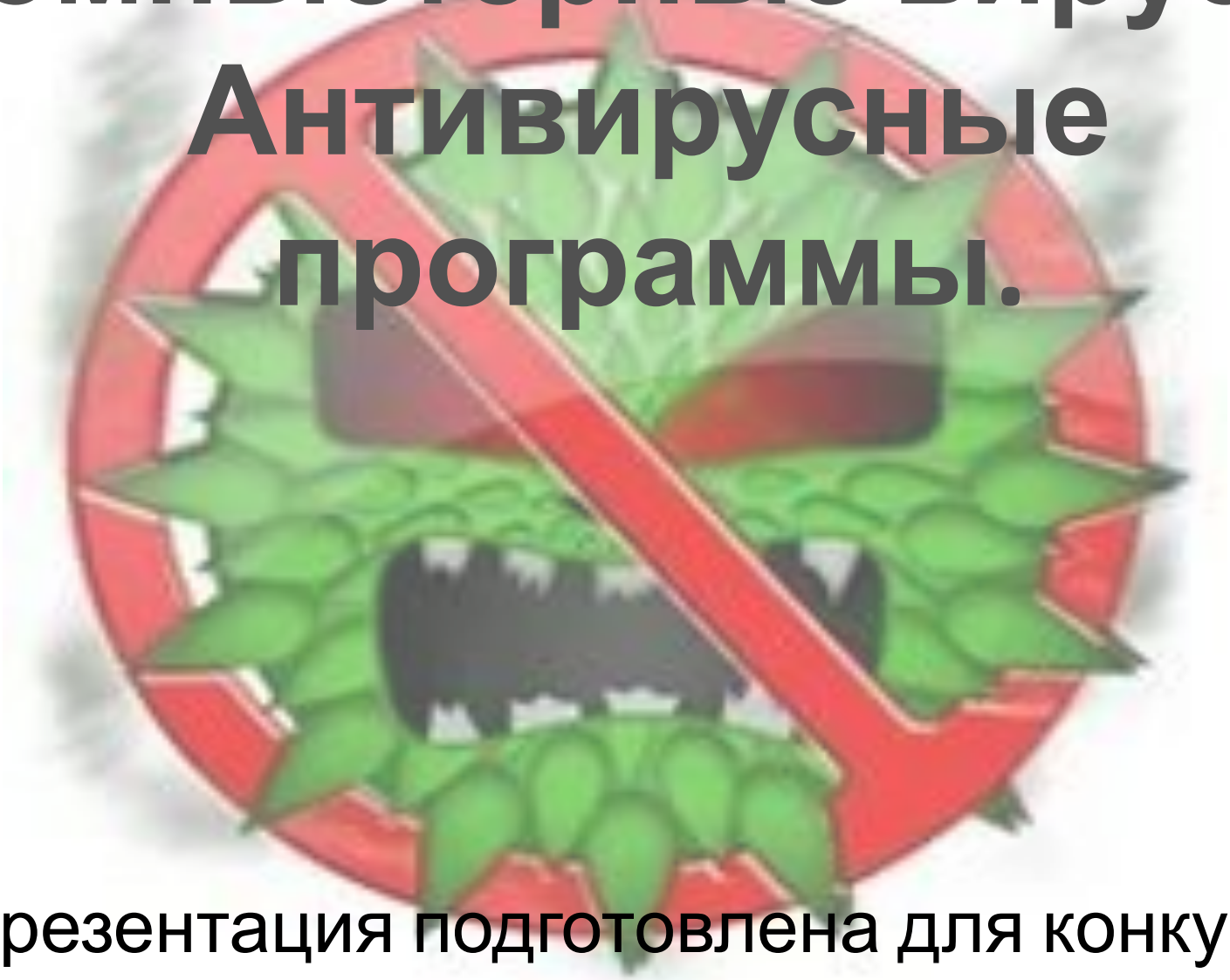
Компьютерные вирусы. Антивирусные программы.



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

- Компьютерный вирус – это вид вредоносного программного обеспечения, способного создавать копии самого себя и внедряться в код других программ, системные области памяти, загрузочные секторы, а также распространять свои копии по разнообразным каналам связи.

Классификация

- Принято разделять вирусы:

-по поражаемым объектам;

-по поражаемым операционным системам и платформам;

-по технологиям, используемым вирусом;

-по языку, на котором написан вирус;

-по дополнительной вредоносной функциональности.


Распространение
Через ИНТЕРНЕТ
Через ЛОКАЛЬНЫЕ СЕТИ
Через СЪЁМНЫЕ НОСИТЕЛИ

- Процесс внедрения вирусом своей копии в другую программу, файлы или системную область диска называется ЗАРАЖЕНИЕМ, а программа или иной объект, содержащий вирус – ЗАРАЖЁННЫМ.

Профилактика и лечение

- В настоящий момент существует множество антивирусных программ, используемых для предотвращения попадания вирусов в ПК. Однако нет гарантии, что они смогут справиться с новейшими разработками. Поэтому следует придерживаться некоторых мер предосторожности.

Меры предосторожности

- Не работать под привилегированными учётными записями без крайней необходимости. (Учётная запись администратора в Windows)
- Не запускать незнакомые программы из сомнительных источников.
- Стараться блокировать возможность несанкционированного изменения системных файлов.
- Отключать потенциально опасную функциональность системы (например, autorun-носителей в MS Windows, сокрытие файлов, их расширений и пр.).
- Не заходить на подозрительные сайты, обращать внимание на адрес в адресной строке обозревателя.
- Пользоваться только доверенными дистрибутивами.
- Постоянно делать резервные копии важных данных, желательно на носители, которые не стираются (например, BD-R) и иметь образ системы со всеми настройками для быстрого развёртывания.
- Выполнять регулярные обновления часто используемых программ, особенно тех, которые обеспечивают безопасность системы.
- Не работать под привилегированными учётными записями без крайней необходимости. (Учётная запись администратора в Windows)
- Не запускать незнакомые программы из сомнительных источников.
- Стараться блокировать возможность несанкционированного изменения системных файлов.
- Отключать потенциально опасную функциональность системы (например, autorun-носителей в MS Windows, сокрытие файлов, их расширений и пр.).
- Не заходить на подозрительные сайты, обращать внимание на адрес в адресной строке обозревателя.
- Пользоваться только доверенными дистрибутивами.
- Постоянно делать резервные копии важных данных, желательно на носители, которые не стираются (например, BD-R) и иметь образ системы со всеми настройками для быстрого развёртывания.

Средства предотвращения заражения

- Резервное копирование
- Избежание использования случайными и неизвестными программами
- Перезагрузка компьютера перед началом работы, если за этим компьютером работали другие пользователи
- Ограничение доступа к информации
- Антивирусные программы


Типы антивирусных программ
ПОЛИФАГИ
РЕВИЗОРЫ
БЛОКИРОВЩИКИ

ПОЛИФАГИ ПРОГРАММЫ – ДЕТЕКТОРЫ ПОЗВОЛЯЮТ ОБНАРУЖИВАТЬ ФАЙЛЫ, ЗАРАЖЁННЫЕ 1-ИМ ИЗ НЕСКОЛЬКИХ ИЗВЕСТНЫХ ВИРУСОВ. ДЛЯ ЭТОГО ОНИ ИСПОЛЬЗУЮТ «МАСКИ».

РЕВИЗОРЫ ПРИНЦИП РАБОТЫ ОСНОВАН НА ПОДСЧЁТЕ КОНТРОЛЬНЫХ СУММ ФАЙЛОВ И НЕКОТОРОЙ ДРУГОЙ ИНФОРМАЦИИ

БЛОКИРОВЩИК
И
ПРОВЕРЯЮТ НА
НАЛИЧИЕ
ВИРУСОВ
ЗАПУСКАЕМЫЕ
ФАЙЛЫ И
ВСТАВЛЯЕМЫЕ
В
ДИСКОВОД
ДИСКЕТЫ


McAfee
Proven Security
AVIRA
symantec.
avast!
AVG
Anti-Virus
NOD32
Panda
VirusOff.ru

СПАСИБО ЗА

Презентация подготовлена Королевой Татьяной
Ученицей 8 «Б» класса Сараевской СОШ