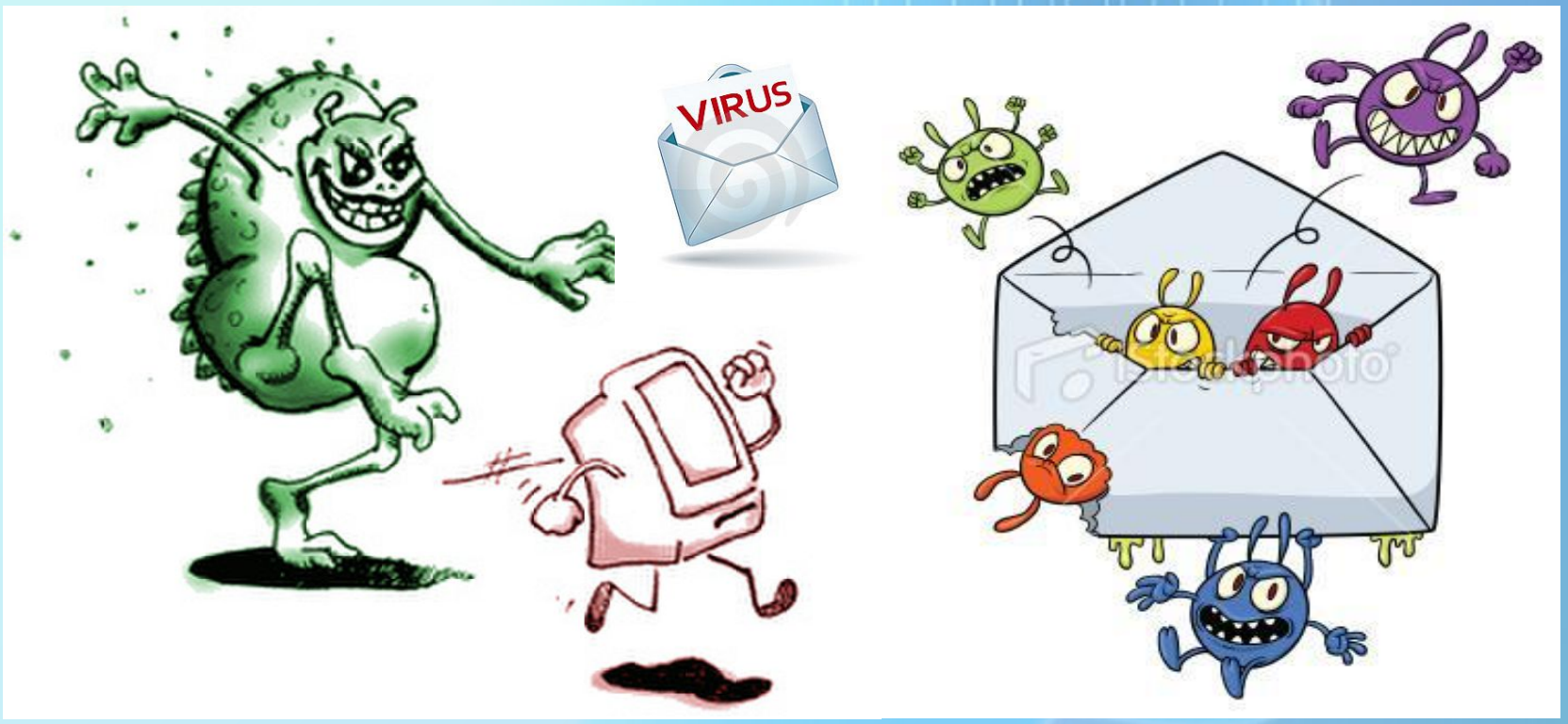
Презентация подготовлена для конкурса "Интернешка" http://interneshka.org/".

отерные вирусы. тивирусные рограммы

Автор: *Рамазанова Мадина ученица 8 класса «А»,*
Руководитель: *Александрова З.В., учитель физики и информатики МБОУ СОШ №5 пгт Печенга, Мурманская обл.*

Цель работы:

- Узнать что такое компьютерные вирусы и как защитить свой ПК от них.



Содержание

1) Что такое компьютерный вирус.
2) История вируса.
3) Классификация вирусов.
4) Распространение вирусов.
5) Механизм распространения.
6) Профилактика и лечение

Что такое компьютерный вирус?

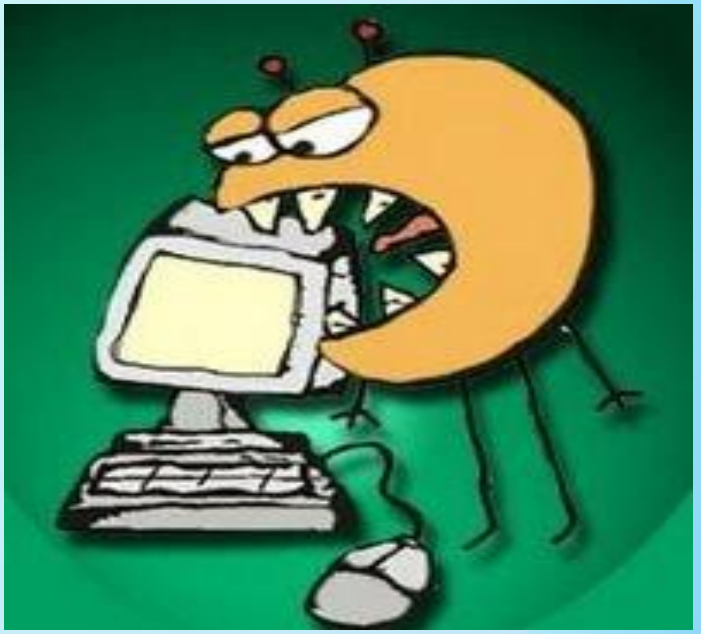
Компьютерный вирус — вид вредоносного программного обеспечения, способного создавать копии самого себя и внедряться в код других программ, системные области памяти, загрузочные секторы, а также распространять свои копии по разнообразным каналам связи. Как правило, целью вируса является нарушение работы программно-аппаратных комплексов: удаление файлов, приведение в негодность структур размещения данных, блокирование работы пользователей или же приведение в негодность аппаратных комплексов компьютера и т. п. Даже если автор вируса не запрограммировал вредоносных эффектов, вирус может приводить к сбоям компьютера из-за ошибок, неучтённых тонкостей взаимодействия с операционной системой и другими программами. Кроме того, вирусы, как правило, занимают место на накопителях информации и потребляют некоторые другие ресурсы системы. В обиходе «вирусами» называют всё вредоносное ПО, хотя на самом деле это лишь один его вид.

История создания вируса

Основы теории самовоспроизводящихся механизмов заложил американец венгерского происхождения Джон фон Нейман, который в 1951 году предложил метод создания таких механизмов. С 1961 года известны рабочие примеры таких программ. Первыми известными вирусами являются Virus 1,2,3 и Elk Cloner для ПК Apple II, появившиеся в 1981 году. Зимой 1984 года появились первые антивирусные утилиты — CHK4BOMB и BOMBSQAD авторства Энди Хопкинса (англ. Andy Hopkins). В начале 1985 года Ги Вонг (англ. Gee Wong) написал программу DPROTECT — первый резидентный антивирус. Первые вирусные эпидемии относятся к 1986—1989 годам: Brain.A[en] (распространялся в загрузочных секторах дискет, вызвал крупнейшую эпидемию), Jerusalem[en] (проявился в пятницу 13 мая 1988 года, уничтожая программы при их запуске), червь Морриса (свыше 6200 компьютеров, большинство сетей вышло из строя на срок до пяти суток), DATACRIME (около 100 тысяч зараженных ПЭВМ только в Нидерландах).

История создания вируса

В 1985 году оформились основные классы двоичных вирусов: сетевые черви (червь Морриса, 1987), «троянские кони» (AIDS, 1989[4]), полиморфные вирусы (Chameleon, 1990), стелс-вирусы (Frodo, Whale, 2-я половина 1990). Параллельно оформляются организованные движения как про-, так и антивирусной направленности: в 1990 году появляются специализированная BBS Virus Exchange, «Маленькая чёрная книжка о компьютерных вирусах» Марка Людвига, первый коммерческий антивирус Symantec Norton AntiVirus.



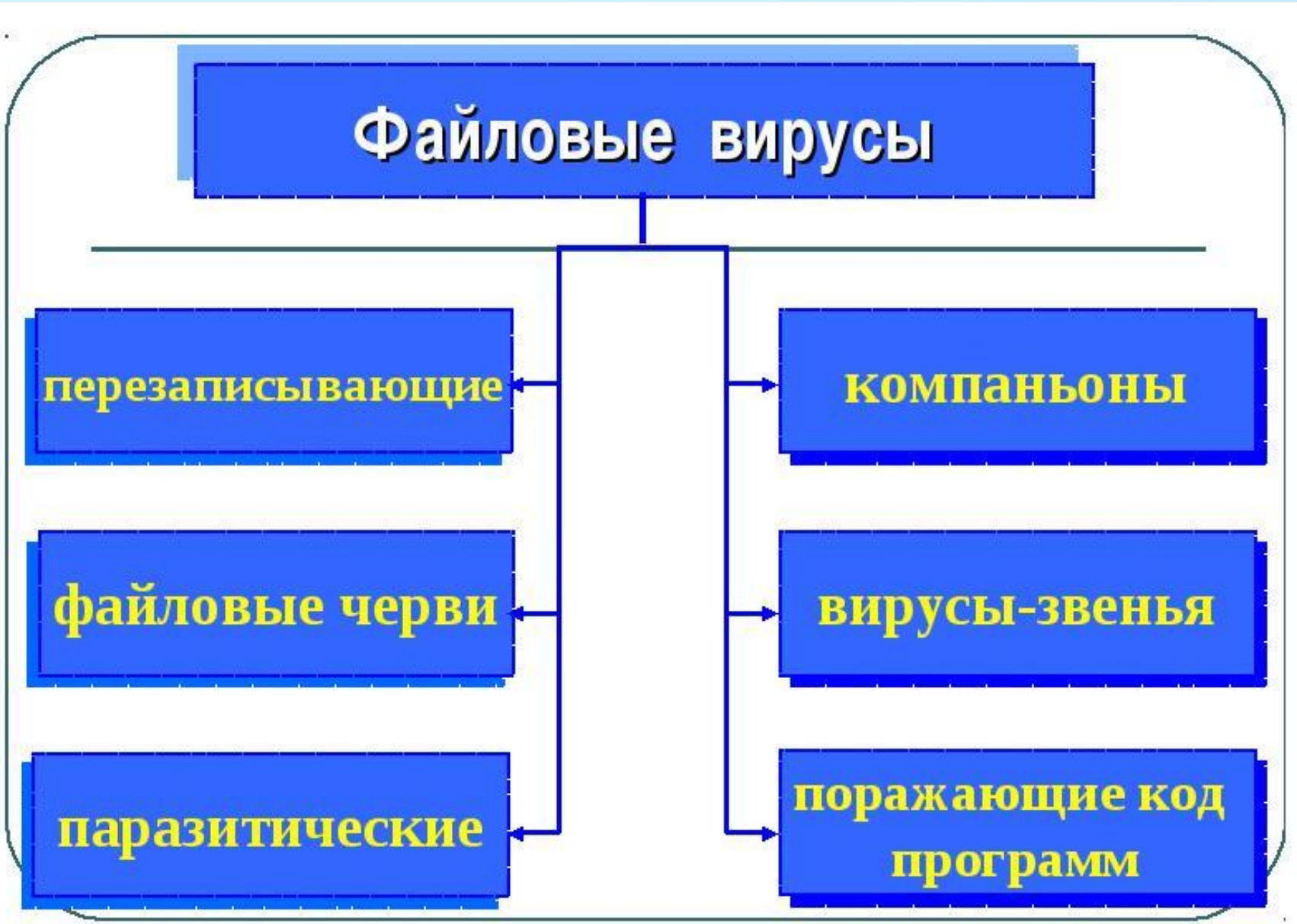
Классификация вирусов

- Ныне существует немало разновидностей вирусов, различающихся по основному способу распространения и функциональности. Если изначально вирусы распространялись на дискетах и других носителях, то сейчас доминируют вирусы, распространяющиеся через Интернет. Растёт и функциональность вирусов, которую они перенимают от других видов программ.
- В настоящее время не существует единой системы классификации и именования вирусов (хотя попытка создать стандарт была предпринята на встрече CARO в 1991 году). Принято разделять вирусы:

по поражаемым объектам (файловые вирусы, загрузочные вирусы, сценарные код);

Классификация вирусов

- файловые вирусы делят по механизму заражения: паразитирующие добавляют себя в исполняемый файл, перезаписывающие невосстановимо портят заражённый файл, «спутники» идут отдельным файлом.
- по поражаемым операционным системам и платформам (DOS, Microsoft Windows, Unix, Linux);
- по технологиям, используемым вирусом (полиморфные вирусы, стелс-вирусы, руткиты);
- по языку, на котором написан вирус (ассемблер, высокоуровневый язык программирования, сценарный язык и др.);
- по дополнительной вредоносной функциональности (бэкдоры, кейлоггеры, шпионы, ботнеты и др.).


Файловые вирусы
перезаписывающие
файловые черви
паразитические
компаньоны
вирусы-звенья
поражающие код программ

Распространение вирусов.

- Через интернет
- Локальные сети
- Съемные носители.

Механизм распространения

Вирусы распространяются, копируя свое тело и обеспечивая его последующее исполнение: внедряя себя в исполняемый код других программ, заменяя собой другие программы, прописываясь в автозапуск и другое. Вирусом или его носителем могут быть не только программы, содержащие машинный код, но и любая информация, содержащая автоматически исполняемые команды — например, пакетные файлы и документы Microsoft Word и Excel, содержащие макросы. Кроме того, для проникновения на компьютер вирус может использовать уязвимости в популярном программном обеспечении (например, Adobe Flash, Internet Explorer, Outlook), для чего распространители внедряют его в обычные данные (картинки, тексты и т. д.) вместе с эксплоитом, использующим уязвимость.

Вредоносные программы

ПРОЦЕСС ЗАРАЖЕНИЯ ВИРУСОМ И ЛЕЧЕНИЯ ФАЙЛА

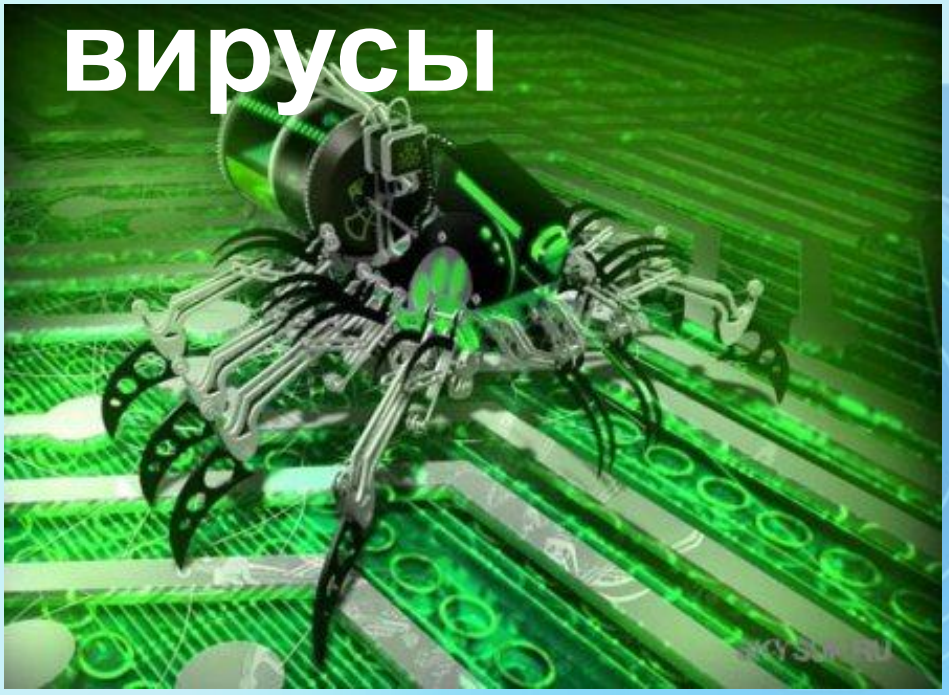
Компьютерный вирус → Незаражённая программа

Заражённый файл | Компьютерный вирус

Антивирусная программа

Вылеченный файл

Скрипт - вирусы



Особой разновидностью вирусов являются активные элементы (программы) на языках JavaScript или VBScript, которые могут выполнять разрушительные действия, то есть являться вирусами (скрипт-вирусами). Такие программы передаются по Всемирной паутине в процессе загрузки Web-страниц с серверов Интернета в браузер локального компьютера.

Профилактика и лечение

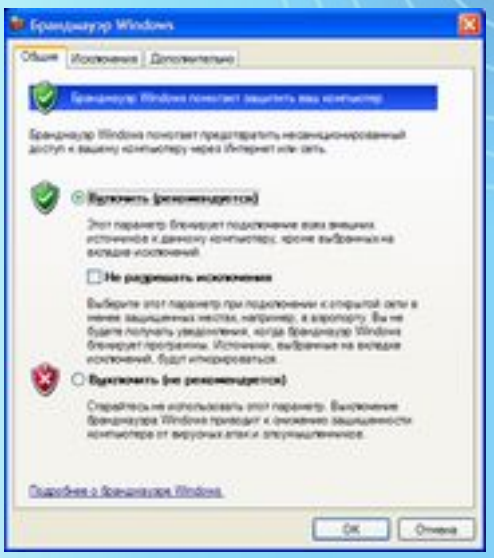
- В настоящий момент существует множество антивирусных программ, используемых для предотвращения попадания вирусов в ПК. Однако нет гарантии, что они смогут справиться с новейшими разработками. Поэтому следует придерживаться некоторых мер предосторожности, в частности:
- Не работать под привилегированными учётными записями без крайней необходимости. (Учётная запись администратора в Windows)
- Не запускать незнакомые программы из сомнительных источников.
- Стараться блокировать возможность несанкционированного изменения системных файлов.

Профилактика и лечение

- 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.

Использование Интернета является безопасным, если выполняются основны правила:

- Регулярно обновляйте операционную систему.
- Используйте антивирусную программу.
- Применяйте брандмауэр.
- Создавайте резервные копии важных файлов.
- Будьте осторожны при загрузке содержимого



ять правил при работе с электронной почтой:

1. Никогда не открывайте подозрительные сообщения или вложения электронной почты, полученные от незнакомых людей. (Вместо этого сразу удалите их)

2. Никогда не отвечайте на спам.

3. Применяйте фильтр спама поставщика услуг Интернета или программы работы с электронной почтой (при наличии подключения к Интернету).

4. Создайте новый или используйте семейный адрес электронной почты для Интернет-запросов, дискуссионных форумов и т.д.

5. Никогда не пересылайте «письма счастья». Вместо этого сразу

Спасибо за внимание!