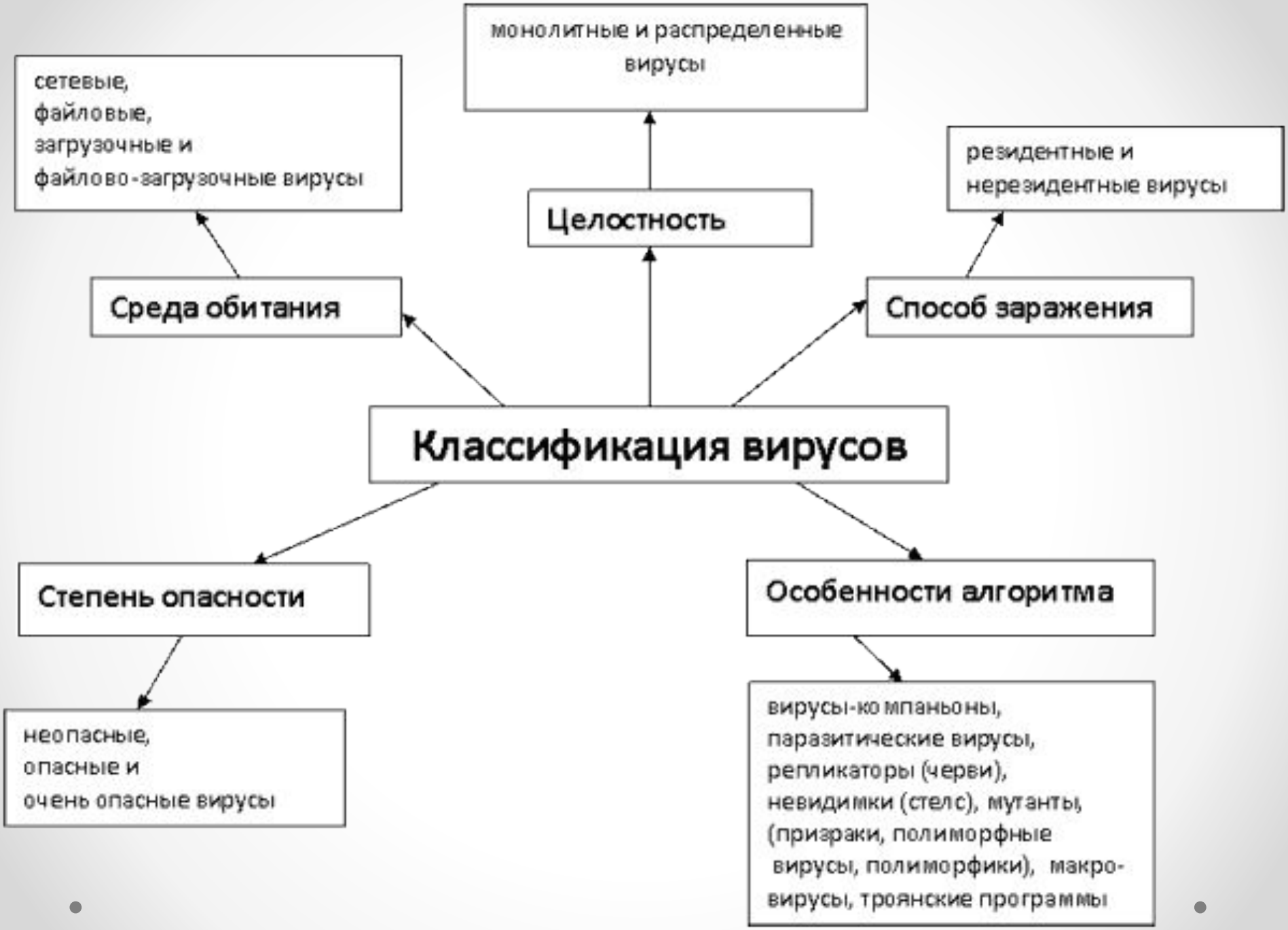
Компьютерные вирусы и антивирусные программы

Подготовил:
Кирьякиди
Илья
10 класс

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

Компьютерный вирус

Вид вредоносного программного обеспечения, способный создавать копии самого себя и внедрятся в код других программ, системные области памяти, загрузочные секторы, а так же распространять свои копии по разнообразным каналам связи, с целью нарушения работы программно-аппаратных комплексов, удаления файлов, приведения в негодность структур размещения данных, блокирования работы пользователей или же приведение в негодность аппаратных комплексов компьютера.


Классификация вирусов
Среда обитания
сетевые,
файловые,
загрузочные и
файлово-загрузочные вирусы
Целостность
монолитные и распределенные
вирусы
Способ заражения
резидентные и
нерезидентные вирусы
Степень опасности
неопасные,
опасные и
очень опасные вирусы
Особенности алгоритма
вирусы-компаньоны,
паразитические вирусы,
репликаторы (черви),
невидимки (стелс), мутанты,
(призраки, полиморфные
вирусы, полиморфики), макро-
вирусы, троянские программы

Стадии функционирования:

- **Латентная стадия**. На этой стадии код вируса находится в системе, но никаких действий не предпринимает. Для пользователя не заметен. Может быть вычислен сканированием файловой системы и самих файлов.

- **Инкубационная стадия**. На этой стадии код вируса активируется и начинает создавать свои копии, распространяя их по устройствам хранения данных компьютера, локальным и глобальным компьютерным сетям, рассылая в виде почтовых сообщений и так далее. Для пользователя может быть заметен, так как начинает потреблять системные ресурсы и каналы передачи данных, в результате чего компьютер может работать медленнее, загрузка информации из Интернет, почты и прочих данных может замедлятся.

- **Активная стадия**. На этой стадии вирус, продолжая размножать свой код доступными ему способами, начинает деструктивные действия на которые ориентирован. Заметен пользователю, так как начинает проявляться основная функция вируса – пропадают файлы, отключаются службы, нарушается функционирование сети, происходит порча оборудования.

Среда обитания:

- **Загрузочные вирусы** проникают в загрузочные сектора устройств хранения данных (жесткие диски, дискеты, переносные запоминающие устройства). При загрузке операционной системы с зараженного диска происходит активация вируса. Его действия могут состоять в нарушении работы загрузчика операционной системы, что приводит к невозможности ее работы, либо изменении файловой таблицы, что делает недоступным определенные файлы.
- **Файловые вирусы** чаще всего внедряются в исполнительные модули программ (файлы с помощью которых производится запуск той или иной программы), что позволяет им активироваться в момент запуска программы, влияя на ее функциональность. Реже файловые вирусы могут внедрятся в библиотеки операционной системы или прикладного ПО, исполнительные пакетные файлы, файлы реестра Windows, файлы сценариев, файлы драйверов. Внедрение может проводиться либо изменением кода атакуемого файла, либо созданием его модифицированной копии. Таким образом, вирус, находясь в файле, активируется при доступе к этому файлу, инициируемому пользователем или самой ОС. Файловые вирусы – наиболее распространенный вид компьютерных вирусов.
- **Файлово-загрузочные вирусы** обедняют в себе возможности двух предыдущих групп, что позволяет им представлять серьезную угрозу работе ко
- **Сетевые вирусы** распространяются посредством сетевых служб и протоколов. Таких как рассылка почты, доступ к файлам по FTP, доступ файлам через службы локальных сетей. Что делает их очень опасными, так как заражение не остается в пределах одного компьютера или даже одной локальной сети, а начинает распространятся по разнообразным каналам связи.мпьютера.
- **Документные вирусы** (их часто называют макровирусами) заражают файлы современных офисных систем (Microsoft Office, Open Office…) через возможность использования в этих системах макросов. Макрос – это определенный, заранее определенный набор действий, микропрограмма, встроенная в документ и вызываемая непосредственно из него для модификации этого документа или других функций. Именно макрос и является целью макровирусов.

В компьютерной сети:

- **Резидентный вирус**, будучи вызван запуском зараженной программы, остается в памяти даже после ее завершения. Он может создавать дополнительные процессы в памяти компьютера, расходуя ресурсы. Может заражать другие запущенные программы, искажая их функциональность. Может “наблюдать” за действиями пользователя, сохраняя информацию о его действиях, введенных паролях, посещенных сайтах и т.д.
- **Нерезидентный вирус** является неотъемлемой частью зараженной программы и может функционировать только во время ее работы.
- Некоторые вирусы тяжелых последствий после завершения своей работы не вызывают; они могут завершить работу некоторых программ, отображать определенные визуальные эффекты, проигрывать звуки, открывать сайты, или просто снижать производительность компьютера, резервируя под себя системные ресурсы. Таких вирусов подавляющее большинство. Однако есть и действительно опасные вирусы, которые могут уничтожать данные пользователя, документы, системные области, приводить в негодность операционную систему или даже аппаратные компоненты компьютера.

Принцип функционирования:

- **Вирусы-паразиты (Parasitic)** – вирусы, работающие с файлами программ, частично выводящие их из строя. Могут быть легко выявлены и уничтожены. Однако, зачастую, файл-носитель остается не пригодным.
- **Вирусы-репликаторы (Worm)** – вирусы, основная задача которых как можно быстрее размножится оп всем возможным местам хранения данных и коммуникациям. Зачастую сами не предпринимают никаких деструктивных действий, а являются транспортом для других видов вредоносного кода.
- **Вирусы-репликаторы (Worm)** – вирусы, основная задача которых как можно быстрее размножится оп всем возможным местам хранения данных и коммуникациям. Зачастую сами не предпринимают никаких деструктивных действий, а являются транспортом для других видов вредоносного кода.
- **Вирусы-невидимки (Stealth)** – нзваны по имени самолета-невидимки "stealth", наиболее сложны для обнаружения, так как имеют свио алгоритмы маскировки от сканирования. Маскируются путем подмены вредоносного кода полезным во время сканирования, временным выведением функциональных модулей из работы в случае обнаружения процесса сканирования, сокрытием своих процессов в памяти и т.д.
- И т.д.

Антивирусная программа

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

Классификации антивирусных программ:

- **Классические антивирусные продукты** (продукты, применяющие только сигнатурный метод детектирования, продукты, применяющие только проактивные технологии антивирусной защиты);
- **Комбинированные продукты** (продукты, применяющие как сигнатурные методы защиты, так и проактивные)
- **Антивирусные продукты** (продукты, обеспечивающие только антивирусную защиту)
- **Комбинированные продукты** (продукты, обеспечивающие не только защиту от вредоносных программ, но и фильтрацию спама, шифрование и резервное копирование данных и другие функции)
- •**Также делятся по целевым платформам**

Антивирусы для сайтов

- **Серверный** — устанавливается на веб-сервер. Поиск вирусов, в этом случае, происходит в файлах всего сервера.

- **Скрипт или компонент CMS** — выполняющие поиск вредоносного кода, непосредственно в файлах сайта.

- **SaaS сервис** — система централизованного управления, позволяющая управлять файлами, базами данных, настройками и компонентами веб-ресурсов на VDS и DS удаленно.