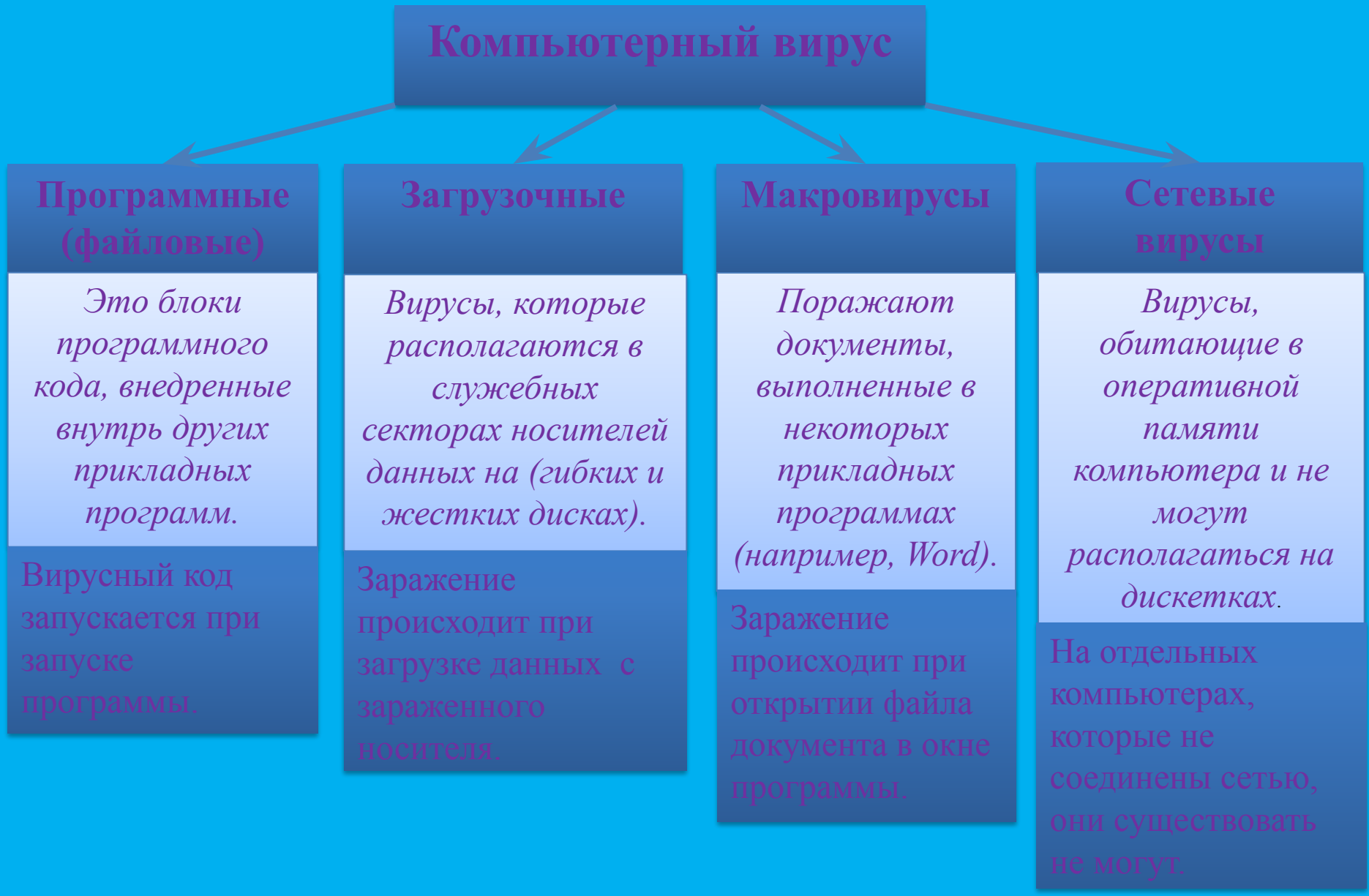
Компьютерная презентация на тему: «Компьютерные вирусы и антивирусные программы»

Классификаций компьютерных вирусов:

1. по среде их обитания;
2. по способу заражения;
3. по степени воздействия;
4. по особенностям алгоритма работы.

1. по среде их обитания:



2. по способу заражения:

Резидентные - попадают в оперативную память компьютера и, находясь в памяти, могут проявлять свою активность вплоть до выключения или перезагрузки компьютера;

Нерезидентные - в память не внедряются и активны только ограниченное время, связанное с выполнением определенных задач.

3. по степени воздействия:

Компьютерный вирус

Безвредные	Неопасные	Опасные	Очень опасные
никак не влияющие на работу компьютера (кроме уменьшения свободной памяти на диске в результате своего распространения).	*не мешают работе компьютера, но уменьшают объем свободной оперативной памяти и памяти на дисках, действия таких вирусов проявляются в каких-либо графических или звуковых эффектах.*	*могут привести к различным нарушениям в работе компьютера.*	*воздействие этих вирусов может привести к потере программ, уничтожению данных, стиранию информации в системных областях диска.*

4. по особенностям алгоритма работы:

- **Простейшие** - *паразитические, они изменяют содержимое файлов и секторов диска и могут быть достаточно легко обнаружены и уничтожены;*
- **Вирусы-репликаторы (черви)** - *распространяются по компьютерным сетям, вычисляют адреса сетевых компьютеров и записывают по этим адресам свои копии;*
- **Вирусы-невидимки (стелс-вирусы)** - *очень трудно обнаружить и обезвредить, так как они перехватывают обращения операционной системы к пораженным файлам и секторам дисков и подставляют вместо своего тела незараженные участки диска;*
- **Вирусы-мутанты** - *содержащие алгоритмы шифровки-расшифровки, благодаря которым копии одного и того же вируса не имеют ни одной повторяющейся цепочки байтов;*
- **Квазивирусные («троянские» программы)** - *не способны к самораспространению, но очень опасны, так как, маскируясь под полезную программу, разрушают загрузочный сектор и файловую систему дисков.*

Пути проникновения вирусов на компьютер:

- Глобальная сеть Internet .
- Электронная почта.
- Локальная сеть.
- Компьютеры «Общего назначения».
- Пиратское программное обеспечение.
- Ремонтные службы.
- Съемные накопители, на которых находятся заражённые вирусом файлы.
- Жёсткий диск, на который попал вирус.
- Вирус, оставшийся в оперативной памяти после предшествующего пользователя.

Методы защиты от компьютерных вирусов

- **Установите на свой персональный компьютер современную антивирусную программу.**
- **Перед просмотром информации принесенной на флэш-карте (дискете) с другого компьютера проверьте носитель антивирусом.**
- **После разархивирования архивных файлов сразу проверьте их на вирусы (не все антивирусные программы могут искать вредоносный код в архивах или могут делать это не корректно).**
- **Периодически проверяйте компьютер на вирусы (если активно пользуетесь Интернетом – запускайте раз в неделю, а то и чаще).**
- **Как можно чаще делайте резервные копии важной информации (backup).**
- **Используйте совместно с антивирусной программой файервол (firewall) если компьютер подключен к Интернет.**
- **Настройте браузер (программа просмотра Интернет страниц – IE, Opera и т.д.) для запрета запуска активного содержимого html-страниц.**

Антивирусные программы

предназначены для предотвращения заражения компьютера вирусом и ликвидации последствий заражения.

В зависимости от назначения и принципа действия различают следующие антивирусные программы:

Сторожа или детекторы – предназначены для обнаружения файлов зараженных известными вирусами, или признаков указывающих на возможность заражения.

Доктора – предназначены для обнаружения и устранения известных им вирусов, удаляя их из тела программы и возвращая ее в исходное состояние. Наиболее известными представителями являются Dr.Web, AidsTest, Norton Anti Virus.

Ревизоры – они контролируют уязвимые и поэтому наиболее атакуемые компоненты компьютера, запоминают состояние служебных областей и файлов, а в случае обнаружения изменений сообщают пользователю.

Резидентные мониторы или фильтры – постоянно находятся в памяти компьютера для обнаружения попыток выполнить несанкционированные действия. В случае обнаружения подозрительного действия выводят запрос пользователю на подтверждение операций.

Вакцины – имитируют заражение файлов вирусами. Вирус будет воспринимать их зараженными и не будет внедряться. Чаще всего используются Aidstest Лозинского, Drweb, Dr.Solomon.