Компьютерный вирус - специально написанная программа, способная самопроизвольно присоединяться к другим программам, создавать свои копии и внедрять их в файлы, системные области компьютера и в вычислительные сети с целью нарушения работы программ, порчи файлов и каталогов, создания всевозможных помех в работе компьютера.

Размножаться	Скрываться	Портить

Механизм распространения

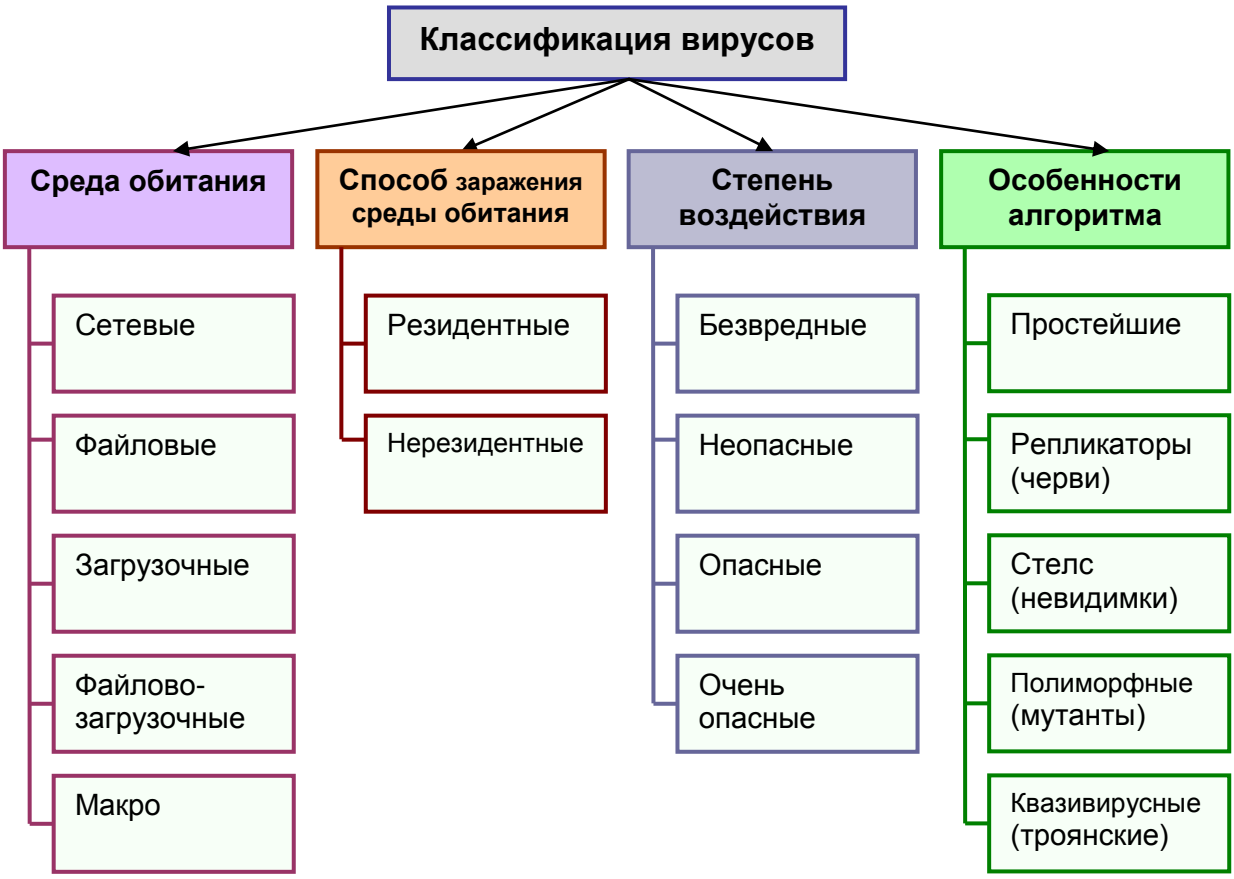
Вирусы распространяются, копируя свое тело и обеспечивая его последующее исполнение: внедряя себя в исполняемый код других программ, заменяя собой другие программы, прописываясь в автозапуск и другое.

Результаты воздействия компьютерного вируса

- безобидные визуальные или звуковые эффекты
- потеря или искажение данных
- утечка личной и конфиденциальной информации

Уголовной Кодекс России, статья 273
«Создание, использование и распространение вредоносных программ для ЭВМ»

1. Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами – наказываются лишением свободы на срок до 3 лет со штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев.
2. Те же деяния, повлекшие по неосторожности тяжкие последствия, - наказываются лишением свободы на срок от трех до семи лет.


Классификация вирусов
Среда обитания
Способ заражения среды обитания
Степень воздействия
Особенности алгоритма
Сетевые
Файловые
Загрузочные
Файлово-загрузочные
Макро
Резидентные
Нерезидентные
Безвредные
Неопасные
Опасные
Очень опасные
Простейшие
Репликаторы (черви)
Стелс (невидимки)
Полиморфные (мутанты)
Квазивирусные (троянские)

Среда обитания вируса	
Сетевые	Распространяются по различным компьютерным сетям.
Файловые	Внедряются в исполняемые модули, т. е. в файлы, имеющие расширения COM и EXE. Могут внедряться и в другие типы файлов, но записанные в таких файлах, они никогда не получают управление и теряют способность к размножению.
Загрузочные	Внедряются в загрузочный сектор диска (Boot-сектор) или в сектор, содержащий программу загрузки системного диска (Master Boot Record).
Файлово-загрузочные	Заражают как файлы, так и загрузочные сектора дисков.
Макро	Заражают файлы-документы и электронные таблицы нескольких популярных редакторов.

Способ заражения среды обитания	
Резидентные	При заражении (инфицировании) компьютера оставляет в оперативной памяти свою резидентную часть, которая потом перехватывает обращение операционной системы к объектам заражения (файлам, загрузочным секторам дисков и т. п.) и внедряется в них. Резидентные вирусы находятся в памяти и являются активными вплоть до выключения или перезагрузки компьютера.
Нерезидентные	Не заражают память компьютера и являются активными ограниченное время.

Способ воздействия вируса	
Безвредные	Не влияющие на работу компьютера (кроме уменьшения свободной памяти на диске в результате своего распространения).
Неопасные	Влияние ограничивается уменьшением свободной памяти на диске и графическими, звуковыми и прочими эффектами.
Опасные	Могут привести к серьезным сбоям в работе компьютера.
Очень опасные	Воздействие вирусов может привести к потере программ, уничтожению данных, стиранию информации в системных областях диска.

Особенности алгоритма	
Простейшие	Изменяют содержимое файлов и секторов диска и могут быть легко обнаружены и уничтожены.
Репликаторы (черви)	Распространяются по компьютерным сетям, вычисляют адреса сетевых компьютеров и записывают по этим адресам свои копии.
Стелс (невидимки)	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.
Полиморфные (мутанты)	Содержат алгоритмы шифровки-расшифровки, благодаря которым копии одного и того же вируса не имеют ни одной повторяющейся цепочки байтов.
Квазивирусные (троянские)	Не способны к самораспространению, но очень опасны, так как, маскируясь под полезную программу, разрушают загрузочный сектор и файловую систему дисков.

Защита от компьютерных вирусов

Признаки заражения компьютерным вирусом

- некоторые программы перестают работать или начинают работать неправильно;
- на экран выводятся посторонние сообщения, символы и т.д.;
- работа на компьютере существенно замедляется;
- некоторые файлы оказываются испорченными и т.д.
- операционная система не загружается;
- изменение даты и времени модификации файлов;
- изменение размеров файлов;
- значительное увеличение количества файлов на диска;
- существенное уменьшение размера свободной оперативной памяти и т.п.

Методы защиты

Программные	Аппаратные	Организационные

- оснастить компьютер современными антивирусными программами;
- при поиске вирусов следует использовать заведомо чистую операционную систему, загруженную с дискеты;
- перед считыванием с дискет информации, записанной на других компьютерах, всегда проверять эти дискеты на наличие вирусов, запуская антивирусные программы;
- при работе на других компьютерах всегда нужно защищать свои дискеты от записи в тех случаях, когда на них не планируется запись информации;
- при переносе на компьютер файлов в архивированном виде проверять их сразу же после разархивации на жестком диске, ограничивая область проверки только вновь записанными файлами;
- периодически проверять на наличие вирусов жесткие диски компьютера, запуская антивирусные программы для тестирования файлов, памяти и системных областей дисков с защищенной от записи дискеты, предварительно загрузив операционную систему с защищенной от записи системной дискеты;
- использовать антивирусные программы для входного контроля всех исполняемых файлов, получаемых из компьютерных сетей. Никогда не следует запускать непроверенные файлы, полученные по компьютерным сетям;
- обязательно делать архивные копии на внешних носителях ценной информации.