Стелс-вирусы могут перехватывать запросы ОС на чтение/запись заражённых файлов. При этом они или временно лечат эти участки, либо подставляют вместо себя незаражённые фрагменты кода.

Резидентные вирусы — это вирусы, которые способны сохраняться в памяти и оставаться активными после окончания работы вирусоносителя. При инфицировании компьютера такие вирусы оставляют в оперативной памяти свою резидентную часть, которая затем перехватывает обращение ОС к объектам заражения и внедряется в них.

## Следующий этап распространения вируса — поиск жертв

По способу поиска жертвы вирусы можно разделить на два класса:

1. Вирусы, осуществляющие поиск с использованием функций ОС.
2. Вирусы, реализующие пассивный механизм поиска («ловушки» для программных файлов).

## Следующий этап — заражение жертв

Вирусы делятся на два класса.

К первому относятся вирусы, которые не внедряют свой код непосредственно в программные файлы, а изменяют имя файла и создают новый, содержащий тело вируса.

Второй класс составляют вирусы, внедряющиеся непосредственно в файлы жертвы. Основные элементы внедрения: внедрение в начало (для COM-файлов), внедрение в конец (для EXE), внедрение в середину (для файлов с заранее известной структурой).

## Следующий этап — выполнение деструктивных функций

1. Безвредный вирус. Это вирус, в котором реализован только механизм самораспространения. Они не наносят вред системе, за исключением расхода свободной памяти.
2. Неопасные вирусы. Это вирусы, присутствие которых в системе связано с различными эффектами (звуковые, видео). Не наносят вред программам и данным, но уменьшают свободную память.
3. Опасные вирусы. Могут привести к серьёзным сбоям с последующим разрушением программ и данных.
4. Очень опасные. В алгоритмах работы этих вирусов заведомо заложены процедуры, непосредственно приводящие к разрушениям программ и данных, а также стиранию информации, записанной в системных областях памяти, необходимой для работы компьютера.

## Следующий этап — передача управления программе-носителю вируса

1. Разрушающие вирусы. Не заботятся о сохранении работоспособности инфицированных программ, поэтому для них этот этап функционирования отсутствует.
2. Неразрушающие вирусы. Восстанавливают в памяти программы в том виде, в котором они должны корректно исполняться.