Вирусы

Вирусы можно разделить на классы по следующим основным признакам:

- Среда обитания
- Особенности алгоритма работы
- Разрушительные действия

Среда обитания

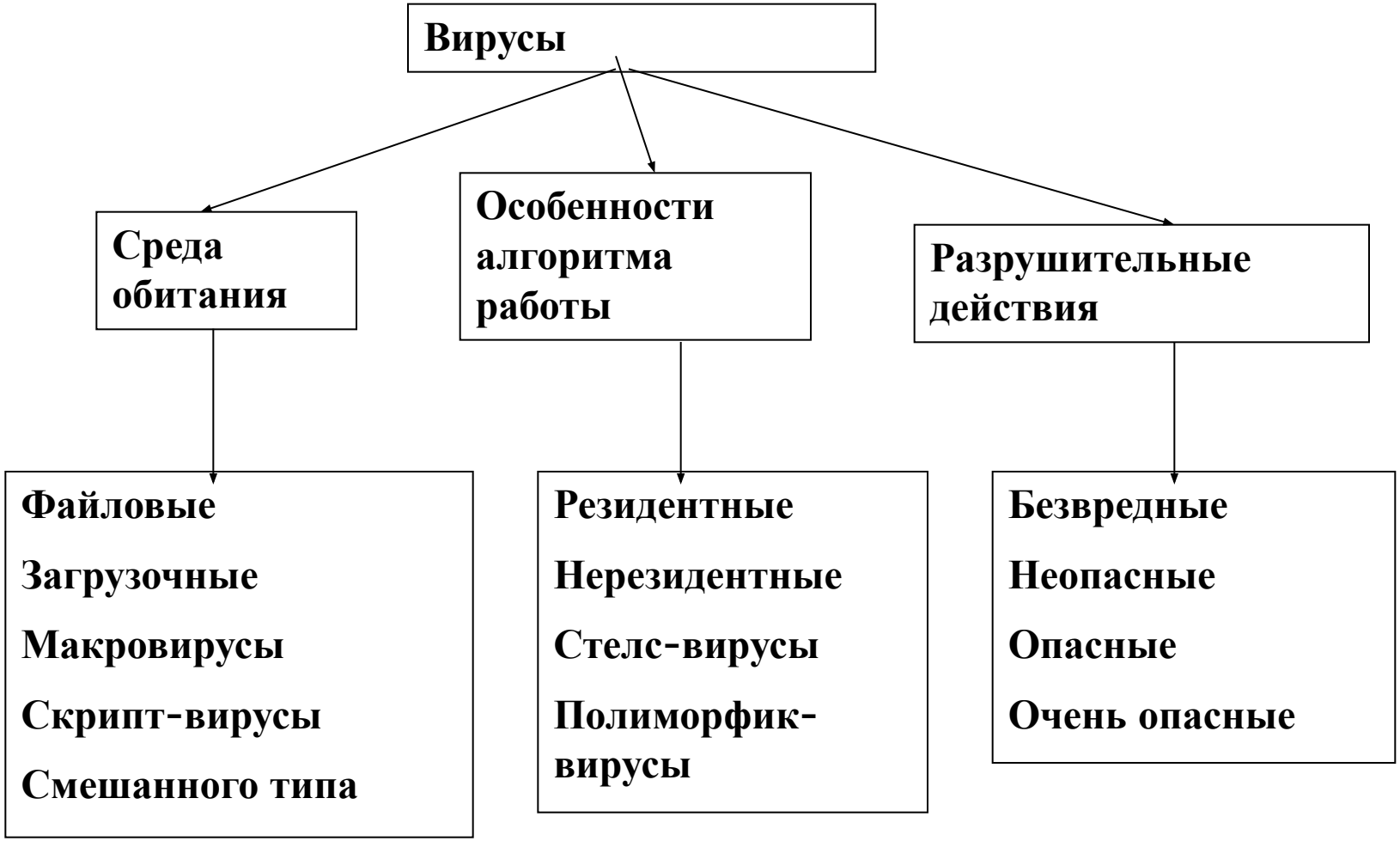
- Файловые
- Загрузочные
- Макро-вирусы
- Скрипт-вирусы
- Смешанного типа

Особенности алгоритма работы

- Резидентные и нерезидентные
- Стелс-вирусы
- Полиморфик-вирусы

Разрушительные действия

- Безвредные
- Неопасные
- Опасные
- Очень опасные


Вирусы
Среда обитания
Особенности алгоритма работы
Разрушительные действия
Файловые
Загрузочные
Макровирусы
Скрипт-вирусы
Смешанного типа
Резидентные
Нерезидентные
Стелс-вирусы
Полиморфик-вирусы
Безвредные
Неопасные
Опасные
Очень опасные

Файловые вирусы

- Файловые вирусы- это вирусы, которые внедряются в файлы операционной системы, активизируются при запуске зараженной программы и распространяются при копировании файлов с компьютера на компьютер.
- Этот тип вирусов самый старый и самый распространенный.
- Внедрение возможно во все операционные системы: DOS, Windows, OS/2, Unix

Классификация файловых вирусов

- Обычные
- Owerwriting
- Паразитические
- Компаньон-вирусы
- Link-вирусы
- Файловые черви

Загрузочные вирусы

- Загрузочные (бутовые) вирусы – это вирусы, заражающие загрузочный boot-сектор. Активизируются при запуске операционной системы.

Макровирусы

- Макровирусы - это небольшие программы, написанные на языках (макроязыках), встроенных в различные системы документооборота (текстовые редакторы, электронные таблицы и т. д.)

Резидентные вирусы

- Вирусы, которые находятся в оперативной памяти, перехватывают обращения операционной системы к тем или иным объектам и внедряются в них. Активны не только в момент работы зараженной программы, но и после того, как программа закончила свою работу.

Нерезидентные вирусы

- Активны непродолжительное время – только в момент запуска зараженной программы. Файлы зараженные нерезидентными вирусами, значительно проще вылечить, при этом вирус не заразит их повторно.

Стелс-вирусы (невидимки)

- Компьютерные вирусы, которые помимо негативных действий, присущих вирусам, пытаются скрыть факт своего присутствия в зараженных объектах. Например, вирус перехватывает команды чтения зараженного сектора и подставляет вместо него незараженный оригинал.

Полиморфик-вирусы

- Вирусы, предпринимающие специальные меры для затруднения их поиска и анализа путем шифрования основного тела вируса и модификациями программы-расшифровщика. Полиморфность – это способность вируса изменять свой код при каждом новом запуске зараженной программы. Это ведет к отсутствию постоянных байтовых сигнатур у вируса.

Сигнатура вируса

- Сигнатура вируса – это последовательность байтов, имеющаяся в любом экземпляре вируса и только в нем. По сигнатурам вирусов создается антивирусная база.

Основные методы определения вирусов

- Сканирование сигнатур
- Проверка целостности
- Эвристический анализ
- Полиморфный анализ
- Анализатор макровирусов

Сканирование сигнатур

- Метод представляет собой идентификацию вирусов по неизменным кодам (эталонам). Он опирается на базу, содержащую сигнатуры вирусов.
- Метод хорошо для поиска вирусов с неизменным кодом, но не справляется с полиморфными вирусами и вирусами-невидимками

Проверка целостности

- Метод основывается на сравнении «контрольной суммы» проверяемого файла и контрольной суммы этого же файла, хранящегося в некоторой базе. Несовпадение сумм свидетельствует о возможном заражении файла.
- Метод неэффективен для вирусов –невидимок.

Эвристический анализ

- Чтобы размножаться, вирус совершает действия: копирование в память, запись загрузочные сектора и пр. Эвристический анализатор содержит список таких действий, просматривает код программы и определяет, что она делает.

Полиморфный анализ

- Использует технологию эмуляции процессора для того, чтобы проанализировать исполняемый код вируса. Эмулятор как бы воспроизводит работу программы в некотором виртуальном пространстве или реконструирует её оригинальное содержимое и всегда способен прервать её выполнение, не давая ничего испортить.

Анализатор макровирусов

- Метод основан на поиске макроопределений в файлах офисных приложений и проверке их на наличие вирусов.

Типы антивирусных программ

- Сканеры
- CRC-сканеры (ревизоры)
- Мониторы (блокировщики)
- Иммунизаторы

Антивирусный сканер

- Программа, осуществляющая проверку файлов, секторов и системной памяти на наличие в них известных и новых (неизвестных сканеру) вирусов. Для поиска используется сигнатура вируса. В сканерах иногда используется алгоритм эвристического анализа.
- Достоинства сканеров – универсальность
- Недостатки- большие размеры антивирусных баз.

CRC – сканеры (ревизоры)

- Программы-ревизоры, осуществляющие контроль над всеми изменениями, которые происходят в файловой системе компьютера. Принцип работы основан на подсчете контрольных сумм. Используют анти-стелс алгоритмы. Недостаток CRC-сканера: не способны поймать вирус в момент его появления в системе, т.е. в новом файле.

Мониторы (блокировщики)

- Резидентные программы, перехватывающие вирусоопасные ситуации и сообщающие об этом пользователю. К вирусоопасным ситуациям относятся: изменение и переименование исполняемых файлов (COM и EXE), запись в загрузочные сектора, форматирование винчестера, попытки программ остаться резидентными и пр. Достоинства мониторов: способность обнаружить и блокировать вирус в момент его появления в системе. Недостатки: ложные срабатывания, проблемы при их установке и настройке.

Иммунизаторы

- Программы, предназначенные для защиты системы от поражения вирусом определенного типа. В память компьютера заносится программа, имитирующая копию вируса. Файлы на дисках модифицируются таким образом, что вирус принимает их за зараженные. Вирус натыкается на них и считает, что система уже заражена.

Сигнатура вируса