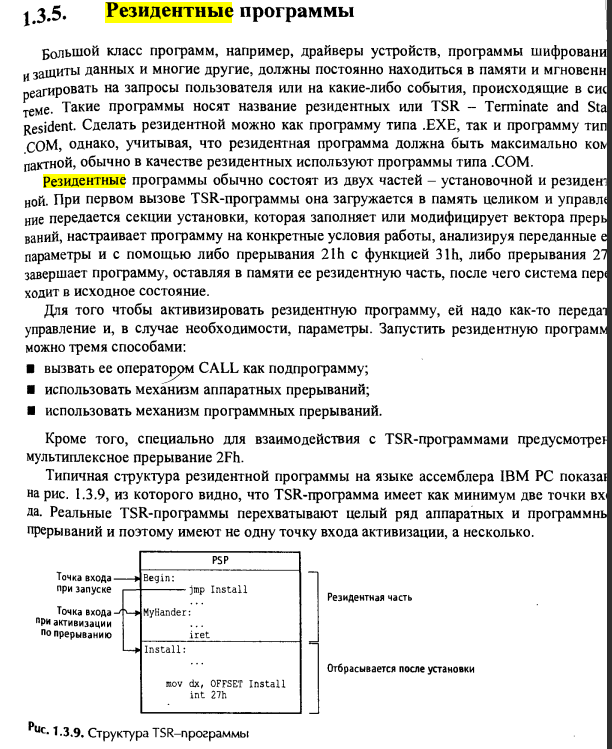
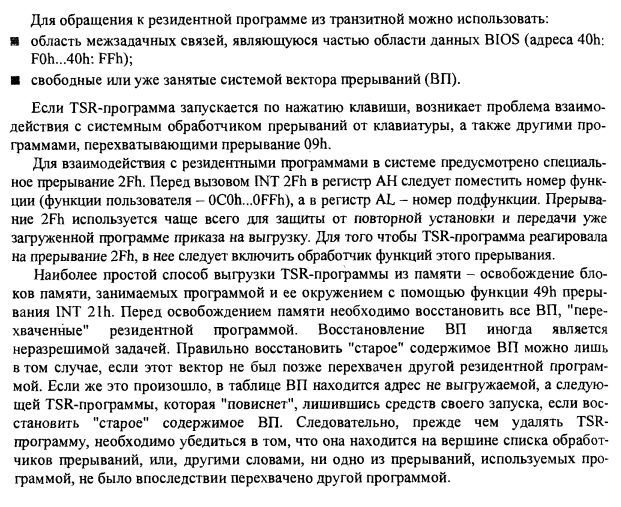
1. Резидентные программы, средства их обнаружения и локализации, описание основных антивирусных программных средств на примере Nod32. Пример разработки «вируса»





Антивирусные программы делятся на: программы-детекторы, программы-доктора, программы-ревизоры, программы-фильтры, программы-вакцины.

Программы-детекторы обеспечивают поиск и обнаружение вирусов в оперативной памяти и на внешних носителях, и при обнаружении выдают соответствующее сообщение. Различают детекторы универсальные и специализированные.

Универсальные детекторы в своей работе используют проверку неизменности файлов путем подсчета и сравнения с эталоном контрольной суммы. Недостаток универсальных детекторов связан с невозможностью определения причин искажения файлов.

Специализированные детекторы выполняют поиск известных вирусов по их сигнатуре (повторяющемуся участку кода). Недостаток таких детекторов состоит в том, что они неспособны обнаруживать все известные вирусы.

Детектор, позволяющий обнаруживать несколько вирусов, называют полидетектором.

Программы-доктора (фаги), не только находят зараженные вирусами файлы, но и "лечат" их, т.е. удаляют из файла тело программы вируса, возвращая файлы в исходное состояние. В начале своей работы фаги ищут вирусы в оперативной памяти, уничтожая их, и только затем переходят к "лечению" файлов. Среди фагов выделяют полифаги, т.е. программы-доктора, предназначенные для поиска и уничтожения большого количества вирусов.

Учитывая, что постоянно появляются новые вирусы, программы-детекторы и программы-доктора быстро устаревают, и требуется регулярное обновление их версий.

Программы-ревизоры относятся к самым надежным средствам защиты от вирусов. Ревизоры запоминают исходное состояние программ, каталогов и системных областей диска тогда, когда компьютер не заражен вирусом, а затем периодически или по желанию пользователя сравнивают текущее состояние с исходным. Обнаруженные изменения выводятся на экран видеомонитора. Как правило, сравнение состояний производят сразу после загрузки операционной системы. При сравнении проверяются длина файла, код циклического контроля (контрольная сумма файла), дата и время модификации, другие параметры.

Программы-ревизоры имеют достаточно развитые алгоритмы, обнаруживают стелс-вирусы и могут даже отличить изменения версии проверяемой программы от изменений, внесенных вирусом.

Программы-фильтры (сторожа) представляют собой небольшие резидентные программы, предназначенные для обнаружения подозрительных действий при работе компьютера, характерных для вирусов. Такими действиями могут являться:

-попытки коррекции файлов с расширениями СОМ и ЕХЕ

-изменение атрибутов файлов

-прямая запись на диск по абсолютному адресу

-запись в загрузочные сектора диска

-загрузка резидентной программы

При попытке какой-либо программы произвести указанные действия "сторож" посылает пользователю сообщение и предлагает запретить или разрешить соответствующее действие. Программы-фильтры весьма полезны, так как способны обнаружить вирус на самой ранней стадии его существования до размножения. Однако они не "лечат" файлы и диски. Для уничтожения вирусов требуется применить другие программы, например фаги. К недостаткам программ-сторожей можно отнести их "назойливость" (например, они постоянно выдают предупреждение о любой попытке копирования исполняемого файла), а также возможные конфликты с другим программным обеспечением.

Вакцины (иммунизаторы) - это резидентные программы, предотвращающие заражение файлов. Вакцины применяют, если отсутствуют программы-доктора, "лечащие" этот вирус. Вакцинация возможна только от известных вирусов. Вакцина модифицирует программу или диск таким образом, чтобы это не отражалось на их работе, а вирус будет воспринимать их зараженными и поэтому не внедрится. В настоящее время программы-вакцины имеют ограниченное применение.

Существенным недостатком таких программ является их ограниченные возможности по предотвращению заражения от большого числа разнообразных вирусов.

Антивирус Eset NOD32 (32-bit) - очень быстро работающая и мало нагружающая систему антивирусная программа, эффективно защищающая от всех видов вирусов и "шпионских" (Adware/Spyware/Riskware) программ. В Eset NOD32 имеется очень мощный эвристический анализатор, позволяющий с большой точностью выявлять еще неизвестные "науке" вирусы (как показывают тесты Virus Bulletin, это единственный антивирус в мире, который уже более 7 лет не пропустил ни один активный на момент тестирования вирус), а также не менее мощный и надежный встроенный виртуальный эмулятор для обнаружения полиморфных вирусов.

Антивирус ESET NOD32 разработан на основе популярной технологии ThreatSense®. Система позволяет проактивно выявлять и обезвреживать больше вирусов, шпионских программ, рекламного ПО, фишинг-атак, руткитов и других интернет-угроз, чем какая-либо другая программа. Антивирус ESET NOD32 — это:

-Проактивная защита. Популярная технология ThreatSense® сочетает несколько уровней обнаружения, заблаговременно предоставляя защиту от интернет-угроз.

-Точное обнаружение. Антивирус ESET NOD32 точно выявляет известные и неизвестные угрозы. Это подтверждается наградами независимых тестирующих лабораторий. При этом следует отметить нулевые показатели в тестах на определение ложного срабатывания.

-Небольшой объем обновлений. Решение требует меньше памяти и мощности ЦП. Работа антивируса практически не сказывается на производительности компьютера, оставляя пользователю больше возможностей для игр, просмотра интернет-ресурсов и работы с электронной почтой.

-Высокая скорость сканирования. Эффективность программы обеспечивает высокую скорость сканирования и обновления продуктов. Фоновый режим работы делает ее практически незаметной для пользователя.

