Федеральное агентство по образованию

Камбарский Машиностроительный Колледж (филиал) ИжГТУ

08110

Сообщение по информатике

На тему: **Антивирусные программы**

Выполнил: Набиуллина О.М

Группа: 23- ЭБ – 09

Проверил: Куликова И.Е

Дата: \_\_\_\_\_\_\_\_\_\_\_\_

Оценка : \_\_\_\_\_\_\_\_\_\_\_\_

**Антивирусные программы.**

Антивирусная программа (антивирус) — программа для обнаружения компьютерных вирусов, а также нежелательных (считающихся вредоносными) программ вообще, и восстановления зараженных (модифицированных) такими программами файлов, а также для профилактики — предотвращения заражения (модификации) файлов или операционной системы вредоносным кодом (например, с помощью вакцинации).

**Классификация антивирусов**

По набору функций и гибкости настроек антивирусы можно разделить на:

Продукты для домашних пользователей:

Собственно антивирусы;

Комбинированные продукты (например, к классическому антивирусу добавлен антиспам, файрвол, антируткит и т. д.);

Корпоративные продукты:

Серверные антивирусы;

Антивирусы на рабочих станциях («endpoint»);

Антивирусы для почтовых серверов;

Антивирусы для шлюзов.

Ложные антивирусы (лжеантивирусы)

В 2009 году различные производители антивирусов стали сообщать о широком распространении нового типа программ — ложных или лжеантивирусов (rogueware). По сути эти программы или вовсе не являются антивирусами (то есть не способны бороться с вредоносным ПО), или даже являются вирусами (воруют данные кредитных карт и т. п.).

**Ложные антивирусы** используются для вымогательства денег у пользователей путём обмана. Один из способов заражения ПК ложным антивирусом следующий. Пользователь попадает на «инфицированный» сайт, который выдаёт ему предупреждающее сообщение вроде «На вашем компьютере обнаружен вирус» и предлагает скачать бесплатную программу для удаления вируса. После установки такая программа производит сканирование компьютера и якобы обнаруживает ещё массу вирусов. Для удаления вредоносного ПО ложный антивирус предлагает купить платную версию программы. Шокированный пользователь платит (суммы колеблются от $10 до $80) и ложный антивирус очищает ПК от несуществующих вирусов.

Характеристика антивирусных программ.

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

Программы-детекторы обеспечивают поиск и обнаружение вирусов воперативной памяти и на внешних носителях, и при обнаружении выдаютсоответствующее сообщение. Различают детекторы универсальные испециализированные.

Универсальные детекторы в своей работе используют проверкунеизменности файлов путем подсчета и сравнения с эталоном контрольнойсуммы. Недостаток универсальных детекторов связан с невозможностьюопределения причин искажения файлов.

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

Детектор, позволяющий обнаруживать несколько вирусов, называют полидетектором.

Недостатком таких антивирусных про грамм является то, что они могут находить только те вирусы, которые известны разработчикам таких программ.

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 ипрограммы-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 н 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.