Е. К. Ловчева, Н. А. Жиляк
(БГТУ, Минск)

АНТИВИРУСНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Компьютерные вирусы – это маленькие программы, созданные на языках низкого уровня (в машинных кодах). В отличие от созданных и находящихся в компьютере объектов, они существуют не в виде отдельных файлов, а в виде дополнительных команд, привязанных к какой-либо компьютерной программе. При загрузке в ОЗУ другой про-

граммы вирус проникает в нее, то есть присоединяет к ней свой код, и таким образом размножается и распространяются в других программах.

Для борьбы с вирусами разрабатываются и применяются антивирусные программы. По характеру их борьбы с вирусами можно классифицировать по нескольким группам: фильтры, детекторы, ревизоры, доктора, вакцинаторы.

Антивирусы-фильтры – это резидентные программы, которые оповещают пользователя обо всех попытках какой-либо программы записаться на диск, а уж тем более отформатировать его, а также о других подозрительных действиях. При этом выводится запрос о разрешении или запрещении данного действия. Принцип работы этих программ основан на перехвате соответствующих векторов прерываний.

К преимуществам программ этого класса можно отнести универсальность по отношению как к известным, так и к неизвестным вирусам. Это особенно актуально сейчас, когда появилось множество вирусов-мутантов, не имеющих постоянного кода.

Антивирусы-детекторы рассчитаны на конкретные вирусы и основаны на сравнении последовательности кодов, содержащихся в теле вируса, с кодами проверяемых программ. Такие программы нужно регулярно обновлять, так как они быстро устаревают и не могут обнаруживать новые виды вирусов.