

Компьютерные вирусы и защита от них

*Компьютерный вирус
Загрузочный вирус
Файловый вирус
Макровирус*

Компьютерный вирус

Вредоносная программа, которая «размножается» и скрытно внедряет свои копии в файлы, загрузочные секторы дисков и документы.



Активизация
компьютерного вируса
может вызывать
уничтожение
программ и данных.

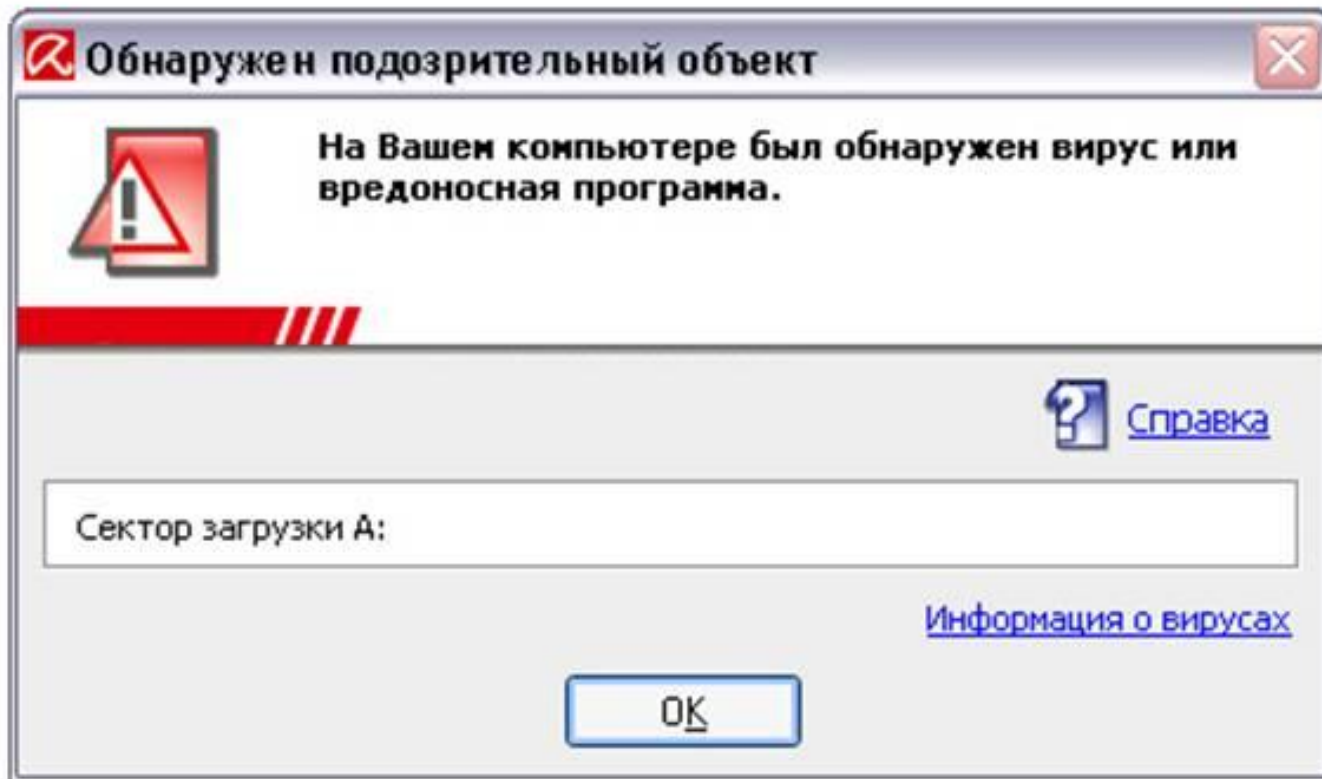


- По среде обитания
- загрузочные
- файловые
- макро-вирусы

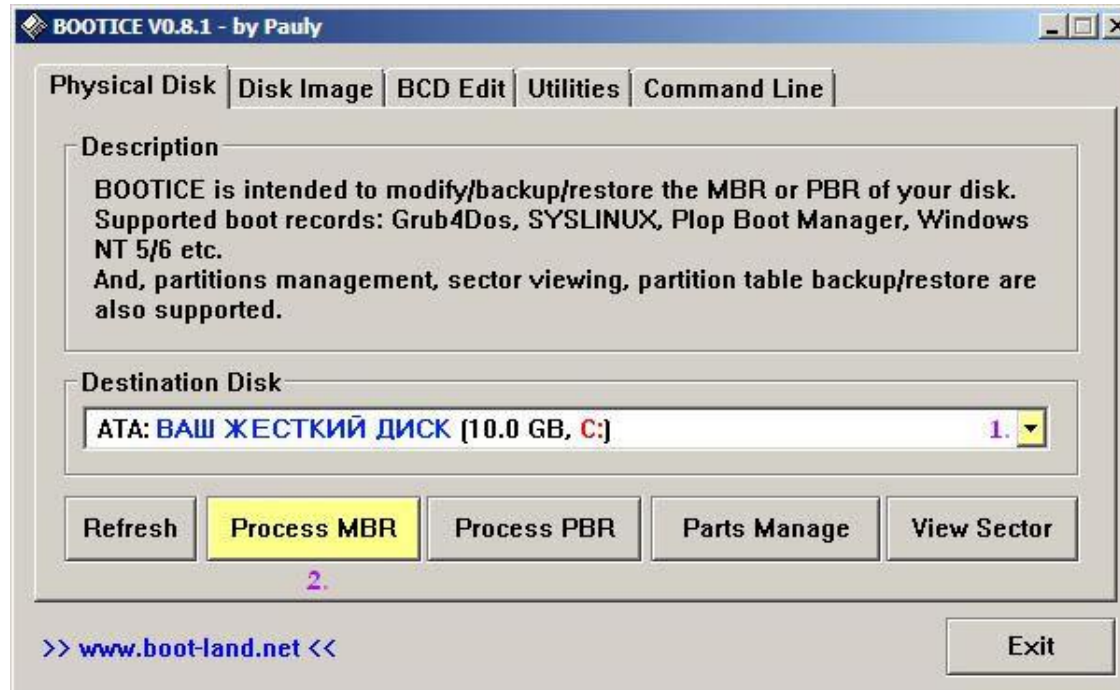


Загрузочные вирусы

Заражают загрузочный сектор гибкого или жесткого диска.

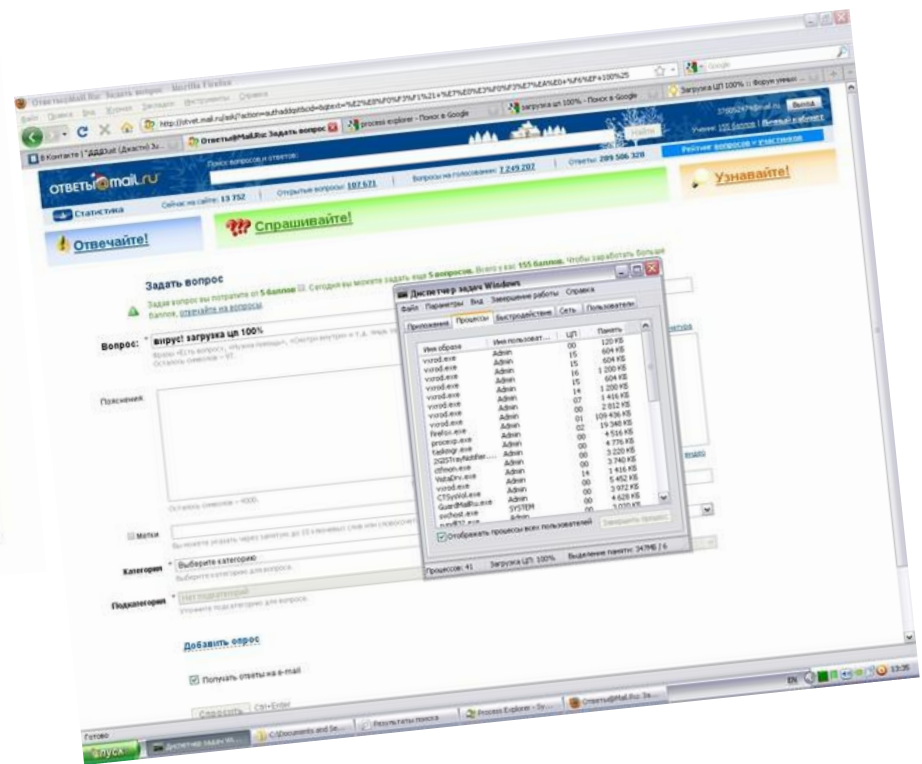
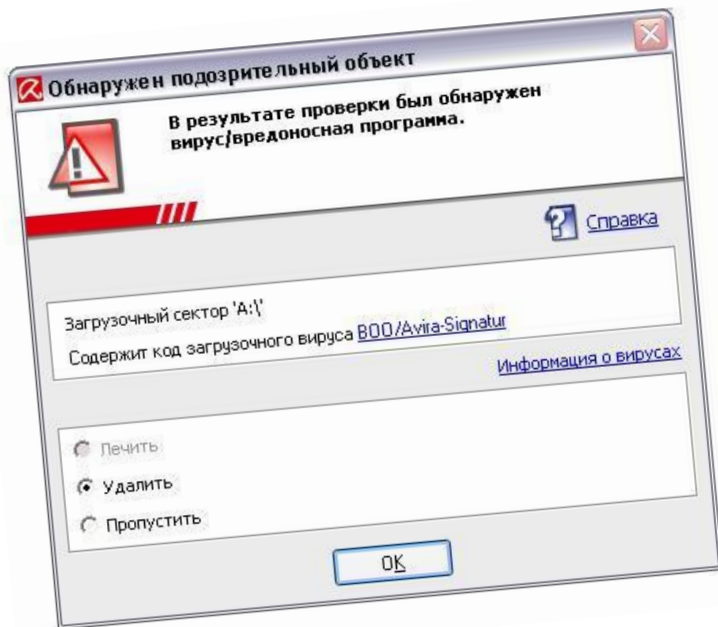


Принцип действия основан на **алгоритмах запуска** операционной системы при включении или перезагрузке компьютера.

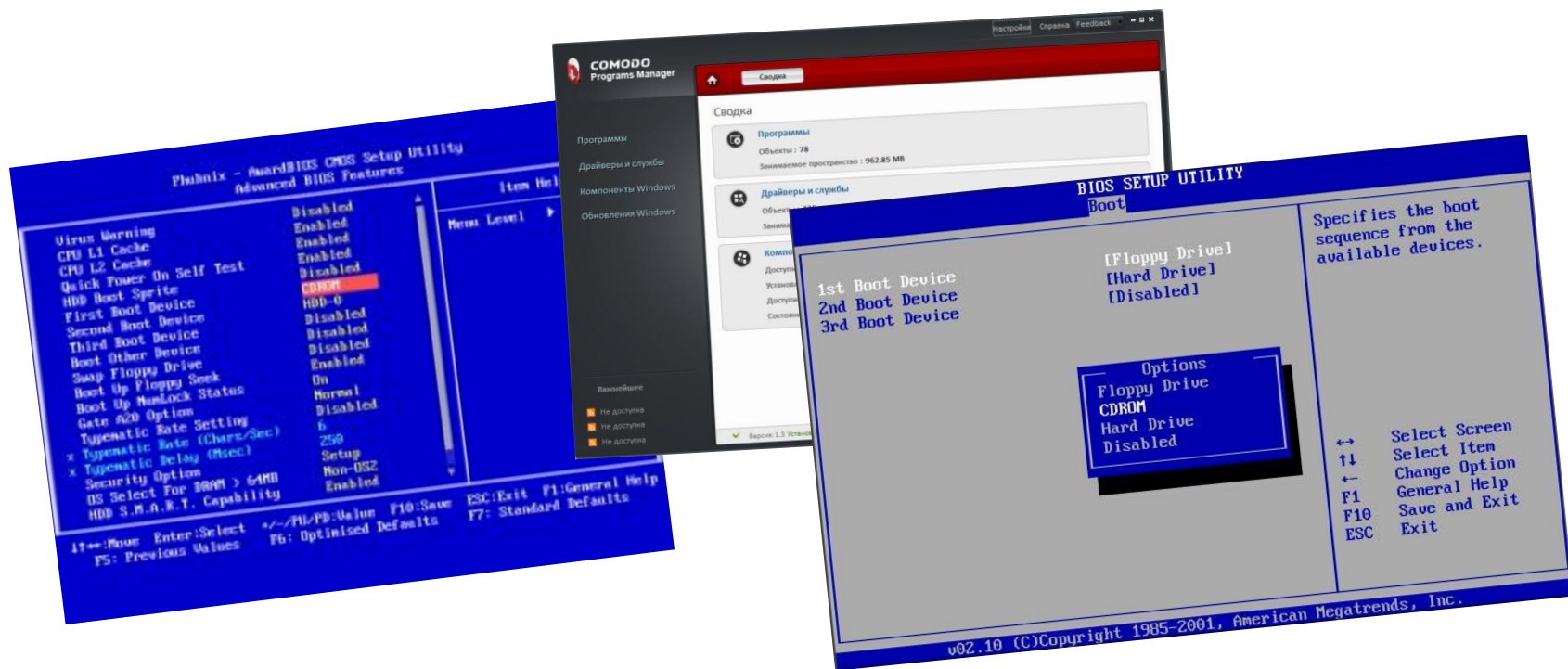


После необходимых тестов программа системной загрузки считывает первый физический сектор загрузочного диска и передает на него управление.

При заражении дисков загрузочные вирусы «подставляют» свой код вместо программы и отдают управление не коду загрузчика, а коду вируса.



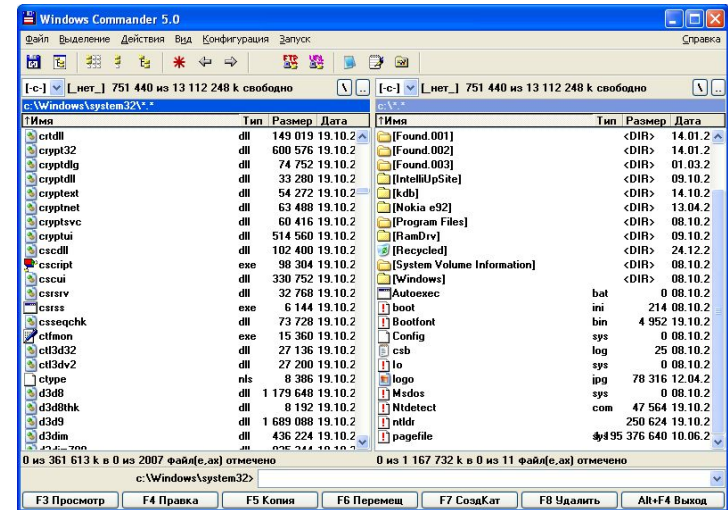
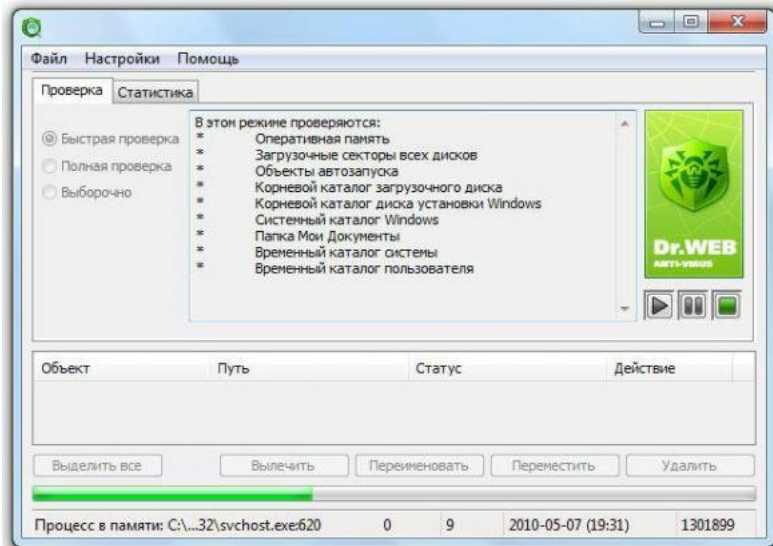
Профилактическая защита состоит в отказе от загрузки ОС с гибких дисков и установке в BIOS компьютера защиты загрузочного сектора от изменений.



С помощью программы BIOS Setup можно провести настройку таким образом, что будет заблокирована любая запись в загрузочный сектор диска и компьютер будет защищен от заражения вирусами.

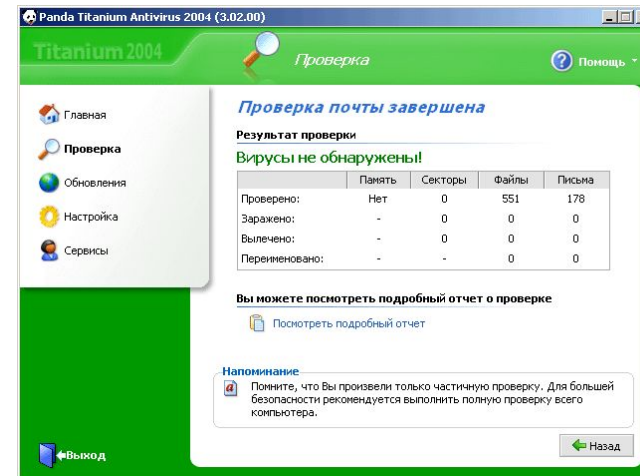
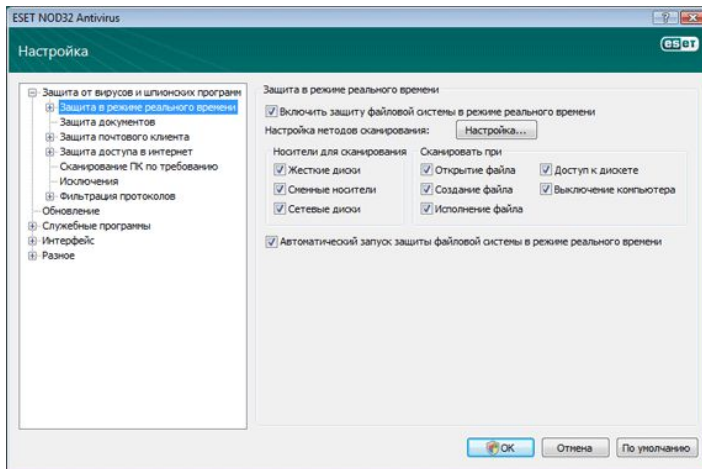
Файловые вирусы

Различными способами внедряются в исполнимые файлы и активируются при их запуске.



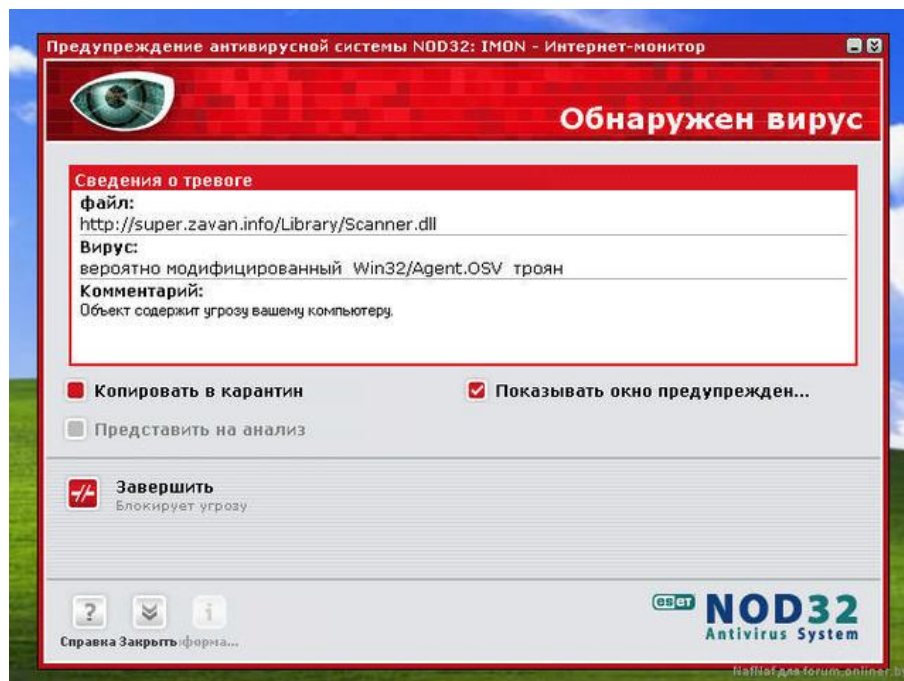
После запуска зараженного файла вирус находится в оперативной памяти и является активным вплоть до момента выключения компьютера.

Практически все загрузочные и файловые вирусы **резидентны**, т.е. они находятся в оперативной памяти компьютера и в процессе работы пользователя могут осуществлять опасные действия (стирать данные на дисках, изменять названия файлов)



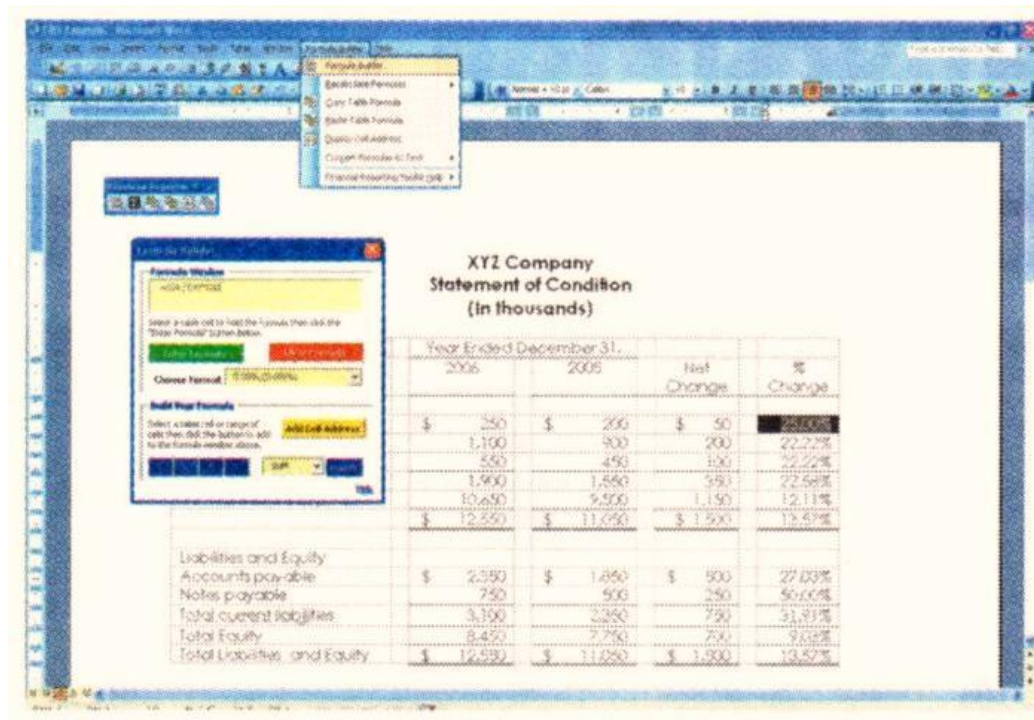
Лечение от резидентных вирусов затруднено, т.к. даже после удаления зараженных файлов с дисков, вирус остается в оперативной памяти и возможно повторное заражение файлов.

Профилактическая защита от файловых вирусов состоит в том, что не рекомендуется запускать на исполнение файлы, полученные от сомнительных источников и предварительно не проверенные антивирусными программами.



Макровирусы

Являются **макрокомандами** (макросами), на встроенном языке программирования Visual Basic, которые помещаются в документ.

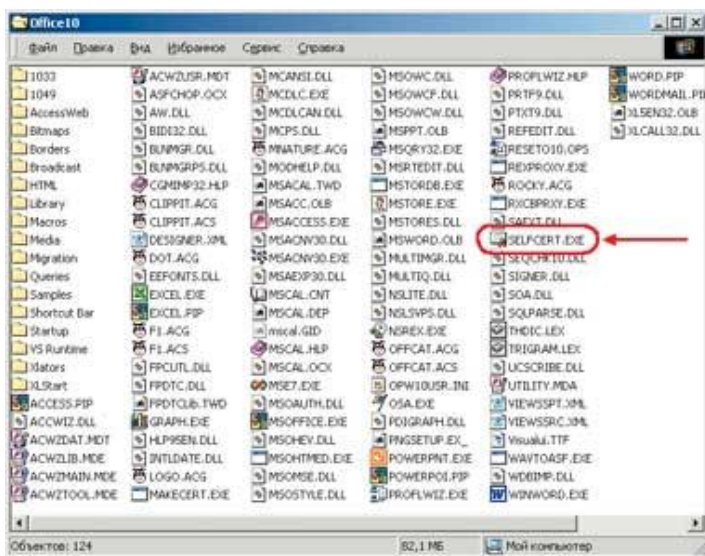


The screenshot shows an Excel spreadsheet titled "XYZ Company Statement of Condition (In thousands)". The data is organized into columns for the years 2005 and 2006, with additional columns for "Net Change" and "% Change". The spreadsheet includes a section for "Liabilities and Equity" with sub-rows for "Accounts payable", "Notes payable", and "Total current liabilities". The "Total Liabilities and Equity" row shows a net change of \$1,000 and a percentage change of 13.47%.

	Year Ended December 31,		Net Change	% Change
	2005	2006		
	\$ 250	\$ 250	\$ 50	20.00%
	1,100	900	200	18.18%
	500	450	50	10.00%
	1,900	1,850	50	2.63%
	10,650	9,500	1,150	10.79%
	\$ 12,500	\$ 11,650	\$ 1,850	14.67%
Liabilities and Equity				
Accounts payable	\$ 2,350	\$ 1,850	\$ 500	21.28%
Notes payable	750	500	250	33.33%
Total current liabilities	3,100	2,350	750	24.19%
Total Equity	8,450	7,750	700	8.28%
Total Liabilities and Equity	\$ 12,550	\$ 11,100	\$ 1,450	11.56%

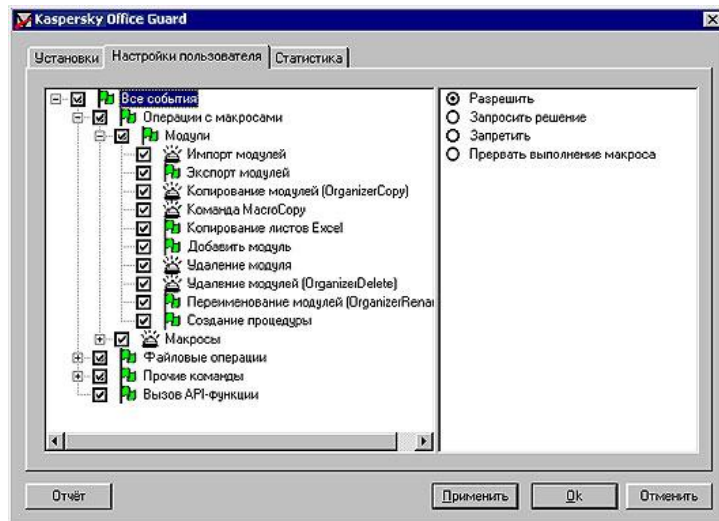
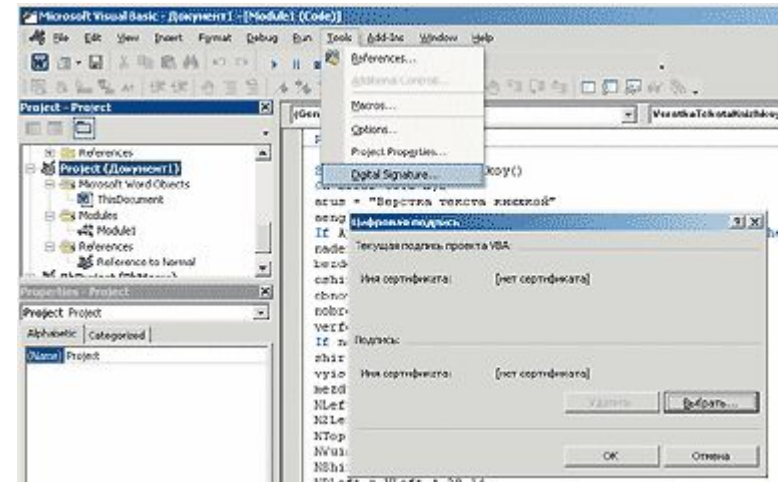
Пользователь выполняет различные действия: открывает документ, сохраняет, печатает, закрывает.

При этом приложение ищет и выполняет соответствующие стандартные макросы.



Макровирусы содержат стандартные макросы, вызываются вместо них и заражают каждый открываемый или сохраняемый документ.

Являются **ограниченно резидентными**, т.к. они находятся в оперативной памяти и заражают документы, пока открыто приложение.



Заражают шаблоны документов и активизируются уже при запуске зараженного приложения.

Профилактическая защита состоит в предотвращении запуска вируса. При открытии документа в приложениях Microsoft Office сообщается о присутствии в них макросов (потенциальных вирусов) и предлагается запретить их загрузку.

