



ВНИМАНИЕ! SYMANTEC ПРЕДОСТАВЛЯЕТ ВАМ ПРАВО ИСПОЛЬЗОВАТЬ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ, СОДЕРЖАЩЕЕСЯ В КОМПЛЕКТЕ ПОСТАВКИ ТОЛЬКО ПРИ УСЛОВИИ ВАШЕГО ПОЛНОГО СОГЛАСИЯ СО ВСЕМИ УСЛОВИЯМИ, СОДЕРЖАЩИМИСЯ В НАСТОЯЩЕМ ЛИЦЕНЗИОННОМ СОГЛАШЕНИИ. ПОЖАЛУЙСТА, ПРОЧТИТЕ ОЧЕНЬ ВНИМАТЕЛЬНО ЭТОТ ДОКУМЕНТ ПЕРЕД ТЕМ КАК ВСКРЫВАТЬ УПАКОВКУ ДИСКЕТ, ТАК КАК САМ ФАКТ НАРУШЕНИЯ (ВСКРЫТИЯ) УПАКОВКИ С ДИСКЕТАМИ ОЗНАЧАЕТ ВАШЕ ПОЛНОЕ СОГЛАСИЕ СО ВСЕМИ УСЛОВИЯМИ НАСТОЯЩЕГО СОГЛАШЕНИЯ. ЕСЛИ ВЫ НЕ СОГЛАСНЫ С НАСТОЯЩИМ СОГЛАШЕНИЕМ, ТО ВЫ НЕ ИМЕЕТЕ ЛЕГАЛЬНОГО ПРАВА ИСПОЛЬЗОВАТЬ ДАННОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ. В ЭТОМ СЛУЧАЕ ВЫ ДОЛЖНЫ ВЕРНУТЬ ПОЛНОСТЬЮ ВЕСЬ ПАКЕТ ВМЕСТЕ С ДОКУМЕНТАМИ, ПОДТВЕРЖДАЮЩИМИ ФАКТ ЕГО ПРИОБРЕТЕНИЯ ВАМИ ТОМУ ПРОДАВЦУ, У КОТОРОГО ВЫ ЕГО ПРИОБРЕЛИ.

Лицензионное Соглашение

НАСТОЯЩИЙ ДОКУМЕНТ ПРЕДСТАВЛЯЕТ СОБОЙ ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ ("СОГЛАШЕНИЕ") МЕЖДУ КОНЕЧНЫМ ПОЛЬЗОВАТЕЛЕМ И SYMANTEC CORPORATION ("SYMANTEC"), НАХОДЯЩЕЕСЯ В ДАННОМ ПАКЕТЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ("ПРОГРАММА"), ОТНОСИТЕЛЬНО КОТОРОГО ДЕЙСТВУЕТ НАСТОЯЩЕЕ СОГЛАШЕНИЕ, ЯВЛЯЕТСЯ СОБСТВЕННОСТЬЮ SYMANTEC ИЛИ СОБСТВЕННОСТЬЮ ТРЕТЬИХ ФИРМ, НАХОДЯЩИХСЯ В ДОВОРОНЫХ ОТНОШЕНИЯХ С SYMANTEC И ОБЛАДАЕТ ВСЕМИ ПРИЗНАКАМИ СОБСТВЕННОСТИ В СООТВЕТСТВИИ С ДЕЙСТВУЮЩИМ ЗАКОНОДАТЕЛЬСТВОМ. ПОЛЬЗОВАТЕЛЬ, СОГЛАСНЫЙ С ПОЛОЖЕНИЯМИ ДАННОГО СОГЛАШЕНИЯ, ПРИОБРЕТАЕТ ОПРЕДЕЛЕННЫЕ ПРАВА НА ИСПОЛЬЗОВАНИЕ ДАННОЙ ПРОГРАММЫ, ПРИ ЭТОМ ВСЕ ПРАВА СОБСТВЕННОСТИ ОСТАЮТСЯ У SYMANTEC. ЕСЛИ ИНОЕ НЕ ОГОВОРЕНО В СПЕЦИАЛЬНОМ ПРИЛОЖЕНИИ К НАСТОЯЩЕМУ СОГЛАШЕНИЮ, ТО ВАШИ ПРАВА И ОБЯЗАТЕЛЬСТВА ПО ИСПОЛЬЗОВАНИЮ ЭТОЙ ПРОГРАММЫ СОСТАВЛЯЮТ СЛЕДУЮЩЕЕ:

ВЫ МОЖЕТЕ:

- ИСПОЛЬЗОВАТЬ ОДНУ КОПИЮ ПРОГРАММЫ НА ОДНОМ КОМПЬЮТЕРЕ; ЕСЛИ НОСИТЕЛЬ, КОТОРЫЙ НАХОДИТСЯ В ДАННОЙ КОРОБКЕ СОДЕРЖИТ ВЕРСИЮ ПРОГРАММЫ БОЛЕЕ ЧЕМ НА ОДНОМ ЯЗЫКЕ И/ИЛИ НЕКОЛЬКО ВЕРСИЙ ПРОГРАММЫ, ЛИЦЕНЗИЯ ПРЕДОСТАВЛЯЕТ ВАМ ПРАВО ЛЕГАЛЬНО ИСПОЛЬЗОВАТЬ ЛЮБУЮ ВЕРСИЮ ТОЛЬКО НА ОДНОМ ЯЗЫКЕ (ВЫ НЕ МОЖЕТЕ СОЗДАВАТЬ И ИСПОЛЬЗОВАТЬ КОПИИ НА ДРУГИХ ЯЗЫКАХ), ПРИ ЭТОМ ВЫ НЕ МОЖЕТЕ ПЕРЕДАВАТЬ КАК СОБСТВЕННО НЕИСПОЛЬЗУЕМЫЕ ВАМИ ВЕРСИИ ТАК И ПРАВО ИХ ИСПОЛЬЗОВАНИЯ ДРУГОМУ ЧЕЛОВЕКУ;
- ИЗГОТОВИТЬ ОДНУ ДОПОЛНИТЕЛЬНУЮ КОПИЮ ПРОГРАММЫ ДЛЯ ЦЕЛЕЙ РЕЗЕРВНОГО КОПИРОВАНИЯ, ИЛИ СКОПИРОВАТЬ ПРОГРАММУ НА ЖЕСТКИЙ ДИСК ВАШЕГО КОМПЬЮТЕРА И ИСПОЛЬЗОВАТЬ ЭТУ КОПИЮ КАК ОРИГИНАЛ ДЛЯ РЕЗЕРВНОГО КОПИРОВАНИЯ.
- ИСПОЛЬЗОВАТЬ ПРОГРАММУ ДЛЯ РАБОТЫ В СЕТИ, ПРИ УСЛОВИИ НАЛИЧИЯ ЛИЦЕНЗИИ НА ИСПОЛЬЗОВАНИЕ ДАННОЙ ПРОГРАММЫ ДЛЯ ВСЕХ КОМПЬЮТЕРОВ, ИМЕЮЩИХ К НЕЙ ДОСТУП С ПОМОЩЬЮ ЭТОЙ СЕТИ.
- ПЕРЕДАТЬ ПРОГРАММУ ДЛЯ ПОСТОЯННОГО ИСПОЛЬЗОВАНИЯ ТРЕТЬЕМУ ЛИЦУ ИЛИ ОРГАНИЗАЦИИ, ПРЕВАРИТЕЛЬНО ОТПЕЧАТАВ ПИСЬМЕННОЕ УВЕДОМЛЕНИЕ SYMANTEC, И ПРИ УСЛОВИИ ЧТО ВЫ УНИЧТОЖИТЕ ВСЕ КОПИИ ПРОГРАММЫ НА ВСЕХ НОСИТЕЛЯХ НЕ ПОДЛЕЖАЩИХ ТАКОЙ ПЕРЕДАЧЕ, А ТАКЖЕ ПРИ УСЛОВИИ ТОГО, ЧТО НОВЫЙ ПОЛЬЗОВАТЕЛЬ ПРОГРАММЫ БУДЕТ СОГЛАСЕН С УСЛОВИЯМИ НАСТОЯЩЕГО СОГЛАШЕНИЯ.
- ЕСЛИ КОМПЬЮТЕР, НА КОТОРОМ УСТАНОВЛЕНА ПРОГРАММА, ИСПОЛЬЗУЕТСЯ ПЕРСОНАЛЬНО (ОДНИМ ЧЕЛОВЕКОМ) В ТЕЧЕНИИ НЕ МЕНЕЕ 80% РАБОЧЕГО ВРЕМЕНИ, ТО ПОСЛЕ ЗАПЛОЧЕНИЯ И ОТПРАВКИ В SYMANTEC РЕГИСТРАЦИОННОЙ КАРТОЧКИ ПОЛЬЗОВАТЕЛЯ, ВХОДЯЩЕЙ В КОМПЛЕКТ ПОСТАВКИ ПРОГРАММЫ, ЭТОТ ПОЛЬЗОВАТЕЛЬ ИМЕЕТ ПРАВО ИСПОЛЬЗОВАТЬ ПРОГРАММУ НА ОДНОМ КОМПЬЮТЕРЕ У СЕБЯ ДОМА.

ВЫ НЕ МОЖЕТЕ:

- КОПИРОВАТЬ ДОКУМЕНТАЦИЮ, ВХОДЯЩУЮ В КОМПЛЕКТ ПОСТАВКИ ПРОГРАММЫ.
- КАК ПОЛНОСТЬЮ ТАК И ЧАСТИЧНО ПРЕДОСТАВЛЯТЬ ПРОГРАММУ В АРЕНДУ ИЛИ ПРЕДОСТАВЛЯТЬ НА НЕЕ СУБЛИЦЕНЗИЮ.
- ПЫТАТЬСЯ ВОССТАНОВЛИВАТЬ ЛЮБЫМ СПОСОБОМ ИСХОДНЫЙ ТЕКСТ ПРОГРАММЫ, ДЕКОМПИЛИРОВАТЬ, ДИЗАССЕМБЛИРОВАТЬ, МОДИФИЦИРОВАТЬ, ПЕРЕВОДИТЬ И ВНОСИТЬ ЛЮБЫЕ ИЗМЕНЕНИЯ В ПРОГРАММУ А ТАКЖЕ ИСПОЛЬЗОВАТЬ ПРОГРАММУ В КАЧЕСТВЕ СОСТАВНОЙ ЧАСТИ ДРУГИХ ПРОДУКТОВ.
- ИСПОЛЬЗОВАТЬ ПРЕДЫДУЩУЮ КОПИЮ ПРОГРАММЫ, ПОСЛЕ ПОЛУЧЕНИЯ ВАМИ НОВОЙ КОПИИ НА ДРУГОМ НОСИТЕЛЕ, ИЛИ ОБНОВЛЕННОЙ ВЕРСИИ В КАЧЕСТВЕ ЗАМЕНЫ ПРЕДЫДУЩЕЙ, КРОМЕ СЛУЧАЯ, КОГДА ВЫ ПЕРЕДАЕТЕ ЭТУ УСТАРЕВШУЮ ВЕРСИЮ КАЧЕСТВЕ БЕЗВОЗМЕЗДНОГО ДАРА ПО СВОЕМУ УСМОТРЕНИЮ И ПРИНИМАЮЩАЯ СТОРОНА ВЫРАЖАЕТ ПИСЬМЕННОЕ СОГЛАСИЕ БЫТЬ КОНЕЧНЫМ И ЕДИНСТВЕННЫМ ПОЛЬЗОВАТЕЛЕМ ДАННОГО ПРОДУКТА И СЛЕДОВАТЬ ПОЛОЖЕНИЯМ НАСТОЯЩЕГО СОГЛАШЕНИЯ. ВО ВСЕХ ПРОЧИХ СЛУЧАЯХ ВСЕ КОПИИ ПРЕДЫДУЩЕЙ ВЕРСИИ ДОЛЖНЫ БЫТЬ УНИЧТОЖЕНЫ.

ОГРАНИЧЕННАЯ ГАРАНТИЯ

SYMANTEC ГАРАНТИРУЕТ, ЧТО НОСИТЕЛИ, НА КОТОРЫХ ПОСТАВЛЯЕТСЯ ПРОГРАММА НЕ БУДУТ ИМЕТЬ ФИЗИЧЕСКИХ ДЕФЕКТОВ В ТЕЧЕНИИ 60 ДНЕЙ С МОМЕНТА ПОСТАВКИ ПРОГРАММЫ ВАМ. В СЛУЧАЕ ОБНАРУЖЕНИЯ ТАКИХ ДЕФЕКТОВ В ТЕЧЕНИЕ ЭТОГО СРОКА SYMANTEC, ПО ВОЗМОЖНОСТИ, ПРОИЗВЕДЕТ ЗАМЕНУ ДЕФЕКТНЫХ НОСИТЕЛЕЙ, ВОЗВРАЩЕННЫХ В SYMANTEC. SYMANTEC НЕ ГАРАНТИРУЕТ, ЧТО ПРОГРАММА УДОВЛЕТВОРЕТ ВАШИМ ТРЕБОВАНИЯМ, ИЛИ ЧТО ПРИ ЕЕ РАБОТЕ НЕ БУДЕТ ПРОИСХОДИТЬ СБОЕВ, ИЛИ ЧТО ПРОГРАММА НЕ СОДЕРЖИТ ОШИБОК.

ПЕРЕЧИСЛЕННЫЕ ГАРАНТИИ НОСЯТ ИСКЛЮЧИТЕЛЬНЫЙ ХАРАКТЕР И МОГУТ ВЫСТУПАТЬ ВМЕСТО ВСЕХ ДРУГИХ ГАРАНТИЙ, ОГОВОРЕННЫХ ЯВНО ИЛИ ПОДРАЗУМЕВАЕМЫХ, ВКЛЮЧАЯ ПОДРАЗУМЕВАЕМЫЕ ГАРАНТИИ КОММЕРЧЕСКОГО УСПЕХА И ПРИГОДНОСТИ ДЛЯ ОПРЕДЕЛЕННОЙ ЗАДАЧИ. НИКАКАЯ УСТНАЯ ИЛИ ПИСЬМЕННАЯ ИНФОРМАЦИЯ, ИСХОДЯЩАЯ ОТ SYMANTEC, ЕЕ СОТРУДНИКОВ, ДИСТРИБУТОРОВ, ДИЛЕРОВ ИЛИ АГЕНТОВ, НЕ ПОВЫСИТ ПРЕДЕЛЫ ОТВЕТСТВЕННОСТИ ПО ПЕРЕЧИСЛЕННЫМ ГАРАНТИЯМ И НЕ СОЗДАСТ НОВЫЕ ГАРАНТИИ.

ОГРАНИЧЕННАЯ ЗАЩИТА ОТ УЩЕРБА

НИ ПРИ КАКИХ ОБСТОЯТЕЛЬСТВАХ SYMANTEC НЕ НЕСЕТ ПЕРЕД ВАМИ ОТВЕТСТВЕННОСТИ ЗА ЛЮБУЮ УМЫШЛЕННУЮ, ЯВЛЯЮЩУСЯ РЕЗУЛЬТАТОМ ЧЕГО ЛИБО, КОСВЕННУЮ ИЛИ ПОДОБНУЮ УЩЕРБ, ВКЛЮЧАЯ ПОТЕРЮ ПРИБЫЛИ ИЛИ ДАННЫХ, СТАВШИХ РЕЗУЛЬТАТОМ ИСПОЛЬЗОВАНИЯ ИЛИ НЕВОЗМОЖНОСТИ ИСПОЛЬЗОВАТЬ ПРОГРАММУ ИЛИ КАКИЕ-НИБУДЬ ДАННЫЕ, ВХОДЯЩИЕ В КОМПЛЕКТ ПОСТАВКИ, ДАЖЕ ЕСЛИ SYMANTEC БЫЛ ПОСТАВЛЕН В ЗНАЕСТНОСТЬ О ВОЗМОЖНОСТИ ПОДОБНОГО РОДА УЩЕРБА.

НИ ПРИ КАКИХ ОБСТОЯТЕЛЬСТВАХ ОТВЕТСТВЕННОСТЬ SYMANTEC НЕ ПРЕВЫШАЕТ СТОИМОСТИ ПРОГРАММЫ.

ОГРАНИЧЕННЫЕ ПРАВА ПРАВИТЕЛЬСТВА США

ИСТОРИЯ ОГРАНИЧЕННЫХ ПРАВ. ИСПОЛЬЗОВАНИЕ, КОПИРОВАНИЕ И РАСПРОСТРАНЕНИЕ ПРОГРАММЫ ПРАВИТЕЛЬСТВОМ США ОГРАНИЧИВАЕТСЯ В СООТВЕТСТВИИ С ПОДРАЗДЕЛОМ (C) (1) (II) ЗАКОНА RIGHTS IN TECHNICAL DATA AND COMPUTER SOFTWARE СТАТЬЯ DFARS 252.227-7013 ИЛИ ПОДРАЗДЕЛ (C) (1) (I) ЗАКОНА COMMERCIAL COMPUTER SOFTWARE-RESTRICTED RIGHTS СТАТЬЯ 48 CFR 52.227-19 ДЕЙСТВИЕ КОТОРЫХ РАСПРОСТРАНЯЕТСЯ НА SYMANTEC CORPORATION, 10201 TORRE AVENUE, CUPERTINO, CA 95014.

ОБЩЕЕ ПОЛОЖЕНИЕ

ДАННОЕ СОГЛАШЕНИЕ СОСТАВЛЕНО В СООТВЕТСТВИИ С ДЕЙСТВУЮЩИМ ЗАКОНОДАТЕЛЬСТВОМ. ЛЮБЫЕ ИЗМЕНЕНИЯ И ДОПОЛНЕНИЯ К СОГЛАШЕНИЮ ЕСЛИ ТАКОВЫЕ ИМЕЮТСЯ, ДОЛЖНЫ БЫТЬ ОФОРМЛЕНЫ В ВИДЕ ОТДЕЛЬНОГО ДОКУМЕНТА И ПОДПИСАНЫ МЕЖДУ ВАМИ И SYMANTEC. В СЛУЧАЕ ВОЗНИКНОВЕНИЯ ЛЮБЫХ ВОПРОСОВ ПО ДАННОМУ СОГЛАШЕНИЮ ВЫ МОЖЕТЕ СВЯЗАТЬСЯ С SYMANTEC ПО СЛЕДУЮЩЕМУ АДРЕСУ: SYMANTEC CUSTOMER SALES AND SERVICE, SYMANTEC EUROPE, KANAALPARK 145, POSTBUS 1143, 2321 JV LEIDEN, THE NETHERLANDS. ТЕЛЕФОН: +31 71 353 111, ФАКС: +31 71 353 150.

Руководство пользователя

SYMANTEC

TM

NORTON

AntiVirus™

Версия 4.0

07-30-90201-RU
MIP001

Norton AntiVirus™ для Windows® NT

Описанное в этой книге программное обеспечение является объектом лицензионного соглашения и может быть использовано только в соответствии с данным соглашением.

Авторское право

Copyright © 1990-1997 Symantec Corporation.

Все права защищены.

Любая техническая документация, предоставляемая Symantec Corporation, является собственностью Symantec Corporation и авторским правом на нее обладает Symantec Corporation.

ОТКАЗ ОТ ГАРАНТИЙ. Настоящая документация предлагается без каких-либо гарантий со стороны Symantec Corporation в отношении ее точности или полезности. Ответственность за использование документации и содержащейся в ней информации возлагается на пользователя. В документации могут быть технические неточности и опечатки. Symantec оставляет за собой право вносить в нее изменения без предварительного уведомления.

Копирование любой части этого документа допускается только с письменного разрешения Symantec Corporation, Peter Norton Group, 10201 Torre Avenue, Cupertino, CA 95014.

Торговые марки

Symantec, Norton AntiVirus, Symantec AntiVirus for Macintosh и Norton Utilities являются зарегистрированными торговыми марками Symantec Corporation.

Windows является зарегистрированной торговой маркой, а Windows NT — торговой маркой Microsoft Corporation. NetWare является торговой маркой Novell Corporation. Другие упомянутые в этом руководстве названия продуктов могут быть торговыми или зарегистрированными торговыми марками соответствующих компаний, что настоящим удостоверяется.

Напечатано в Ирландии.

10 9 8 7 6 5 4 3 2 1

С О Д Е Р Ж А Н И Е

Установка

Что Norton AntiVirus делает автоматически:	ix
Что необходимо делать вам	ix
Установка Norton AntiVirus для Windows NT	x
Требования для установки	x
Процедура установки	x
Вопросы, возникающие при установке	xi
Удаление Norton AntiVirus	xii

Глава 1

Norton AntiVirus

Защищен ли мой компьютер от вирусов?	1
Что такое компьютерный вирус?	2
Жизненный цикл вируса	2
Как Norton AntiVirus борется с вирусами	4
Ручной поиск	4
Запланированный поиск	4
Автозащита	5
Файлы описаний вирусов	5
Как Norton AntiVirus сигнализирует о вирусах	5
Риск заражения вирусами в системе Windows NT	7
Загрузочные вирусы	7
Программные вирусы	8
Макровирусы	8
Рекомендации по безопасности	9
MS-DOS и Windows NT	11

Глава 2

Работа с Norton AntiVirus

Как избежать вирусов	13
Запуск и выход из Norton AntiVirus	14
Получение справочной информации	15
Поиск вирусов	17
Обход проверки загрузочных записей	19
Планирование поиска вирусов	20
Включение и отключение автозащиты	23
Просмотр журнала работ	25
Защита от вирусов из Internet	26
Netscape и Norton AntiVirus	27
Прочие браузеры Internet и Norton AntiVirus	27

Глава 3	Уничтожение вирусов	
	Уничтожение вирусов, обнаруженных при поиске	29
	Командные кнопки	32
	Уничтожение вирусов, обнаруженных автозащитой	33
	Что делать, если исправление неудачно	34
	Если невозможно исправить файл приложения	35
	Если невозможно исправить системный файл	35
	Если невозможно исправить загрузочную запись	35
	Удаление вирусов из сжатых файлов	35
	Устранение проблем общего характера	36
Глава 4	Как защититься от новых вирусов	
	Автоматическое обновление описаний вирусов	37
	Планирование автоматического обновления	38
	Ручное обновление описаний вирусов	39
	Где можно найти файлы описания вирусов	40
	Установка новых файлов описания вирусов	42
	Просмотр списка вирусов	43
Глава 5	Настройка поиска вирусов	
	Настройка ручного поиска	45
	Замечания по поиску вирусов в сети	50
	Выбор проверяемых файлов	50
	Установка расширений программных файлов	51
	Работа с исключениями	53
	Настройка сигналов	55
	Отправка сетевых сигналов	56
	Настройка журнала работ	57
	Установка параметров резервирования	58
	Настройка автозащиты	59
	Автозащита программных файлов	60
	Автозащита гибких дисков	62
	Установка паролей	62
	Приложение А О компьютерных вирусах	
	Что такое компьютерные вирусы	66
	Объекты заражения	68
	Программные вирусы	68
	Загрузочные вирусы	69
	Макровирусы	70
	Технологии вирусов	71
	Обновление вирусной базы	73

Приложение Б Аварийное восстановление

Горячая линия	75
Если невозможно запустить компьютер	75

Приложение В Ключи командной строки

Словарь терминов

Предметный указатель

У С Т А Н О В К А

Norton AntiVirus — это самая надежная и универсальная из всех существующих программ, предназначенных для поиска и уничтожения вирусов независимо от источника заражения. Norton AntiVirus защищает компьютер от проникновения вирусов с жестких и гибких дисков, по локальной сети и через Internet.

Что Norton AntiVirus делает автоматически:

- Уничтожает вирусы и исправляет зараженные файлы.
- Защищает компьютер от вирусов при его запуске.
- Осуществляет поиск вирусов при использовании:
 - Программного обеспечения на компьютере.
 - Дискет.
 - Скопированных или созданных файлов документов. (Например, для поиска новейшего типа макровирусов, которые распространяются через макросы Microsoft Word и Excel.)
- Контролирует работу компьютера с целью выявления подозрительных симптомов, которые могут свидетельствовать о присутствии неизвестного вируса.
- Запускает плановый поиск вирусов один раз в неделю.
- Защищает компьютер от вирусов, передающихся через Internet.

Что необходимо делать вам

Инструкции по обновлению на *страница 37.*

- Ежемесячно получать из Symantec обновленные описания вирусов, которые требуются этой программе для обеспечения полной защиты. Новые файлы описания вирусов можно получить по электронным каналам (например, через Internet) или по почте.

ЗАЧЕМ ЭТО НУЖНО? Новые компьютерные вирусы появляются чуть не каждый день. Поэтому необходимо регулярно обновлять файлы описания вирусов, т. к. в них содержится самая полная информация о существующих вирусах. В противном случае, вы останетесь беззащитны перед вирусами, появившимися после приобретения вами данного программного продукта.

Установка Norton AntiVirus для Windows NT

Если при установке Norton AntiVirus в точности следовать всем сообщениям на экране, то сразу же после перезагрузки компьютера вам будет обеспечена полная защита от вирусов. Она включает следующее:

- Автоматическая загрузка Norton AntiVirus при запуске компьютера
- Ежедневный автоматический поиск вирусов на дисках
- Проверка на вирусы файлов, принимаемых из Internet

Требования для установки

Чтобы установить Norton AntiVirus для Windows NT, вам необходимо иметь права администратора. Минимальные требования к компьютеру:

- 16 Мб памяти (рекомендуется 32 Мб или более)
- Microsoft Windows NT Workstation версии 3.51 или 4.0
- 16 Мб свободного места на диске

Процедура установки

Для получения максимальной защиты нужно просто нажимать “Далее” во всех экранах установки, принимая таким образом все параметры по умолчанию.

Как начать установку на Windows NT Workstation версии 4.0:

- 1 Необходимо выполнить одно из следующих действий:
 - При установке с компакт-диска, вставить диск в устройство CD-ROM. Установка Norton AntiVirus начнется автоматически.
 - При установке с дискет, вставить в дисковод A: “Диск 1 Norton AntiVirus”, нажать кнопку “Пуск” на панели задач Windows, выбрать команду “Выполнить”, ввести в текстовом поле A: SETUP и затем нажать ОК.
- 2 Следовать инструкциям на экране. *Если что-то будет непонятно, см. “Вопросы, возникающие при установке” на странице xi.*

Как начать установку на Windows NT Workstaion версии 3.51:

- 1 Выполнить одно из следующих действий:
 - Компакт-диск: вставить его в устройство CD-ROM, в меню “Файл” выбрать команду “Выполнить”, в текстовом поле ввести d : SETUP (вместо d : может быть другая буква, соответствующая вашему устройству CD-ROM), затем нажать ОК.
 - Дискеты: вставить “Диск 1 Norton AntiVirus” в дисковод A:, в меню “Файл” выбрать команду “Выполнить”, в текстовом поле ввести A : SETUP и нажать ОК.
- 2 Следовать инструкциям на экране. *Если что-то будет непонятно, см. следующий раздел.*

Вопросы, возникающие при установке

Norton AntiVirus помогает вам правильно выполнить установку, выдавая на экран подсказки и выделяя рекомендуемые действия. Вам необходимо выбрать следующее:

Что предлагается	Что от вас требуется	Почему?
Выбрать папку для Norton AntiVirus.	Принять папку: C:\Program Files\Norton AntiVirus	Почему бы нет? Если очень нужно, можете указать другую папку.
Запланировать раз в неделю автоматическую проверку жестких дисков на вирусы.	Не отключать этот параметр.	Еженедельная проверка на вирусы бывает очень полезна.
Автоматически запускать Автозащиту.	Не отключать этот параметр.	Автозащита непрерывно следит за попытками вирусов проникнуть на ваш компьютер.
Выполнять проверку на вирусы при запуске компьютера.	Не отключать этот параметр.	Это гарантирует чистоту системных файлов при каждом запуске ПК.
Norton AntiVirus обнаружил присутствие браузера Netscape. Установить компоненты plug-in?	Выбрать “Да”.	Это позволит программе Norton AntiVirus проверять на вирусы файлы, принимаемые с помощью браузера Netscape.
Выполнить LiveUpdate после установки.	Не отключать эту функцию, если у вас есть модем или соединение Internet.	LiveUpdate подключается к серверу Symantec и копирует с него обновленные версии файлов описаний вирусов.

Удаление Norton AntiVirus

Для удаления установленной программы Norton AntiVirus следует:

- Windows NT 4.0: на панели задач Windows нажать “Пуск”, выбрать “Программы”, затем “Norton AntiVirus” и нажать “Удаление Norton AntiVirus”.
- Windows NT 3.51: в программной группе Norton AntiVirus двойным нажатием выбрать “Удаление Norton AntiVirus”.

Norton AntiVirus

Norton AntiVirus для Windows NT — самая надежная и универсальная из всех существующих программ, предназначенных для поиска и уничтожения вирусов независимо от источника заражения. Norton AntiVirus защищает компьютер от проникновения вирусов с жестких и гибких дисков, по локальной сети и через Internet.

Защищен ли мой компьютер от вирусов?

Если Norton AntiVirus установлен со стандартными параметрами, то защита вашему компьютеру уже обеспечена. Компьютер, прежде всего, проверяется на наличие вирусов в процессе установки. А после нее функция автозащиты непрерывно следит за вирусами в процессе работы программ. Обнаружив вирус, Norton AntiVirus последовательно проведет вас через все этапы его устранения.

Если вы не большой знаток компьютера, не волнуйтесь! Стандартные параметры Norton AntiVirus обеспечивают баланс производительности и защиты, и менять в настройке программы ничего не потребуется. Просто установите Norton AntiVirus и получите надежный щит от компьютерных вирусов.

Norton AntiVirus умеет автоматически:

- проверять на вирусы системные файлы и загрузочные записи при запуске системы
- искать вирусы в выполняемых программах
- проверять компьютер на вирусы один раз в неделю
- контролировать работу компьютера при подозрении на вирус
- регистрировать все обнаруженные вирусы

Norton AntiVirus также позволяет:

- проверить на вирусы отдельные файлы, папки или целые диски
- запланировать регулярную проверку в назначенное время.
- в любой момент или в запланированное время обновить файлы описаний вирусов.
- настроить уровень защиты Norton AntiVirus соответственно степени риска заражения в существующей рабочей среде

Что такое компьютерный вирус?

Компьютерный вирус — это программа, созданная программистом со злыми намерениями. Программа-вирус разрабатывается так, чтобы при загрузке в память она внедрялась в другую программу. Затем, при каждом запуске зараженной программы внедренная программа-вирус активизируется и проникает в другие программы. Например, компьютерный вирус, проникая в компьютер с дискеты, взятой у кого-нибудь на время, заражает другие программы на вашей машине. Можно сказать, что компьютерный вирус, подобно биологическому, живет для того, чтобы размножаться.

Ряд вирусов, кроме размножения, имеют своей целью преднамеренное разрушение данных путем повреждения программ, удаления файлов и даже форматирования всего жесткого диска. К счастью, большинство вирусов не наносят серьезного ущерба: они просто размножаются или выводят сообщения.

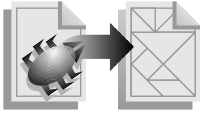
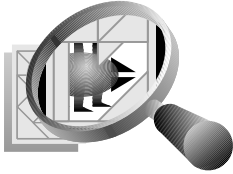

Вирусы могут только заражать файлы и портить данные. Они не способны вредить аппаратным средствам, например, клавиатуре или монитору. Хотя при заражении вирусом в работе этих устройств и возможны сбои — искажения на экране или потеря вводимых с клавиатуры символов, — но фактически вирус поражает не само устройство, а управляющую им программу. Подобным же образом не получают физических повреждений и диски, а лишь разрушается то, что на них хранилось.

Жизненный цикл вируса

Жизненный цикл компьютерного вируса состоит из трех этапов: заражения, обнаружения и уничтожения. На стадии заражения вирус внедряется в хранящиеся на компьютере файлы. На стадии происходит его распознавание и изоляция. И, наконец, на стадии уничтожения вирус стирается из системы. До тех пор, пока вирус не уничтожен, он продолжает поражать файлы и, возможно, разрушать данные на дисках. Таблица 1–1, *“Этапы жизни вируса,”* на странице 3 подробнее описывает каждый этап.

Norton AntiVirus является наиболее эффективным из всех существующих средств, служащих для прерывания данного цикла. Имеющаяся в этой программе функция автозащиты позволяет остановить вирусы на подходе к вашим файлам.

Таблица 1: Этапы жизни вируса

Заражение	Источник	Дискеты сомнительного происхождения, принесенные из дома или из школы, взятые у друзей. Программы, скопированные с BBS и т. п. Программы, купленные у малоизвестных дилеров. Бесплатно распространяемые программы. Нелицензионные копии программ. Предварительно отформатированные дискеты.
	Заражение	Запуск ПК с зараженного диска. Перезагрузка с забытой в дисковом диске зараженной дискеты. Запуск зараженной программы.
	Распространение	Совместное использование диска или зараженной программы. Подключение к сети.
Обнаружение	Подозрение	Странное поведение системы. Потеря файлов или ненормальная работа программ.
	Поиск	Обнаружение вирусов специальными антивирусными программами.
Восстановление	Удаление	Повторная установка программы с оригинальных дисков. Исправление файлов с помощью антивирусной программы. Восстановление данных с незараженной копии.
	Дальнейшие действия	Повторная проверка всех файлов с целью выявить источник заражения. Проверка всех дисков для обнаружения источника заражения. Уничтожение резервных копий, которые могут быть зараженными. Усиление антивирусной защиты
Профилактика	Используйте Norton AntiVirus для профилактики вирусов.	
		

Как Norton AntiVirus борется с вирусами

Известные вирусы — это те, которые удалось идентифицировать. Инженеры Symantec непрерывно собирают информацию о всех случаях заражения компьютеров для того, чтобы выявлять новые вирусы. Сразу после идентификации вируса его код (сигнатура) заносится в файл описаний вирусов. В процессе проверки дисков и файлов Norton AntiVirus ищет вирусы по этим сигнатурам. Если будет обнаружен файл, зараженный одним из таких вирусов, Norton AntiVirus сможет этот вирус автоматически уничтожить.

При обнаружении каждого нового вируса его сигнатура заносится в файл описаний вирусов. Поэтому этот файл необходимо регулярно обновлять (Symantec выпускает его новые версии ежемесячно). Имея самую последнюю версию этого файла, Norton AntiVirus будет располагать информацией, необходимой для обнаружения всех известных вирусов. Подробные указания по обновлению файла описаний вирусов можно найти в главе 4, *“Как защититься от новых вирусов”*.

Ключевой технологией Norton AntiVirus является функция поиска, исследующая программные файлы с целью выявления сигнатур известных вирусов. Поиск вирусных сигнатур осуществляется в ручном, запланированном или в автоматическом режиме (при каждой загрузке компьютера). Поиск вирусов выполняется также функцией автозащиты при запуске любого файла.

Ручной поиск

Запустить поиск вирусов вручную можно кнопкой “Поиск” в главном окне Norton AntiVirus. Эта операция позволяет обнаружить известные вирусы в конкретных файлах, папках или на дисках компьютера. Подробные сведения о проверке файлов, папок и дисков на вирусы приводятся в главе *“Поиск вирусов” на странице 17*.

Запланированный поиск

Запланированный поиск — это ручной поиск, запускаемый автоматически в заданное время. Эта операция дополняет другие автоматические функции защиты для гарантии отсутствия вирусов в компьютере. Norton AntiVirus по умолчанию планирует еженедельный автоматический поиск (в пятницу вечером). Инструкции по планированию поиска приводятся в разделе *“Планирование поиска вирусов” на странице 20*.

Автозащита

Автозащита — это функция Norton AntiVirus, выполняющая автоматическую проверку на вирусы программных файлов, документов и шаблонов при каждом обращении к ним. Дополнительным важным свойством автозащиты является то, что она реагирует на различные вирусоподобные действия (например, попытки форматирования жесткого диска) и предупреждает о них, чтобы пользователь мог вмешаться. В функции автозащиты применена новая технология поиска вирусов: так называемый “вирусный датчик”, сигнализирующий о попытках вирусов внедриться в программные файлы.

По умолчанию автозащита включается сразу после установки NAV и действует до тех пор, пока не будет отключена пользователем. Инструкции по настройке автозащиты и включении вирусного датчика приводятся в разделе *“Настройка автозащиты” на странице 59.*

Файлы описаний вирусов

Файлы описаний вирусов содержат информацию, которую Norton AntiVirus использует для обнаружения известных вирусов. Norton AntiVirus незамедлительно, если владеет самой последней информацией. При появлении нового вируса его сигнатура добавляется в файл описаний вирусов. Поэтому эти файлы следует регулярно обновлять.

Фирма Symantec ежемесячно и бесплатно распространяет новые файлы описаний вирусов. При наличии модема и выхода в Internet программа Norton AntiVirus может обновлять эти файлы автоматически. Необходимые инструкции приводятся в разделе *“Автоматическое обновление описаний вирусов” на странице 37.*

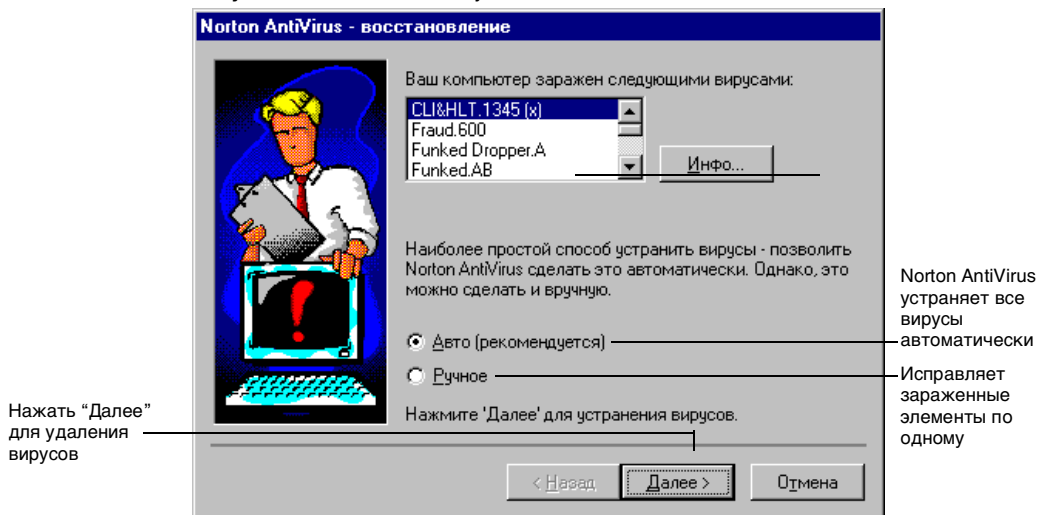
Как Norton AntiVirus сигнализирует о вирусах

У программы Norton AntiVirus имеется в распоряжении два способа оповещения о возможном заражении вирусами в зависимости от того, каким образом был обнаружен вирус:

- Вирус обнаружен во время ручного или запланированного поиска (см. рис. 1-1)
- Вирус обнаружен автозащитой (рис. 1-2)

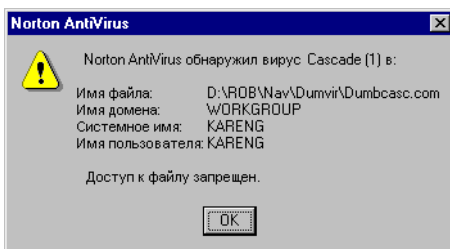
Если вирус обнаружен во время ручного или запланированного поиска, то лечащий модуль Norton AntiVirus позволяет устранить вирус автоматически (рис. 1-1). Инструкции по работе с лечащим модулем даны в разделе *“Уничтожение вирусов, обнаруженных при поиске” на странице 29.*

Рисунок 1-1 Лечащий модуль Norton AntiVirus



Автозащита Norton AntiVirus немедленно выводит диалоговое окно "Сигнал о вирусе" при любом событии, связанном с вирусами. (на рис. 1-2 показан пример сигнала автозащиты.) В этом окне имеются кнопки, позволяющие уничтожить вирус. Инструкции по использованию лечащего модуля приводятся в разделе *"Настройка автозащиты"* на [странице 59](#).

Рисунок 1-2 Сигнал автозащиты



Риск заражения вирусами в системе Windows NT

Компьютерные вирусы делятся на типы по методу и объекту заражения:

- **Загрузочные вирусы.** Некоторые вирусы способны заражать диски, внедряясь в программы, хранящиеся в особых областях дисков, которые называются загрузочными и главными загрузочными записями. Эти программы необходимы для начальной загрузки компьютера.
- **Программные вирусы.** Они заражают исполнимые файлы, например, текстовые процессоры, электронные таблицы, компьютерные игры или программы операционной системы.
- **Макровирусы.** Многие программы, например, текстовые процессоры и электронные таблицы, содержат средства написания макросов для автоматического повторения последовательности операций. Нередко макросы хранятся внутри файлов данных. Вот такие файлы и подвергаются нападению макровирусов. Наиболее часто это происходит с документами и шаблонами Microsoft Word и электронными таблицами Microsoft Excel.

Загрузочные вирусы

Загрузочные вирусы представляют собой особую группу риска в среде Windows NT. При запуске компьютера выполняется программа загрузочной записи (программа самозагрузки), которая считывает дополнительную информацию из загрузочных записей, необходимую для загрузки операционной системы. Загрузочный вирус активизируется при запуске системы еще до загрузки Windows NT. В сущности, загрузочные вирусы являются независимыми от типа операционной системы.

Загрузочные записи имеются на всех жестких и гибких дисках, независимо от наличия на них файлов операционной системы или нет. Загрузочный вирус заражает не только диски с операционной системой, но и диски, содержащие только данные. Обычно загрузочный вирус попадает в компьютер при перезагрузке с зараженной дискеты, которую случайно оставили в дисковом. Даже если эта дискета и не является системной (загрузочной), вирус сможет активизироваться и начнет распространяться.

Windows NT управляет памятью не так, как MS-DOS. Если Windows NT загрузилась, несмотря на наличие вируса, то в памяти вирус становится недееспособным. Компьютер, тем не менее, заражен, хотя вирус и не проявляет своих обычных симптомов и не распространяется во время запуска системы. Даже если Windows NT загружается нормально, компьютер все равно подвергается риску при каждом запуске системы. Вирус может активизироваться в самом начале запуска ПК и запортить данные на диске. Нередки случаи, когда после проникновения вируса система сразу перестает

загружаться. А если загрузить MS-DOS в системе с множественной загрузкой, то вирус становится полностью дееспособным, угрожая всем дискам, включая гибкие.

Программные вирусы

В среде Windows NT могут обитать все программные вирусы MS-DOS, которые заражают исполнимые файлы. Программных вирусов, созданных специально для Windows NT, пока еще не обнаружено.

Под Windows NT программы для DOS запускаются в области памяти DOS. Находясь в памяти, зараженная DOS-программа может распространяться на другие программы и мешать нормальной работе. Как правило, программные вирусы после завершения работы зараженной программы остаются активными в памяти компьютера до окончания сеанса DOS.

Если у вас открыто одновременно несколько сеансов DOS, то память может быть заражена в каждом из них. Если один сеанс закрывается, вирус остается в памяти остальных. При обнаружении вируса закройте все сеансы DOS и повторите операцию поиска.

Примечание. При поиске вирусов в программах Norton AntiVirus проверяет также документы Microsoft Word и таблицы Excel. Хотя эти файлы и не являются программными, они могут быть заражены новым классом вирусов под названием “макровирусы”.

Макровирусы

Современные приложения обладают развитыми системами макрокоманд. Внутри текстового редактора или электронной таблицы можно написать целую макропрограмму, которая прикрепляется непосредственно к файлу документа или электронной таблицы. Возможность переносить вместе с файлом данных один или несколько макросов чрезвычайно привлекательна. Но она также привлекательна и для создателей макровирусов.

Типичный процесс распространения макровируса начинается с того, что зараженный документ или электронная таблица открывается в соответствующем приложении, и при этом также загружаются хранящиеся в файле макросы. После загрузки и выполнения макровирус ждет, когда начнется редактирование файла. Он внедряет свою копию в новый документ в виде макропрограммы, затем позволяет приложению нормально сохранить документ. При открытии этого нового файла на другом компьютере вся процедура повторится: вирус снова загрузится, будет выполнен приложением и найдет очередной объект для заражения.

Можно сказать, что приложение служит для макровируса своего рода операционной системой. Любой макровирус может, в принципе, поселиться на любой платформе, где используется приложение. Например, макровирус для Microsoft Word одинаково легко заразит документы в среде Windows 3.x, Windows 95, Window NT и Macintosh.

Рекомендации по безопасности

Так как Windows NT является гибкой системой, это создает особые проблемы в отношении защиты от вирусов. В файловой системе NT (NTFS) каждому пользователю или группе можно предоставить различные права для доступа на уровне файлов, папок или объектов (например, загрузочных записей). Не каждый пользователь имеет возможность проверить на вирусы все элементы системы.

Компьютер с Windows NT может использоваться для различных целей:

- Автономный компьютер с одним пользователем
- Сетевой компьютер с одним пользователем
- Компьютер коллективного доступа со входом в систему под разными паролями
- Сервер

Для проверки загрузочных записей в любой конфигурации требуются права администратора. Что касается автономного компьютера, то его зарегистрированный пользователь, как правило, обладает такими правами. При всех других конфигурациях данную проверку на вирусы должен выполнять системный администратор.

Если говорить о компьютерах коллективного пользования, то в этом случае доступ к файлам ограничен — пользователю доступны только его собственные файлы. Каждый пользователь должен серьезно относиться к защите своих файлов от вирусов. Одному из пользователей можно выделить права администратора для проверки на вирусы системных файлов и загрузочных записей.

В любой сети риск заражения чрезвычайно высок, так как вирусы могут распространиться очень быстро. Поиск вирусов на серверах должен осуществлять администратор. Следует отметить, что проверять файлы можно на любом диске, с которому имеется доступ.

В следующих таблицах указаны права доступа, необходимые для использования Norton AntiVirus. Если вы постоянно наталкиваетесь на сообщение об отказе в доступе, проверьте у себя наличие прав, необходимых для работы с загрузочными записями, папками или файлами.

Примечание. Для внесения изменений в программу NT Scheduler, запускающую плановый поиск вирусов, а также для включения и выключения служб Norton AntiVirus Agent и Auto-Protect, являющихся элементами автозащиты, требуются права администратора.

Таблица 2: Загрузочные записи — права доступа

Права	Поиск	Исправление	Удаление
Права администратора	Да	Да	Да

Таблица 3: Папки — права доступа

Права в папках (файлах)	Поиск	Исправление	Удаление
Полный контроль	Да	Да	Да
Изменение (RWXD) (RWXD)	Да	Да	Да
Добавление и чтение (RWX) (RX)	Да	Нет	Нет
Чтение (RX) (RX)	Да	Нет	Нет
Добавление (WX) (не указано)	Нет	Нет	Нет
Просмотр списка (RX) (не указано)	Нет	Нет	Нет
Нет доступа	Нет	Нет	Нет

Таблица 4: Файлы — права доступа

Полномочия для файлов	Поиск/Обнаружение	Исправление	Удаление
Полный контроль (RWD)	Да	Да	Да
Изменение (RW)	Да	Да	Нет
Чтение (R)	Да	Нет	Нет

MS-DOS и Windows NT

Конфигурация большинства компьютеров позволяет загружать либо Windows NT, либо MS-DOS. Естественно, что в этом случае риск заражения значительно возрастает. Так, вирусы, сдерживаемые в Windows NT ограничениями доступа к загрузочным записям, легко распространяются в среде MS-DOS. Кроме того, загрузочный вирус, проникший в систему через DOS, может помешать последующей загрузке Windows NT.

Чтобы усилить средства защиты Norton AntiVirus в среде Windows NT, фирма Symantec бесплатно предлагает программу для поиска вирусов в MS-DOS, которая может оказаться очень полезной в аварийных ситуациях, например, когда вирус нарушил загрузку Windows NT. Поисковый модуль Norton AntiVirus для DOS (NAVSCAN.EXE) можно получить по различным электронным каналам, описанным в разделе *“Где можно найти файлы описания вирусов” на странице 40*. Сопроводительный файл README.TXT содержит подробные инструкции по работе с этой программой.

Вирус активизируется только при запуске (или попытке запуска) компьютера с дискеты, зараженной загрузочным вирусом, или при выполнении зараженной программы или открытии документа, шаблона или электронной таблицы. Однако после установки Norton AntiVirus компьютер получает надежную защиту от вирусов.

Как избежать вирусов

Приведенные ниже профилактические меры снизят до минимума риск заражения вирусами:

- Держать автозащиту всегда включенной. При установке Norton AntiVirus автозащита включается по умолчанию. Подробную информацию можно найти в разделе *“Настройка автозащиты”* на *странице 59*.
- Выполнять ручной поиск вирусов (или в запланированном автоматическом режиме) на жестких дисках не реже одного раза в неделю. Эта мера дополняет автозащиту и гарантирует отсутствие вирусов на вашем ПК. При установке Norton AntiVirus с параметрами по умолчанию задается еженедельный автоматический поиск. См *“Поиск вирусов”* на *странице 17* и *“Планирование поиска вирусов”* на *странице 20*.
- Проверять все дискеты перед их использованием. См. *“Поиск вирусов”* на *странице 17*.
- Ежемесячно обновлять файлы описания вирусов. См. *“Автоматическое обновление описаний вирусов”* на *странице 37*.
- Периодически делать резервные копии всего жесткого диска.
- Пользоваться легально приобретенными программами и хранить их резервные копии, защищенные от записи.

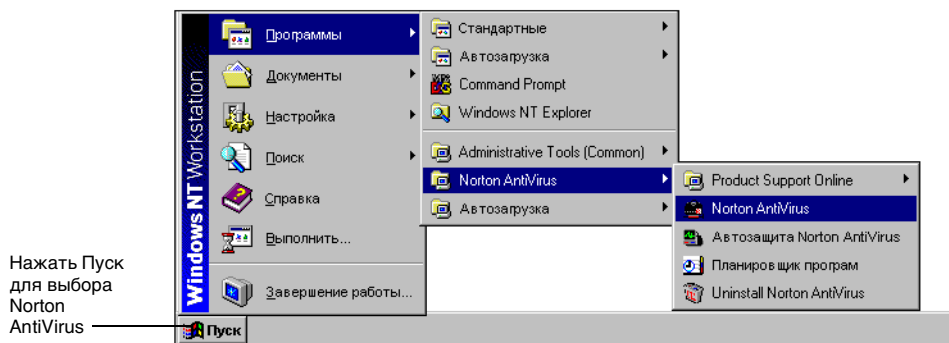
Запуск и выход из Norton AntiVirus

В главном окне Norton AntiVirus имеются средства, позволяющие произвести поиск вирусов вручную, запланировать автоматический поиск, проверить и изменить параметры настройки и обновить файлы описания вирусов. Автозащита работает постоянно (о функции автозащиты см. *“Включение и отключение автозащиты” на странице 23*).

Как запустить Norton AntiVirus:

- В Windows NT 4.0 — на панели задач нажать “Пуск”, выбрать “Программы”, затем группу “Norton AntiVirus”, а в ней пункт “Norton AntiVirus” (рис. 2-1). На экране появится главное окно программы (см. рис. 2-2).
- В Windows NT 3.51 — выбрать “Norton AntiVirus” в группе антивирусных средств.

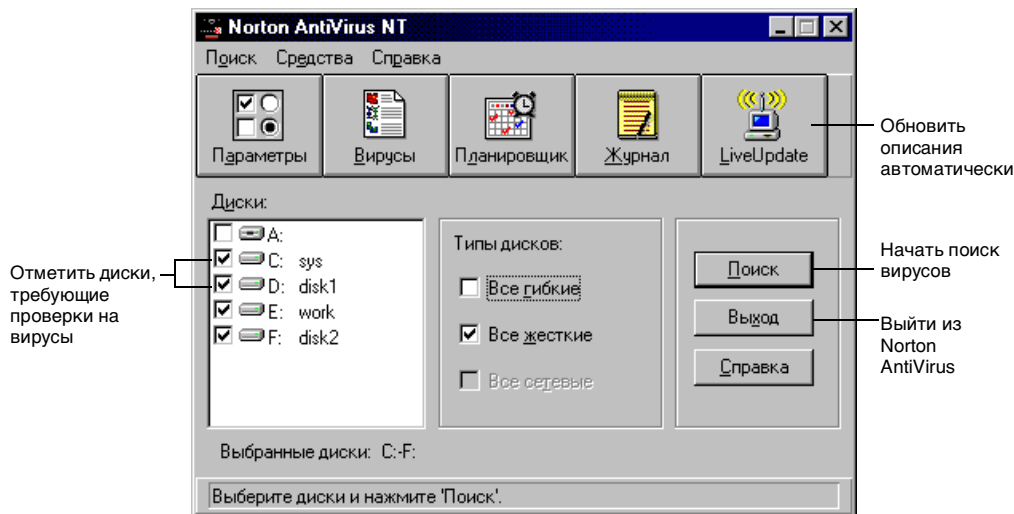
Рисунок 2-1 Запуск Norton AntiVirus



Как выйти из Norton AntiVirus:

- Нажать “Выход” в главном окне Norton AntiVirus.

Рисунок 2-2 Главное окно Norton AntiVirus



Получение справочной информации

По всем функциям Norton AntiVirus предоставляется интерактивная справочная информация. Для получения сведений о принципах работы программы, ее терминологии и всех процедурах можно выполнить любое из следующих действий:

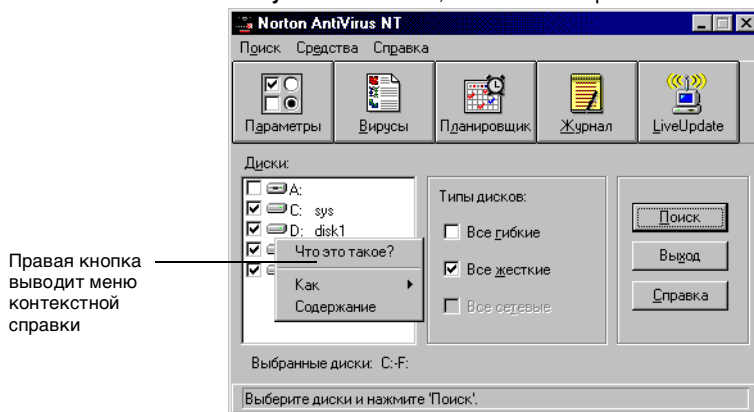
- Нажать правой кнопкой мыши на интересующем элементе диалогового окна.
- Выбрать нужный пункт в меню “Справка”.
- Нажать кнопку “Справка” в диалоговом окне.

Справочная система включает в себя оглавление, предметный указатель и глоссарий. В окне справки можно найти и распечатать интересующие вас разделы, вставить примечания и закладки. Интерфейс Windows NT обеспечивает быстрый доступ к контекстной справочной информации по любой функции Norton AntiVirus.

Как получить контекстную справку:

- 1 Установить курсор на интересующем элементе окна и нажать правую кнопку мыши. Появится контекстное меню справки.

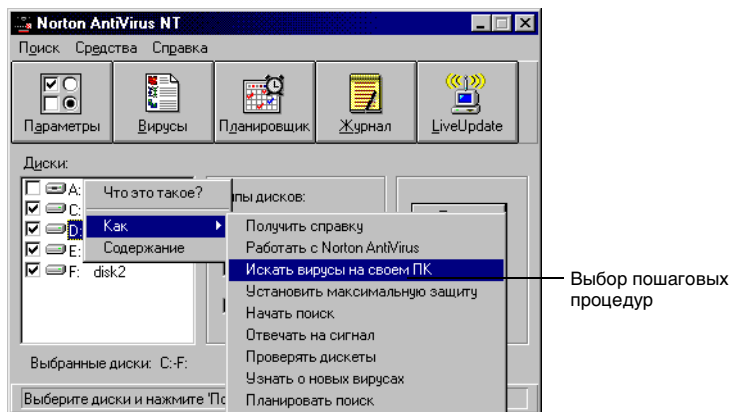
Рисунок 2-3 Меню, вызываемое правой кнопкой мыши



- 2 В контекстном меню выбрать нужный пункт:

- *Что это такое?* — для получения краткой информации об элементе окна.
- *КАК...* — для вызова меню справки по процедурам, имеющим отношение к данному элементу или окну (рис. 2-4).
- *СТОЛ СПРАВОК* — для просмотра перечня разделов справочной системы.

Рисунок 2-4 Справочное меню Как...



Контекстное меню справки по элементам диалогового окна можно вызвать также с помощью знака вопроса, присутствующего в строке заголовка любого диалогового окна.

Как получить справку по элементам окна:

- 1 Нажать на вопросительный знак в строке заголовка окна.
Рядом с указателем мыши появится вопросительный знак.
- 2 Нажать на интересующий элемент диалогового окна.
На экране появится его краткое описание.

Поиск вирусов

Поиск вирусов можно выполнить в любое время. Общепринятая практика заключается в проверке жестких дисков не реже одного раза в неделю вручную или в автоматическом запланированном режиме. Необходимо также проверять любые дискеты перед их использованием и все программы, полученные с BBS и других электронных служб.

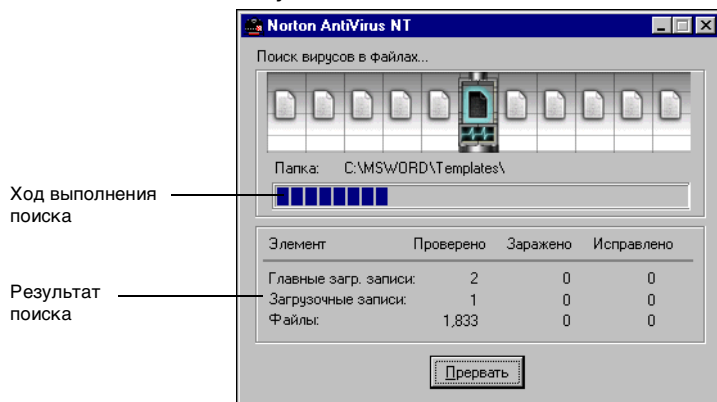
По окончании операции поиска Norton AntiVirus сообщает о результатах. Если обнаружены какие-либо проблемы, появляется экран лечащего модуля N AV, предлагающий выполнить восстановительные действия (см. *“Уничтожение вирусов, обнаруженных при поиске” на странице 29*). После устранения проблемы, а также если ничего серьезного не обнаружено, выдается сводка с подробной информацией о результатах поиска.

Совет: Стандартные значения параметров Norton AntiVirus поддерживают баланс максимальной защиты с оптимальным быстродействием во время поиска. В большинстве случаев изменение параметров не требуется. Однако при желании можно изменить, например, такие параметры программы, как что именно она должна проверять и как поступить при обнаружении вируса. См. *“Настройка ручного поиска” на странице 45*.

Как проверить один или несколько дисков:

- 1 Запустить Norton AntiVirus.
- 2 В главном окне программы отметить нужные устройства в списке “Диски” или целую группу дисков, выбрав соответствующий флажок в окне группы “Типы дисков” (см. рис. 2-2).
- 3 Нажать кнопку “Поиск”.
В диалоговом окне будет отражаться ход операции поиска.

Рисунок 2-5 Ход поиска



Как проверить на вирусы отдельный файл:

- 1 Выбрать “Файл...” из меню “Поиск” в главном окне Norton AntiVirus.
- 2 Выбрать файл, требующий проверки на вирусы, и нажать “Открыть”.

Как проверить на вирусы отдельную папку:

- 1 Выбрать “Папки...” из меню “Поиск” в главном окне Norton AntiVirus.
- 2 Выбрать нужную папку.
- 3 Нажать кнопку “Поиск”.

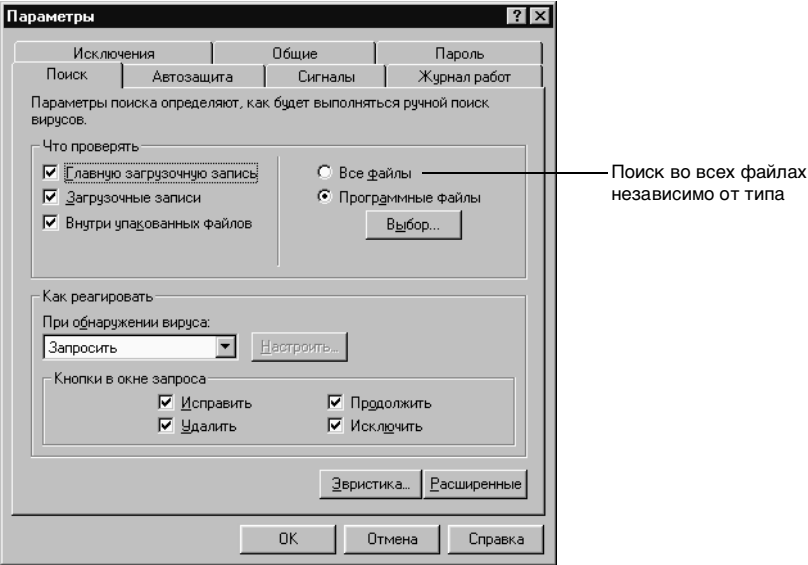
Norton Antivirus по умолчанию проверяет программы файлы, документы и шаблоны, так как эти типы файлов наиболее подвержены воздействию вирусов. Однако в некоторых случаях, например, после явной вирусной атаки, рекомендуется проверить все файлы, чтобы убедиться в полном отсутствии зараженных файлов на компьютере.

Как проверить на вирусы все файлы, независимо от типа:

- 1 В главном окне Norton AntiVirus нажать кнопку “Параметры”.
- 2 Открыть вкладку “Поиск” (рис. 2-6).
- 3 Установить переключатель “Все файлы”.
- 4 Нажать ОК для возврата в главное окно Norton AntiVirus.
- 5 Выбрать нужный диск и нажать кнопку “Поиск”.

Дополнительные инструкции по выбору файлов для проверки см. в разделе *“Выбор проверяемых файлов” на странице 50*.

Рисунок 2-6 Вкладка параметров поиска

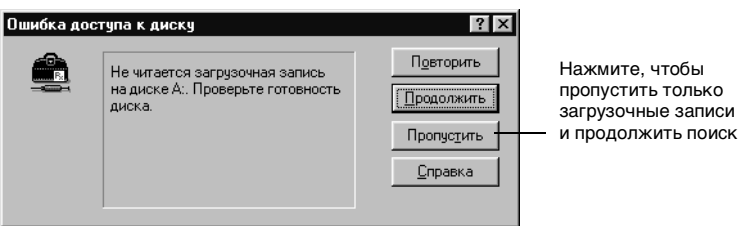


Обход проверки загрузочных записей

Параметры по умолчанию Norton AntiVirus предусматривают поиск вирусов в загрузочных записях дисков, что является неотъемлемой частью его обычной работы. Загрузочные записи представляют собой специальные области на дисках, в которых хранятся программы и данные, необходимые для загрузки операционной системы.

В целях безопасности, некоторые системы Windows NT сконфигурированы так, чтобы пользователи не могли получить доступ к этим областям диска. Для поиска вирусов в загрузочных записях необходимо иметь права администратора. При появлении диалогового окна с отказом в доступе к загрузочным записям (рис. 2-7) вы можете обойти данный этап процедуры поиска вирусов.

Рисунок 2-7 Запрет доступа к загрузочным записям



Как обойти поиск вирусов в загрузочных записях:

- 1 Нажать “Параметры” в главном окне Norton AntiVirus.
- 2 Открыть вкладку “Поиск”.
- 3 Отключить первые два элемента в окне группы “Что проверять”:
 - Главную загрузочную запись
 - Загрузочные записи
- 4 Нажать ОК, чтобы сохранить настройки и закрыть окно.

Осторожно! Отключение этих параметров приводит к общей отмене поиска в загрузочных записях жестких и гибких дисков.

Инструкции по установке других параметров поиска даны в разделе *“Настройка ручного поиска” на странице 45.*

Планирование поиска вирусов

Автоматический поиск вирусов можно запланировать либо на определенные дату и время для единичного запуска, либо для регулярного запуска через определенные интервалы. Если в указанное время компьютер занят другими программами, то запланированный поиск будет выполняться в фоновом режиме, не препятствуя вашей работе. При установке Norton AntiVirus с параметрами по умолчанию автоматический поиск вирусов планируется раз в неделю.

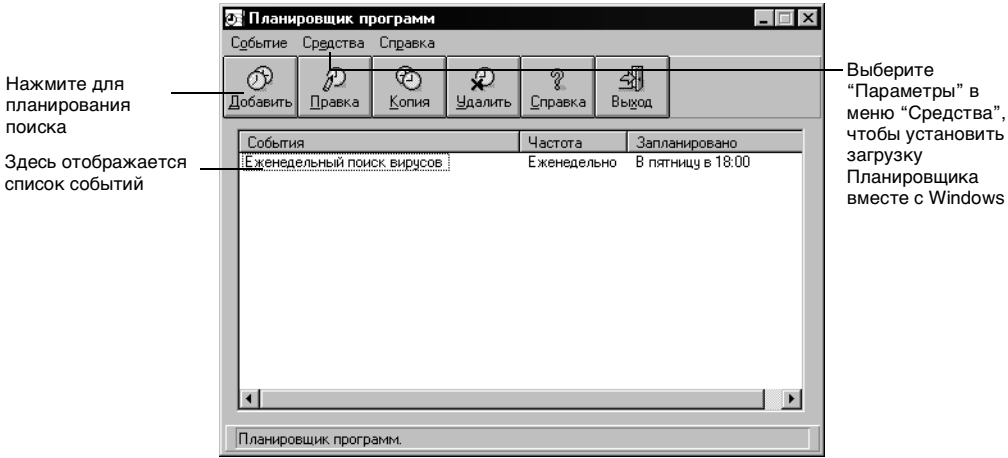
Как вызвать программу-планировщик:

Для этого можно выполнить любое из следующих действий:

- Нажать кнопку “Планировщик” в главном окне Norton AntiVirus.
- Выбрать *ПЛАНИРОВЩИК ПРОГРАММ* из меню “Пуск” Windows.

Если никакие события не запланированы, то кнопки “Правка”, “Копия” и “Удалить” недоступны.

Рисунок 2-8 Планировщик программ

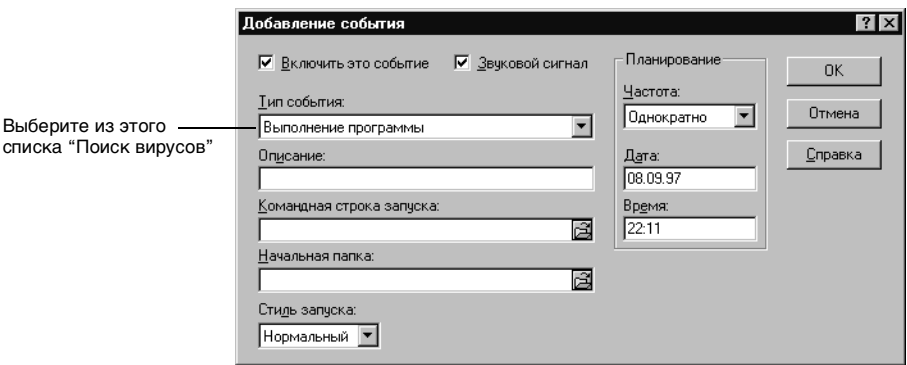


Как запланировать поиск вирусов:

1. Выбрать команду "Добавить".

Появится диалоговое окно "Добавление события", служащее для планирования любых типов событий.

Рисунок 2-9 Диалоговое окно "Добавление события"



2. Выбрать "Поиск вирусов" из ниспадающего списка "Тип события".

Диалоговое окно изменится — в нем появятся элементы для ввода информации о поиске вирусов.

Рисунок 2-10 Добавление события с настройкой Поиск вирусов

Отметьте, чтобы
сделать поиск
возможным

Описание события
напомнит вам о его цели

Укажите элементы, в
которых будет
выполняться поиск

Когда
выполнять по
иск вирусов

- 3 Установить флажок “Включить это событие”.
При снятом флажке поиск не запускается.
- 4 Установить флажок “Звуковой сигнал” для того, чтобы компьютер подавал сигнал при запуске процедуры поиска.
- 5 В текстовом поле “Описание” следует ввести краткую характеристику события, которая будет отображаться в списке событий планировщика.
- 6 В текстовом поле “Что проверять” указать имя диска или путь к папке или файлу, которые подлежат проверке на вирусы.

Примечание. Поле “Что проверять” не должно оставаться пустым. Обязательно укажите, что следует проверять на вирусы.

Если это жесткий диск, следует ввести букву диска с двоеточием.

C :

Чтобы задать несколько элементов, между ними нужно ставить пробел.

C : D:\Applications

Если в пути используются пробелы, то весь элемент заключается в двойные кавычки.

"C:\Rad Was Here\Hithere.exe"

При планировании поиска вирусов можно ввести любые из параметров командной строки NAVW32.EXE. Их перечень содержится в приложении В, в разделе “*Ключи командной строки*” на [странице 77](#).

- 7 Указать интервал выполнения поиска в ниспадающем списке “Частота”.
- 8 Указать дату и время запуска события.
- 9 Нажать ОК. При необходимости нажать также ОК в диалоговом окне подтверждения.

Совет: В командной строке можно использовать команду AT для планирования множественных проверок под Windows NT. Инструкции по запуску поиска (NAVWNT) прямо из командной строки даны в приложении В, “Ключи командной строки”.

Включение и отключение автозащиты

Norton AntiVirus по умолчанию загружает автозащиту — технологию автоматической защиты от вирусов — при каждой загрузке компьютера. Значок автозащиты Norton AntiVirus появляется на панели задач в системе Windows NT 4.0 (рис. 2-9). В Windows NT 3.51 на рабочем столе появляется соответствующий значок.


Как правило, автозащиту не отключают, поскольку она является мощным оружием против вирусов. Если ее и отключают, то лишь в случае крайней необходимости, например, когда это требуется для установки новой программы.

Рисунок 2-11 Панель задач Windows



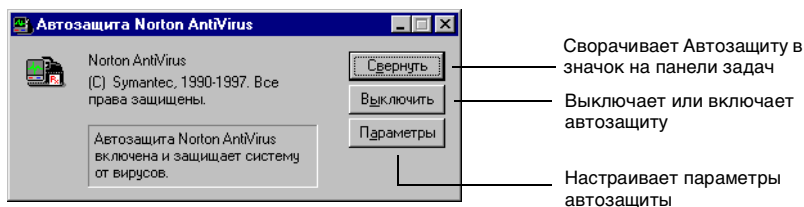
Значок работающей автозащиты в Windows NT 4.0

Как временно отключить автозащиту:

- 1 Дважды нажать на значок автозащиты на панели задач Windows (рис. 2-7).
Появится диалоговое окно “Автозащита Norton AntiVirus” (рис. 2-8).
- 2 Нажать кнопку “Выключить”.
Надпись на кнопке сменится на “Включить”, а значок примет вид .
- 3 Нажать кнопку “Свернуть” для закрытия диалогового окна автозащиты.

В системе Windows NT 3.51 нет панели задач. Чтобы временно отключить или включить автозащиту, следует нажать на кнопку автозащиты в главном окне Norton AntiVirus или дважды нажать на значок автозащиты на рабочем столе.

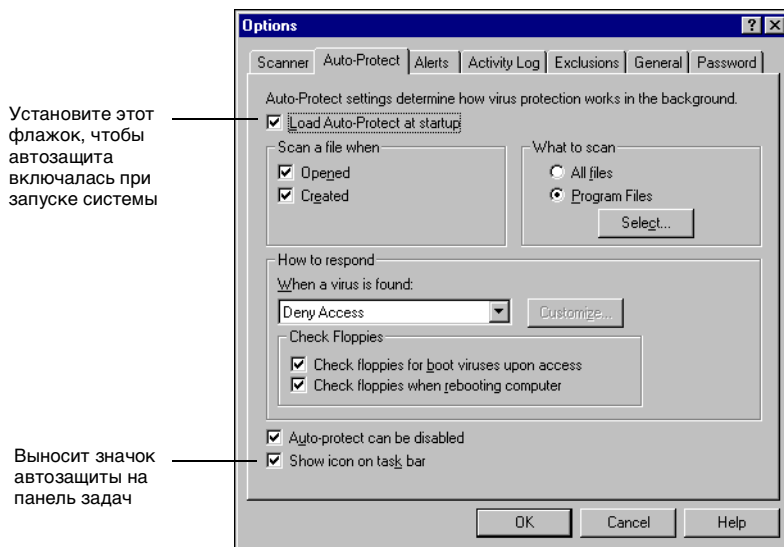
Рисунок 2-12 Диалоговое окно автозащиты Norton AntiVirus



Как установить загрузку автозащиты при запуске компьютера:

- 1 Открыть Norton AntiVirus.
- 2 Нажать кнопку “Параметры” в главном окне программы (см. рис. 2-2).
- 3 Выбрать вкладку “Автозащита”.

Рисунок 2-13 Установка параметров автозащиты



- 4 Включить параметр “Загружать автозащиту при запуске”.
- 5 Нажать ОК.

Теперь Norton AntiVirus будет активизировать автозащиту сразу после запуска компьютера.

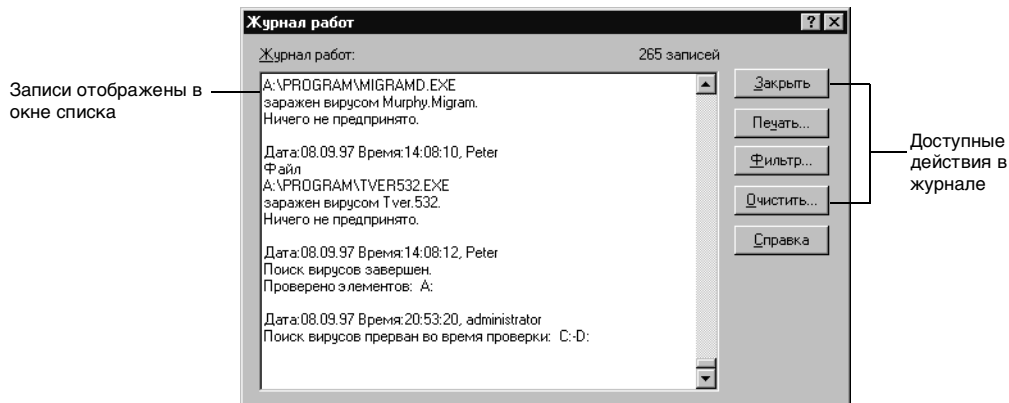
Просмотр журнала работ

В журнале работ протоколируются все действия, выполняемые Norton AntiVirus, такие как обнаружение вирусов и меры по их обезвреживанию. Сведения о настройке журнала работ см. в разделе *“Настройка журнала работ” на странице 57.*

Как просмотреть все записи журнала работ:

- 1 В главном окне Norton AntiVirus нажать кнопку “Журнал”.

Рисунок 2-14 Журнал работ



- 2 Для выхода из журнала работ следует нажать кнопку “Закрыть”.

Примечание. Все операции Norton AntiVirus регистрируются также в Windows NT Application Event Log.

В диалоговом окне журнала работ имеются следующие команды:

Печать...

Кнопка “Печать” выводит содержимое журнала на принтер или в файл. Распечатываются только записи, показанные в данный момент в списке, а при установке фильтра — только отфильтрованные.

Фильтр...

Кнопка “Фильтр” позволяет просматривать события определенного типа, например, все случаи обнаружения вирусов.

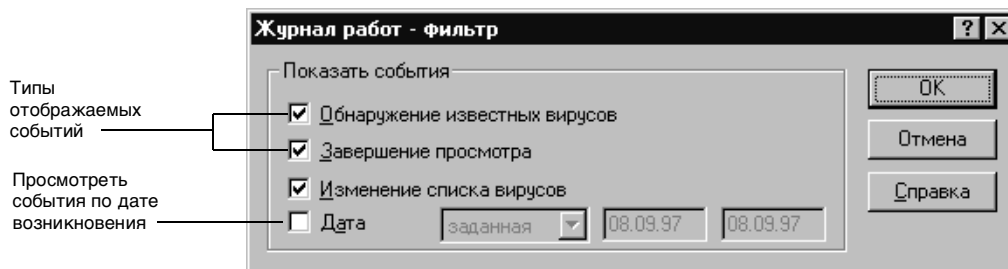
Очистить...

Кнопка “Очистить” удаляет все записи из журнала работ.

Как отфильтровать записи в журнале работ:

- 1 Нажать кнопку “Фильтр...” в диалоговом окне журнала работ (рис. 2-12).
Появится следующее диалоговое окно.

Рисунок 2-15 Фильтр журнала работ



- 2 Выбрать типы событий, необходимые для просмотра. Если в журнале нет записей, соответствующих заданному фильтру, то появится сообщение "Записи не найдены". В этом случае будут отменены все изменения фильтра и восстановлена предыдущая настройка.
 - Обнаружение известных вирусов: выводятся данные об обнаружении известных вирусов.
 - Завершение поиска: выводятся данные о времени и дате поиска как при ручном, так и запланированном запуске.
 - Изменение списка вирусов: выводятся данные о фактах изменения списка вирусов.
 - Дата: здесь указывается дата или интервал для отображения выбранных событий. Необходимо выбрать нужный параметр в ниспадающем списке “Дата”, затем ввести либо одну дату, либо начальную конечную даты интервала.
- 3 Нажать ОК.

Защита от вирусов из Internet

Norton AntiVirus для Windows NT при нормальной работе с параметрами по умолчанию надежно защищает компьютер от вирусов, проникающих из сети Internet. Нет никакой необходимости в использовании дополнительных программы или изменении настройки Norton AntiVirus. Автозащита автоматически проверяет файлы программ и документов во время их приема из Internet, а также файлы внутри архивов при их распаковке (“Параметры”\вкладка “Автозащита”\флажок “Проверять при создании”).

Пользователи, отключающие автозащиту Norton AntiVirus, остаются с браузерами Internet один на один.

Netscape и Norton AntiVirus

Во время своей установки Norton AntiVirus выясняет наличие в системе браузера Netscape. Если он установлен, то Norton AntiVirus устанавливается как вспомогательное приложение Netscape для автоматической проверки на вирусы файлов, получаемых из Internet. Если браузер Netscape ставится после Norton AntiVirus, то для включения данной функции необходимо переустановить Norton AntiVirus.

Прочие браузеры Internet и Norton AntiVirus

Если отключить автозащиту, то можно сконфигурировать и любые другие браузеры для использования Norton AntiVirus в качестве их вспомогательного приложения. В Windows NT 4.0 с этой целью вводится командная строка, запускающая NAV для каждого типа MIME и набора расширений:

```
"C:\Program Files\NAVNT\NAVWNT" /DOWNLOAD
```

В Windows NT 3.51 вводится следующая команда:

```
"C:\Win32app\NAVNT\NAVWNT" /DOWNLOAD
```

При вводе не забывайте про двойные кавычки ("). Если Norton AntiVirus установлен в другой папке, укажите в командной строке соответствующий путь.

В следующей таблице перечислены стандартные типы MIME и ассоциированные расширения.

Тип MIME	Расширения
application/octet-stream	386, BIN, CLA, COM, CPL, DLL, DRV, EXE, NCP, NED, NNL, OCX, OVL, SCR, SYS, VBX, VXD
application/binary	386, BIN, CLA, COM, CPL, DLL, DRV, EXE, NCP, NED, NNL, OCX, OVL, SCR, SYS, VBX, VXD
application/zip	ZIP, LHA, LZH
application/msword	DOC, DOT
application/word	DOC, DOT
application/msexcel	XLB, XLM, XLS, XLT, XLW
application/x-excel	XLB, XLM, XLS, XLT, XLW

Дополнительную информацию о вспомогательных приложениях и типах MIME можно найти в документации или в справке по браузерам Internet.

Уничтожение вирусов

Norton AntiVirus может сигнализировать о возможном присутствии вируса двумя различными способами в зависимости от того, каким образом был обнаружен вирус:

- Вирус обнаружен при выполнении ручного или запланированного поиска: по завершении поиска появляется диалоговое окно лечащего модуля NAV, предлагающее уничтожить все обнаруженные вирусы. См. *“Уничтожение вирусов, обнаруженных при поиске” на странице 29.*
- Вирусы обнаружены автозащитой: функция автозащиты, непрерывно следящая за появлением вирусов, немедленно выдает сигнал при обнаружении зараженного элемента. Командные кнопки в окне сигнала о вирусе позволяют выбрать действие в отношении вируса. См. *“Уничтожение вирусов, обнаруженных автозащитой” на странице 33.*

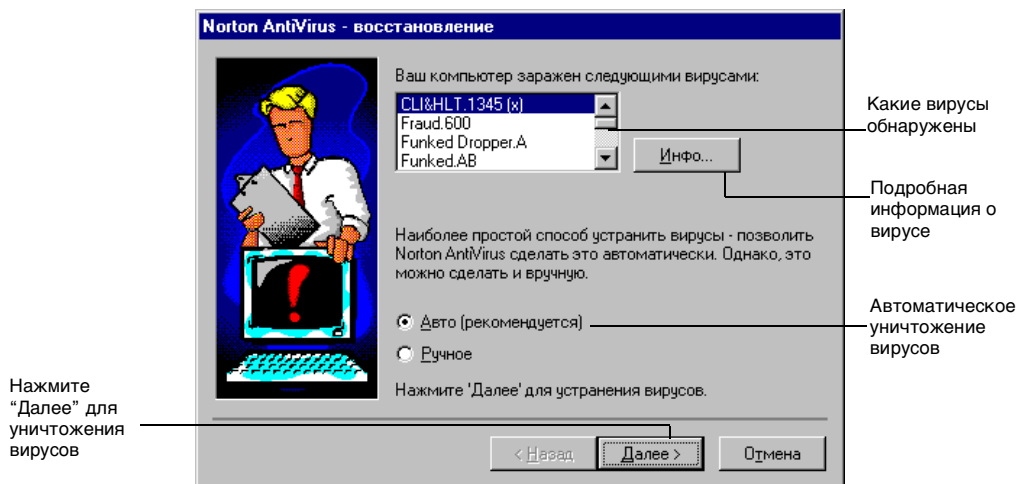
Уничтожение вирусов, обнаруженных при поиске

Действие, предпринимаемое программой Norton AntiVirus по отношению к зараженному элементу, обнаруженному при поиске, определяется настройкой. Существуют следующие варианты: “Запросить”, “Только известить”, “Сразу исправить” и “Сразу удалить”. Запросить — это действие по умолчанию. Инструкции по настройке даны в разделе *“Настройка ручного поиска” на странице 45.*

Если во вкладке параметров поиска выбрано “Запросить” (по умолчанию), и во время поиска будут обнаружены вирусы, то по его окончании появляется экран лечащего модуля (рис. 3-1). Можно разрешить программе уничтожать все вирусы автоматически или выбрать уничтожение их вручную по одному.

Если заданы параметры “Только известить”, “Сразу исправить” или “Сразу удалить”, то программа выполняет эти действия автоматически без каких-либо запросов. По окончании процедуры поиска появляется диалоговое окно с отчетом о всех действиях, которые были предприняты во время поиска.

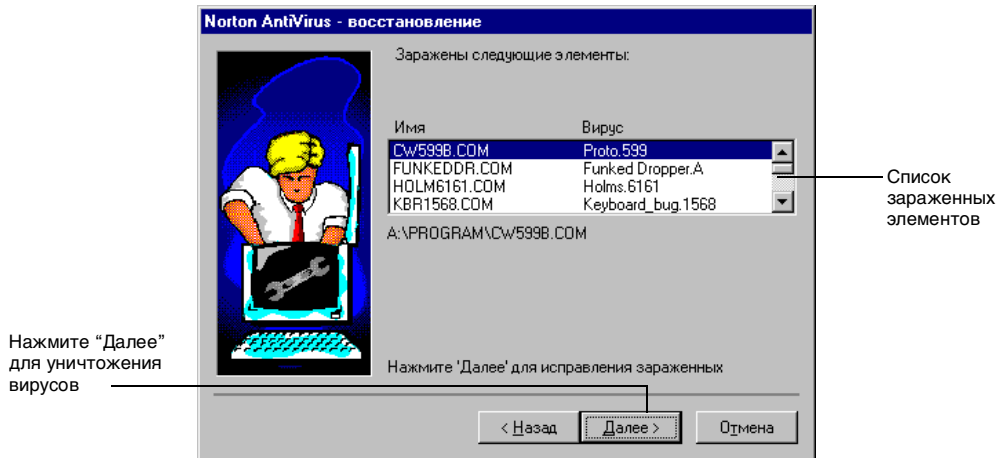
Рисунок 3-1 Лечащий модуль Norton AntiVirus



Как уничтожить найденные вирусы автоматически:

- 1 С помощью Norton AntiVirus выполнить поиск вирусов на диске, в папке или файле.
При обнаружения вируса появится окно лечащего модуля (рис. 3-1).
 - 2 Выбрать в диалоговом окне переключатель “Авто” и нажать кнопку “Далее”.
При выборе параметра “Ручное” смотрите инструкции в разделе *“Как уничтожить вирусы вручную по одному:” на странице 31.*
 - 3 Внимательно просмотреть сообщения в каждом последующем экране (рис. 3-2), чтобы понять действия Norton AntiVirus, затем нажать “Далее” для продолжения.
- Лечащий модуль не предпринимает никаких действий без вашего согласия.

Рисунок 3-2 Зараженные элементы



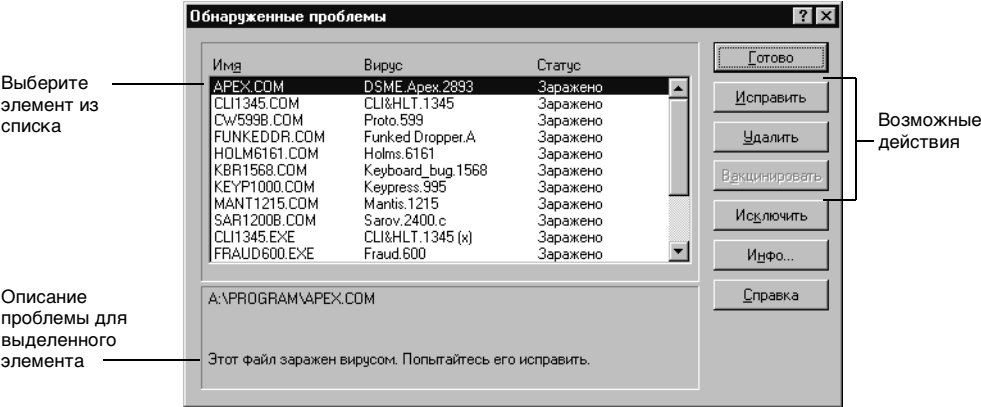
Примечание. Завершив свою работу, лечащий модуль выдает последний экран, суммирующий все выполненные действия. В этом экране можно нажать кнопку "Инфо..." для просмотра или вывода на печать подробной информации о том, что было заражено и исправлено.

Если в окне лечащего модуля выбрать режим "Ручное", то появится диалог "Обнаруженные проблемы" (рис. 3-3) с перечнем всех зараженных элементов.

Как уничтожить вирусы вручную по одному:

- 1 Установить переключатель "Ручное" в окне лечащего модуля (см. рис. 3-1) и нажать "Далее".
Появится диалоговое окно "Обнаруженные проблемы" (рис. 3-3) с перечнем всех зараженных элементов.
- 2 Выбрать элемент из списка.
- 3 Прочитать сообщение в нижней части диалогового окна для ознакомления с характером проблемы. Это сообщение относится только к текущему выбранному элементу.
- 4 Прочитать раздел *"Командные кнопки" на странице 32* для ознакомления с кнопками в окне "Обнаруженные проблемы", затем нажать нужную кнопку.

Рисунок 3-3 Диалоговое окно “Обнаруженные проблемы”



Примечание. Некоторые пользователи предпочитают, чтобы программа выдавала сигнал “Обнаружен вирус” сразу после его выявления, не дожидаясь окончания процедуры поиска. Инструкции по установке немедленного оповещения даны в разделе *“Как настроить дополнительные режимы поиска вирусов:”* на странице 49.

Командные кнопки

В таблице 3-1 объясняется назначение всех кнопок, используемых в Norton AntiVirus для действий по отношению к найденным вирусам. Эти кнопки появляются в диалоговом окне “Обнаружены проблемы”. Следует отметить, что некоторые кнопки могут выглядеть тусклыми или не появляться вовсе по следующим причинам:

- Данная функция несовместима с текущей конфигурацией Norton AntiVirus.
Это определяется установками во вкладках “Поиск” и “Автозащита”. Дополнительную информацию об изменении стандартных установок см. в главе 5, “Настройка поиска вирусов”.
- Программа Norton AntiVirus определила, что в текущей ситуации выполнение данной функции невозможно.

Кнопка	Действие	Примечание
Исправить	Уничтожает вирус, восстанавливая исходное состояние зараженного файла или загрузочной записи.	См. <i>“Уничтожение вирусов, обнаруженных автозащитой” на странице 33.</i>
Удалить	Устраняет вирус путем удаления зараженного файла.	Удаленный файл восстановить невозможно. Его необходимо заменить незараженной копией.
Прервать	Прерывает текущую операцию. Если идет поиск, то он будет остановлен.	Выбор кнопки “Прервать” не решает проблему, о которой сообщается. Но если она вызвана вирусом, то вирус деактивизируется, хотя и остается в компьютере и продолжает ему угрожать.
Продолжить	Продолжить текущую операцию. Если идет поиск, то он будет продолжен.	Выбор этой кнопки не решит проблему, о которой сообщается. При последующем запуске NAV вы снова получите такое же извещение.
Исключить	Продолжает операцию и исключает указанный файл из следующих сигналов данного типа.	Нажимать эту кнопку следует только при абсолютной уверенности в том, что сигнал не вызван вирусом. Исключение файла означает, что NAV не будет больше на него реагировать. См. <i>“Работа с исключениями” на странице 53.</i>

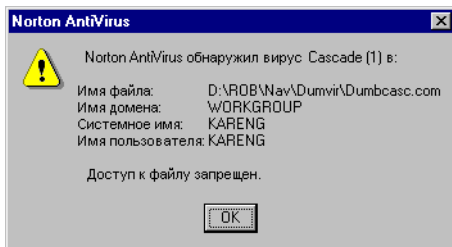
Уничтожение вирусов, обнаруженных автозащитой

Автозащита Norton AntiVirus, ведя непрерывное наблюдение за вирусами, немедленно выводит диалоговое окно сигнала при любом событии, которое может быть связано с вирусами (рис. 3-4). Сигнал о вирусе может быть выдан в следующих ситуациях:

- При попытке запустить зараженную программу
- При попытке открыть зараженный документ или электронную таблицу
- При попытке воспользоваться дискетой, зараженной загрузочным вирусом

Действие, предпринимаемое программой Norton AntiVirus при обнаружении зараженного элемента, зависит от настройки автозащиты. Существуют следующие варианты: “Сразу исправить”, “Сразу удалить” или “Запретить доступ”. Последнее является действием по умолчанию. Инструкции по смене параметров автозащиты даны в разделе *“Настройка автозащиты” на странице 59.*

Рисунок 3-4 Сигнал о вирусе



Если автозащита обнаружила вирус, и ее настройка позволяет запретить доступ к зараженному элементу, то необходимо проверить диски, чтобы найти и обезвредить вирус, а также удостовериться в том, что он не успел распространиться дальше. Обезвредить вирус можно двумя способами:

- Исправить зараженный файл, загрузочную запись или главную загрузочную запись.
- Удалить с диска зараженный файл.

К сожалению, нельзя удалить зараженные системные файлы, а также загрузочные записи и главную загрузочную запись, поскольку в них содержится информация, необходимая для запуска компьютера. Если зараженный файл нельзя ни исправить, ни удалить, прочтите инструкции в разделе *“Что делать, если исправление неудачно”* на [странице 34](#).

Как только у вас появится уверенность в том, что вирусы в системе отсутствуют, замените удаленные файлы незараженными копиями. Перед копированием файлов на жесткий диск обязательно проверьте их на вирусы. Если вы забыли, какие файлы следует заменить, загляните в журнал работ, где должны быть указаны имена этих файлов. См. *“Просмотр журнала работ”* на [странице 25](#).

Что делать, если исправление неудачно

В тех редких случаях, когда NAV не способен восстановить файл или загрузочную запись, вы получите сообщение о неудачной попытке их исправления.

Совет. Прежде чем делать что-то еще, удостоверьтесь в наличии самых последних файлов описания вирусов и повторите поиск. См. *“Автоматическое обновление описаний вирусов”* на [странице 37](#).

Если невозможно исправить файл приложения

Если Norton AntiVirus не может исправить зараженный программный файл, то единственный способ обезвредить вирус — удалить сам файл. Удаленный файл можно затем заменить незараженной копией. Лучше всего взять незараженный файл с оригинального дистрибутива программного обеспечения. При отсутствии резервной копии и оригинальных дисков свяжитесь с разработчиком ПО для получения замены.

Если невозможно исправить системный файл

Если заражен системный файл, то удалять его нельзя. Перезапустите компьютер с аварийной системной дискеты, созданной при установке Windows NT, и замените зараженный файл. Если это не поможет, придется переустановить Windows NT.

Если невозможно исправить загрузочную запись

Если Norton AntiVirus не смог исправить загрузочную запись или главную загрузочную запись жесткого диска, перезапустите компьютер с аварийной системной дискеты, созданной при установке Windows NT, и попытайтесь устранить проблему. Если это не поможет, придется переустановить Windows NT.

Если Norton AntiVirus не может исправить загрузочную запись гибкого диска, у вас остается возможность перезаписать наиболее важные файлы с этого диска на другой. Но будьте осторожны, ведь гибкий диск заражен. Все переписанные с него файлы нужно еще раз проверить на вирусы. После копирования файлов с зараженного диска его следует выбросить или отформатировать (на незараженном ПК).

Удаление вирусов из сжатых файлов

Хотя Norton AntiVirus и способен находить зараженные файлы внутри сжатого файла, он не сможет их исправить, пока они остаются упакованными. Для уничтожения вируса необходимо сначала распаковать файл.

Как удалить вирусы из сжатых файлов:

- 1 Создать временную папку.
- 2 Нажать на значок автозащиты в панели задач Windows и временно отключить автозащиту.
- 3 Распаковать сжатый файл во временную папку.
- 4 Удалить зараженный файл.

- 5 Проверить на вирусы временную папку и либо исправить, либо удалить все найденные зараженные файлы.
- 6 При необходимости повторно запаковать файлы во временной папке.
- 7 Снова нажать на значок автозащиты в панели задач Windows для включения автозащиты.

Устранение проблем общего характера

Далее объясняется, как можно устранить некоторые проблемы общего характера, возникающие при использовании программы Norton AntiVirus. Прежде чем обращаться в службу технической поддержки, попробуйте решить эти проблемы с помощью следующих процедур.

После обнаружения и удаления вируса файлы остаются зараженными

Причина:	Источник заражения — дискета.
Решение:	Проверить все имеющиеся дискеты. См. <i>“Поиск вирусов” на странице 17.</i>
Причина:	Возможно, вирус содержится в программном файле с нестандартным расширением.
Решение:	<p>Изменить параметры во вкладке “Поиск”, установив “Все файлы”, чтобы проверять не только “Программные файлы”. Проверить все используемые диски и исправить зараженные файлы. Добавить расширения зараженных файлов в список расширений программных файлов.</p> <p>Инструкции по установке типов проверяемых файлов даны в разделах <i>“Выбор проверяемых файлов” на странице 50</i> и <i>“Установка расширений программных файлов” на странице 51.</i></p>
Причина:	Вирус активен в другом открытом сеансе DOS.
Решение:	Закройте все открытые сеансы DOS и выполните еще раз поиск вирусов.

Некорректная работа программы после исправления

Причина:	Несмотря на то, что Norton AntiVirus уничтожил вирус, файлу мог быть поврежден в результате исправления.
Решение:	Замените программу незараженной копией.

Как защититься от новых вирусов

Norton AntiVirus ищет вирусы, используя данные файлов описания вирусов. Как только на свет появляется новый вирус, инженеры Symantec вносят его код (сигнатуру) в файл описания вирусов. Для того, чтобы защитить компьютер от новейших вирусов, необходимо регулярно обновлять эти файлы. Их обновленные версии выпускаются ежемесячно.

Автоматическое обновление описаний вирусов

Для обеспечения постоянной и надежной защиты от всех вирусов в программе Norton AntiVirus имеется средство автоматического обновления файлов описания вирусов. С вашей стороны должны быть выполнены следующие условия:

- Доступ к сети Internet
- Правильно установленный модем

Ежемесячное обновление файлов описания вирусов должно войти у вас в привычку.

Рисунок 4-1 Автоматическое обновление описаний вирусов



Как выполнить автоматическое обновления описания вирусов:

- 1 В главном окне Norton AntiVirus нажать “Обновление” (рис. 4-1).
- 2 В выпадающем списке “Как установить связь с сервером Symantec” выбрать один из методов соединения:
 - Автоматический поиск устройств: Norton AntiVirus определяет, имеется ли доступ в Internet и можно ли ваш модем использовать для подсоединения.
 - Internet: Norton AntiVirus подключается к серверу FTP фирмы Symantec через Internet.
 - Модем: Norton AntiVirus набирает указанный номер и подключается к серверу Symantec через модем.
- 3 Нажать “Далее” для запуска процедуры обновления.

Вне зависимости от выбранного метода связи, Norton AntiVirus соединяется с сервером, копирует с него нужные файлы и устанавливает их на компьютере. На этом все ваши действия закончены.

По окончании процедуры обновления рекомендуем прочитать новые текстовые документы (*.TXT) в папке Norton AntiVirus, в которых содержится самая последняя информация о появившихся вирусах и необходимых мерах предосторожности.

Примечание. Если осуществлять соединение по модему, то вы получите счет за междугородную телефонную связь.

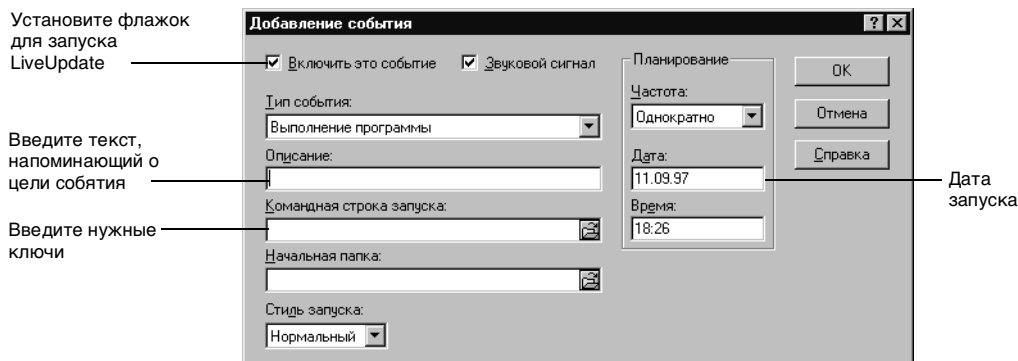
Планирование автоматического обновления

После первого успешного обновления можно запланировать эти операции, чтобы они выполнялись автоматически через определенный интервал в назначенное время. О работе планировщика см. *“Планирование поиска вирусов” на странице 20.*

Как запланировать автоматическое обновление:

- 1 Любым из нижеуказанных способов запустить планировщик:
 - Нажать кнопку “Планировщик” в главном окне Norton AntiVirus.
 - Выбрать “NORTON PROGRAM SCHEDULER” из меню “Пуск” Windows.
- 2 Нажать кнопку “Добавить”.
Появится диалоговое окно “Добавление события”.
- 3 В выпадающем списке “Тип события” выбрать “Запуск LiveUpdate”.
В диалоговом окне появятся параметры, необходимые для LiveUpdate.

Рисунок 4-2 Окно Добавление события “Запуск LiveUpdate”



- 4 Установить флажок “Включить это событие”.
Иначе автоматический запуск LiveUpdate будет невозможен.
- 5 Установить параметр “Звуковой сигнал”, чтобы слышать момент запуска LiveUpdate.
- 6 Ввести короткий текст в текстовом поле “Описание”.
Этот текст появится в списке событий в диалоговом окне планировщика.
- 7 Ввести /PROMPT в текстовом поле “Командная строка”, чтобы иметь возможность дать подтверждение перед каждым плановым запуском LiveUpdate.
- 8 В ниспадающем списке “Частота” выбрать интервал запуска LiveUpdate.
- 9 Указать время и дату для данного события.
- 10 Нажать ОК. Если появится запрос подтверждения, нажать ОК еще раз.

Ручное обновление описаний вирусов

Получить предоставляемые фирмой Symantec файлы описания вирусов можно в любой момент из различных источников. Выберите для себя наиболее подходящий. Но даже если вы пользуетесь функцией автоматического обновления описаний вирусов, на указанные ниже адреса все равно стоит заглянуть, ибо там можно найти обширнейшие сведения о вирусах вообще, а также информацию и обновленные версии по всей гамме программных продуктов Symantec.

Где можно найти файлы описания вирусов

Файл, который выгружается из сети, представляет собой специальную программу обновления, которая автоматически определяет местонахождение Norton AntiVirus на компьютере и устанавливает новые файлы описания вирусов. Его имя меняется ежемесячно с соблюдением следующего формата: *ммNAVгг.EXE*, где *мм* означает месяц, а *гг* - год. Инструкции по использованию программы автоматического обновления даны в разделе *“Установка новых файлов описания вирусов” на странице 42.*

Symantec BBS

Параметры Symantec BBS:

- 8 бит, 1 стоповый бит, отсутствие контроля четности

Для доступа к Symantec BBS используйте номер:

- (541) 484-6669 [круглосуточно]

Как перейти в раздел описаний вирусов из основного меню Symantec BBS:

- 1 Ввести F для получения меню файлов.
- 2 Ввести N для выбора последней версии описаний вирусов NAV.
- 3 Выполнить появляющиеся на экране инструкции по передаче файлов.

Ввести /GO GETFILE в командной строке для возврата в меню файлов.

America Online

Как перейти в Symantec Forum:

- 1 В меню GoTo выбрать *KEYWORD*.
- 2 Ввести SYMANTEC .
- 3 Выбрать Virus Control Central.
- 4 Выбрать Virus Definitions Library.

CompuServe

Как перейти в Symantec Forum:

- 1 Выполнить любое из следующих действий:
 - В меню Services выбрать *Go* и ввести SYMNEW.
 - В ответ на любое приглашение (!) ввести *GO SYMNEW*.
- 2 Взять файлы из библиотеки Norton AntiVirus.

Internet

Как подключиться к серверу FTP:

- 1 Войти на `ftp.symantec.com`
- 2 Перейти в каталог `/public/AntiVirusDefs/nav/`.
- 3 Забрать последние версии файлов.

Как подключиться к FTP через интерфейс World Wide Web:

- 1 Войти на `www.symantec.com`
- 2 Выбрать AntiVirus Research Center.
- 3 Выбрать Download Updates.
- 4 Выбрать Norton AntiVirus.
- 5 Выполнить появляющиеся на экране указания.

Microsoft Network

Как перейти к службам Symantec:

- 1 В меню View выбрать *Go To*.
- 2 Выбрать Other Location.
- 3 Ввести SYMANTEC
- 4 Дважды нажать на Support Solutions.
- 5 Дважды нажать на Symantec File Library.
- 6 Взять описания вирусов в разделе Norton AntiVirus File Library.

Получение дискеты с описаниями вирусов по почте

В фирме Symantec можно заказать регулярную доставку обновленных файлов описаний вирусов на дискете по почте. Информация о заказе приводится в главе Служба Symantec и решения поддержки.

Установка новых файлов описания вирусов

Файл обновления, принимаемый из сети, является специальной программой, которая автоматически устанавливает новые файлы описания вирусов на компьютер.

Как установить новые описания вирусов:

- 1 Скопировать программу обновления в любую папку на вашем компьютере.
Имя файла соответствует формату: *мм*NAV*гг*.EXE, где *мм* это месяц, а *гг* - год.
- 2 Выполнить одно из следующих действий:
 - В Windows NT 4.0, в окне “Мой компьютер” или “Проводник” дважды нажать на программу обновления.
 - В Windows NT 3.51, выбрать команду “Выполнить” в меню “Файл” для запуска программы обновления.Эта программа сама определит местонахождение Norton AntiVirus на вашем компьютере.
- 3 Выполнить все указания, появляющиеся на экране.
- 4 Программа обновления автоматически установит новые файлы описания вирусов в соответствующей папке.
На запрос о перезаписи файлов следует ответить “Да”. Тогда старые файлы описания вирусов будут заменены новыми.
- 5 В программе Norton AntiVirus запустить поиск вирусов для активизации новых описаний.
- 6 Перезагрузить ПК, чтобы автозащита могла воспользоваться новыми описаниями вирусов.
- 7 Прочитать новые текстовые документы (*.TXT) в папке Norton AntiVirus для ознакомления с последней информацией о появившихся вирусах и специальных мерах защиты.

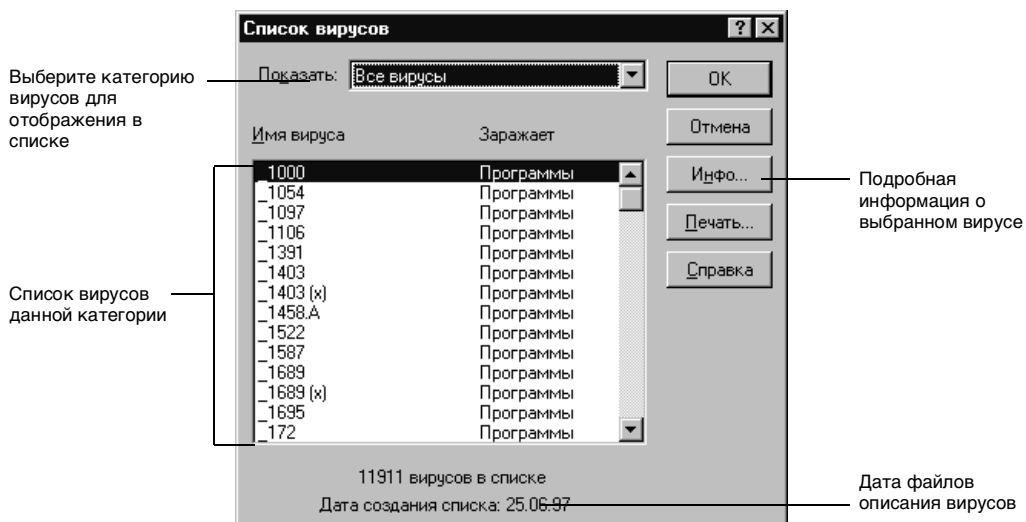
Просмотр списка вирусов

Список вирусов Norton AntiVirus позволяет узнать, какие вирусы умеет распознавать эта программа. Распознавание вирусов происходит на основе информации файлов описания вирусов. В списке можно также получить подробную характеристику каждого вируса, включая его симптомы заражения и псевдонимы.

Как открыть список названий вирусов:

- Нажать кнопку “Вирусы” в главном окне Norton AntiVirus.

Рисунок 4-3 Список вирусов



В окне списка указывается название вируса и объекты заражения (программные файлы, загрузочные записи или то и другое). Можно настроить список на отображение вирусов только определенной категории — нужная категория выбирается в ниспадающем списке “Показать”.

Все вирусы

Отображаются все вирусы, которые умеет находить Norton AntiVirus.

Часто встречающиеся вирусы

Отображаются только самые распространенные вирусы, встреча с которыми наиболее вероятна.

Программные вирусы

Отображаются вирусы, заражающие программные файлы в момент их выполнения.

Загрузочные вирусы	Отображаются вирусы, заражающие загрузочные и главные загрузочные записи дисков.
Скрытые вирусы	Отображаются вирусы, умеющие маскироваться, чтобы избежать обнаружения и нейтрализации.
Полиморфные вирусы	Отображаются вирусы, изменяющие свой внешний вид при заражении каждого нового файла, что затрудняет их обнаружение.
Многоцелевые вирусы	Отображаются вирусы, поражающие как программные файлы, так и загрузочные записи.
Макровирусы	Отображаются вирусы, заражающие документы Microsoft Word и электронные таблицы Excel.

Инфо...

Кнопка “Инфо...” выводит подробную информацию об отдельном вирусе, включая вероятность его появления, характеристики и псевдонимы.

Печать...

Кнопка “Печать...” выводит список вирусов на принтер или в файл.

Как найти имя вируса в списке:

1Открыть экран списка вирусов (рис. 4-2).

2Начать вводить имя нужного вируса в текстовом поле названия.

По мере ввода имени курсор в окне списка вирусов будет перемещаться к нужному пункту.

Если интересующий вас вирус отсутствует в окне списка, то, скорей всего, вы просто задали отображение не всех вирусов. Для вывода имен всех вирусов установите значение “Все вирусы” в параметре “Показать”.

Настройка поиска вирусов

Norton AntiVirus является мощным оружием против компьютерных вирусов. Стандартные значения параметров Norton AntiVirus обеспечивают оптимальную защиту для любой вычислительной среды. Если программа установлена с параметрами по умолчанию, то надежная защита вам уже гарантирована.

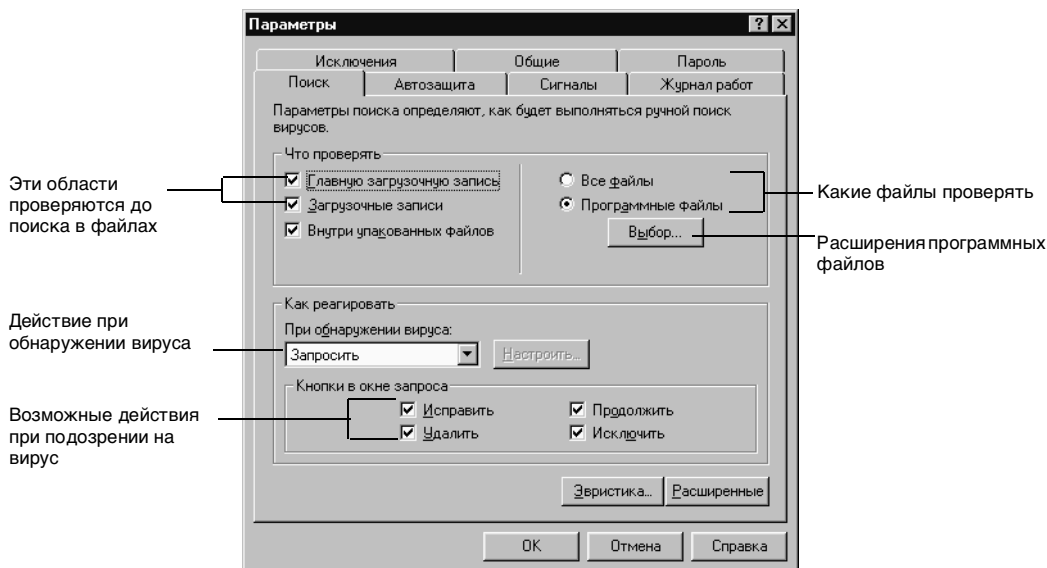
Настройка ручного поиска

Параметры ручного поиска определяют режимы поиска вирусов, запускаемого кнопкой “Поиск” или выполняемого автоматически (запланированных).

Как выбрать элементы, требующие проверки:

- 1 Нажать кнопку “Параметры” в главном окне Norton AntiVirus.
- 2 Открыть вкладку “Поиск”.

Рисунок 5-1 Параметры поиска



- 3** В группе параметров “Что проверять” необходимо указать, какие области системы должны проверяться перед проверкой файлов. По умолчанию для большей безопасности установлены первые три флажка. Если вы часто получаете сжатые файлы, установите также флажок “Внутри упакованных файлов”.

- **Память:** поиск вирусов в оперативной памяти.

Установка этого параметра крайне важна, т. к. резидентные в памяти вирусы активно распространяются на другие файлы. Если этот параметр отключить, то резидентный вирус может проникнуть во все открываемые файлы.

- **Главная загрузочная запись:** поиск вирусов в главной загрузочной записи жесткого диска.
- **Загрузочные записи:** поиск вирусов в загрузочных записях жестких и гибких дисков. Если имеется много сжатых файлов, то процедура поиска может затянуться.
- **Внутри сжатых файлов** NAV проверяет файлы, сжатые любыми популярными утилитами (ZIP, LHA и LHZ). Следует иметь в виду, что упакованные файлы внутри упакованных файлов не проверяются.

- 4 В группе параметров “Что проверять” выбрать также переключатель типа проверяемых файлов:
 - Все файлы: проверяются все файлы указанной папки или диска, в т. ч. и те, которые наименее подвержены заражению вирусами.
 - Программные файлы: проверяются файлы, наиболее подверженные заражению, с расширениями, указанными в списке расширений программных файлов. Инструкции по выбору расширений в списке даны в разделе *“Выбор проверяемых файлов” на странице 50.*

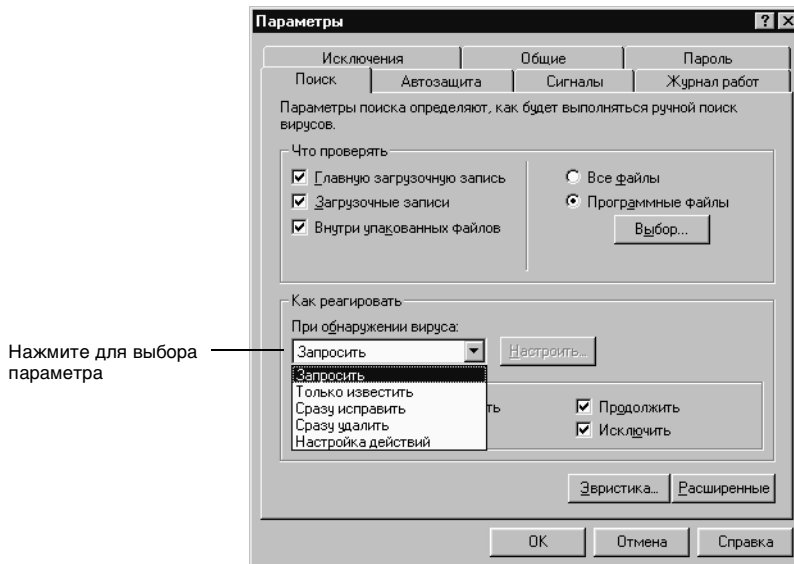
Примечание. Расширения документов Microsoft Word и таблиц Excel включены в группу программных файлов. Хотя эти файлы не являются программными, они могут быть заражены новым классом макровирусов.

- 5 Нажать ОК для сохранения параметров и закрытия диалогового окна или для перехода к следующей процедуре.

Как настроить реакцию программы на обнаружение вирусов:

- 1 Нажать кнопку “Параметры” в главном окне Norton AntiVirus.
- 2 Открыть вкладку “Поиск” (рис. 5-2).
- 3 Выбрать нужный режим в списке “Как реагировать”.

Рисунок 5-2 Что делать при обнаружении вируса



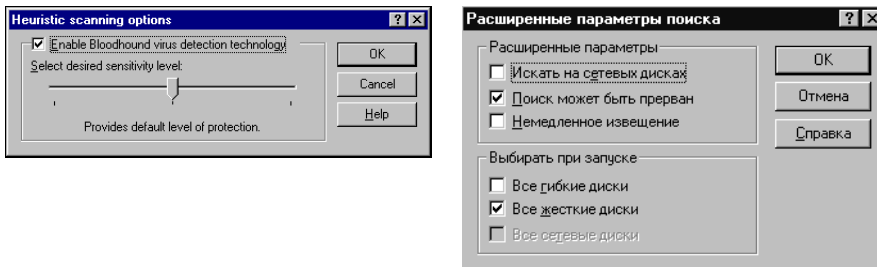
- Запросить: программа сообщит об обнаружении вируса и предложит ответные действия. Это наиболее удобный режим.
 - Только известить: NAV будет только сообщать о вирусе, не давая возможности исправить или удалить зараженный файл.
 - Сразу исправить: программа, не выдавая никаких запросов, сразу попытается вылечить зараженный файл или загрузочную запись. По окончании поиска результаты восстановления записываются в отчет и журнал работ.

аИмейте в виду, что Norton AntiVirus по умолчанию создает резервные копии файлов перед их восстановлением. См. *“Установка параметров резервирования” на странице 58.*
 - Сразу удалить: зараженный файл или загрузочная запись удаляется без запроса. Результаты заносятся в отчет и журнал работ. Будьте осторожны при использовании этого параметра — файлы, удаленные таким образом, восстановить уже невозможно.
 - Настраиваемый ответ: позволяет задать различные действия при обнаружении вируса в файле, макросе или загрузочной записи. После выбора режима “Настраиваемый ответ”, следует нажать кнопку “Настроить...” для указания конкретных действий.
- 4 Если в пункте 3 выбрано “Запросить”, то необходимо также указать, какие кнопки должны выводиться в окне запроса — для этого предусмотрена группа флажков “Кнопки в окне запроса”:
- Исправить: позволяет исправить файл или загрузочную запись. Если исправление невозможно, например, когда файл открыт, то эта кнопка будет недоступна.
 - Удалить: используется для удаления файла. Если заражен элемент, удалить который невозможно, например, загрузочная запись, то эта кнопка будет недоступна.
 - Продолжить: позволяет продолжить процедуру поиска, не принимая никаких мер. Эта кнопка работает только при включенном режиме “Немедленно известить” (см. следующую процедуру).
 - Исключить: исключает файл из перечня проверяемых на известные вирусы. Этой кнопкой следует пользоваться осторожно — она может снизить общий уровень защиты системы от вирусов.
- 5 Нажать ОК, чтобы сохранить настройки и закрыть диалоговое окно или перейти к другим процедурам..

Как настроить дополнительные режимы поиска вирусов:

- 1 Нажать кнопку “Эвристика” на вкладке “Поиск” (рис. 5-2).
Откроется диалог “Параметры эвристического поиска” (Рис. 5-3).
- 2 Установить флажок “Включить технологию Bloodhound”.
Norton AntiVirus использует новую технологию “Bloodhound” для борьбы с трудно распознаваемыми вирусами.

Рисунок 5-3 Дополнительные параметры поиска вирусов



- 3 Передвинув движок вправо, можно повысить чувствительность технологии Bloodhound в среде повышенного риска, но это приведет к замедлению поиска.
- 4 Нажать ОК для закрытия окна “Параметры эвристического поиска”.
- 5 Нажать кнопку “Расширенные” во вкладке “Поиск” (рис. 5-2).
Появится окно “Расширенные параметры поиска” (см. Рис. 5-3).
- 6 Установить нужные флажки расширенных параметров:
 - Искать на сетевых дисках: помимо локальных, поиск вирусов будет также возможен на сетевых дисках. О некоторых особенностях проверки сетевых устройств говорится в следующем разделе *“Замечания по поиску вирусов в сети” на странице 50*.
 - Поиск может быть прерван: чтобы можно было в любой момент прервать процедуру поиска. Если этот флажок установлен, то в ходе поиска можно нажать на кнопку “Прервать”.
 - Немедленное извещение: при обнаружении проблемы программа, не дожидаясь окончания поиска, сразу же выдает сигнальное окно, где можете выбрать ответное действие.

Примечание. Если выбрано “Немедленное извещение”, то по окончании поиска экран лечащего модуля не появляется. Вместо этого все проблемы решаются с помощью сигнальных окон.

- 7 В группе “Выбирать при запуске” указать диски, которые будут автоматически выбраны для проверки при запуске Norton AntiVirus.
- 8 Нажать кнопку ОК для сохранения параметров и закрытия диалогового окна.

Замечания по поиску вирусов в сети

Поскольку ваши права доступа к сетевым дискам могут отличаться от прав на локальных, то при поиске вирусов на сетевых дисках могут иметь место следующие ограничения.

Проверка сетевых дисков занимает больше времени, чем локальных, т. к. при этом другие пользователи могут создавать, удалять или перемещать файлы.

Права доступа к диску	Что можно выполнять
Никаких	Ничего
Только чтение	Поиск вирусов в файлах и проверка вакцинации без исправления
Чтение и запись	Поиск вирусов, исправление, удаление и вакцинация

Выбор проверяемых файлов

В большинстве случаев достаточно проверить лишь программные файлы, поскольку вирусы в основном поражают файлы именно этого типа. Ниже дается подробное объяснение выбираемых NAV типов файлов, которое поможет вам решить, какая настройка предпочтительнее для каждого конкретного случая.

Все файлы

Проверяется каждый файл — данные (базы данных, документы, текстовые файлы и файлы электронных таблиц) и программы (системные файлы, программы текстовой обработки, утилиты и т. п.). Проверка всех файлов занимает больше времени, но зато проверяются все типы программных файлов или документов Microsoft Word, даже с нестандартными расширениями. Проверка только программных файлов обычно бывает достаточной, если только не будет найден вирус. В этом случае необходимо проверить все файлы, иначе гарантировать отсутствие вирусов на диске нельзя.

Только программные файлы

Проверяются файлы на основе списка расширений программных файлов. В нем содержатся все наиболее распространенные расширения исполнимых файлов, которые более других подвержены заражению и опасности стать разносчиками вирусов. В большинстве случаев можно вполне ограничиться проверкой лишь программных файлов.

Примечание. Расширения документов Microsoft Word и электронных таблиц Microsoft Excel включены в группу программных файлов. Хотя они и не являются программными, тем не менее, эти файлы легко могут быть заражены новым классом макровирусов.

Если файлы какой-либо программы имеют расширение, не входящее в список расширений, его можно туда добавить. Но даже если вы этого не сделаете, NAV все равно может обнаружить вирус в данном файле. Вирус сначала заражает программные файлы со стандартными расширениями и лишь затем пытается проникнуть в файлы с другими расширениями. После обнаружения вируса в программном файле со стандартным расширением можно проверить и все остальные файлы. Инструкции по установке данных параметров даны в разделах *“Настройка ручного поиска” на странице 45* и *“Настройка автозащиты” на странице 59*.

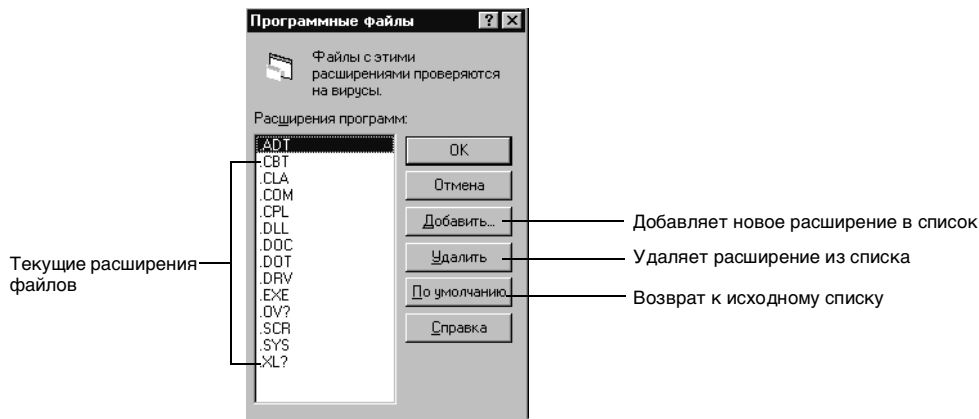
Установка расширений программных файлов

Norton AntiVirus при проверке и вакцинировании программ пользуется списком расширений программных файлов. В этом списке содержатся расширения файлов, которые скорее других могут заразиться и стать разносчиками вирусов. В расширениях всегда используется 3 символа.

Как просмотреть текущие расширения программных файлов:

- 1 Нажать “Параметры” в главном окне Norton AntiVirus.
- 2 Открыть вкладку “Поиск”.
- 3 Выбрать “Программные файлы” в группе “Что проверять” (рис. 5-2).
- 4 Нажать кнопку “Выбор”.

Рисунок 5-4 Расширения программных файлов

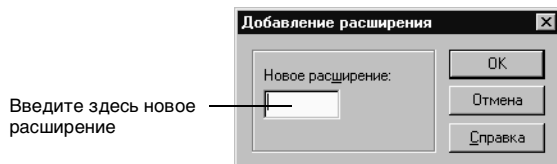


По умолчанию список содержит большинство расширений, используемых программными файлами. Если у какой-либо программы есть файл с нестандартным расширением, его можно добавить в список.

Как добавить в список расширение программного файла:

- 1 Нажать кнопку “Добавить” в диалоговом окне “Программные файлы” (рис. 5-5).

Рисунок 5-5 Диалоговое окно “Добавление расширения”



- 2 Ввести новое расширение имени файла в текстовом поле “Новое расширение” и нажать **OK**.

В расширении можно использовать шаблоны, но не для всех трех символов. Скажем, `OV?` будет означать расширения, начинающиеся с `OV`, например: `.OVL` или `.OV1`.

Как удалить расширение программного файла из списка:

- 1 Выбрать расширение в окне списка (рис. 5-5).
- 2 Нажать кнопку “Удалить”, затем **OK**.

Как вернуть список расширений в исходное состояние:

- 1 В диалоговом окне “Программные файлы” (рис. 5-5) нажать кнопку “По умолчанию”.

Список расширений будет восстановлен в том виде, в котором он был создан при установке Norton AntiVirus.

- 2 Нажать ОК.

Работа с исключениями

Norton AntiVirus использует список исключений во всех режимах поиска вирусов. Пункты данного списка не подвергаются проверке на вирусы. Исключения назначаются для дисков, папок, групп файлов или отдельных файлов. При этом программа запоминает полный путь исключенного элемента. Если файл, внесенный в список исключений, будет перемещен или переименован, то его исключение станет недействительным.

Добавлять элементы в список исключений можно вручную, однако необходимо отдавать себе отчет в том, что вы делаете. Можно, например, определить в качестве исключений сетевые тома или ветви древовидной структуры данных, чтобы они не проверялись при выполнении обычного поиска вирусов.

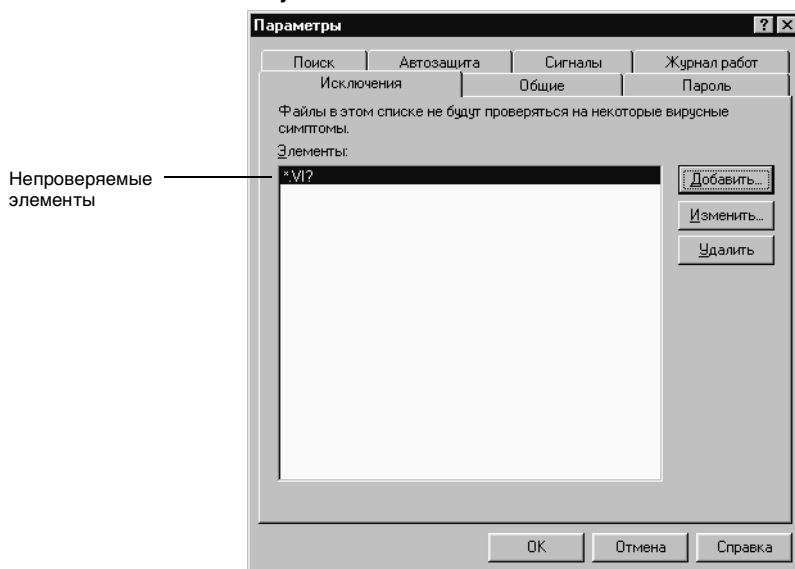
На практике, элементы попадают в список исключений при нажатии кнопки “Исключить” в диалоговом окне “Обнаруженные проблемы” по окончании поиска вирусов. Исключая каждый элемент, помните, что вы тем самым открываете брешь для вирусов.

Осторожно: Не следует изменять стандартный список исключений без особой на причины. В нем указано только расширение резервных копий, которые Norton AntiVirus создает перед исправлением зараженных файлов (см. *“Установка параметров резервирования” на странице 58*).

Как просмотреть список исключений:

- 1 Нажать кнопку “Параметры” в главном окне Norton AntiVirus.
- 2 Открыть вкладку “Исключения”.

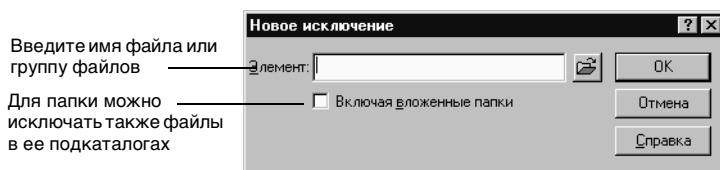
Рисунок 5-6 Список исключений



Как добавить исключение вручную:

- 1 Нажать кнопку “Добавить” во вкладке “Исключения” (рис. 5-6).

Рисунок 5-7 Добавление нового исключения



- 2 В текстовом поле “Элемент” ввести имя файла или группы файлов.
- 3 Если необходимо также исключить файлы в подкаталогах, следует установить флажок “Включая вложенные папки”.
- 4 Нажать ОК.

Как удалить исключение:

- 1 Выбрать файл или группу файлов в списке элементов во вкладке “Исключения” (рис. 5-6).
- 2 Нажать кнопку “Удалить” и затем ОК.

Исключение удаляется из списка, и для данного элемента восстанавливается полная защита от вирусов.

Как изменить существующее исключение:

- 1 Выбрать файл или группу файлов из списка элементов во вкладке “Исключения” (рис. 5-7).
- 2 Нажать кнопку “Изменить” и внести необходимые изменения.
- 3 Нажать ОК.

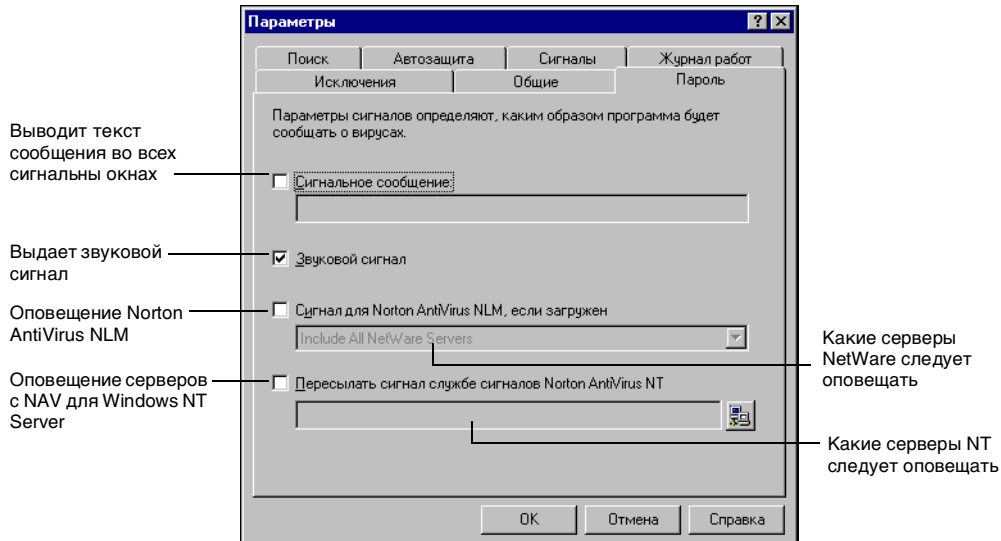
Настройка сигналов

Параметры сигналов Norton AntiVirus определяют внешний вид сообщений, выдаваемых при обнаружении вирусов или при подозрении на вирус. Эти параметры действуют всякий раз, когда Norton AntiVirus выполняет поиск вирусов (ручной, запланированный или как действие автозащиты).

Как настроить выдачу сигналов:

- 1 Выбрать “Параметры” в главном окне Norton AntiVirus.
- 2 Открыть вкладку “Сигналы”.

Рисунок 5-8 Настройка сигналов



- 3 Установить флажок “Сигнальное сообщение”, чтобы добавить сообщение с инструкциями и специальными предупреждениями во все сигнальные окна, выводимые Norton AntiVirus. Затем в нижнем поле набрать текст сообщения.
- 4 Установить флажок “Звуковой сигнал” для звуковой сигнализации.
- 5 Установить флажок “Убрать сигнальное окно после n секунд” для указания интервала, в течение которого сигнальное сообщение будет оставаться на экране. Ввести длительность интервала (от 1 до 99) в текстовом поле секунд.
- 6 Нажать ОК.

Отправка сетевых сигналов

При обнаружении на сетевой рабочей станции вируса или прочего события Norton AntiVirus может посылать сигналы в адрес Norton AntiVirus для NetWare NLM на сервере Novell NetWare. Можно задать конкретный сервер или оповестить все серверы NetWare с загруженными NLM. Что касается сетей с серверами Windows NT, то сигналы могут направляться в адрес серверов, на которых работают программы Norton AntiVirus для Windows NT Server.

Как установить отправку сетевых сигналов:

- 1 Нажать “Параметры” в главном окне Norton AntiVirus.
- 2 Нажать вкладку “Сигналы” (рис. 5-8).
- 3 Для сетей Novell NetWare следует отметить флажок “Сигнал для Norton AntiVirus NLM, если загружен”.
- 4 Выполнить одно из следующих действий:
 - В ниспадающем списке выбрать конкретный сервер NetWare с загруженным Norton AntiVirus NLM.
 - Выбрать в ниспадающем списке все NetWare-серверы. В этом случае Norton AntiVirus будет оповещать все серверы с загруженными NLM.
- 5 Для серверов Windows NT отметить флажок “Пересылать сигнал службе сигналов Norton AntiVirus NT”.
- 6 Ввести имя получателя сообщения либо нажать кнопку обзора и выбрать его в сетевом окружении.
- 7 Нажать ОК.

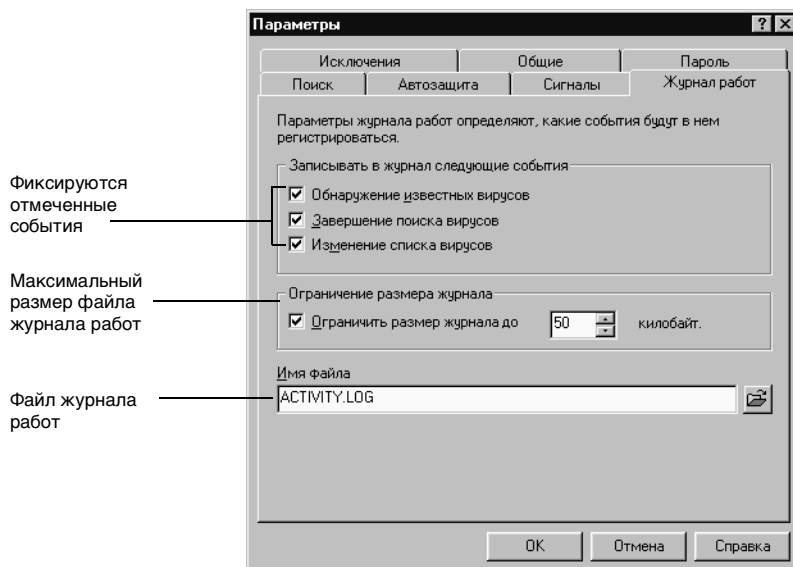
Настройка журнала работ

В журнале работ отражается хронология деятельности Norton AntiVirus на вашем компьютере. Например, по умолчанию Norton AntiVirus настроен на запись всех фактов обнаружения известных вирусов и мер, принятых по отношению к зараженным файлам (были ли они исправлены, удалены, добавлены в список исключений или оставлены без изменений). Можно настроить журнал работ на фиксацию других типов событий (например, обнаружение неизвестных вирусов или изменение в списке вирусов).

Как настроить журнала работ:

- 1 Нажать кнопку “Параметры” в главном окне Norton AntiVirus.
- 2 Открыть вкладку “Журнал”.

Рисунок 5-9 Параметры журнала работ



- 3 В окне группы “Записывать в журнал следующие события” отметьте все типы событий, которые должны заноситься в журнал:
 - **Обнаружение известных вирусов:** запись фактов обнаружения известных вирусов (вирусный датчик автозащиты).
 - **Завершение поиска вирусов:** запись даты и времени окончания поиска вирусов (ручного или планового).
 - **Изменение списка вирусов:** регистрация данных об изменениях в списке вирусов.

- 4 Чтобы ограничить размер файла журнала работ, следует установить флажок “Ограничить размер журнала до” и в соседнем поле ввести нужное значение Кбайт.

По достижении указанного размера файла каждая новая запись в журнале вытесняет самую старую.

- 5 В текстовом поле “Имя файла журнала” ввести путь, в котором будет храниться журнал работ.
- 6 Нажать ОК для сохранения настройки и выхода из диалогового окна.

Установка параметров резервирования

В качестве меры предосторожности, Norton AntiVirus создает резервную копию файла, прежде чем приступить к его исправлению. Для резервных копий зараженных файлов расширением по умолчанию является VIR. Вы можете задать другое расширение или вообще отказаться от создания резервных копий.

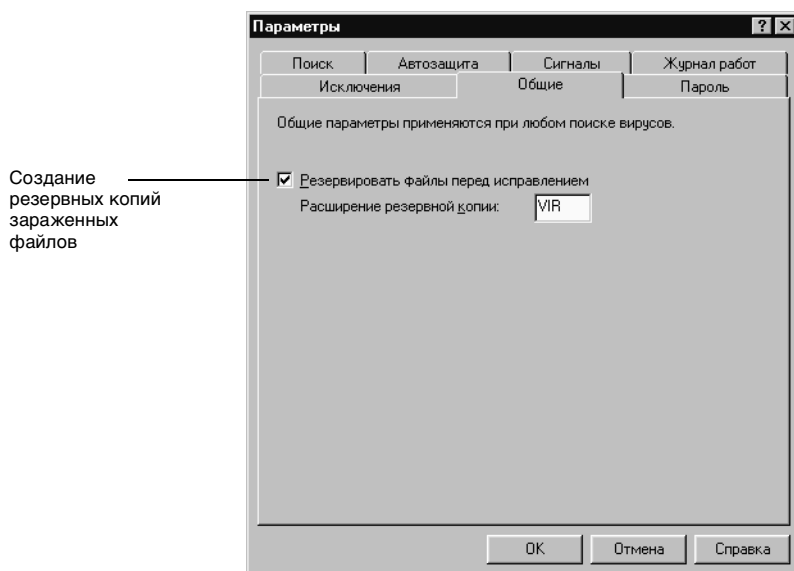
Все файлы с расширением резервных копий автоматически добавляются в список исключений, и поэтому сообщения о них во время поиска вирусов не выдаются. См. также *“Работа с исключениями” на странице 53.*

После успешного исправления файлов их резервные копии следует удалить. Несмотря на то, что зараженные резервные копии невозможно запустить (расширение файла VIR не позволяет это сделать), в них, тем не менее, присутствует вирус.

Как изменить параметры резервирования:

- 1 Нажать “Параметры” в главном окне Norton AntiVirus.
- 2 Открыть вкладку “Общие”.

Рисунок 5-10 Вкладка общих параметров



- 3 Установить флажок “Резервировать файлы перед исправлением”, чтобы Norton AntiVirus создавал копии зараженных файлов перед их исправлением.
- 4 При желании можно ввести другое расширение файла в текстовом поле.
- 5 Нажать ОК.

Настройка автозащиты

Функция автозащиты обеспечивает автоматическую защиту от вирусов следующими методами:

- Поиск вирусов в программах при их выполнении.
- Поиск вирусов на гибких дисках при обращении к ним.
- Блокирование вирусов при копировании или установке файлов в системе.

О том, как выполняется поиск вирусов средствами автозащиты, рассказывается в разделе *“Настройка ручного поиска” на странице 45.*

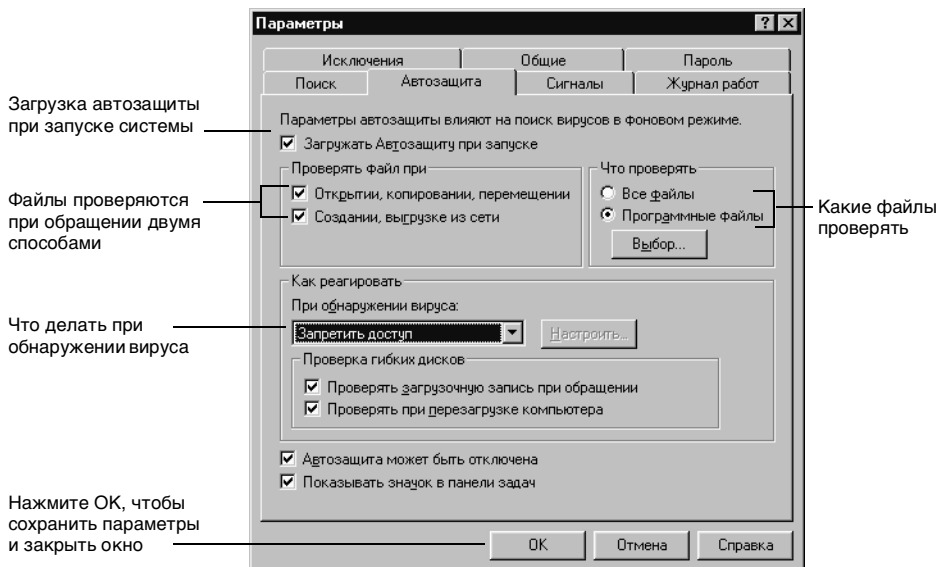
Автозащита программных файлов

Norton AntiVirus может выполнять проверку на вирусы при открытии файла или при запуске программы. Можно указать типы проверяемых файлов и ответные действия при обнаружении вируса.

Как установить автозащиту на программные файлы:

- 1 Нажать кнопку “Параметры” в главном окне Norton AntiVirus.
- 2 Открыть вкладку “Автозащита”.

Рисунок 5-11 Параметры автозащиты



- 3 Установить флажок “Загружать автозащиту при запуске”, чтобы ваш компьютер был защищен от вирусов с момента включения.

Примечание. Снятие этого флажка резко снижает уровень защиты от вирусов.

- 4 Указать, при каких операциях файлы будут проверяться на вирусы, отметив следующие флажки в группе “Проверять файл при”.
- Открытии: файлы проверяются при их открытии. Например, файл будет проверен при копировании его с дискеты.
 - Создании: файлы проверяются при их создании на диске программами установки, при распаковке или получении по электронной почте.

- 5 Выберите один из переключателей в группе “Что проверить”:
 - Все файлы: проверка всех файлов, к которым будет обращение. Сюда относятся и файлы, менее восприимчивые к вирусной инфекции.
 - Программные файлы: проверка файлов, наиболее подверженных действию вирусов — их расширения указаны в списке расширений программных файлов.

Инструкции по работе со списком расширений программных файлов даны в разделе *“Выбор проверяемых файлов” на странице 50.*
- 6 Нажать кнопку ОК, чтобы сохранить настройку и закрыть диалоговое окно или перейти к другим процедурам.

Как определить реакцию программы на обнаружение вируса:

- 1 Нажать кнопку “Параметры” в главном окне Norton AntiVirus.
- 2 Открыть вкладку “Автозащита” (рис. 5-12).
- 3 Выбрать одну из следующих реакций в окне списка “При обнаружении вируса”:
 - Запросить: программа сообщает о найденном вирусе и предоставляет выбор дальнейших действий. Этот режим обеспечивает максимальную гибкость при работе с зараженным файлом.
 - Запретить доступ: при обнаружении известного вируса закрывается доступ к файлу. Результат заносится в журнал работ.
 - Сразу исправить: зараженный файл или загрузочная запись исправляется без предупреждения. Результат заносится в журнал работ.

Имейте в виду, что Norton AntiVirus по умолчанию создает резервные копии зараженных файлов перед их исправлением. См. *“Установка параметров резервирования” на странице 58.*
 - Сразу удалить: зараженный файл стирается с диска без предупреждения. Результат заносится в журнал работ. Этим режимом следует пользоваться осторожно. Файлы, удаляемые средствами Norton AntiVirus, не поддаются восстановлению.
- 4 Установить флажок “Автозащита может быть отключена”, если хотите иметь возможность временно отключать автозащиту нажатием на значок автозащиты в панели задач Windows.
- 5 Установить флажок “Показывать значок в панели задач”, чтобы всегда видеть наличие автозащиты и иметь возможность ее временно отключать и включать.
- 6 Нажать кнопку ОК, чтобы сохранить настройки и закрыть диалоговое окно или перейти к следующей процедуре.

Автозащита гибких дисков

Поскольку загрузочные вирусы чаще всего распространяются через гибкие диски, необходимо проверять каждую дискету перед использованием. Norton AntiVirus позволяет контролировать любые гибкие диски, как используемые для работы, так и случайно оставленные в дисковом диске.

Как установить автозащиту для гибких дисков:

- 1 Нажать кнопку “Параметры” в главном окне Norton AntiVirus.
- 2 Открыть вкладку “Автозащита”.
- 3 Нажать кнопку “Расширенные” на вкладке “Автозащита”.
- 4 В группе “Проверка гибких дисков” (рис. 5-11) указать, при каких условиях Norton AntiVirus должен проверять загрузочные записи дискет:
 - Проверять загрузочную запись при обращении: поиск загрузочных вирусов на каждой дискете, к которой идет обращение (при чтении каталога, копировании файла, записи в файл, запуске файла).
 - Проверять при перезагрузке компьютера: поиск загрузочных вирусов на диске A: при останове машины.
- 5 Нажать ОК для сохранения настроек и закрытия диалогового окна.

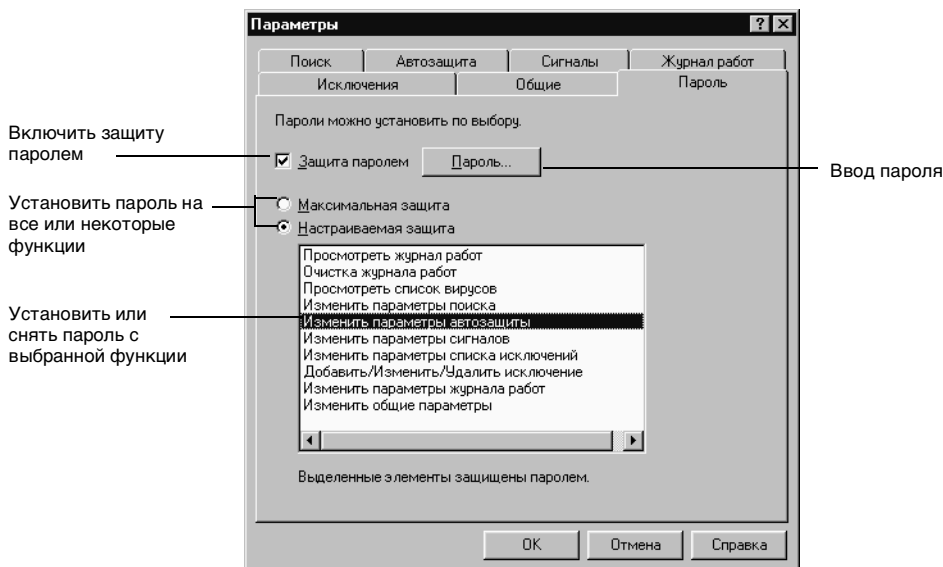
Установка паролей

Парольная защита гарантирует неизменность конфигурации Norton AntiVirus. Пароль можно установить как на отдельные параметры, так и на всю настройку целиком.

Как установить пароли:

- 1 Нажать “Параметры” в главном окне Norton AntiVirus.
- 2 Открыть вкладку “Пароль”.

Рисунок 5-12 Параметры пароля



- 3 Установить флажок “Защита паролем” для активизации этой функции.
- 4 Выполнить одно из следующих действий:
 - Для защиты всех функций Norton AntiVirus — выбрать “Максимальную защиту”.
 - Для защиты только отдельных функций — выбрать “Настраиваемую защиту”, затем в нижнем списке отметить нажатием мыши функции, на которые нужно установить пароль.
- 5 Нажать “Пароль...” и в диалоговом окне “Установка пароля” ввести пароль, который будет использоваться. Пароль применяется один ко всем защищенным функциям.

Пароль может содержать от 1 до 16 символов. Регистр в пароле не учитывается (маленькое “а” соответствует большой “А”). При вводе пароля в целях безопасности символы на экране отображаются звездочками (*).
- 6 Нажать ОК для закрытия окна параметров.

Прежде чем дать разрешение на замену функций, защищенных паролем, Norton AntiVirus будет также запрашивать пароль.

Как изменить пароль:

- 1 Нажать “Параметры” в главном окне Norton AntiVirus.
- 2 Открыть вкладку “Пароль” (рис. 5-12).
- 3 Нажать кнопку “Пароль...”.
- 4 Ввести существующий пароль в текстовом поле “Старый пароль”.
- 5 Ввести новый пароль в текстовом поле “Новый пароль”, затем набрать его снова в текстовом поле “Подтвердите новый пароль”.
- 6 Нажать ОК.

Как снять защиту паролем:

- 1 Нажать “Параметры” в главном окне Norton AntiVirus.
- 2 Открыть вкладку “Пароль” (рис. 5-12).
- 3 Выполнить одно из следующих действий:
 - Для полного отключения защиты паролем — снять флажок “Защита паролем”.
 - Для снятия паролей только с некоторых функций — нажать переключатель “Настраиваемая защита” и поочередно снять выделение нужных пунктов в списке функций.
- 4 Нажать ОК.



О компьютерных вирусах

Наличие правильно настроенной антивирусной программы стало непреложным требованием для надежной и безопасной работы на компьютере. Хотя оценки числа реально распознаваемых компьютерных вирусов даются весьма неодинаковые, тем не менее, можно достаточно уверенно говорить о том, что сейчас их существует около 8000. Эта цифра отражает тот факт, что многие из обнаруженных вирусов имеют различные модификации кода. Автору достаточно изменить в сигнатуре вируса всего лишь один байт, и на свет появится его новая модификация.

Создатели вирусов часто общаются друг с другом по BBS и Internet, обмениваясь идеями, инструментарием и кодами. К счастью, большинство вирусов не выходит за границы этой вирусотворящей общины. Лишь малая часть существующих вирусов вырывается "на свободу", т. е. распространяется по каналам, легко доступным широкой общественности.

Как правило, авторы вирусов не блещут особым талантом программирования, даже в сравнении с рядовыми профессиональными кодировщиками. В результате множества ошибок, часто допускаемых в коде вируса, его действие может оказаться разрушительным для программ или данных, хотя его создатель и не намеревался сделать свой вирус вредоносным.

Как бы то ни было, количество известных вирусов и случаев заражения ими продолжает расти:

- На свободу вырвались уже многие разрушительные вирусы.
- Растущее число типов вирусов и их модификаций представляет угрозу для массы компьютерных пользователей.
- Потенциальный ущерб, как следствие разрушения информации, чрезвычайно высок.

Что такое компьютерные вирусы

Компьютерный вирус — это просто-напросто компьютерная программа, которая, подобно биологическому, ищет для себя среду обитания и, найдя, внедряется в нее. Средой обитания вируса может быть загрузочная область диска (загрузочная запись) или исполнимый файл.

После своего внедрения, или заражения, файла или другого компонента системы, вирус распространяется и на другие окружающие компоненты. Проникновение вируса в общедоступные и массово используемые ресурсы позволяет ему "развернуться" во всю свою мощь. Чем большее пространство успевает захватить вирус, тем выше его жизнеспособность, и тем труднее от него избавиться.

Существует множество заблуждений относительно того, что в действительности могут делать вирусы и чего не могут.

Вирус может заразить...

- Программные файлы; нефайловые области диска, используемые при запуске (загрузочные записи); файлы данных, содержащие макросы
- Диски с данными и диски, используемые для переноса программ
- Компьютер во время приема и отправки файлов через электронные службы
- Файл до его вложения в электронное сообщение

Вирус не может заразить...

- Аппаратные средства, такие как клавиатура и монитор, графические файлы, файлы данных без макросов, не являющиеся исполнимыми компоненты программ
- Диски, защищенные от записи
- Компьютер при чтении сообщений в электронной службе
- Текстовые сообщения электронной почты

За вирусы часто принимают программы типа "троянский конь". Так как они не реплицируются и не распространяются, они не являются вирусами.

“Троянский конь” — это программа, внешне преследующая какую-либо полезную или развлекательную цель. Ее всегда хочется запустить и попробовать. Но, как и троянский конь из античной истории, она, помимо внешней, выполняет еще и скрытую внутри задачу, например: запортировать файлы или заразить компьютер вирусом.

Методы заражения

Вирусы активизируются в момент загрузки (выполнения) зараженной программы или при запуске компьютера с зараженной загрузочной записью. После активизации вирусы начинают распространяться одним из двух методов в зависимости от характера вируса:

- Метод прямого действия
- Резидентный метод

Вирус, обладающий методом прямого действия, активизируется при запуске зараженной программы. Он перехватывает управление системой и, если затем запускаются другие, еще не зараженные, программы, то он их заражает. При закрытии зараженной программы распространение вируса прекращается.

Вирус, заражающий резидентным методом, подобен типичной резидентной программе (TSR), которая после выполнения остается в памяти. Такой вирус при активизации перехватывает управление системой и действует до тех пор, пока память компьютера не будет очищена (путем перезагрузки), даже если все зараженные программы закрыты.

Триггер вируса

Некоторые, хотя и не все, вирусы запрограммированы на включение по истечении произвольного периода инкубации. Как только вирус поселяется в компьютере, он не проявляет себя сразу, а ожидает сигнала на активизацию - определенного события, или триггера. Вот несколько примеров событий, используемых в качестве триггеров для вирусов: определенная дата, счетчик времени (например, 60 минут) с момента запуска зараженной программы или счетчик порядкового номера программных файлов (например, семнадцатый файл). Ряд вирусов активизируется по произвольному триггеру.

Действие вируса

Подобно тому, как огнестрельное оружие при нажатии на курок производит выстрел, при возникновении триггера вирус начинает выполнять запрограммированное в нем действие. Следует иметь в виду, что некоторые вирусы не дожидаются триггера, а начинают действовать сразу после активизации.

Действие некоторых вирусов является преднамеренно вредоносным: например, форматирование жесткого диска или разрушение файлов. Другие же вирусы достаточно безобидны по своему действию и не делают ничего, кроме вывода какого-либо сообщения на экран. Например, вирус Windows 95 Воza в 30-й день каждого месяца (триггер) выводит на экран длинное сообщение, начинающееся со слов "The taste of fame just got tastier!" (действие).

Вирусы стараются скрыть от пользователя свое присутствие, даже после того, как что-то натворят. Например, вирус Ripper вносит изменения в произвольные файлы на диске, но делает это чрезвычайно медленно, чтобы не привлечь к себе внимание.

Объекты заражения

По объектам заражения вирусы подразделяются на следующие категории:

- Программные вирусы заражают файлы программ, имеющие обычно расширения .COM, .EXE, .SYS, .DLL, .OVL или .SCR. Первоочередными объектами заражения являются стандартные DOS-программы с расширениями файлов .COM и .EXE. Программные файлы служат наиболее легкой мишенью для вирусов, потому что они наиболее широко распространены и имеют относительно простую структуру для внедрения вирусов.
- Загрузочные вирусы заражают нефайловые (системные) области жестких и гибких дисков, наличие которых позволяет вирусам легко переноситься с одного компьютера на другой. Заражение загрузочными вирусами происходит более часто, чем программными.
- Макровирусы поражают файлы данных, содержащие макросы. Они появились сравнительно недавно и представляют серьезную угрозу для массового пользователя. Наиболее подвержены нападению макровирусов документы и шаблоны Microsoft Word вследствие их частой передачи через различные электронные службы и Internet.

Теперь рассмотрим типы вирусов, использующие различные методы заражения своих объектов.

Программные вирусы

Как любая программа, программный вирус должен быть написан для определенной операционной системы. Преобладающее множество вирусов создано для работы под DOS, но уже существуют вирусы и для Windows 3.x, Windows 95 и даже UNIX.

Все версии Windows совместимы с DOS и потому с различной долей вероятности могут быть заражены DOS-вирусами. В следующей таблице описывается поведение программных вирусов для DOS в различных версиях Windows.

Версия Windows	Поведение вируса
Windows 3.x	Большинство вирусов для DOS прекрасно чувствуют себя в этой среде, потому что Windows 3.x использует DOS для всех своих базовых функций.
Windows 95	Windows 95 обеспечивает полную совместимость почти со всеми программами старого типа, а потому и с программными вирусами. При активизации загрузочного вируса резидентного действия Windows 95 может выводить предупреждающие сообщения во время запуска, и работа системы обычно в целом замедляется.
Windows NT	Windows NT обладает наименьшей совместимостью с DOS, но, тем не менее, и в этой среде могут существовать программные вирусы. Вирусы резидентного действия в Windows NT могут распространяться при запуске зараженной программы в сеансе DOS и перестают быть активными вместе с закрытием сеанса DOS. Благодаря существующей в NT защите на уровне файлов программные вирусы не могут заразить или разрушить файлы, к которым у пользователя нет доступа.

Загрузочные вирусы

Любой диск, будь то жесткий или гибкий, имеет загрузочные записи, независимо от наличия на нем операционной системы. Для заражения загрузочным вирусом диск не обязательно должен быть загрузочным (системным), такой вирус может спокойно проникнуть и на диск, содержащий только данные. Чаще всего компьютер заражается загрузочным вирусом при перезагрузке с зараженной дискеты, вольно или невольно оставленной в флоппи-дисковом, даже если дискета не является загрузочной.

В отличие от программных, почти все загрузочные вирусы способны заразить DOS, Windows 3.x, Windows 95, Windows NT и даже Novell Netware. Для своего распространения и активизации эти вирусы используют внутренние средства компьютера (а не операционной системы).

Многие загрузочные вирусы предполагают, что на жестком диске имеется обычная файловая система DOS. Но файловая система может быть и другого типа, если на диске установлена операционная система, отличная от DOS или Windows 3.x. Например, в Windows NT вместо типичной для DOS файловой системы FAT может работать файловая система NTFS. Если вирус встретит на своем пути систему NTFS, он все равно с успехом поселится на компьютере, но при этом может случайно повредить некоторые файлы и загрузочные записи (в системной области диска). Результат будет довольно плачевным — NT перестанет загружаться, и потребуются переустановка всей системы.

Другой интересной особенностью системы Windows NT является то, что она в самом начале процедуры запуска деактивирует любой загрузочный вирус и

продолжает с успехом загружаться. Для вируса это означает, что он может поселиться на компьютере с Windows NT, но, пока система работает, его дальнейшее распространение по ней невозможно. Не следует однако думать, что вирус совершенно безопасен в этой среде. При каждом запуске зараженного компьютера вирус активизируется и, пока Windows NT не загружена, он может успеть получить команду своего триггера и выполнить заложенное в нем действие. Например, 6-го марта вирус Stoned.Michelangelo записывает произвольные байты в каждый цилиндр жесткого диска, разрушая таким образом данных. В результате, за считанные доли секунды, в течение которых выполняется процедура начальной загрузки, критические системные области диска окажутся заперченными. После того, как в таком вирусе сработал триггер, и он начал свое "грязное дело", остановить его практически невозможно.

Макровирусы

Многие старые приложения имели примитивный механизм макрокоманд для записи и воспроизведения последовательности действий внутри приложения. Записанную последовательность действий можно было активизировать путем нажатия на присвоенную макросу комбинацию клавиш.

Прикладные программы нового поколения обладают более сложными системами макрокоманд. Теперь внутри текстового редактора или электронной таблицы можно написать целую макропрограммы, которая прикрепляется непосредственно к файлу документа или электронной таблицы. Возможность переносить вместе с файлом данных один или несколько макросов чрезвычайно привлекательна. Но она также привлекательна и для создателей макровирусов.

Типичный процесс распространения макровируса начинается с того, что зараженный документ или электронная таблица открывается в соответствующем приложении, и при этом также загружаются хранящиеся в файле макросы. При определенных параметрах макросов приложение может сразу же начать их выполнение. А макровирусы только этого и ждут, чтобы захватить управление системой макросов приложения.

После загрузки и выполнения макровирус ждет, когда начнется редактирование файла. Он внедряет свою копию в новый документ в виде макропрограммы, затем позволяет приложению нормально сохранить документ. Так он поселяется в новом файле, причем делает это очень аккуратно, чтобы пользователь ничего не заметил. При открытии этого нового файла на другом компьютере вся процедура повторится: вирус снова загрузится, будет выполнен приложением и найдет очередной объект для заражения.

Можно сказать, что приложение служит для макровируса своего рода операционной системой. Любой макровирус может в принципе поселиться на любой платформе, где используется приложение. Например, макровирус для

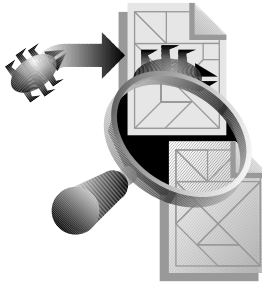
Microsoft Word одинаково легко заразит документы в среде Windows 3.x, Windows 95, Window NT и Macintosh.

Технологии вирусов

Программные и загрузочные вирусы также подразделяются на категории в зависимости от технологий, используемых ими для распространения и маскировки. Эти категории рассмотрены ниже.

Скрытые (stealth) вирусы

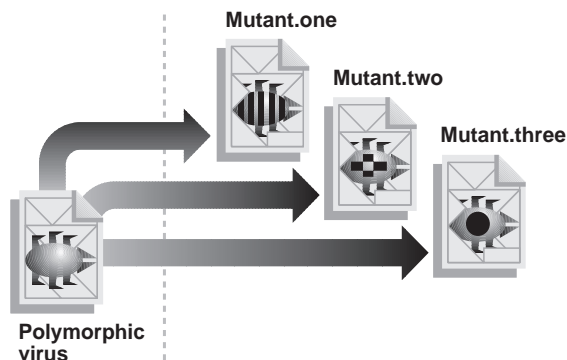
Stealth-вирусы активно стараются замаскировать себя, чтобы не быть обнаруженными. Для этого они используют такие технологии, как перехват операций чтения диска с целью подмены зараженной копии объекта незараженной (скрывающие чтение), изменение данных каталога для зараженных программных файлов (скрывающие размер) или оба этих метода..



Например, вирус Whale является скрывающим размер. Он заражает EXE-файлы и изменяет для них данные каталога, когда другая программа пытается их прочитать. К зараженному файлу вирус Whale добавляет 9216 байта, а так как изменение размера файла - один из признаков заражения, то вирус, чтобы скрыть свое присутствие, уменьшает на такое же число (9216) значение размера файла в соответствующей записи каталога.

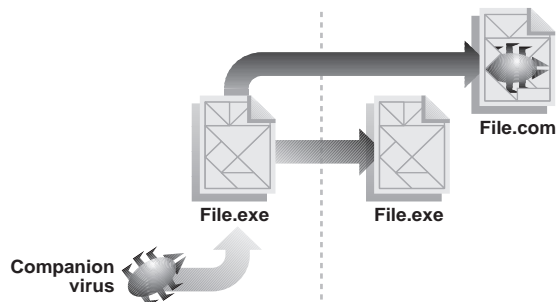
Полиморфные вирусы

Многие простые вирусы прикрепляют к зараженному файлу свою копию. Так как код такого вируса (сигнатура) всегда одинаков, антивирусная программа может его легко обнаружить и удалить. Чтобы избежать этого, полиморфные вирусы используют несколько другую технологию заражения. Они шифруют свой код в теле программы, причем делают это по-разному в каждом новом зараженном файле, что значительно затрудняет обнаружение вируса.



Вирусы-компаньоны

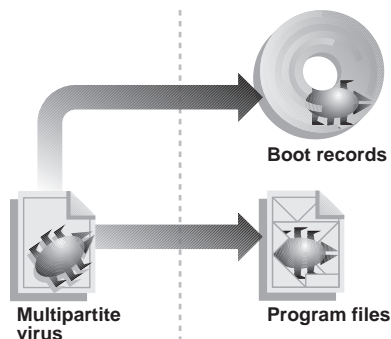
Вирусы-компаньоны являются исключением из того правила, что вирус должен прикрепляться к файлу. Вместо этого вирус-компаньон создает новый файл и пытается заставить DOS выполнять его, а не тот файл, который обычно используется для запуска программы.



Технологии вирусов-компаньонов бывают различны. Некоторые создают COM-файл с таким же именем, как у файла EXE. Например, вирус может создать файл CHKDSK.COM и поместить его в том же каталоге, где находится CHKDSK.EXE. Когда DOS видит два одинаковых имени файла, у одного из которых расширение EXE, а у другого — COM, то в первую очередь запускается файл COM.

Многоцелевые вирусы

Многоцелевыми называются вирусы, заражающие как программы, так и загрузочные области диска. Например, при открытии текстового редактора, зараженного вирусом Tequila, вирус активизируется и заражает загрузочную запись жесткого диска. Затем, при следующем запуске компьютера вирус снова активизируется и начинает заражать все используемые программы, открываемые с жестких или гибких дисков.



Обновление вирусной базы

Norton AntiVirus умеет предотвращать любые попытки вирусов себя замаскировать и распознает их на основе известных сигнатур. Сигнатуры хранятся в файлах описания вирусов Norton AntiVirus. Эта программа может распознавать ровно столько вирусов, сколько хранится в имеющихся файлах описания вирусов. Чем более свежие используются файлы описания вирусов, тем более надежна ваша защита.

Рекомендуется регулярно обновлять файлы описания вирусов, новые версии которых распространяются фирмой Symantec бесплатно каждый месяц. Различные способы обновления этих файлов объясняются в главе 4, *“Как защититься от новых вирусов”*.

Новые компьютерные вирусы появляются с невероятной быстротой. Советуем обновлять файлы описания вирусов не реже, чем раз в месяц.

Аварийное восстановление

Горячая линия

Группа Norton AntiVirus в корпорации Symantec занимается вопросами защиты от компьютерных вирусов. В ней работает специальная “горячая” телефонная линия для оказания помощи при заражении вирусами, независимо от используемых вами антивирусных программ. Для получения помощи или просто ответов на вопросы о вирусах звоните по следующим номерам телефонов:

(541) 984-7879

На ваши звонки ответят специалисты высшей квалификации. Звонить можно с 7:00 до 16:00 (по тихоокеанскому времени), с понедельника по пятницу, кроме праздников.

Если невозможно запустить компьютер

Загрузочные вирусы иногда полностью препятствуют запуску компьютера. В этом случае вы лишаетесь возможности воспользоваться программой Norton AntiVirus для диагностики и устранения проблем.

В этой ситуации вам поможет бесплатно предоставляемый фирмой Symantec вирусный сканнер для MS-DOS. Эту программу (NAVSCAN.EXE) можно получить по электронным каналам, описанным в разделе *“Где можно найти файлы описания вирусов” на странице 40.*

Совет. На всякий случай советуем скопировать программу NAVSCAN при очередном обновлении файлов описания вирусов по электронным каналам связи.

Чтобы использовать NAVSCAN в аварийной ситуации, необходимо загрузить компьютер с помощью системного диска MS-DOS, а не Windows NT. Инструкции по использованию этой программы содержатся в прилагаемом к ней файле README.TXT.

Ключи командной строки

NAVWNT.EXE, программа поиска вирусов под Windows NT, может запускаться с ключами командной строки, которые перекрывают сохраненные параметры конфигурации. При использовании ключей командной строки Norton AntiVirus запускается в свернутом виде, но, как только будет найден вирус, программа откроется на экране.

Некоторые ключи используются сами по себе, другие сопровождаются параметром, например, знаками "+" или "-". В командной строке можно использовать несколько ключей и параметров. Символ () означает, что из ряда параметров можно использовать только один. Указанные в примере скобки в командной строке не вводятся. При запуске NAVWNT с ключами используется следующий синтаксис:

NAVWNT [путь] [параметры]

путь	Проверяются любые диск, папка, файл или их сочетание. Несколько элементов должны разделяться пробелами. При вводе пути для группы файлов можно применять шаблоны (напр., NAVWNT A: C:\MYDIR*.EXE).
/A	Просматриваются все диски, кроме A: и B:. Сетевые диски проверяются, если в диалоговом окне "Расширенные параметры поиска" задано "Разрешить поиск в сети".
/L	Проверяются все локальные диски, кроме A: и B:.
/S [+ -]	Включает (+) или отключает (-) поиск в каталогах любых папок, указанных в пути. По умолчанию используется S+.
/B [+ -]	Включает (+) или отключает (-) проверку загрузочных записей; например, NAVWNT A: /B+ или NAVWNT A: /B- (по умолчанию этот параметр включен).
/BOOT	Проверяются только загрузочные записи указанных дисков.

Примеры синтаксиса командной строки:

- Чтобы проверить все файлы .EXE в каталоге WIN32APP и его подкаталогах, введите:
`NAVWNT C:\WIN32APP*.EXE`
- Для проверки всех файлов .EXE только в каталоге WIN32APP введите:
`NAVWNT C:\WIN32APP*.EXE /S-`
- Для проверки папки и подкаталогов с длинными именами файлов (LFN) используйте двойные кавычки:
`NAVWNT "C:\Program Files"`
- Для проверки всего диска C: и одного каталога на другом диске введите:
`NAVWNT C: D:\NEWFILES`
- Для проверки папки PROGRAMS на сетевом диске P: без проверки подкаталогов введите:
`NAVWNT P:\PROGRAMS /S-`
- Для проверки только загрузочных записей дисков C: и A: введите:
`NAVWNT C: A: /BOOT`
- Чтобы использовать службу Windows NT Scheduler Service для автоматического запуска поиска вирусов на всех локальных дисках (кроме A: и B:) в 17:30 по рабочим дням, нужно ввести следующую команду одной строкой.
Применительно к Windows NT 4.0:
`at 17:30 /interactive /every:M,T,W,Th,F
"c:\Program Files\NAVNT\NAVWNT" /L`
Применительно к Windows NT 3.51:
`at 17:30 /interactive /every:M,T,W,Th,F
"c:\Win32app\NAVNT\NAVWNT" /L`

Параметр `/interactive` необходим при планировании запуска Norton AntiVirus. Обратитесь к документации по Windows NT для получения подробной информации об использовании службы Scheduler Service.

С Л О В А Р Ь Т Е Р М И Н О В

вирус	Специально разработанная саморазмножающаяся программа, предназначенная для несанкционированного вмешательства в работу компьютера.
вложенная папка	Папка внутри другой папки.
выгрузить	Скопировать файл с одного компьютера на другой по модему. Чаще всего так говорят о приеме файлов с электронной доски объявлений (BBS).
главная загрузочная запись	Первый физический сектор жесткого диска. Он содержит главную программу начальной загрузки и информацию о разделах жесткого диска.
главная программа начальной загрузки	Программа, служащая для запуска программы начальной загрузки активного раздела жесткого диска.
загрузить	Запустить компьютер, либо загрузить или выполнить приложение.
загрузочная запись	Первый физический сектор дискеты или первый логический сектор раздела жесткого диска. В нем описана архитектура диска (например, размер сектора, кластера и другие характеристики). Там же хранится программа начальной загрузки.
загрузочный вирус	Вирус, заражающий программу начальной загрузки — как жесткого, так и гибкого диска — и (или) главную загрузочную запись жесткого диска. Загрузочный вирус попадает в память до загрузки операционной системы, перехватывает управление компьютером и заражает все диски, с которыми вы работаете.
загрузочный диск	Диск, содержащий операционную систему, необходимую для запуска (загрузки) компьютера.
запуск	См. загрузить.
зараженный файл	Файл, содержащий вирус.
защищенный от записи диск	Диск, запись на который невозможна. Диски, защищенные от записи, защищены и от заражения вирусами. Чтобы защитить от записи 3.5-дюймовую дискету, передвиньте ползунок на обратной стороне так, чтобы открылось сквозное отверстие.
известный вирус	Вирус, который Norton AntiVirus способен обнаружить и идентифицировать по имени.

исключение	Условие или процесс, которые, по вашему указанию, будут игнорироваться программой Norton AntiVirus по отношению к определенному файлу. Например, можно настроить программу так, чтобы она не реагировала на программу DOS FORMAT при форматировании гибких дисков.
исполнимый файл	Файл, содержащий программу, которая может быть выполнена. Исполнимые файлы обычно имеют расширения .COM, .EXE, .OVR, .OVL, .DRV, .BIN или .SYS.
исправление	Удаление вируса и восстановление исходного состояния файла, которое он имел до заражения.
каталог	См. папка.
ключ командной строки	Служит для установки параметров программы. Параметры можно задавать в командной строке DOS или с помощью команды "Выполнить..." в Windows.
макровирус	Вирус, заражающий файлы документов. Обычно макровирус активизируется при открытии, сохранении или закрытии документа и затем проникает в другие документы. Макросы — это небольшие программы, встроенные внутрь документа и служащие для автоматизации различных процедур его обработки.
многоцелевой вирус	Вирус, способный заражать как программные файлы, так и загрузочные записи.
неизвестный вирус	Вирус, описание которого отсутствует в программе Norton AntiVirus. См. также описания вирусов.
ОЗУ	См. оперативная память.
оперативная память	Рабочая память компьютера (ОЗУ или RAM), от объема которой зависят размер и число одновременно выполняемых программ и количество одновременно обрабатываемых данных.
операционная система	Главная управляющая программа, загружаемая в память при запуске (загрузке) компьютера. Она контролирует и управляет всеми процессами и программами в компьютере.
описания вирусов	Информация о вирусах, позволяющая Norton AntiVirus обнаруживать конкретные вирусы и предупреждать вас об их присутствии.
панель задач	Элемент рабочего стола, предоставляющий доступ к меню "Пуск" и другим программам. Значки автозащиты и планировщика на панели задач напоминают о том, что эти программы активны.

папка	Логический элемент диска, предназначенный для хранения информации о файлах. Папки упрощают организацию файлов на диске. Другое название — каталог.
перезагрузка	Перезапуск компьютера. <i>См. также</i> теплая загрузка и холодная загрузка.
подкаталог	<i>См.</i> вложенная папка.
поиск вирусов	Основная операция, выполняемая программой Norton AntiVirus с целью обнаружения вирусов.
полиморфный вирус	Вирус, изменяющий собственные сегменты кода для того, чтобы “выглядеть” по-другому в каждом новом зараженном файле. Обнаружить такой вирус нелегко.
приложение	<i>См.</i> программа.
программа	Исполнимый файл (или группа файлов), созданный для выполнения определенной задачи: например, для обработки текстов или создания электронной таблицы.
программа начальной загрузки	Программа, выполняющая загрузку операционной системы.
программный вирус	Вирус, заражающий выполняемые программные файлы, например: .COM, .EXE, .OVL, .DRV (драйвер) и .SYS (драйвер устройства).
путь	информация о размещении файла или папки на диске. Например, если файл с именем QTR1.DOC хранится в папке OFFICE на диске C:, то путь к нему: C:\OFFICE\QTR1.DOC.
разносчик	Программа, служащая для установки вируса на компьютер. Разносчик — это не вирус, а “троянский конь”. <i>См. также</i> троянский конь.
резидентная программа	Программа, загружаемая в ОЗУ и остающаяся там после выполнения с тем, чтобы ее можно было активизировать снова в любой момент. Резидентные программы удаляются из памяти при выключении компьютера.
сжатый файл	Файл или группа файлов, сжатые в один с помощью программы-архиватора (например, PKZIP или ARJ).
системный файл	Файл, являющийся компонентом операционной системы.
системный диск	<i>См.</i> загрузочный диск.

скрытый (stealth) вирус

Вирус, активно пытающийся скрыть свое присутствие от обнаружения, или защищающийся от попыток его анализа и удаления.

таблица разделов

Таблица в главной загрузочной записи жесткого диска, содержащая информацию о его структуре, например: размер и расположение разделов, тип ОС в каждом из них и какой из разделов является загрузочным (активным).

теплая загрузка

Перезапуск компьютера нажатием Ctrl + Alt + Del или выполнением команды “Завершить работу” с последующей перезагрузкой. Некоторые вирусы умеют распознавать данную команду и имитируют теплую загрузку, что позволяет им оставаться в памяти и по ее завершении. *См. также* холодная загрузка.

только для чтения

Так говорят о диске или файле, который можно считывать, но нельзя в него записывать или удалять на нем данные.

троянский конь

Программа, которая на вид кажется полезной или интересной (например, игра), а, на самом деле, скрытым образом наносит вред компьютеру: например, разрушает или удаляет файлы. “Троянские кони” — это не вирусы, т. к. они не способны размножаться.

холодная загрузка

Запуск компьютера путем выключения и включения питания. При холодной загрузке оперативная память компьютера очищается, что приводит к уничтожению всех вирусов, которые могли там находиться. *См. также* теплая загрузка.

файл данных

Файл, создаваемый или связанный с приложением и не содержащий исполняемого кода (машинных команд).

электронная доска объявлений

Система интерактивного доступа (BBS), обеспечивающая такие услуги, как обмен сообщениями, электронная почта и передача файлов. Связь пользователей с BBS осуществляется с помощью модема.

BBS

См. электронная доска объявлений.

CMOS

Сокращенное название технологии “Комплементарный Металл-Оксид-Полупроводник”. Питается от отдельной батареи микросхема в компьютерах моделей 80286 и выше, где хранятся основные данные об аппаратной конфигурации системы.

COM-файл

См. исполнимый файл.

EXE-файл

См. исполнимый файл.

LHA-файл

Один или несколько файлов, сжатых в один с помощью архиватора LHARC.

TSR

См. резидентная программа.

ZIP-файл

Файл или несколько файлов, сжатые в один с помощью программы PKZIP (обычно имеют расширение .ZIP).

ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ

A

America Online, обновление описаний
вирусов 40

C

CompuServe, обновление описаний
вирусов 41

I

Internet
Netscape и другие браузеры 27
настройка автозащиты 26
Internet, обновление описаний вирусов 41

L

LiveUpdate 38

N

Norton AntiVirus
выход 14
запуск 14
и Netscape 27
и браузеры Internet 27
технологии защиты от вирусов 4 – 6
Norton AntiVirus для Windows
удаление установки xii
установка x

S

stealth-вирусы
описание 71
Symantec BBS, обновление описаний
вирусов 40

W

Windows NT
меры безопасности 9
риск заражения 7 – 9

Z

аварийное восстановление 75
аварийный загрузочный диск NAV
См. тж. аварийные диски

автозащита 23 – 24
автоматическая загрузка 24
включение 23
временное отключение 23, 24
выключение 23
гибкие диски 62
настройка 59 – 62
настройка для Internet 26
описание 5
программные файлы 60 – 61
сигнал о вирусе 34
устранение обнаруженных
вирусов 33 – 34

B

вирус, компьютерный. *см.* компьютерный
вирус
вирусный датчик автозащиты
описание 5
вирусный сканер NAV для DOS 75
вирусный сканер MS-DOS 11
вирусы
действие 67
источники 3
механизмы заражения 3
неудачное исправление
загрузочная запись 34 – 35
зараженный файл 34 – 35
обнаружение 29
объекты заражения 68
описание 66
повторное заражение после
удаления 36
просмотр названий и
характеристик 43 – 44
триггеры 67
вирусы-компаньоны
описание 72
вкладка Автозащита 60
вкладка Исключения 54
вкладка Пароли 63
вкладка Сигналы 55, 56

включение

автозащита 23

автоматическая загрузка

автозащиты 24

звуковые сигналы 22, 39

планирование поиска вирусов 22, 39

восстановление. *См.* исправление

вспышки вирусов

аварийное восстановление 75

источники 3

механизмы заражения 3

профилактика 13

вызов контекстной справки 16 – 17

выключение автозащиты 23

выход из Norton AntiVirus 14

Г

гибкие диски

ежемесячное обновление описаний

вирусов 42

наблюдение за вирусами 62

поиск вирусов 17

главная загрузочная запись

поиск вирусов

вручную 46

Д

действие вируса 67

диск описания вирусов. *см.* диск описания

вирусов NAV

диски

поиск вирусов 17

см. тж. жесткие диски, гибкие диски

добавление

исключений в список 54

расширения программных файлов 52

Ж

журнал работ

настройка 57 – 58

просмотр всех записей 25

файлы требующие замены 34

фильтрация записей 26

журнал работ, просмотр 25 – 26

З

загрузка

автоматическая автозащиты 24

загрузочные вирусы

механизм заражения 69

описание 44

поиск на гибких дисках 62

просмотр списка 44

загрузочные записи

запрет доступа 19

исправление зараженных

автоматическое 48

неудачное 34

неудачное исправление 35

обход поиска вирусов 19

поиск вирусов

вручную 46

загрузочный диск. *См.* аварийный

загрузочный диск NAV

заккрытие

журнал работ 25

запрет доступа к зараженным

программным файлам 61

запуск компьютера

с дискеты

проверка на вирусы 62

заражение. *см.* вспышки вирусов

зараженные файлы и загрузочные записи

удаление 34, 48

удаление вирусов из них 34, 36

зараженные файлы. *см.* файлы

защита

автоматическая ix

звуковой сигнал, включение 56

звуковые сигналы, включение 22, 39

И

известные вирусы 4

просмотр записей в журнале работ 25

см. тж. неизвестные вирусы; вирусы

список 43

изменение

список исключений 55

текст сообщения в сигнале 55

исключение

расширения программных файлов 52

исключение подкаталогов из поиска 54

исключение файлов

обнаружение известных вирусов 48

исключения

описание 53

удаление и изменение 55

исправление файлов и загрузочных записей
 автоматическое
 поиск вручную 48
 программные файлы 61
исправление файлов и загрузочных записей
 сбой выполнения 36

К

Как
 пункт меню справки 16
ключи командной строки 77 – 78
кнопка Вакцинировать. *см.* разворот
 передней обложки
кнопка Исключить. *см.* разворот передней
 обложки
кнопка Удалить. *см.* разворот передней
 обложки
кнопки команд 32 – 33
 см. тж. окно обнаруженных проблем
компьютерный вирус
 горячая линия 75
 двойная загрузка ОС 11
 описание 2
 профилактика 13
 процедуры поиска 17 – 18
 типы 7
 цикл жизни 2 – 3
компьютеры
 защита от вирусов 1
 меры безопасности 9
контекстная справка, вызов 16 – 17

Л

лечащий модуль 30
 автоматическое устранение вирусов 29
 ручное устранение вирусов 29

М

макровирусы
 описание 7, 70
меры безопасности, Windows NT 9
методы обнаружения, вирусы 3
многоцелевые вирусы
 описание 44, 73
 просмотр списка 44

Н

настройка
 автозащита
 программные файлы 61
журнал работ 57 – 58
параметры ручного поиска 48 – 49
расширение резервной копии 58
реакция на сигналы 47 – 48
сигналы 55 – 56
список исключений 53
немедленное извещение о вирусах 32

О

о программе Norton AntiVirus *ix*
обнаружение вирусов
 автозащита 29
 поиск вручную 29
 поиск при запуске ПК 29
обновление, описания вирусов 4, 5, 39
окно добавления исключения 54
окно добавления события 21
окно обнаруженных проблем 32
окно параметров автозащиты 60
окно параметров журнала работ 57
окно параметров исключений 54
окно параметров сигналов 55
окно расширений программных файлов 52
окно расширенных параметров поиска 49
окно списка вирусов 43
окно установки пароля 63
окно фильтра журнала работ 26
описания вирусов
 обновление 37 – 42

П

память
 поиск вирусов
 вручную 46
параметры резервной копии 58 – 59
параметры, справка 17
пароль
 смена 64
парольная защита
 полная 63
 снятие 64
 установка 62 – 64
 частичная 63

печать

- журнал работ 25
- список вирусов 44

планирование автоматического поиска

- 20 – 23

планировщик

- автоматический поиск вирусов 21
- вызов 20

планировщик программ (пункт меню Пуск в Windows)

- 20, 38

поиск вирусов

- автозащита 5
- автоматический 59 – 62
- запланированный 4
- исключение подкаталогов 54
- настройка

- расширения программных файлов 51 – 53

- планирование 20
- сетевые диски 50

поиск вирусов вручную

- описание 4

поиск названий вирусов 44

поиск при запуске

- устранение обнаруженных вирусов 33 – 36

полиморфные вирусы

- описание 44, 72
- просмотр списка 44

попытки устранения, неуспешные 75

права доступа

- загрузочная запись 10
- папки 10
- файлы 10

программные вирусы

- механизм заражения 68
- описание 43, 68
- просмотр списка 43

программные расширения. см. расширения

- программных файлов

программные файлы

- включение поиска вирусов 47
- сбой выполнения после исправления 36
- только проверка 61
- удаление вирусов 61

просмотр

- журнал работ 25 – 26
- плановый поиск 21
- список вирусов 43 – 44
- список исключений 54

профилактика вирусов 13

Р

расширение резервной копии

- настройка 58

расширения программных файлов

- включение в поиск 47
- включение в поиск вирусов 51 – 53
- просмотр текущих 51 – 52
- сброс по умолчанию 53

ручной поиск вирусов

- настройка 45 – 48
- описание 4

С

сетевые диски

- ограничения при поиске вирусов 50

сетевые сигналы

- настройка параметров 56
- отправка в NLM Norton AntiVirus для NetWare 56

сжатые файлы

- поиск вирусов вручную 46
- удаление вирусов 35

сигнал о вирусе 34

сигналы

- автозащита 6, 32 – 34
- включение звука 56
- настройка 55 – 56
- настройка реакции 47 – 48, 61
- о вирусе 34
- отправка по сетям Novell NetWare 56
- реакция в ответ
- методы удаления вирусов 32 – 36
- ситуации для вывода 33

сигнатуры вирусов 4, 5

скрывающиеся вирусы

- описание 71

скрытые вирусы

- описание 44
- просмотр списка 44

словарь терминов 79 – 83

список вирусов
 изменение 26
 обновление. См. т.ж. файл описания
 вирусов, обновление 37
 просмотр и печать 43 – 44
 список исключений 53
 добавление 54
 просмотр 54
 справка 15 – 17
 во время установки х
 значок знака вопроса 17
 Как
 пункт меню справки 16
 контекстная 16 – 17
 Стол справок
 пункт меню справки 16
 Что это такое?
 пункт меню справки 16
 справка, автозащита 15 – 17
 Стол справок пункт меню справки 16

Т

типичные проблемы
 методы решения 36
 требования к системе х
 триггер вируса 67

У

удаление
 вирусы
 сжатые файлы 35
 файлы и загрузочные записи 34,
 36
 исключения 55
 расширения программных файлов 52
 файлы
 автоматически 48
 в ответ на сигнал 34
 невосстановимые 35
 удаление установки хii
 установка
 Norton AntiVirus х
 вопросы хi
 требования к системе х
 удаление установки хii
 файлы описания вирусов, новые 42
 устранение вирусной инфекции
 обзор 3

Ф

файлы
 выбор для поиска вирусов 51
 добавление в список исключений 54
 неудачное исправление 35
 повторное заражение удаленными
 вирусами 36
 резервные копии 58 – 59
 типы заражаемые вирусами 50
 требующие замены, поиск в
 журнале 34
 удаление вирусов из них 34, 36
 удаление зараженных 34, 48
 файлы описания вирусов
 обновление 41
 причины для обновления 4, 5
 фильтрация записей журнала работ 25, 26

Ц

цикл жизни вируса 2 – 3

Ч

частые вирусы
 описание 43
 просмотр списка 43
 Что это такое? пункт меню справки 16

