# F-Secure Anti-Virus 2013

# Содержание


## Глава 1: Установка.....5

Перед первой установкой.....6
Первая установка продукта.....6
Установка и обновление приложений.....6
Справка и поддержка.....7

## Глава 2: Начало работы.....9

Использование автоматического обновления.....10
Проверка состояния обновлений.....10
Изменение параметров подключения к Интернету.....10
Проверьте состояние сети защиты в реальном времени.....11
Как узнать результаты работы программы.....11
Просмотр истории уведомлений.....11
Изменение настроек уведомлений.....11
Сеть защиты в реальном времени.....12
Что такое сеть защиты в реальном времени.....12
Преимущества сети защиты в реальном времени.....12
Тип отправляемых данных.....13
Охрана конфиденциальности.....14
Активное участие в Сети защиты в реальном времени.....14
Вопросы по поводу сети защиты в реальном времени.....15
Как узнать, действительна ли подписка.....15
Центр действий.....15
Активация подписки.....16

## Глава 3: Введение.....17

Просмотр общего статуса защиты.....18
Просмотр статистики продукта.....18
Работа с обновлениями продукта.....19
Просмотр версий баз данных.....19
Изменение настроек мобильной широкополосной связи.....19
Что такое вирусы и другие вредоносные программы.....20
Вирусы.....20
Шпионские программы.....21
Наборы сторонних средств полного доступа.....21
Подозрительные программы.....21

**Глава 4: Защита компьютера от вредоносных программ.....23**
Как проверить компьютер.....24
Автоматическая проверка файлов.....24
Проверка файлов вручную.....26
Проверка электронной почты.....30
Просмотр результатов проверки.....30
Как исключить файлы из проверки.....31
Исключение типов файлов.....31
Исключение файлов по расположению.....31
Просмотр исключенных программ.....32
Как пользоваться карантином.....33
Просмотр элементов в карантине.....33
Восстановление элементов из карантина.....34
Что такое DeepGuard.....34
Включение или выключение DeepGuard.....34
Разрешение программ, заблокированных функцией DeepGuard.....35
Использование DeepGuard в режиме совместимости.....35
Что делать при появлении предупреждений о подозрительном поведении.....35

Глава

1

# Установка

**Разделы:**


- *Перед первой установкой*
- *Первая установка продукта*
- *Установка и обновление приложений*
- *Справка и поддержка*

## Перед первой установкой

Благодарим за выбор F-Secure.

Для установки продукта необходимо следующее.

- Установочный компакт-диск или пакет. Если используется нетбук без дисковода компакт-дисков, можно загрузить установочный пакет со страницы *www.f-secure.com/netbook*.
- Ваш ключ подписки.
- Подключение к Интернету.

Если на компьютере установлен продукт для обеспечения безопасности от другого разработчика, программа установки попытается удалить его автоматически. Если этого не произойдет, удалите его вручную.

**Примечание:** Если на компьютере создано несколько учетных записей, выполните вход в учетную запись администратора перед установкой.

## Первая установка продукта

Инструкции по установке программы.

Чтобы установить программу, выполните следующие инструкции:

1. Вставьте компакт-диск или дважды щелкните загруженную программу установки.

   Если компакт-диск не запустится автоматически, перейдите в проводник Windows, дважды щелкните значок дисковода компакт-дисков и дважды щелкните установочный файл, чтобы запустить установку.

2. Следуйте инструкциям на экране.

   - Если программы была приобретена на компакт-диске в магазине, ключ подписки можно найти на обложке руководства по быстрой установке.
   - Если программа была загружена из интернет-магазина F-Secure, ключ подписки указывается в электронном письме, подтверждающем заказ на приобретение.

   Возможно, потребуется перезапустить компьютер перед проверкой подписки и загрузки последних обновлений из Интернета. Если установка выполняется с компакт-диска, обязательно извлеките диск перед перезапуском компьютера.

## Установка и обновление приложений

Инструкции по активации новой подписки.

Следуйте этим инструкциям, чтобы активировать новую подписку или установить новое приложение с помощью панели запуска.

**Примечание:** Значок панели запуска находится на панели задач Windows.

1. На панели запуска щелкните правой кнопкой мыши крайний значок справа.
   Откроется всплывающее меню.
2. Выберите**Посмотреть мои подписки**.

3. В области **Мои подписки** перейдите на страницу **Статус подписки** и нажмите **Активировать подписку**.
   Открывается окно **Активация подписки**.
4. Введите ключ подписки для приложения и нажмите кнопку **OK**.
5. После завершения проверки и активации подписки нажмите кнопку **Закрыть**.
6. В области **Мои подписки** перейдите на страницу **Состояние установки**. Если установка не начнется автоматически, выполните следующие действия.
   a) Нажмите кнопку **Установить**.
      Откроется окно программы установки.
   b) Щелкните **Далее**.
      Приложение загружено, начинается установка.
   c) После завершения установки нажмите кнопку **Закрыть**.

Активирована новая подписка.

## Справка и поддержка

Чтобы открыть онлайн-справку по продукту, щелкните значок "Справка" или нажмите клавишу F1, когда активен любой экран продукта.

После регистрации лицензии вам предоставляются дополнительные услуги, такие как бесплатные обновления программы и поддержка программы. Зарегистрироваться можно на странице *www.f-secure.com/register*.

Глава

2

# Начало работы

**Разделы:**


- *Использование автоматического обновления*
- *Как узнать результаты работы программы*
- *Сеть защиты в реальном времени*
- *Как узнать, действительна ли подписка*


Сведения о начале работы с продуктом

В этом разделе описывается порядок изменения общих настроек и управления подписками с помощью панели запуска.

Общие настройки панели запуска применяются ко всем установленным в ней программам. Вместо того чтобы изменять настройки в каждой программе по отдельности, можно просто внести изменения в общие настройки, которые затем будут применены ко всем установленным программам.

К общим настройкам панели управления относятся следующие:

- Загрузки: здесь можно просмотреть сведения о загруженных обновлениях и вручную проверить наличие новых обновлений.
- Настройки подключения: здесь можно изменить способ подключения компьютера к Интернету.
- Уведомления: здесь можно просмотреть прошлые уведомления и настроить типы уведомлений, которые должны отображаться.
- Настройки конфиденциальности: здесь можно разрешить или запретить подключение компьютера к сети защиты в реальном времени.

С помощью панели запуска также можно управлять подписками на установленные программы.

# Использование автоматического обновления

Автоматическое обновление обеспечивает актуальную защиту компьютера.

Продукт загружает последние обновления на компьютер, когда он подключается к Интернету. Он отслеживает сетевой трафик и не мешает другим процессам, связанным с использованием Интернета, даже при низкой скорости подключения.

## Проверка состояния обновлений

Просмотрите дату и время последнего обновления.

Когда включено автоматическое обновление, программа автоматически получает последние обновления при подключении компьютера к Интернету.

Чтобы убедиться, что вы используете последние обновления:

1. На панели запуска щелкните правой кнопкой мыши крайний значок справа.
   Откроется меню.
2. Выберите **Открыть общие настройки**.
3. Выберите **Автоматические обновления** > **Загрузки**.
4. Щелкните **Проверить**.
   Продукт подключается к Интернету и проверяет последние обновления. Если защита устарела, он загружает последние обновления.

   **Примечание:** При использовании модема или подключения к Интернету через ISDN для проверки обновлений необходимо активное подключение.

## Изменение параметров подключения к Интернету

Как правило, настройки по умолчанию изменять не требуется, но можно настроить способ подключения сервера к Интернету, чтобы обеспечить автоматическое получение обновлений.

Чтобы изменить параметры подключения к Интернету:

1. На панели запуска щелкните правой кнопкой мыши крайний значок справа.
   Откроется меню.
2. Выберите **Открыть общие настройки**.
3. Выберите **Автоматические обновления** > **Подключение**.
4. В списке **Подключение к Интернету** выберите способ подключения компьютера к Интернету.
   - Выберите **Всегда рассматривать как активное**, если существует постоянное подключение к сети.

     **Примечание:** Если не существует постоянного подключения компьютера к сети и задано подключение по требованию, выбор параметра **Всегда рассматривать как активное** может привести к многочисленным попыткам подключения.
   - Выберите **Определить подключение**, чтобы загрузить обновления только в том случае, если продукт определяет активное подключение к сети.
   - Выберите **Определять трафик**, чтобы загружать обновления, только если продукт определит другой сетевой трафик.

     **Совет:** Если используется необычная конфигурация оборудования, из-за которой параметр **Определить подключение** обнаруживает активное подключение к сети даже в случае его отсутствия, выберите вместо него параметр **Определить по трафику**.

5. В списке **HTTP-прокси** выберите, будет ли использоваться *прокси-сервер* для подключения компьютера к Интернету.
   - Выберите **HTTP-прокси отсутствует**, если компьютер подключается к Интернету напрямую.
   - Выберите параметр **Настройка HTTP-прокси вручную**, чтобы настроить параметры *HTTP-прокси*.
   - Выберите **Использовать HTTP-прокси обозревателя**, чтобы использовать те же параметры *HTTP-прокси*, которые заданы при настройке веб-обозревателя.

## Проверьте состояние сети защиты в реальном времени.

Для правильной работы многих функций продукта требуется подключение к сети защиты в реальном времени.

Если имеют место проблемы с сетью или брандмауэр блокирует трафик сети защиты в реальном времени, отображается состояние "Отключена". Если не установлены функции продукта, которым требуется доступ к сети защиты в реальном времени, отображается состояние "Не используется".

Чтобы проверить состояние, выполните следующие действия.

1. На панели запуска щелкните правой кнопкой мыши крайний значок справа.
   Откроется меню.
2. Выберите **Открыть общие настройки**.
3. Выберите **Автоматические обновления** > **Подключение**.

В области **Сеть защиты в реальном времени** отображается текущее состояние сети.

# Как узнать результаты работы программы

На странице **Уведомления** можно посмотреть, какие действия предприняты продуктом с целью защиты компьютера.

Продукт показывает уведомление, когда предпринимает то или иное действие, например, когда обнаруживает вирус и блокирует его. Некоторые уведомления также могут отправляться поставщиком услуг, например, чтобы сообщить о новых предоставляемых услугах.

## Просмотр истории уведомлений

В истории уведомлений можно посмотреть, какие уведомления выводила программа.

Чтобы просмотреть историю уведомлений, выполните следующие действия.

1. На панели запуска щелкните правой кнопкой мыши крайний значок справа.
   Откроется меню.
2. Выберите **Открыть общие настройки**.
3. Выберите **Другие** > **Уведомления**.
4. Нажмите **Показать историю уведомлений**.
   Откроется список истории уведомлений.

## Изменение настроек уведомлений

Можно выбрать типы уведомлений, которые должны отображаться.

Чтобы изменить настройки уведомлений, выполните следующие действия.

1. На панели запуска щелкните правой кнопкой мыши крайний значок справа.

Откроется меню.

2. Выберите **Открыть общие настройки**.
3. Выберите **Другие** > **Уведомления**.
4. Установите или снимите флажок **Разрешить сообщения о программах**, чтобы включить или выключить отображение сообщений о программах.

   Когда этот параметр включен, программа выводит оповещения об установленных программах.
5. Установите или снимите флажок **Разрешить рекламные сообщения**, чтобы включить или выключить отображение рекламных сообщений.
6. Щелкните **OK**.

# Сеть защиты в реальном времени

В этом документе описана сеть защиты в реальном времени, интерактивная служба корпорации F-Secure, которая идентифицирует доброкачественные приложения и веб-сайты и защищает от вредоносного ПО и эксплойтов на веб-сайтах.

## Что такое сеть защиты в реальном времени

Сеть защиты в реальном времени является интерактивной службой, предоставляющей быструю ответную реакцию на возникающие Интернет-угрозы.

Будучи корреспондентом сети защиты в реальном времени, вы можете помочь нам усилить защиту от недавно появившихся и будущих угроз. Сеть собирает статистику по определенным неизвестным, вредоносным и подозрительным приложениям и их действиям на вашем устройстве. Информация анонимно отправляется в корпорацию F-Secure для анализа сводных данных. Мы используем результаты анализа для повышения устойчивости вашего устройства к новейшим угрозам и вредоносным файлам.

### Как работает сеть защиты в реальном времени

Корреспонденты Сети защиты в реальном времени предоставляют информацию о неизвестных программах и веб-сайтах, а также о вредоносных программах и средствах использования уязвимостей на веб-сайтах. Сеть защиты в реальном времени не отлеживает действия пользователей в Интернете и не собирает информацию об уже проанализированных веб-сайтах, а также о безопасных программах, установленных на компьютере.

Если вы не желаете передавать данные, Сеть защиты в реальном времени не собирает сведения об установленных приложениях и посещенных веб-сайтах людей, не являющихся активными корреспондентами. Тем не менее, продукту приходится запрашивать репутацию приложений, веб-сайтов, сообщений и других объектов с серверов F-Secure. Запрос передается в виде криптографической контрольной суммы; сам объект не пересылается. Мы не отслеживаем данные отдельных пользователей, увеличивается только значение счетчика файла или веб-сайта.

Полностью устранить сетевой трафик в сети защиты в реальном времени невозможно, поскольку он является необходимым элементом защиты.

## Преимущества сети защиты в реальном времени

Сеть защиты в реальном времени более быстро и точно защищает от новейших угроз. Вы не получите ненужных предупреждений о подозрительных приложениях, которые не являются вредоносными.

Как корреспондент Сети защиты в реальном времени вы можете помочь нам обнаруживать новые и неизвестные вредоносные программы и веб-сайты, а также удалять потенциальные ложноположительные результаты из базы определений вирусов.

Все участники сети защиты в реальном времени помогают друг другу. Когда сеть находит на вашем устройстве подозрительное приложение, вы пользуетесь результатами анализа ранее обнаруженных на других устройствах приложений. Сеть повышает эффективность устройства в целом, поскольку установленной антивирусной программе не приходится снова обрабатывать проанализированные и признанные безопасными приложения. Аналогичным образом, информация о вредоносных веб-сайтах и не затребованных рассылках совместно используется участниками сети. Мы можем обеспечить более четкую защиту от эксплойтов на веб-сайтах и спама.

Чем больше людей участвуют в Сети защиты в реальном времени, тем лучше защищен каждый участник.

## Тип отправляемых данных

Корреспонденты Сети защиты в реальном времени отправляют информацию о приложениях, которые хранятся на их устройствах и посещаемых веб-сайтах. Сеть может обеспечить защиту от новейших вредоносных приложений и подозрительных сайтов.

### Анализ репутации файла

Сеть защиты в реальном времени собирает только информацию о приложениях, не имеющих известной репутации и подозрительных или заведомо вредных файлах.

Сеть защиты в реальном времени собирает анонимную информацию о чистых и подозрительных программах на устройстве. Собираются данные только о портативных исполняемых файлах (например, портативные исполняемые файлы в ОС Windows с расширениями .cpl, .exe, .dll, .ocx, .sys, .scr и .drv).

Собираются следующие данные:

- Путь к файлу приложения на устройстве.
- Размер файла и время создания или изменения.
- атрибуты файлов и привилегии,
- Подпись файла.
- Текущая версия файла и компания-изготовитель.
- Происхождение файла или URL-адрес для загрузки.
- результаты анализа файлов, проверенных F-Secure DeepGuard и антивирусом, и
- Прочая подобная информация.

Сеть защиты в реальном времени никогда не собирает данные о личных документах, если только они не заражены. При обнаружении вредоносных файлов любого типа собираются данные об имени инфекции и о состоянии дезинфекции файла.

Также с помощью сети защиты в реальном времени можно отправлять подозрительные приложения на анализ. Для этого пригодны только исполняемые файлы. Сеть защиты в реальном времени никогда не собирает сведений о личных документах. Они никогда не отправляются на анализ автоматически.

### Отправка файлов на анализ

С помощью сети защиты в реальном времени также можно отправлять подозрительные приложения на анализ.

Отдельные подозрительные приложения можно отправлять вручную при появлении запроса. Можно отправлять только портативные исполняемые файлы (Portable Executable). Сеть защиты в реальном времени никогда не загружает на сервер личные документы.

### Анализ репутации веб-сайта

Сеть защиты в реальном времени не отслеживает ваши действия в сети и не собирает информации об уже проанализированных веб-сайтах. Это гарантирует, что посещенные веб-сайты безопасны для

обозревателя. При посещении веб-сайта сеть проверяет его на безопасность и сообщает о том, нет ли у него рейтинга подозрительного или вредоносного.

Если на посещенном веб-сайте есть вредоносное или подозрительное содержимое или известная проблема, есть определяет полный URL-адрес сайта для анализа содержимого веб-страницы.

При заходе на сайт, еще не имеющий рейтинга сеть защиты в реальном времени определяет доменное и субдоменное имя и, в некоторых случаях, путь к посещенной странице (для анализа и определения рейтинга). Все параметры URL-адреса, которые могут содержать идентифицирующую вас информацию в определяемом формате, удаляются для защиты конфиденциальности.

**Примечание:** Сеть защиты в реальном времени не присваивает рейтинг и не анализирует веб-страницы в частных сетях, то есть никогда не собирает сведений об IP-адресах в таких сетях (например, в корпоративных интрасетях).

### Анализ системных данных

Сеть защиты в реальном времени определяет название и версию операционной системы, Интернет-соединении и статистику использования сети защиты (например, количество запросов репутации веб-сайта и среднее время на получение результата) с целью мониторинга и улучшения обслуживания.

## Охрана конфиденциальности

Мы передаем информацию безопасным методом и автоматически удаляем все личные сведения, которые могут содержаться в данных.

Сеть защиты в реальном времени удаляет идентифицирующие данные перед отправкой в F-Secure и при передаче шифрует всю собранную информацию для защиты от несанкционированного доступа. Собранная информация не обрабатывается отдельно, а добавляется к данным других пользователей. Проводится сводный анонимный статистический анализ всех данных, никак не связанных с вами.

Информация, пригодная для идентификации, в состав собранных данных не включается. Сеть защиты в реальном времени не собирает частные IP-адреса или личные данные, например, адреса электронной почты, имена пользователя и пароли. Мы прилагаем все возможные усилия для удаления всех идентифицирующих данных, но некоторые из них могут остаться в выборке. В таком случае мы не будем использовать случайно полученные сведения для вашей идентификации.

Мы применяем жесткие меры безопасности и физические, административные и технические механизмы для защиты собранной информации при передаче, сортировке и обработке. Информация хранится в безопасных местах и на серверах, контролируемых нами и находящихся либо в наших офисах, либо в офисах субподрядчиков. К выборкам имеют доступ только уполномоченные лица.

F-Secure может использовать собранные данные совместно с филиалами, субподрядчиками, дистрибьюторами, но только в анонимном, неидентифицируемом формате.

## Активное участие в Сети защиты в реальном времени

Передавая сведения о вредоносном ПО и веб-сайтах, вы помогаете нам улучшать сеть защиты в реальном времени.

Во время установки можно присоединиться к Сети защиты в реальном времени. Параметры по умолчанию подразумевают отправку данных в Сеть защиты в реальном времени. Эту настройку можно изменить позже в программе.

Выполните следующие действия, чтобы изменить настройки Сети защиты в реальном времени.

1. На панели запуска щелкните правой кнопкой мыши крайний значок справа.
   Откроется меню.
2. Выберите **Открыть общие настройки**.

3. Выберите **Другие** > **Конфиденциальность**.
4. Установите флажок участия, чтобы стать корреспондентом Сети защиты в реальном времени.

## Вопросы по поводу сети защиты в реальном времени

Информация о контактах по любым вопросам относительно сети защиты в реальном времени

Если у вас есть дополнительные вопросы относительно сети защиты в реальном времени, обращайтесь по адресу:

---

F-Secure Corporation

Tammasaarenkatu 7

PL 24

00181 Helsinki

Finland

*http://www.f-secure.com/en/web/home_global/support/contact*

---

Новейшая версия описания этой политики уже есть на нашем веб-сайте.

# Как узнать, действительна ли подписка

Тип и состояние подписки отображаются на странице **Статус подписки**.

Незадолго до окончания срока действия подписки или после этого на соответствующем значке панели запуска меняется индикатор общего состояния защиты.

Чтобы проверить, действительна ли подписка:

1. На панели запуска щелкните правой кнопкой мыши крайний значок справа.
   Откроется меню.
2. Выберите**Посмотреть мои подписки**.
3. Выберите **Статус подписки**, чтобы посмотреть сведения о подписках на установленные программы.
4. Выберите **Состояние установки**, чтобы узнать, какие программы можно установить.

Состояние подписки и дата окончания срока действия также отображаются на странице **Статистика**. Если срок действия подписки истек, ее необходимо возобновить, чтобы дальше пользоваться программой и получать обновления.

**Примечание:** После окончания срока действия подписки значок состояния продукта мигает на панели задач.

## Центр действий

Центр действий показывает все важные уведомления, требующие вашего внимания.

Если срок вашей подписки истекает или истек, центр действий уведомит вас об этом. Цвет фона и содержимое сообщения центра действий зависит от типа и состояния подписки:

- Если срок вашей подписки истекает и есть доступные подписки, у сообщения будет белый фон и кнопка **Активировать**.

- Если срок вашей подписки истекает и доступных подписок нет, у сообщения будет желтый фон и кнопки **Купить** и **Ввести ключ**. Если вы уже купили новую подписку, можно нажать кнопку **Ввести ключ**, чтобы указать ключ новой подписки и активировать ее.
- Если срок вашей подписки истек и есть доступные подписки, у сообщения будет красный фон и кнопка **Активировать**.
- Если срок вашей подписки истекает и доступных подписок нет, у сообщения будет красный фон и кнопки **Купить** и **Ввести ключ**. Если вы уже купили новую подписку, можно нажать кнопку **Ввести ключ**, чтобы указать ключ новой подписки и активировать ее.

**Примечание:** Ссылка **Показать историю уведомлений** на экране центра действий показывает список уведомлений по продукту, а не прежние сообщения центра действий.

## Активация подписки

Получив новый ключ подписки или код кампании для продукта, его необходимо активировать.

Чтобы активировать подписку, выполните следующие действия.

1. На панели запуска щелкните правой кнопкой мыши крайний значок справа.
   Откроется меню.
2. Выберите**Посмотреть мои подписки**.
3. Выполните одно из следующих действий.
   - Щелкните **Активировать подписку**.
   - Щелкните **Активировать код кампании**.
4. В открытом диалоговом окне введите новый ключ подписки или код кампании и нажмите **OK**.

   **Совет:** Если вы получили ключ подписки по электронной почте, можно скопировать ключ из сообщения электронной почты и вставить в это поле.

После того как введен новый ключ подписки, откройте страницу **Статус подписки**, чтобы узнать новый срок действия подписки.

Глава

3

# Введение

**Разделы:**


- *Просмотр общего статуса защиты*
- *Просмотр статистики продукта*
- *Работа с обновлениями продукта*
- *Что такое вирусы и другие вредоносные программы*


Данный продукт защищает компьютер от вирусов и других вредоносных программ.

Данный продукт проверяет файлы, анализирует программы и обновляется автоматически. Вмешательство пользователя не требуется.

## Просмотр общего статуса защиты

На странице **Статус** отображается краткий список функций установленной программы и их текущий статус.

Чтобы открыть страницу **Статус**:

На главной странице выберите **Статус**.

Откроется страница **Статус**.

Значки сообщают о состоянии программы и ее функций безопасности.

| Значок состояния | Название статуса | Описание |
|---|---|---|
| | ОК | Компьютер защищен. Функция включена и работает надлежащим образом. |
| | Информация | Программа информирует вас об особом статусе функции.<br>Например, выполняется обновление функции. |
| | Предупреждение | Компьютер защищен не полностью.<br>Например, продукт долго не обновлялся или необходимо обратить внимание на состояние функции. |
| | Ошибка | Ваш компьютер не защищен.<br>Например, срок действия подписки истек или важная функция выключена. |
| | Выкл. | Некритическая функция отключена. |

## Просмотр статистики продукта

Узнать о результатах работы программы с момента установки можно на странице **Статистика**.

Чтобы открыть страницу **Статистика**:

На главной странице выберите **Статистика**.

Откроется страница **Статистика**.

- **Последняя проверка успешного обновления** отображает время последнего обновления.

- **Проверка на вирусы и программы-шпионы** отображает количество файлов, обнаруженных и удаленных программной с момента ее установки.
- **Программы** показывает, для какого числа программ компонент DeepGuard разрешил или заблокировал установку.
- На странице **Подключения брандмауэра** показано число разрешенных и заблокированных подключений с момента установки.
- На странице **Фильтрация спама и фишинговых сообщений** показано, сколько сообщений электронной почты было отнесено к категориям допустимых сообщений и спама.

# Работа с обновлениями продукта

Данный продукт обновляет защиту автоматически.

## Просмотр версий баз данных

На странице **Обновления базы данных** можно посмотреть время последнего обновления и номера версий.

Чтобы открыть страницу **Обновления базы данных**, выполните следующее:

1. На главной странице выберите **Настройки**.

   **Примечание:** Для изменения настроек потребуются права администратора.

2. Выберите **Другие настройки** > **Версии базы данных**.

На странице **Версии базы данных** показаны дата последнего обновления описаний вирусов и шпионского ПО, службы DeepGuard и фильтрации спама и фишинговых сообщений, а также их версии.

## Изменение настроек мобильной широкополосной связи

Выберите, требуется ли загружать обновления безопасности при подключении к сети мобильной широкополосной связи.

**Примечание:** Эта функция доступна только в ОС Microsoft Windows 7.

По умолчанию обновления безопасности всегда загружаются при подключении к сети домашнего оператора. Однако проверка обновлений безопасности приостанавливается при подключении к сети другого оператора. Это происходит по той причине, что за подключение может взиматься плата, которая варьируется в зависимости от операторов, например, в разных странах. Эту настройку можно оставить как есть, если требуется сократить использование мобильной широкополосной связи и затраты во время пребывания в зоне действия чужой сети.

**Примечание:** Эта настройка применяется только для подключений к мобильной широкополосной сети. Когда компьютер подключен к стационарной или беспроводной сети, происходит автоматическое обновление программы.

Чтобы изменить настройку, выполните следующие действия.

1. На главной странице выберите **Настройки**.

   **Примечание:** Для изменения настроек потребуются права администратора.

2. Выберите **Другие настройки** > **Мобильный широкополосный доступ** > **Загрузка обновлений безопасности**.
3. Выберите нужный вариант обновления для мобильных подключения:

- **Только в домашней сети моего оператора**

  Обновления всегда загружаются при подключении к сети домашнего оператора. При попадании в зону действия сети другого оператора обновление приостанавливается. Рекомендуется выбрать этот вариант, чтобы обеспечить актуальность программы, не выходя за рамки ожидаемых затрат.
- **Никогда**

  Обновления не загружаются, если используется мобильное широкополосное подключение.
- **Всегда**

  Обновления загружаются всегда, независимо от используемой сети. Выберите этот вариант, если требуется обеспечить надежную защиту компьютера независимо от затрат.

4. Чтобы принимать решение каждый раз при выходе за пределы домашней сети оператора, выберите параметр **Спрашивать каждый раз, когда я покидаю домашнюю сеть моего оператора**.

### Приостановка обновлений безопасности

Проверку обновлений безопасности можно приостановить, когда используется сеть передачи данных другого оператора.

В этом случае можно заметить уведомление **Приостановлено** в правом нижнем углу экрана. Обновления приостановлены, поскольку цена за соединение может изменяться в зависимости от оператора, например в разных странах. Возможно, вы захотите оставить эту настройку неизменной, если необходимо сохранить пропускную способность и, возможно, сэкономить затраты во время поездки. Однако, если вы тем не менее хотите изменить эти настройки, щелкните ссылку **Изменить**.

**Примечание:**

Эта функция доступна только в ОС Microsoft Windows 7.

## Что такое вирусы и другие вредоносные программы

Вредоносное программное обеспечение — это программы, специально разработанные для того, чтобы повредить компьютер, использовать компьютер для противозаконных целей без ведома пользователя или похитить информацию с компьютера.

Вредоносное программное обеспечение может:

- перехватить управление веб-обозревателем,
- перенаправлять поисковые запросы,
- показывать нежелательные рекламные объявления,
- отслеживать посещаемые веб-узлы,
- похищать личные данные, например банковскую информацию,
- использовать компьютер для рассылки нежелательной почты и
- использовать компьютер для атак на другие компьютеры.

Вредоносные программы могут вызвать замедление и нестабильность работы компьютера. Вы можете заподозрить, что какое-либо *вредоносное программное обеспечение* запущено на компьютере, если внезапно замедлилась его работа и часто происходят сбои.

### Вирусы

Вирус — это, как правило, программа, которая может прикрепляться к файлам и постоянно реплицироваться. Вирусы могут изменять и замещать собой содержимое других файлов таким образом, что это может нанести вред компьютеру.

*Вирус* — это программа, которая обычно устанавливается на компьютер без вашего ведома. После установки вирус пытается реплицироваться. Вирус:

- использует часть ресурсов компьютера;
- может изменить или повредить файлы компьютера;
- возможно, пытается использовать компьютер, чтобы заразить другие компьютеры;
- может допустить использование компьютера в незаконных целях.

## Шпионские программы

Шпионские программы — это программы, собирающие личные сведения пользователей.

Шпионские модули могут собирать личные данные, в том числе:

- посещенные веб-узлы,
- адреса электронной почты компьютера,
- пароли или
- номера кредитных карт.

Шпионские программы чаще всего устанавливаются сами, не получая разрешения явным образом. Шпионские программы могут устанавливаться вместе с полезными программами или посредством нажатия кнопки в обманном всплывающем окне.

## Наборы сторонних средств полного доступа

Наборы сторонних средств полного доступа усложняют поиск *вредоносного программного обеспечения*.

Наборы сторонних средств полного доступа скрывают файлы и процессы. Как правило, они делают это, чтобы скрыть вредоносную активность на компьютере. Если набор сторонних средств полного доступа скрывает *вредоносное программное обеспечение*, вам будет трудно обнаружить, что на компьютере установлено вредоносное программное обеспечение.

Этот продукт содержит сканнер, выполняющий поиск наборов сторонних средств полного доступа, чтобы *вредоносное программное обеспечение* не могло легко скрывать свои файлы и процессы.

## Подозрительные программы

Подозрительные программы не создаются специально для того, чтобы нанести вред компьютеру, но могут оказаться опасными при неправильном использовании.

Подозрительное программное обеспечение не является однозначно вредоносным. Подозрительное программное обеспечение выполняет некоторые полезные, но потенциально опасные функции.

Примеры подозрительного программного обеспечения:

- программы для мгновенного обмена сообщениями (например, IRC),
- программы для передачи файлов по Интернету с одного компьютера на другой,
- или телефонные интернет-программы (*VoIP*, протокол передачи голоса через Интернет).
- программное обеспечение удаленного доступа, например VNC-приложения,
- поддельные антивирусные программы, которые могут осуществлять мошеннические попытки запугивания пользователей, чтобы те приобретали поддельное программное обеспечение безопасности или
- программное обеспечение, созданное для обхода проверки компакт-дисков или защиты от копирования.

Если вы сами установили программу и правильно ее настроили, маловероятно, что она вредоносная.

Если подозрительная программа установлена без вашего ведома, она скорее всего была установлена со злым умыслом и должна быть удалена.

Глава

4

# Защита компьютера от вредоносных программ

**Разделы:**


- *Как проверить компьютер*
- *Как исключить файлы из проверки*
- *Как пользоваться карантином*
- *Что такое DeepGuard*


Проверка на вирусы и шпионские программы защищает компьютер от программ, которые могут похищать личную информацию, наносить вред компьютеру или использовать его в незаконных целях.

По умолчанию обработка всех типов вредоносного ПО осуществляется сразу после обнаружения, чтобы они не успели причинить вреда.

По умолчанию при поиске вирусов и программ-шпионов выполняется автоматическая проверка локальных жестких дисков, любых съемных носителей (например, портативных дисков или компакт-дисков) и загружаемого содержимого.

При поиске вирусов и программ-шпионов также выполняется проверка компьютера на выявление изменений, которые могут обозначить присутствие *вредоносного программного обеспечения*. При обнаружении каких-либо опасных изменений, например в настройках системы или в важных системных процессах, модуль DeepGuard останавливает работу данной программы, так как скорее всего она является *вредоносной*.

# Как проверить компьютер

Когда проверка на вирусы и шпионское ПО включена, автоматически выполняется проверка наличия вредоносных файлов на компьютере. Можно также выполнить проверку файлов вручную и настроить расписания проверок.

Рекомендуется оставлять функцию проверки на вирусы и шпионское ПО постоянно включенной. Можно проверить файлы вручную, чтобы убедиться, что на компьютере отсутствуют вредоносные файлы, или чтобы проверить файлы, исключенные из проверки в режиме реального времени.

При настройке расписания проверки функция проверки на вирусы и шпионское ПО удаляет вредоносные файлы с компьютера в указанное время.

## Автоматическая проверка файлов

Функция проверки в режиме реального времени защищает компьютер, проверяя все файлы при попытке их использовать, и блокирует доступ к тем, файлам, которые содержат *вредоносное программное обеспечение*.

Прежде чем разрешить доступ к файлу на компьютере, функция проверки в режиме реального времени проверяет файл на наличие вредоносного ПО. Если функция проверки в режиме реального времени обнаруживает какое-либо вредоносное содержимое, она помещает файл в карантин, прежде чем он нанесет вред.

### Влияет ли проверка в режиме реального времени на быстродействие компьютера?

Обычно процесс проверки незаметен, так как он требует мало времени и системных ресурсов. Количество времени и системных ресурсов, которые требуются для проверки в режиме реального времени, зависит, например, от содержимого, местоположения и типа файла.

Файлы, проверка которых требует более длительного времени:

- Файлы на съемных носителях, таких как компакт-диски, DVD-диски и портативные USB-диски.
- Сжатые файлы, например файлы с расширением *ZIP*.

  **Примечание:** Проверка сжатых файлов не выполняется по умолчанию.

Проверка в режиме реального времени может замедлить работу компьютера, если:

- При наличии компьютера, который не отвечает системным требованиям, или
- При одновременном доступе к большому количеству файлов. Например, при открытии каталога, содержащего большое количество файлов, которые необходимо проверить.

### Включение и выключение проверки в режиме реального времени

Не выключайте проверку в режиме реального времени, чтобы остановить *вредоносное ПО*, прежде чем оно нанесет вред компьютеру.

Чтобы включить или выключить проверку в режиме реального времени, выполните следующее:

1. На главной странице выберите **Статус**.
2. Щелкните **Изменить настройки на этой странице**.

   **Примечание:** Для выключения функций безопасности требуются права администратора.

3. Включите или выключите функцию **Проверка на вирусы и шпионское ПО**.
4. Щелкните **Закрыть**.

## Автоматическая обработка вредоносных файлов

В процессе проверки в режиме реального времени можно выбрать автоматическую обработку вредоносных файлов без вывода запросов.

Чтобы выбрать автоматическую обработку вредоносных файлов в процессе проверки в режиме реального времени, выполните следующее:

1. На главной странице выберите **Настройки**.

   **Примечание:** Для изменения настроек потребуются права администратора.

2. Выберите **Безопасность компьютера** > **Проверка на вирусы и шпионское ПО**.
3. Выберите **Обрабатывать вредоносные файлы автоматически**.

Если автоматическая обработка вредоносных файлов не выбрана, при обнаружении вредоносного файла при проверке в режиме реального времени появится запрос выбрать действие.

## Работа со шпионскими программами

Функция проверки на вирусы и шпионское ПО немедленно блокирует шпионские программы при их запуске.

Перед запуском шпионской программы продукт блокирует ее и позволяет пользователю выбрать, что необходимо сделать с программой.

При обнаружении шпионской программы выберите одно из следующих действий:

| Предпринимаемое действие | Что происходит со шпионскими модулями |
|---|---|
| Обрабатывать автоматически | Позволить продукту выбрать наиболее подходящее действие на основе обнаруженной шпионской программы. |
| Поместить шпионскую программу в карантин | Переместить шпионскую программу в карантин, откуда она не сможет нанести вред компьютеру. |
| Удалить шпионскую программу | Удалить с компьютера все файлы, связанные со шпионской программой. |
| Только заблокировать шпионскую программу | Блокировать доступ к шпионской программе, но оставить ее на компьютере. |
| Исключить шпионскую программу из проверки | Разрешить выполнение шпионской программы и исключить ее из проверки в будущем. |

## Работа с потенциально опасными программами

Функция проверки на вирусы и шпионское ПО немедленно блокирует потенциально опасные программы при их запуске.

Перед запуском потенциально опасной программы продукт блокирует ее и позволяет пользователю выбрать, что необходимо сделать с программой.

При обнаружении потенциально опасной программы выберите одно из следующих действий:

| Предпринимаемое действие | Что происходит с подозрительным программным обеспечением |
|---|---|
| Только заблокировать потенциально опасную программу | Заблокировать доступ к потенциально опасной программе, но оставить ее на компьютере. |
| Переместить потенциально опасную программу в карантин | Переместить потенциально опасную программу в карантин, откуда она не сможет нанести вред компьютеру. |

| Предпринимаемое действие | Что происходит с подозрительным программным обеспечением |
|---|---|
| Удалить потенциально опасную программу | Удалить с компьютера все файлы, связанные с потенциально опасной программой. |
| Исключить потенциально опасную программу из проверки | Разрешить выполнение потенциально опасной программы и исключить ее из проверки в будущем. |

### Автоматическое удаление отслеживающих cookie-файлов

Благодаря удалению отслеживающих cookie-файлов веб-сайты не смогут отслеживать историю просмотра сайтов в Интернете.

Отслеживающие cookie-файлы - это небольшие файлы, с помощью которых веб-сайты могут записывать данные о посещении пользователем других веб-сайтов. Выполните следующие действия для удаления отслеживающих cookie-файлов с компьютера.

1. На главной странице выберите **Настройки**.

   **Примечание:** Для изменения настроек потребуются права администратора.

2. Выберите **Безопасность компьютера** > **Проверка на вирусы и шпионское ПО**.
3. Выберите **Удалять отслеживающие cookie-файлы**.
4. Щелкните **OK**.

## Проверка файлов вручную

Можно проверить файлы вручную, например, чтобы убедиться в том, что на внешнем устройстве, подключенном к компьютеру, отсутствуют какие-либо вредоносные программы.

### Запуск проверки вручную

Можно выполнить проверку компьютера полностью, а можно проверить его на наличие определенного типа *вредоносного программного обеспечения* или выполнить проверку в определенном местоположении.

Если вы подозреваете наличие определенного типа *вредоносного программного обеспечения*, можно выполнить проверку только на этот тип. Если вы подозреваете, что вредоносное программное обеспечение находится в определенном месте, можно выполнить проверку только этой части компьютера. Такие проверки потребуют значительно меньше времени, чем полная проверка компьютера.

Чтобы начать проверку компьютера вручную, необходимо выполнить следующие действия:

1. На главной странице щелкните стрелку под пунктом **Проверка**.

   Отобразятся параметры проверки.

2. Выберите тип проверки.

   Выберите **Изменить параметры проверки**, чтобы оптимизировать выполняемую вручную проверку компьютера на наличие вирусов и других вредоносных программ.

3. Если выбрать пункт **Выберите, что нужно проверить**, откроется окно, в котором можно выбрать объект для проверки.
   Откроется **Мастер проверки**.

### Типы проверки

Можно выполнить проверку компьютера полностью, а можно проверить его на наличие определенного типа вредоносного программного обеспечения или выполнить проверку в определенном местоположении.

В следующей таблице перечислены разные типы проверки.

| Тип проверки | Объект проверки | Когда использовать этот тип |
|---|---|---|
| Проверка на вирусы | Части компьютера проверяются на вирусы, шпионские и подозрительные программы | Этот тип проверки выполняется намного быстрее полной проверки. Просматриваются только части системы, в которых содержатся файлы установленных программ. Эта проверка рекомендуется, когда нужно проверить, не заражен ли компьютер, так как она эффективно обнаруживает и удаляет активные вредоносные программы на компьютере. |
| Полная проверка компьютера | Весь компьютер (включая внутренние и внешние жесткие диски) проверяется на вирусы, шпионские и подозрительные программы | Если вы хотите убедиться, что вредоносное программное обеспечение или подозрительное программное обеспечение отсутствует на компьютере.На выполнение этого типа проверки требуется больше всего времени. Она включает быструю проверку на вредоносные программы и проверку жестких дисков. Также проверяются элементы, которые могут быть скрыты с помощью наборов сторонних средств полного доступа. |
| Выберите, что нужно проверить | Конкретный файл, папка или диск проверяется на вирусы, шпионские или подозрительные программы. | Если вы подозреваете, что в определенном месте компьютера существует вредоносное программное обеспечение, например, если в нем находятся файлы, загруженные из потенциально опасных источников, таких как одноранговая сеть обмена файлами. Время, затрачиваемое на проверку, зависит от размера проверяемого объекта. Проверка завершается быстро, если, к примеру, в проверяемой папке содержится несколько небольших файлов. |
| Поиск наборов сторонних средств полного доступа | Важные места в системе, где наличие подозрительного элемента может свидетельствовать о проблеме с безопасностью. Проверяется наличие скрытых файлов, папок, дисков или процессов | Когда есть подозрения на наличие набора сторонних средств полного доступа. Например, если недавно на компьютере было обнаружено вредоносное программное обеспечение и нужно проверить, что не установлен набор сторонних средств полного доступа. |

## Проверка в Проводнике Windows

Проверку дисков, папок и файлов на *вирусы*, *шпионские программы* и *подозрительное программное обеспечение* можно выполнять через Проводник Windows.

Чтобы проверить диск, папку или файл:

1. Наведите курсор на диск, папку или файл, которые необходимо проверить, и щелкните правой кнопкой мыши.
2. Щелкнув правой кнопкой мыши, выберите в меню **Проверить папки на вирусы** (название параметра зависит от того, что нужно проверить: диск, папку или файл).
   Открывается окно **Мастер проверки** и начинается проверка.

В случае обнаружения *вируса* или *шпионской программы* **Мастер проверки** укажет этапы очистки.

## Выбор файлов для проверки

Выберите типы файлов, которые необходимо проверять на *вирусы* и *шпионские модули* при запланированных или ручных проверках.

1. На главной странице выберите **Настройки**.

   **Примечание:** Для изменения настроек потребуются права администратора.

2. Выберите **Другие настройки** > **Проверка вручную**.
3. В группе **Параметры проверки** выберите один из вариантов:

| | |
|---|---|
| **Проверка только известных типов файлов** | Чтобы проверить только те типы файлов, которые вероятней всего содержат вирусы, например исполняемые файлы. Кроме того, это позволяет ускорить выполнение проверки. Проверяются только файлы со следующими расширениями: .ani, .asp, .ax, .bat, .bin, .boo, .chm, .cmd, .com, .cpl, .dll, .doc, .dot, .drv, .eml, .exe, .hlp, .hta, .htm, .html, .htt, .inf, .ini, .job, .js, .jse, .lnk, .lsp, .mdb, .mht, .mpp, .mpt, .msg, .ocx, .pdf, .php, .pif, .pot, .ppt, .rtf, .scr, .shs, .swf, .sys, .td0, .vbe, .vbs, .vxd, .wbk, .wma, .wmv, .wmf, .wsc, .wsf, .wsh, .wri, .xls, .xlt, .xml, .zip, .jar, .arj, .lzh, .tar, .tgz, .gz, .cab, .rar, .bz2 и .hqx. |
| **Проверка сжатых файлов** | Для проверки архивных файлов и папок. |
| **Использовать расширенную эвристику** | Использование эвристики рекомендуется во время выполнения проверки для улучшения результатов поиска нового или вредоносного программного обеспечения.<br>**Примечание:** Если выбрать этот параметр, проверка займет больше времени, и в результате может быть больше ложных срабатываний (безопасные файлы могут расцениваться как подозрительные). |

4. Щелкните **OK**.

**Примечание:** Исключенные файлы в списках исключенных элементов не проверяются, даже если пользователь выбрал их проверку в этом разделе.

## Действия, предпринимаемые при обнаружении вредоносных файлов

Выберите действие, выполняемое при обнаружении вредоносных файлов.

Чтобы выбрать действие, предпринимаемое при обнаружении вредоносного содержимого во время проверки вручную, выполните следующее:

1. На главной странице выберите **Настройки**.

   **Примечание:** Для изменения настроек потребуются права администратора.

2. Выберите **Другие настройки** > **Проверка вручную**.
3. В разделе **Когда обнаружена вредоносная программа** выберите один из следующих параметров:

| Параметр | Описание |
|---|---|
| **Спросить меня (по умолчанию)** | Можно выбрать действие, выполняемое с каждым элементом, обнаруженным в ходе проверки вручную. |
| **Очистить файлы** | Предпринимается попытка автоматического лечения зараженных файлов, обнаруженных в ходе проверки вручную.<br>**Примечание:** Если очистка зараженного файла невозможна, файл помещается в карантин (если он не находится в сети или на съемных дисках) и не может нанести вред компьютеру. |

| Параметр | Описание |
|---|---|
| **Поместить файлы в карантин** | Все вредоносные файлы, обнаруженные в ходе проверки вручную, перемещаются в карантин, откуда они не могут нанести вред компьютеру. |
| **Удалить файлы** | Все вредоносные файлы, обнаруженные в ходе проверки вручную, удаляются. |
| **Только отчет** | Все вредоносные файлы, обнаруженные в ходе проверки вручную, остаются без изменения, и сведения об обнаружении записываются в отчет о проверке.<br>**Примечание:** Если выбран этот вариант и выключена проверка в реальном времени, вредоносная программа может нанести вред компьютеру. |

**Примечание:** Вредоносные файлы, обнаруженные в ходе проверки вручную, очищаются автоматически.

## Планирование проверки

Настройте автоматическое выполнение проверки и удаления вирусов и других вредоносных программ во время бездействия компьютера или настройте периодическую проверку безопасности компьютера.

Чтобы запланировать проверку:

1. На главной странице выберите **Настройки**.

   **Примечание:** Для изменения настроек потребуются права администратора.

2. Выберите **Другие настройки** > **Запланированная проверка**.
3. Включите функцию **Запланированная проверка**.
4. Выберите, когда должна начинаться проверка.

| Параметр | Описание |
|---|---|
| **Ежедневно** | Ежедневная проверка компьютера. |
| **Еженедельно** | Проверка компьютера в выбранные дни недели. Выберите дни в списке. |
| **Ежемесячно** | Проверка компьютера в выбранные дни месяца. Чтобы выбрать дни, выполните следующее:<br>1. Выберите вариант **День**.<br>2. Выберите число месяца в списке рядом с выбранным днем. |

5. Укажите время начала проверки в выбранные дни.

| Параметр | Описание |
|---|---|
| **Время начала** | Запуск проверки в указанное время. |
| **Компьютер не используется в течение** | Запуск проверки, если компьютер не используется в течение указанного периода времени. |

При проверке компьютера по расписанию используются параметры проверки вручную. Исключением является то, что каждый раз проверяются архивы и автоматически удаляются вредоносные файлы.

## Проверка электронной почты

Функция проверки электронной почты защищает от получения вредоносных файлов в сообщениях электронной почты.

Функция проверки на вирусы и шпионское ПО должна быть включена для антивирусной проверки электронной почты.

Чтобы включить или выключить проверку электронной почты, выполните следующие действия.

1. На главной странице выберите **Настройки**.

   **Примечание:** Для изменения настроек потребуются права администратора.

2. Выберите **Безопасность компьютера** > **Проверка на вирусы и шпионское ПО**.
3. Выберите **Удалять вредоносные вложения электронной почты**.
4. Щелкните **OK**.

### Когда проверяются сообщения электронной почты и вложения

Функция проверки на вирусы и шпионское ПО может удалять вредоносное содержимое из входящих сообщений электронной почты.

Функция проверки на вирусы и шпионской ПО удаляет вредоносные сообщения электронной почты, получаемые в таких почтовых программах, как Microsoft Outlook и Outlook Express, Почта Microsoft или Mozilla Thunderbird. Она проверяет незашифрованные сообщения электронной почты и их вложения каждый раз, когда они передаются в почтовую программу с почтового сервера по протоколу POP3.

Функция проверки на вирусы и шпионское ПО не проверяет сообщения веб-почты, которая включает приложения электронной почты, выполняемые в веб-браузере, например Hotmail, Yahoo! mail или Gmail. Защита от *вирусов* обеспечивается, даже если вредоносные вложения не удалены или используется веб-почта. При открытии файлов, вложенных в сообщения электронной почты, функция проверки в режиме реального времени удаляет все вредоносные вложения, прежде чем они нанесут вред.

**Примечание:** Функция проверки в режиме реального времени проверяет только ваш компьютер, но не компьютеры ваших друзей. Вложенные файлы проверяются только при их открытии. Это значит, что, если вы пересылаете сообщение, не открывая его вложение, через веб-почту, вы можете переслать друзьям зараженное сообщение.

## Просмотр результатов проверки

В журнале вирусов и шпионского ПО показаны все обнаруженные вредоносные файлы.

Иногда выполнение выбранного действия с обнаруженным вредоносным содержимым невозможно. Например, если выбрана очистка файлов, но файл не может быть очищен, файл перемещается в карантин. Эту информацию можно посмотреть в журнале вирусов и шпионского ПО.

Чтобы просмотреть историю:

1. На главной странице выберите **Настройки**.

   **Примечание:** Для изменения настроек потребуются права администратора.

2. Выберите **Безопасность компьютера** > **Проверка на вирусы и шпионское ПО**.
3. Щелкните **Просмотр журнала удаления**.

В журнале вирусов и шпионского ПО отображается следующая информация:

- дата и время обнаружения вредоносного файла;

- имя вредоносного ПО и его расположение на компьютере;
- выполненное действие.

# Как исключить файлы из проверки

Иногда требуется исключить некоторые файлы или программы из проверки. Исключенные элементы не проверяются до тех пор, пока они не будут удалены из списка исключенных элементов.

**Примечание:** Для проверки в режиме реального времени и проверки вручную предусмотрены отдельные списки исключений. Например, если файл исключен из проверки в режиме реального времени, он будет проверяться в ходе проверки вручную до тех пор, пока также не будет исключен из этой проверки.

## Исключение типов файлов

При исключении файлов по их типу файлы с указанными расширениями не проверяются на наличие вредоносного содержимого.

Чтобы добавить или удалить исключаемый тип файлов, выполните следующее:

1. На главной странице выберите **Настройки**.

   **Примечание:** Для изменения настроек потребуются права администратора.

2. Выберите, необходимо ли исключить тип файлов из проверки в режиме реального времени или вручную:
   - Выберите **Безопасность компьютера** > **Проверка на вирусы и шпионское ПО**, чтобы исключить тип файлов из проверки в режиме реального времени.
   - Выберите **Другие настройки** > **Проверка вручную**, чтобы исключить тип файлов из проверки вручную.
3. Щелкните **Исключить файлы из проверки**.
4. Чтобы исключить тип файла, выполните следующие действия.
   a) Откройте вкладку **Типы файлов**.
   b) Выберите **Исключить файлы с этими расширениями**.
   c) Введите расширение файла, определяющее тип исключаемых файлов, в поле рядом с кнопкой **Добавить**.

      Чтобы указать файлы без расширения, введите ".". Можно также использовать подстановочный знак "?" для представления любого одного символа или "*" для представления любого числа символов.

      Например, чтобы исключить исполняемые файлы, введите exe в это поле.
   d) Щелкните **Добавить**.
5. Повторите предыдущий шаг для любого другого расширения, которое не следует проверять на вирусы.
6. Нажмите кнопку **OK**, чтобы закрыть диалоговое окно **Исключить из проверки**.
7. Нажмите кнопку **OK** для применения новых параметров.

Выбранные типы файлов исключаются из будущих проверок.

## Исключение файлов по расположению

При исключении файлов по расположению файлы на указанных дисках или в указанных папках не проверяются на наличие вредоносного содержимого.

Чтобы добавить или удалить исключаемые расположения файлов, выполните следующее:

1. На главной странице выберите **Настройки**.

   **Примечание:** Для изменения настроек потребуются права администратора.

2. Выберите, необходимо ли исключить расположение из проверки в режиме реального времени или вручную:
   - Выберите **Компьютер** > **Проверка на вирусы и шпионское ПО**, чтобы исключить расположение из проверки в режиме реального времени.
   - Выберите **Компьютер** > **Проверка вручную**, чтобы исключить расположение из проверки вручную.
3. Щелкните **Исключить файлы из проверки**.
4. Чтобы исключить файл, диск или папку, выполните следующие действия.
   a) Откройте вкладку **Объекты**.
   b) Выберите **Исключить объекты (файлы, папки...)**.
   c) Щелкните **Добавить**.
   d) Выберите файл, диск или папку, которые необходимо исключить из проверки на вирусы.

      **Примечание:** Некоторые диски могут быть съемными, например компакт-диски, DVD-диски или сетевые диски. Невозможно исключить сетевые диски и пустые съемные носители.

   e) Щелкните **OK**.
5. Повторите предыдущий шаг для исключения из проверки других файлов, дисков или папок.
6. Нажмите кнопку **OK**, чтобы закрыть диалоговое окно **Исключить из проверки**.
7. Нажмите кнопку **OK** для применения новых параметров.

Выбранные файлы, диски и папки исключаются из будущей проверки.

## Просмотр исключенных программ

Можно посмотреть программы, исключенные из проверки, и удалить их из списка исключенных элементов для проверки в будущем.

Если в ходе проверки в режиме реального времени или проверки вручную обнаружена программа, которая ведет себя так, как шпионская или потенциально опасная программа, но вам известно, что она является безопасной, можно исключить программу из проверки, чтобы предупреждение о ней больше не появлялось.

**Примечание:** Если поведение программы похоже на поведение вируса или вредоносного ПО, ее исключение невозможно.

Нельзя исключать программы напрямую. Новые программы появляются в списке исключений, только если они исключаются во время проверки.

Чтобы просмотреть программы, исключенные из проверки:

1. На главной странице выберите **Настройки**.

   **Примечание:** Для изменения настроек потребуются права администратора.

2. Выберите, необходимо ли посмотреть программы, исключенные из проверки в режиме реального времени или проверки вручную:
   - Выберите **Компьютер** > **Проверка на вирусы и шпионское ПО** для просмотра программ, исключенных из проверки в режиме реального времени.

- Выберите **Компьютер** > **Проверка вручную** для просмотра программ, исключенных из проверки вручную.

3. Щелкните **Исключить файлы из проверки**.
4. Откройте вкладку **Приложения**.

   **Примечание:** Исключать можно только шпионские или подозрительные программы, но не вирусы.

5. Чтобы снова проверить исключенную программу, выполните следующее:
   a) Выберите программу, которую необходимо включить в проверку.
   b) Щелкните **Удалить**.
6. Нажмите кнопку **OK**, чтобы закрыть диалоговое окно **Исключить из проверки**.
7. Нажмите кнопку **OK** для выхода.

# Как пользоваться карантином

Карантин — это безопасное хранилище для файлов, которые могут быть вредоносными.

Файлы из карантина не могут распространяться или причинить какой-либо вред компьютеру.

*Вредоносное программное обеспечение*, *шпионские модули* и *опасное программное обеспечение* можно обезвредить, поместив в карантин. При необходимости можно восстановить программы или файлы из карантина.

Если нет необходимости помещать файлы в карантин, их можно удалить. Удаление элемента в карантине приведет к его окончательному удалению с компьютера.

- Как правило, можно удалить *вредоносное программное обеспечение*, помещенное в карантин.
- В большинстве случаев можно удалить *шпионские модули*, помещенные в карантин. *Шпионские модули* могут являться частью законной программы и после их удаления программа не будет работать должным образом. Если вам необходимо, чтобы программа продолжала работать на компьютере, можно восстановить *шпионские модули* из карантина.
- Помещенное в карантин *подозрительное программное обеспечение* может быть обычной программой, не являющейся вредоносной. Если вы самостоятельно установили и настроили программу, ее можно восстановить из карантина. Если *подозрительное программное обеспечение* установлено без вашего ведома, вероятнее всего, оно было установлено со злым умыслом, и его следует удалить.

## Просмотр элементов в карантине

Можно просмотреть дополнительные сведения об элементах в карантине.

Чтобы просмотреть подробные сведения об элементах в карантине:

1. На главной странице выберите **Настройки**.

   **Примечание:** Для изменения настроек потребуются права администратора.

2. Выберите **Безопасность компьютера** > **Проверка на вирусы и шпионское ПО**.
3. Щелкните **Просмотр карантина**.
   На странице **Карантин** указано общее число элементов, помещенных в карантин.
4. Чтобы просмотреть подробные сведения об элементах в карантине, выберите **Сведения**.

   Элементы можно сортировать по названию вредоносного ПО или пути к файлу.

   В списке отображаются первые 100 элементов, указывается их тип, имя и путь установки файлов.

5. Чтобы просмотреть дополнительные сведения об элементе в карантине, щелкните значок рядом с элементом в столбце **Состояние**.

## Восстановление элементов из карантина

Можно восстановить из карантина элементы, необходимые пользователю.

Можно восстановить приложения или файлы из карантина, если они необходимы. Не восстанавливайте элементы из карантина, если вы не уверены, что они не представляют угрозы. Восстановленные элементы перемещаются обратно в свое местоположение на компьютере.

Восстановление элементов из карантина

1. На главной странице выберите **Настройки**.

   **Примечание:** Для изменения настроек потребуются права администратора.

2. Выберите **Безопасность компьютера** > **Проверка на вирусы и шпионское ПО**.
3. Щелкните **Просмотр карантина**.
4. Выберите файлы в карантине, которые требуется восстановить.
5. Щелкните **Восстановить**.

# Что такое DeepGuard

DeepGuard анализирует содержимое файлов и поведение приложений и следит за ненадежными приложениями.

DeepGuard блокирует новые и необнаруженные *вирусы*, *черви* и другие вредоносные программы, которые пытаются изменить настройки компьютера, и предотвращает получение доступа в Интернет подозрительными программами.

Когда программа DeepGuard обнаруживает новую программу, которая пытается внести потенциально опасные изменения в систему, она разрешает выполнение этой программы в безопасной зоне. В безопасной зоне программа не может нанести вред компьютеру. Программа DeepGuard анализирует изменения, которые пыталась внести программа, и на основе этого определяет вероятность того, что программа является *вредоносной*. Если вероятность того, что программа является *вредоносной*, высокая, DeepGuard блокирует ее.

В числе потенциально опасных системных изменений, обнаруживаемых программой DeepGuard:

- изменения системных параметров (реестра Windows),
- попытки отключить важные системные программы, например программы обеспечения безопасности, подобные этому продукту и
- попытки изменить важные системные файлы.

## Включение или выключение DeepGuard

Не выключайте функцию DeepGuard, чтобы подозрительные программы не могли внести потенциально опасные системные изменения на компьютере.

Перед включением DeepGuard в ОС Windows XP убедитесь, что установлен пакет обновления 2.

Чтобы включить или выключить DeepGuard, выполните следующее:

1. На главной странице выберите **Статус**.
2. Щелкните **Изменить настройки на этой странице**.

**Примечание:** Для выключения функций безопасности требуются права администратора.

3. Включите или выключите функцию **DeepGuard**.
4. Щелкните **Закрыть**.

## Разрешение программ, заблокированных функцией DeepGuard

Можно управлять программами, разрешаемыми и блокируемыми функцией DeepGuard.

Иногда DeepGuard блокирует выполнение безопасной программы, даже если пользователю необходимо использовать программу и известно, что она безопасная. Это происходит, поскольку программа пытается внести системные изменения, которые являются потенциально опасными. Пользователь также может случайно заблокировать программу при появлении всплывающего окна DeepGuard.

Чтобы разрешить программу, заблокированную DeepGuard, выполните следующее:

1. На главной странице нажмите **Инструменты**.
2. Щелкните **Приложения**.
   Отображается список **Отслеживаемые программы**.
3. Найдите программу, которую необходимо разрешить.

   **Примечание:** Можно щелкнуть заголовок столбца для сортировки списка. Например, щелкните столбец **Разрешение**, чтобы сгруппировать разрешенные и запрещенные программы в списке.

4. Выберите **Разрешить** в столбце **Разрешение**.
5. Щелкните **Закрыть**.

DeepGuard разрешает программе внести системные изменения повторно.

## Использование DeepGuard в режиме совместимости

Для обеспечения максимальной защиты DeepGuard временно изменяет выполняющиеся программы. Некоторые программы выполняют проверку того, что они не повреждены или не изменены, и могут быть несовместимы с этой функцией. Например, интерактивные игры со средствами защиты от мошенничества при выполнении проверяют отсутствие в них каких-либо изменений. В этих случаях можно включить режим совместимости.

Чтобы включить режим совместимости, выполните следующее:

1. На главной странице выберите **Настройки**.

   **Примечание:** Для изменения настроек потребуются права администратора.

2. Выберите **Безопасность компьютера** > **DeepGuard**.
3. Выберите **Использовать режим совместимости**.
4. Щелкните **OK**.

## Что делать при появлении предупреждений о подозрительном поведении

DeepGuard отслеживает ненадежные приложения. Если такое приложение пытается получить доступ в Интернет, изменить настройки системы или выполняет подозрительные операции, DeepGuard блокирует его.

Если в настройках DeepGuard выбран параметр **Предупреждать о подозрительном поведении**, при обнаружении потенциально опасной программы или при запуске программы с неизвестной репутацией появляется уведомление.

Чтобы выбрать действие, которое необходимо выполнить с программой, заблокированной функцией DeepGuard:

1. Щелкните **Сведения** для просмотра дополнительной информации о программе.
   В разделе сведений показано следующее:
   - расположение программы;
   - репутация программы в сети защиты в реальном времени;
   - насколько распространенной является программа.
2. Выберите, необходимо ли доверять программе, заблокированной функцией DeepGuard:
   - Выберите **Я доверяю программе. Разрешить выполнение.**, чтобы не блокировать программу.

     Скорее всего, программа является безопасной, если:
     - функция DeepGuard заблокировала программу в результате действия пользователя;
     - вы знакомы с этой программой;
     - программа получена из надежного источника.
   - Выберите **Я не доверяю программе. Заблокировать ее.**, чтобы оставить программу заблокированной.

     Скорее всего, программа является небезопасной, если:
     - программа является редко используемой;
     - программа имеет неизвестную репутацию;
     - программа вам неизвестна;
3. Чтобы отправить подозрительную программу для анализа, выполните следующее:
   a) Щелкните **Сообщить о программе в F-Secure**.
   Отображаются условия отправки.
   b) Щелкните **Принимаю**, если вы принимаете условия и хотите отправить образец.

   Образец рекомендуется отправлять в следующих случаях:
   - функция DeepGuard заблокировала программу, которая является безопасной;
   - вы подозреваете, что программа является *вредоносной*.