bitdefender

ANTIVIRUS 2009

Руководство пользователя

bitdefender

BitDefender Antivirus 2009

Руководство пользователя

Опубликовано 2009.03.03

Правовые положения

bitdefender

Содержание

Лицензионное соглашение для конечного пользователя

ЕСЛИ ВЫ НЕ СОГЛАСНЫ С УСЛОВИЯМИ ДАННОГО СОГЛАШЕНИЯ, НЕ УСТАНАВЛИВАЙТЕ ДАННОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ; ВЫБИРАЯ "Я ПРИНИМАЮ","ОК","ПРОДОЛЖИТЬ","ДА", УСТАНАВЛИВАЯ, ЛИБО ЛЮБЫМ ДРУГИМ ОБРАЗОМ ИСПОЛЬЗУЯ ДАННЫЙ ПРОДУКТ, ВЫ ПОДТВЕРЖДАЕТЕ ПОЛНОЕ ПОНИМАНИЕ И СОГЛАСИЕ С УСЛОВИЯМИ ДАННОГО СОГЛАШЕНИЯ.

РЕГИСТРАЦИЯ ПРОДУКТА. Принимая это Соглашение, вы даете согласие зарегистрировать ваше программное обеспечение, с помощью "Моей Учетной Записи", что является условием использования программного обеспечения (получения обновлений) и Вашего права на Поддержку. Такой контроль помогает убедиться, что программное обеспечение функционирует только на компьютерах с действительной лицензией, и что пользователь получает помощь от службы поддержки согласно этой действительной лицензии. Регистрация требует действительный серийный номер продукта и действующий адрес электронной почты для обновления и других легальных уведомлений.

Данные условия относятся ко всем продуктам и услугам BitDefender для домашних пользователей, лицензии на которые вы имеете, включая документацию и обновления любых приложений, приобретенных согласно лицензии, либо любое другое сервисное соглашение, определенное в документации, либо их копии.

Данное Лицензионное Соглашение - юридическое соглашение между Вами (как частным или юридическим лицом) и BITDEFENDER об использовании программных продуктов BITDEFENDER, указанных выше, которые включают программное обеспечение и услуги, а также могут включать сопутствующие медиа-, печатные материалы, "онлайн" и электронную документацию (здесь и далее - "BitDefender"), полностью защищенные международными законами и соглашениями об авторском праве. Устанавливая, копируя или используя BitDefender, вы соглашаетесь принять условия данного соглашения.

Если Вы не согласны с условиями данного соглашения, не устанавливайте и не используйте BitDefender.

Лицензия BitDefender. Программный продукт BitDefender защищен законами об авторском праве и международными соглашениями об авторском праве, а также законами и соглашениями об интеллектуальной собственности. Он не продается без лицензии.

ПРЕДОСТАВЛЕНИЕ ЛИЦЕНЗИИ. Компания BITDEFENDER предоставляет Вам и только Вам следующую неисключительную, ограниченную, без права передачи, предусматривающую уплату роялти лицензию на использование программного продукта BitDefender.

ПРИКЛАДНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ. Вы можете установить и использовать BitDefender на необходимом количестве компьютеров, но соответсвующему общему количеству лицензированных пользователей. Вы можете сделать одну дополнительную резервную копию.

ЛИЦЕНЗИЯ ПЕРСОНАЛЬНОГО ПОЛЬЗОВАТЕЛЯ. Данная лицензия относится к программному обеспечению BitDefender, которое может быть установлено на персональном компьютере и которое не имеет серверных функций. Каждый пользователь может установить данный программный продукт на персональном компьютере, а также может сделать дополнительную резервную копию на другом устройстве.

УСЛОВИЯ ЛИЦЕНЗИРОВАНИЯ. Предоставленная лицензия действительна со дня приобретения BitDefender до конца периода, на который данная лицензия приобретена.

ПРЕКРАЩЕНИЕ СРОКА ДЕЙСТВИЯ: Продукт прекращает выполнять свои функции немедленно по истечению срока лицензии.

ОБНОВЛЕНИЯ. В случае, когда BitDefender является обновлением, вы можете обновлять свой программный продукт только тогда, когда Ваша лицензия, предоставленная компанией BITDEFENDER, действительна. Обновление BitDefender заменяет и/или дополняет исходный программный продукт, лицензия на который у Вас уже есть. Вы можете использовать обновленный продукт только согласно условиям данного Лицензионного соглашения. Если BitDefender является обновлением какой-либо программы из лицензионного пакета, лицензированного как один продукт, программный продукт BitDefender может использоваться только как часть пакета и не может быть использован в количестве, большем чем общее количество лицензированных пользователей. Условия данной лицензии заменяют и превалируют над всеми предыдущими соглашениями, которые были заключены между Вами и BITDEFENDER относительно оригинального продукта или итогового обновленного продукта.

АВТОРСКИЕ ПРАВА. Все права, в том числе и авторское право, на программный продукт BitDefender (включая, но не ограничивая: изображения, фотографии, логотипы, анимированные изображения, видео, звук, тексты и прикладные мини программы, входящие в программный продукт BitDefender), сопутствующие печатные материалы и любые копии программного продукта BitDefender являются собственностью компании BITDEFENDER. BitDefender защищен законом об

авторском праве и международными соглашениями. Поэтому Вы должны обращаться с ним, как и с любым другим лицензионным продуктом. Вы не имеете права копировать сопутствующие печатные материалы. На всех копиях должна стоять пометка об авторских правах, независимо от того, на каком носителе или в какой форме существует продукт BitDefender. Вы не имеете права выдавать сублицензии, сдавать в аренду или продавать BitDefender. Вы не имеете права восстанавливать алгоритм работы, вносить изменения, раскодировать, создавать свои продукты на основе BitDefender, изменять, переводить или предпринимать какие-либо попытки дешифровать исходный код программного продукта BitDefender.

ОГРАНИЧЕННАЯ ГАРАНТИЯ. Компания BITDEFENDER дает тридцатидневную гарантию со дня покупки, что все носители, на которых распространяется программный продукт BitDefender, не имеют дефектов. При нарушении гарантии компания BITDEFENDER может на свое усмотрение заменить поврежденный экземпляр или вернуть уплаченные деньги. Компания BITDEFENDER не гарантирует, что программный продукт BitDefender будет работать без ошибок или сбоев, или что ошибки будут исправлены. Компания BITDEFENDER не гарантирует, что программный продукт BitDefender будет отвечать всем Вашим требованиям.

КРОМЕ ОГОВОРЕННЫХ УСЛОВИЙ ДАННОГО СОГЛАШЕНИЯ, BITDEFENDER ОТКАЗЫВАЕТСЯ ОТ ПРЕДОСТАВЛЕНИЯ ЛЮБЫХ ГАРАНТИЙ В ОТНОШЕНИИ ПРОГРАММНОГО ПРОДУКТА, УСОВЕРШЕНСТВОВАНИЙ, ПОДДЕРЖКИ И ПРОЧИХ УСЛУГ. НАСТОЩИМ BITDEFENDER ОТКАЗЫВАЕТСЯ ОТ ГАРАНТИЙ, ВКЛЮЧАЯ БЕЗ ОГРАНИЧЕНИЯ ЛЮБЫЕ ПОДРАЗУМЕВАЕМЫЕ ГАРАНТИИ КАЧЕСТВА И ПРИГОДНОСТИ ПРОГРАММЫ ДЛЯ ИСПОЛЬЗОВАНИЯ ПО НАЗНАЧЕНИЮ ИЛИ ДЛЯ КАКОЙ-ЛИБО ОПРЕДЕЛЕННОЙ ЦЕЛИ,ТОЧНОСТЬ ДАННЫХ, ТОЧНОСТЬ ИНФОРМАЦИОННОГО СОДЕРЖАНИЯ, СИСТЕМНУЮ ИНТЕГРАЦИЮ, А ТАКЖЕ НЕНАРУШЕНИЯ ПРАВА СОБСТВЕННОСТИ И ПРАВ НА ИНТЕЛЛЕКТУАЛЬНУЮ СОБСТВЕННОСТЬ ТРЕТЬИХ СТОРОН ПРИ ОТКЛЮЧЕНИИ ИЛИ УДАЛЕНИИ ПРОГРАММНЫХ ПРОДУКТОВ, ПРОГРАММ-ШПИОНОВ, РЕКЛАМНЫХ ПРОДУКТОВ, ЭЛЕКТРОННЫХ СООБЩЕНИЙ, КУКОВ, ДОКУМЕНТОВ И ПРОЧИХ АСПЕКТОВ.

ОТКАЗ ОТ ОТВЕТСТВЕННОСТИ ЗА ПОВРЕЖДЕНИЯ. Любое лицо, использующее, тестирующее или оценивающее программный продукт BitDefender несет все риски, касающиеся качества его работы и его функциональности. Компания BITDEFENDER не несет никакой ответственности за любой ущерб, включая, и не ограничиваясь, прямой и непрямой ущерб, возникший в результате неправильного использования, работы или установки BitDefender, даже если компания BITDEFENDER предупреждала о такой возможности ущерба.

В НЕКОТОРЫХ ШТАТЫ НЕ ПОЗВОЛЯЮТ ОГРАНИЧЕНИЕ ИЛИ ИСКЛЮЧЕНИЕ ОТВЕТСТВЕННОСТИ ЗА НЕПРЕДНАМЕРЕННЫЙ ИЛИ НЕПРЯМОЙ УЩЕРБ, ПОЭТОМУ УКАЗАННЫЕ ВЫШЕ ОГРАНИЧЕНИЯ ИЛИ ИСКЛЮЧЕНИЯ МОГУТ БЫТЬ НЕ ПРИМЕНИМЫ К ВАМ.

НИ В КАКОМ СЛУЧАЕ ОТВЕТСТВЕННОСТЬ BITDEFENDER НЕ МОЖЕТ ПРЕВЫШАТЬ СТОИМОСТИ, УПЛАЧЕННОЙ ПРИ ПОКУПКЕ ВАМИ BITDEFENDER. Установленные отказы и ограничения, упомянутые выше, будут применены не зависимо от Вашего принятия использования, оценивания или тестирования BitDefender.

ВАЖНОЕ ЗАМЕЧАНИЕ ДЛЯ ПОЛЬЗОВАТЕЛЕЙ. ДАННОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ НЕ ОТКАЗОУСТОЙЧИВО И НЕ ПРЕДНАЗНАЧЕНО ДЛЯ РАБОТЫ В ОПАСНЫХ УСЛОВИЯХ, ТРЕБУЮЩИХ БЕСПЕРЕБОЙНОЙ РАБОТЫ. ДАННОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ НЕ ПРЕДНАЗНАЧЕНО ДЛЯ ИСПОЛЬЗОВАНИЯ В СИСТЕМАХ НАВИГАЦИИ САМОЛЕТОВ, В ЯДЕРНЫХ ЦЕНТРАХ ИЛИ СИСТЕМАХ СВЯЗИ, В СИСТЕМАХ ВООРУЖЕНИЯ, В СИСТЕМАХ ПРЯМОГО ИЛИ НЕПРЯМОГО ЖИЗНЕОБЕСПЕЧЕНИЯ, В УПРАВЛЕНИИ ПОЛЕТАМИ ИЛИ В ЛЮБЫХ ДРУГИХ ВИДАХ ДЕЯТЕЛЬНОСТИ, ГДЕ ОШИБКА МОЖЕТ ПОВЛЕЧЬ ЗА СОБОЙ СМЕРТЬ, СЕРЬЕЗНЫЕ ПОВРЕЖДЕНИЯ ИЛИ БОЛЬШОЙ УЩЕРБ.

РАЗРЕШЕНИЕ НА ЭЛЕКТРОННЫЕ СООБЩЕНИЯ. BitDefender может посылать вам легальные уведомления или другие сообщения о программном обеспечении и подписку от службы поддержки, используя информацию, предоставленную вами ("Сообщения"). BitDefender будет отправлять вам сообщения посредством внутрипрограммных уведомлений, через электронную почту на первостепенно зарегистрированный адрес, или будет размещать сообщения на своих сайтах. Принимая это Соглашение, вы даете согласие получать все сообщения посредством только этих электронных способов и подтверждаете, что будете ознакамливаться с сообщениями на сайте.

ОБЩИЕ СВЕДЕНИЯ. Данное соглашение регулируется законами России и международными законами и соглашениями об авторских правах. Местом разрешения любых споров, возникших по данным Условиям лицензирования, являются судебные инстанции России, имеющие исключительную компетенцию.

Цены, издержки и штрафы за использование программного продукта BitDefender могут изменяться без предварительного уведомления.

В случае, если любой из пунктов Соглашения окажется недействительным, это не повлияет на остальные пункты данного Соглашения.

Название BitDefender и логотип BitDefender являются торговыми марками компании BITDEFENDER. Все остальные торговые марки являются собственностью их обладателей.

Лицензия будет немедленно отозвана без уведомления в случае, если Вы нарушите любые условия. Вы не имеете права требовать возмещения средств от BITDEFENDER или любых его дилеров при расторжении лицензии. Условия, касающиеся конфиденциальности и использования, остаются в силе и после расторжения.

BITDEFENDER оставляет за собой право пересмотреть данные Условия в любой момент, и пересмотренные условия автоматически будут применены к соотвествующим версиям программных продуктов, распространенных в указанные сроки. В случае, если любой из пунктов Условий лишится юридической или исковой силы, это не повлияет на остальные пункты данных Условий, которые останутся в силе.

В случае противоречия или несовместимости переводов данных условий на другие языки, версия на английском языке, предоставленная BITDEFENDER имеет высшую юридическую силу.

Свяжитесь с BITDEFENDER по адресу 24, Preciziei Boulevard, West Gate Building H2, ground floor, Sector 6, Bucharest, Romania, или телефону: 40-21-206.34.70 или факсу: 40-21-264.17.99, адрес электронной почты: office@bitdefender.com.

Предисловие

Данное руководство пользователя предназначено для всех пользователей, которые выбрали **BitDefender Antivirus 2009** для обеспечения защиты персональных компьютеров. Информация, представленная в этой книге, доступна не только для опытных компьютерных пользователей, но и для любого пользователя, знакомого с операционной системой Windows.

В этой книге Вы найдете описание программного продукта **BitDefender Antivirus 2009**, а также найдете сведения о нашей компании и группе разработчиков этого продукта, процесс установки и получите инструкции по настройки данной программы. Вы узнаете, как использовать продукт **BitDefender Antivirus 2009**, как обновлять, проверять и переделывать его под свои нужды. Вы узнаете,как добиться наилучших результатов при работе с BitDefender.

Мы желаем Вам увлекательного и поучительного чтения.

1. Соглашения, используемые в данной книге

1.1. Типографские обозначения

Для удобства читателей в этой книге используется несколько различных текстовых стилей для обозначения объектов, представленных в следующей таблице.

Виды шрифтов и стилей	Описание
`sample syntax`	Образцы написания напечатаны с `шрифтом с фиксированной шириной` символов.
http://www.bitdefender.com	Ссылки URL на внешние источники (http или ftp серверы).
support@bitdefender.com	Адреса электронной почты в тексте приводятся в качестве контактной информации.
«Предисловие» (p. xiv)	В кавычках приводятся внутренние ссылки на другие материалы в пределах этого документа.

Виды шрифтов и стилей	Описание
`filename`	Названия файлов и каталогов приводятся с использованием шрифтов с `фиксированной шириной символов`.
option	Все варианты программы напечатаны, используя **сильный** символы.
`sample code listing`	Программные коды приводятся с помощью шрифтов с `фиксированной ширины` символов.

1.2. Замечания

Замечания – это текстовая информация, выделенная в основном тексте различными графическими символами, целью которых является привлечь ваше внимание к дополнительной информации, имеющей отношение к содержанию текущего раздела руководства.

Замечание

Примечание – это краткое замечание. Хотя Вы можете пропустить его, в нем может содержаться ценная информация, например, определенная особенность или ссылка на источник, имеющий отношение к данному материалу.

Важно

Эта информация требует вашего внимания, и ее не рекомендуется пропускать. Обычно, здесь приводится важная информация о факторах, которые не имеют угрожающего характера для безопасности вашей системы.

Внимание

Это критическая информация, к которой следует отнестись с максимальным вниманием. Только неукоснительно следуя инструкциям, Вы сможете избежать угроз системе. Внимательно прочтите и попытайтесь понять суть предупреждения, поскольку в нем описываются весьма опасные угрозы для безопасности вашей системы.

2. Структура книги

Данная книга состоит из нескольких разделов, описывающих основные темы. Кроме того, приводится глоссарий, в котором разъясняются некоторые технические термины.

Установка. Пошаговые инструкции по установке BitDefender на рабочую станцию. Это подробное руководство по установке **BitDefender Antivirus 2009**. После проверки выполнения необходимых условий для успешной установки программы, Вы узнаете о всех этапах инсталляции. В конце дается описание процедуры в случае необходимости удалить программу BitDefender.

Основны администрирования. Описание основных процедур администрирования и обслуживания BitDefender.

Расширенное Администрирование. Детальное описание всех возможностей обеспечения безопасности при помощи продукта BitDefender. Вы узнаете как настраивать и пользоваться всеми модулями BitDefender для эффективной защиты Вашего компьютера от всевозможных угроз (вирусов, программ-шпионов, руткитов и т.д.).

Получение справки. Места, где следует искать справочную информацию и куда обращаться за помощью в случае возникновения неожиданных проблем.

BitDefender Rescue CD. Описание компакт-диска Реаниматор BitDefender. Этот материал поможет Вам изучить и использовать возможности, которые дает использование этого самозагружаемого компакт-диска.

Глоссарий. В глоссарии даются пояснения некоторых технические и непривычных терминов, которые встречаются в данном документе.

3. Ваши комментарии

Мы будем приветствовать ваши замечания по улучшению этой книги. Мы очень тщательно проверили всю информацию, изложенную в этой книге. Пожалуйста, напишите нам о любых погрешностях и ошибках, найденных Вами в этой книге, а также ваши рекомендации по ее улучшению. Учет ваших замечаний поможет нам обеспечивать Вас максимально улучшенной документацией.

Пожалуйста, направляйте свои замечания по электронной почте по адресу documentation@bitdefender.com.

Важно

Пожалуйста, присылайте все Ваши электронные сообщения относительно документации на русском языке, чтобы мы могли оперативно их обработать.

Установка

1. Системные требования

Вы можете устанавливать BitDefender Antivirus 2009 только на компьютерах, работающих под следующими операционными системами.

- Windows XP Сервисный Пакет 2 (32/64 bit) или выше
- Windows Vista (32/64 bit) или Windows Vista с Сервисным Пакетом 1
- Домашний Сервер Windows

Перед установкой убедитесь, что ваш компьютер отвечает минимальным требованиям программного обеспечения и комплектующих.

Замечание
Чтобы узнать, на какой операционной системе работает ваш компьютер и информацию о его комплектующих, нажмите правой клавишей мышки **Мой Компьютер** на Рабочем столе и далее выберите **Свойства** в меню.

1.1. Требования к комплектующим компьютера

Для Windows XP

- 800 МГц процессор или выше
- 256 Мб оперативной памяти (рекомендуется 1Гб)
- 170 Мб свободного пространства на жестком диске (200 Мб рекомендуется)

Для Windows Vista

- 800 МГц процессор или выше
- 512Мб оперативной памяти (рекомендуется 1Гб)
- 170 Мб свободного пространства на жестком диске (200 Мб рекомендуется)

Для Домашнего Сервера Windows

- 800 МГц процессор или выше
- 512Мб оперативной памяти (рекомендуется 1Гб)
- 170 Мб свободного пространства на жестком диске (200 Мб рекомендуется)

1.2. Требования Программного обеспечения

- Internet Explorer 6.0 (или выше)
- .NET Framework 1.1 (также доступен в установочном наборе)

Антифишинг защита предоставляется только для:

- Internet Explorer 6.0 или выше
- Mozilla Firefox 2.0
- Yahoo! Messenger 8.1
- Windows Live (MSN) Messenger 8.5

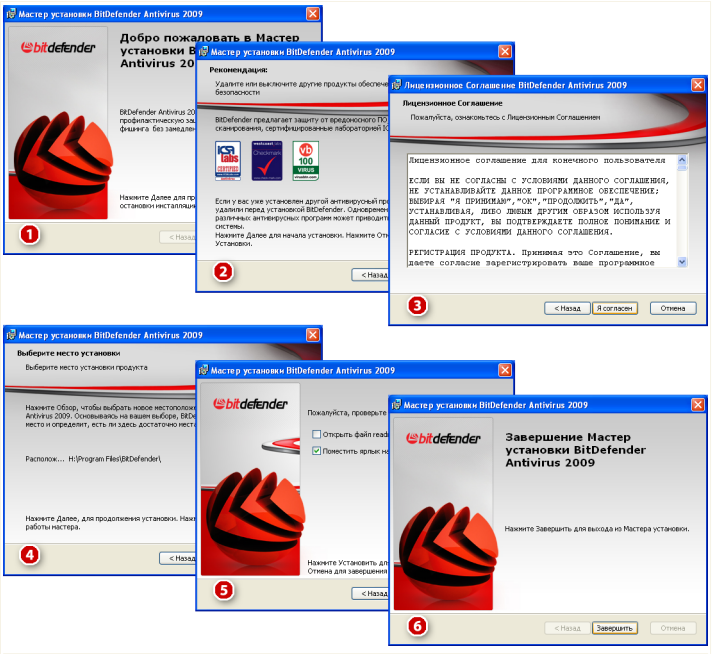
Шифрование мгновенных сообщений (IM) осуществляется только для:

- Yahoo! Messenger 8.1
- Windows Live (MSN) Messenger 8.5

2. Установка BitDefender

Найдите файл setup и дважды щелкните по нему. Запустится мастер установки программы.

Перед запуском мастера установки, BitDefender проверит наличие более новых версий пакета установки. Если доступна более новая версия, Вам предложат загрузить ее. Нажмите **Да**, чтобы загрузить более новую версию, или **Нет**, чтобы продолжать установку версии, предусмотренной в файле установки.



Пошаговая установка

Выполните следующие шаги для установки BitDefender Antivirus 2009:

1. Щелкните по кнопке **Далее** чтобы продолжить, или по кнопке **Отменить** если Вы хотите прервать установку.
2. Щелкните по кнопке **Далее**.

   BitDefender Antivirus 2009 предупредит Вас, если на вашем компьютере установлены другие антивирусные продукты. Нажмите **Удалить**, чтобы деинсталлировать соответствующий продукт. Если Вы хотите продолжить, не удаляя обнаруженные продукты, нажмите **Далее**.

   Внимание
   Убедительно рекомендуем Вам удалить все другие антивирусные программы перед установкой BitDefender. Одновременная работа двух или более антивирусных продуктов на компьютере обычно приводит к нарушению стабильности системы.

3. Пожалуйста, прочтите Лицензионное Соглашение и нажмите **Согласен**.

   Важно
   Если вы не согласны с условиями, нажмите **Отмена**. Установка будет прервана, и Вы выйдете из программы установки.

4. По-умолчанию, BitDefender Antivirus 2009 будет установлен в директорию `C:\Program Files\BitDefender\BitDefender 2009`. Если вы хотите выбрать другую папку для установки, нажмите **Обзор**, а затем в открывшемся окне выберите папку, куда хотите установить BitDefender.

   Щелкните по кнопке **Далее**.

5. Выберите опции, имеющие отношения к процессу установки. Некоторые из них будут выбраны по умолчанию::
   - **Открыть ознакомительный файл** - открывает ознакомительный файл в конце установки.
   - **Создать ярлык на рабочем столе** - создает ярлык BitDefender Antivirus 2009 на рабочем столе в конце установки.
   - **Извлечь CD из привода после окончания установки** - позволяет извлечь диск из привода после окончания установки; данная опция появляется при установке продукта с CD.

- **Выключить Защиту Windows** - выключает Защиту Windows (доступна только для Windows Vista).

Щелкните по кнопке **Установить** и начните установку программы. BitDefender установит сначала .NET Framework 1.1, если он еще не установлен.

Подождите, пока завершится процесс установки.

6. Щелкните мышкой на кнопке **Завершить**. Может появиться сообщение с просьбой перезагрузить вашу систему для того, чтобы мастер установки мог завершить процесс установки. Мы рекомендуем выбрать эту функцию.

Важно

После окончания установки и перезагрузки компьютера, мастер регистрации и мастер настроек появятся. Запустите эти мастера для регистрации и конфигурации BitDefender Antivirus 2009 и для создания учетной записи BitDefender.

Если вы приняли настройки установки по умолчанию, вы можете увидеть в `Program Files` новую папку `BitDefender`, в которой будет находиться подкаталог `BitDefender 2009`.

2.1. Мастер регистрации

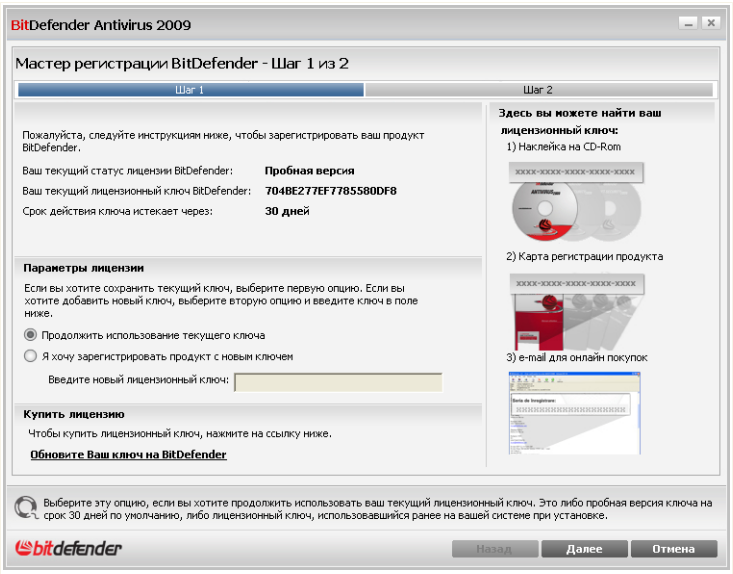
Когда вы перезагрузите компьютер после установки, появится мастер регистрации. Этот мастер поможет вам зарегистрировать BitDefender и настроить учетную запись BitDefender.

Вам НЕОБХОДИМО создать учетную запись BitDefender чтобы получать обновления BitDefender. Учетная запись BitDefender также даст вам доступ к бесплатной технической поддержке, специальным предложениям и поощрениям. Если вы утеряете BitDefender лицензионный ключ, вы сможете зайти в свою учетную запись по ссылке http://myaccount.bitdefender.com, чтобы восстановить его.

Замечание

Если Вы не хотите запускать этот мастер, нажмите **Отмена**. Вы сможете запустить мастер регистрации в любое время, нажав на ссылку **Зарегистрировать**, расположенной внизу пользовательского интерфейса.

2.1.1. Шаг 1/2 - Регистрация BitDefender Antivirus 2009



Регистрация

Вы можете просмотреть статус регистрации BitDefender, действующий лицензионный ключ, и количество дней, которые остались до окончания срока действия лицензии.

Чтобы продолжить пользоваться пробной версией продукта, выберите **Продолжить пользоваться текущим ключем**.

Для регистрации BitDefender Antivirus 2009:

1. Выберите **Я хочу зарегистрировать продукт с новым ключем**.
2. Введите лицензионный ключ в поле для редактирования.

Замечание

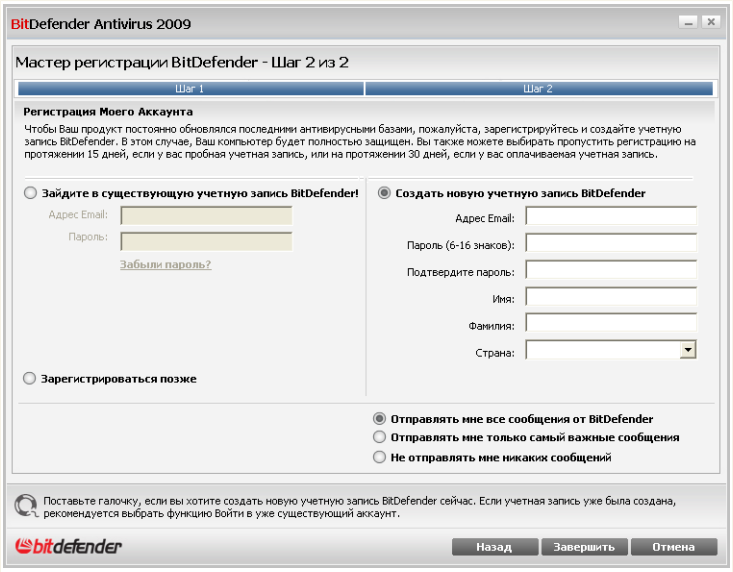
Вы можете найти ваш лицензионный ключ:

- на обложке CD.
- на регистрационной карточке продукта.
- в электронном письме о покупке.

Если у Вас нет лицензионного ключа BitDefender, нажмите соответствующую ссылку для перехода в онлайн-магазин BitDefender и приобретите лицензионный ключ.

Для продолжения нажмите **Далее**.

2.1.2. Шаг 2/2 - Создание учетной записи BitDefender



Создание учетной записи

Если Вы не хотите создавать учетную запись BitDefender, выберите **Пропустить регистрацию** и нажмите **Завершить**. В другом случае, действуйте исходя из вашей ситуации:

- «У меня нет учетной записи BitDefender» (p. 9)
- «У меня уже есть учетная запись BitDefender» (p. 10)

Важно

Вам необходимо создать учетную запись в течении 15 дней со дня установки BitDefender (если вы его зарегистрировали, в течении 30 дней). В противном случае, BitDefender не будет обновляться.

У меня нет учетной записи BitDefender

Для создания учетной записи BitDefender выберите **Создать новую учетную запись BitDefender** и введите требуемую информацию. Предоставленные Вами данные конфиденциальны.

- **Адрес электронной почты** - введите адрес своей электронной почты.
- **Пароль** - введите пароль Вашей учетной записи BitDefender. Длина пароля должна быть не менее шести символов.
- **Повторите пароль** - снова введите набранный ранее пароль.
- **Имя** - введите Ваше имя.
- **Фамилия** - введите Вашу фамилию.
- **Страна** - выберите страну, в которой находитесь.

Замечание

Используйте указанные адрес электронной почты и пароль для доступа к своей учетной записи на http://myaccount.bitdefender.com.

Чтобы успешно создать учетную запись, Вы должны прежде всего активировать свой электронный адрес. Проверьте электронную почту и следуйте инструкциям в письме, которое будет выслано Вам службой регистрации BitDefender.

Дополнительно, BitDefender может информировать вас о специальных предожениях и поощрениях, через адрес электронной почты, указанной в вашей учетной записи. Выберите одну из доступных функций:

- **Отправлять мне все сообщения от BitDefender**
- **Отправлять мне наиболее важные сообщения**
- **Не отправлять мне сообщения**

Щелкните мышкой на кнопке **Завершить**.

У меня уже есть учетная запись BitDefender

BitDefender автоматически определит, если вы решистрировали учетную запись BitDefender ранее на этом компьютере. В этом случае, предоставьте пароль вашей учетной записи.

Если у Вас уже есть активная учетная запись, но BitDefender не определяет ее, выберите **Использовать существующую учетную запись BitDefender** и укажите e-mail и пароль Вашей учетной записи.

Если Вы забыли пароль, нажмите **Забыли пароль?** и следуйте инструкциям.

Дополнительно, BitDefender может информировать вас о специальных предожениях и поощрениях, через адрес электронной почты, указанной в вашей учетной записи. Выберите одну из доступных функций:

- **Отправлять мне все сообщения от BitDefender**
- **Отправлять мне наиболее важные сообщения**
- **Не отправлять мне сообщения**

Щелкните мышкой на кнопке **Завершить**.

2.2. Мастер Конфигурации

Когда вы закончите работу с мастером регистрации, появится мастер настроек. Этот мастер поможет вам сконфигурировать особые модули продукта и настроить BitDefender для выполнения важных задач безопасности.

Завершение всех шагов мастера необязательно; однако, мы рекомендуем Вам завершить все шаги, чтобы сэкономить время и убедиться, что Ваша система находится в безопасности еще до установки BitDefender Antivirus 2009.

Замечание

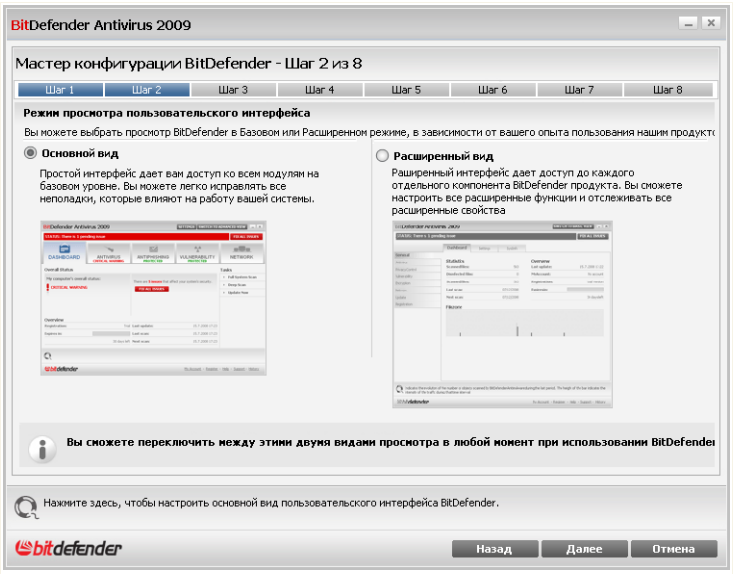
Если Вы не хотите запускать этот мастер, нажмите **Отмена**. BitDefender уведомит вас о необходимости настройки компонентов, когда вы откроете пользовательский интерфейс.

2.2.1. Шаг 1/8 - Окно приветствия

Окно приветствия

Для продолжения нажмите **Далее**.

2.2.2. Шаг 2/8 - Режим Просмотра



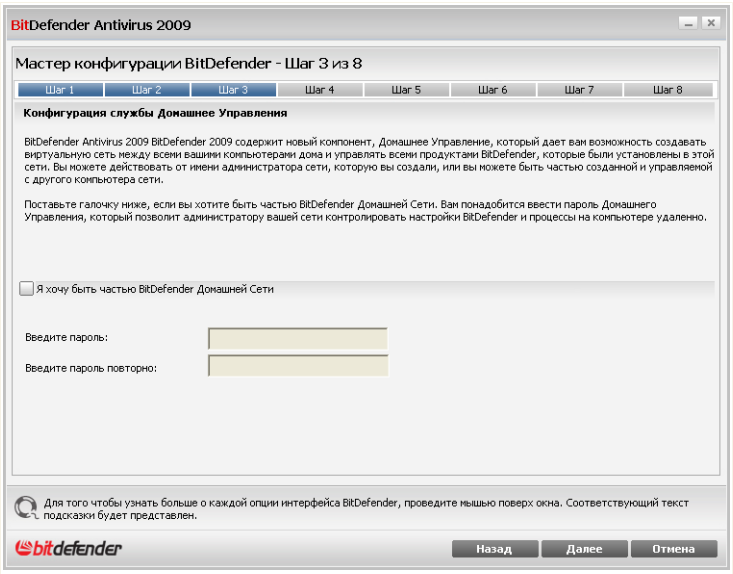
Режимы Просмотра

Выберите между двумя режимами просмотра в пользовательском интерфейсе, зависимо от вашего опыта работы с BitDefender:

- **Основной вид.** Простой интерфейс подходит для начинающих и тех пользователей, которые хотят выполнять основные задачи и легко решать проблемы. Вам просто следует следить за предупреждениями и сигналами BitDefender и устранять появляющиеся неполадки.
- **Расширенный вид.** Расширенный интерфейс подходит для более опытных технических пользователей, которые хотят полностью настроить продукт. Вы можете проводить конфигурацию каждого компонента продукта и выполнять дополнительные задачи.

Для продолжения нажмите **Далее**.

2.2.3. Шаг 3/8 - Настроить Сеть BitDefender



Конфигурация сети BitDefender

BitDefender позволяет вам создать виртуальную сеть компьютеров для домашнего использования и управлять продуктами BitDefender, установленными в этой сети.

Если вы хотите чтобы этот компьютер был частью домашней сети BitDefender, необходимо выполнить следующие шаги:

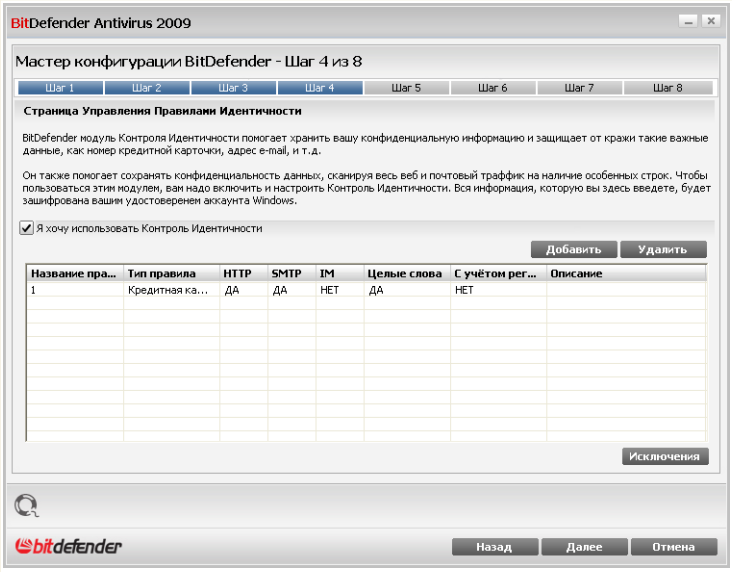
1. Выберите **Я хочу быть частью домашней сети BitDefender**.
2. Введите один и тот же пароль администратора в каждое поле для редактрирования.

Важно

Пароль позволяет администратору управлять этим продуктом BitDefender с другого компьютера.

Для продолжения нажмите **Далее**.

2.2.4. Шаг 4/8 - Настройка Контроля конфиденциальности



Настройка контроля конфиденциальности

Контроль конфиденциальности защищает вас от кражи уязвимых данных, когда вы в режиме онлайн. Основываясь на созданные вами правила, Контроль Конфиденциальности сканирует веб-траффик, электронную почту и траффик мгновенных сообщений, которые требуют от вашего компьютера особых строк символов (например, номер вашей кредитной карточки). Если есть совпадение, соответствующая веб-страница, адрес электронной почты или мгновенное сообщение блокируется.

Если вы хотите использовать Контроль конфиденциальности, необходимо выполнить следующие шаги:

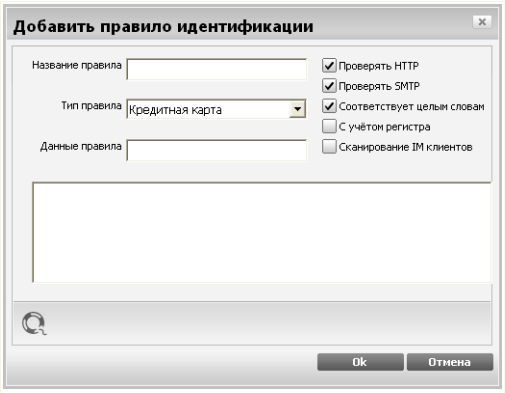
1. Выберите **Я хочу произвести конфигурацию сейчас**.

2. Создавайте правила для защиты ваших уязвимых данных. Чтобы узнать больше, обращайтесь «Создание правил Контроля конфиденциальности» (p. 15).
3. При необходимости, определите особые исключения для правил, которые вы создали. Чтобы узнать больше, обращайтесь «Определение исключений в контроле конфединциальности» (p. 16).

Для продолжения нажмите **Далее**.

Создание правил Контроля конфиденциальности

Для создания правила Контроля конфиденциальности, нажмите **Добавить**. Появится окно настроек.



Правило Контроля конфиденциальности

Вам необходимо настроить следующие параметры:

- **Имя правила** - введите имя правила в поле для редактирования.
- **Тип правила** - выберите тип правила (адрес, имя, кредитная карта, PIN-код и т.д.).
- **Данные Правила** - введите данные, которые вы хотите защитить, в это поле для редактирования. К примеру, если вы хотите защитить номер вашей кредитной карточки, введите его частично или весь здесь.

Замечание
Если Вы введете менее трех символов, Вам будет предложено уточнить данные. Рекомендуем Вам ввести минимум три символа, чтобы избежать блокирования по ошибке сообщений и веб-страниц.

Вы можете применять правило только в случае, если совпадение произойдет по целому слову, или же если совпадение произойдет по вхождению искомой строки.

Для более идентификации информации в блоках правил, введите детальное описание правила в поле редактирования.

Чтобы выбрать тип трафика для сканирования, настройте эти функции:

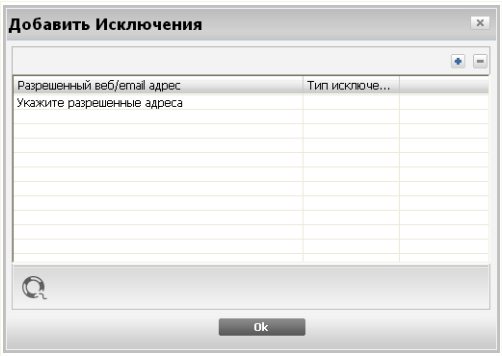
- **Проверять HTTP** - поверяет HTTP (веб) трафик и блокирует исходящие данные, содержащие данные правила.
- **Проверять SMTP** - поверяет SMTP (почта) трафик и блокирует исходящие электронные сообщения, содержащие данные правила.
- **Проверка мгновенных сообщений** - поверяет трафик мгновенных сообщений и блокирует исходящие сообщения в чатах, содержащие данные правила.

Нажмите **OK**, чтобы добавить правило.

Определение исключений в контроле конфединциальности

Есть случаи, когда Вы должны определить исключения к определенным правилам конфиденциальности. Давайте рассмотрим пример, когда Вы хотите создать правило, предотвращающее отсылание номера Вашей кредитной карты через HTTP (веб). Каждый раз, когда номер Вашей кредитной карты будет отправлен с веб-сайта со страницы Вашей учетной записи, соответствующая страница будет заблокирована. Если, например, вы хотите совершить покупку в Интернет-магазине (в безопасности которого Вы уверены), Вам необходимо будет создать исключение из соответствующего правила.

Откройте окно где вы можете управлять исключениями, нажмите **Исключения**.



Исключения Контроля конфиденциальности

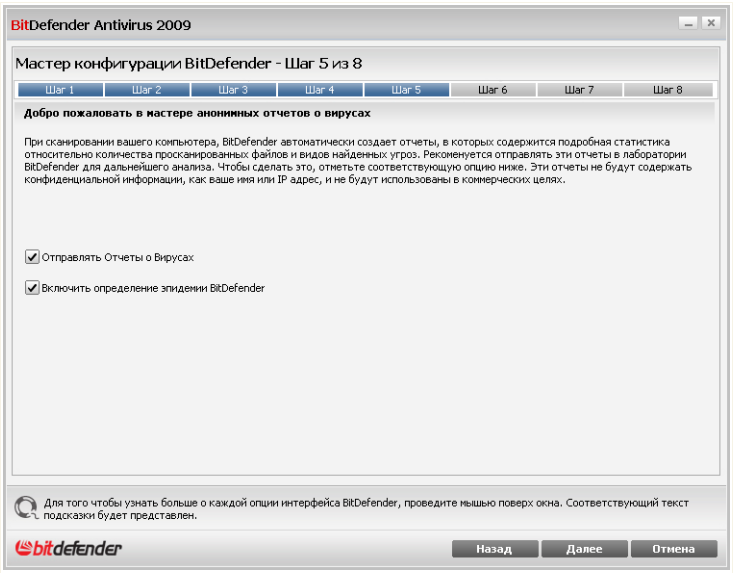
Добавить исключение, следуя по этим шагам:

1. Нажмите **Добавить** чтобы добавить в таблицу.
2. Двойной щелчок на **Указать допустимые адреса** и укажите веб-адрес или электронный почтовый адрес, который Вы хотите добавить в качестве исключения.
3. Двойной щелчок на **Выберите тип** и выберите в меню соответствующий тип ранее указанного адреса.
   - Если у Вас есть определенный веб адрес, выберите **HTTP**.
   - Если у Вас есть определенный почтовый адрес, выберите **SMTP**.

Чтобы удалить, выберите нажмите кнопку **Удалить**.

Щелкните мышкой на кнопке **OK** и закройте окно.

2.2.5. Шаг 5/8 - Создание отчета



Настройки отчета

С целью отслеживания распространения компьютерных вирусов приложение BitDefender может отправлять в лабораторию BitDefender анонимные отчёты о вирусах, обнаруженных на вашем компьютере.

Вы можете установить следующие параметры:

- **Отправлять отчеты о вирусах** - Отправлять в лабораторию BitDefender отчеты о вирусах, обнаруженных на вашем компьютере.
- **Включить определение эпидемии BitDefender** - отправлять в лабораторию BitDefender отчеты о потенциальных вирусных эпидемиях.

Замечание
Отчеты не будут содержать конфиденциальной информации, такой как, например, ваше имя или IP-адрес, и они не будут использоваться в коммерческих целях.

Для продолжения нажмите **Далее**.

2.2.6. Шаг 6/8 - Выбор задач для запуска

Выбор задачи

Настройте BitDefender Antivirus 2009 на выполнение важных задач для обеспечения безопасности вашей системы. Доступными являются следующие варианты:

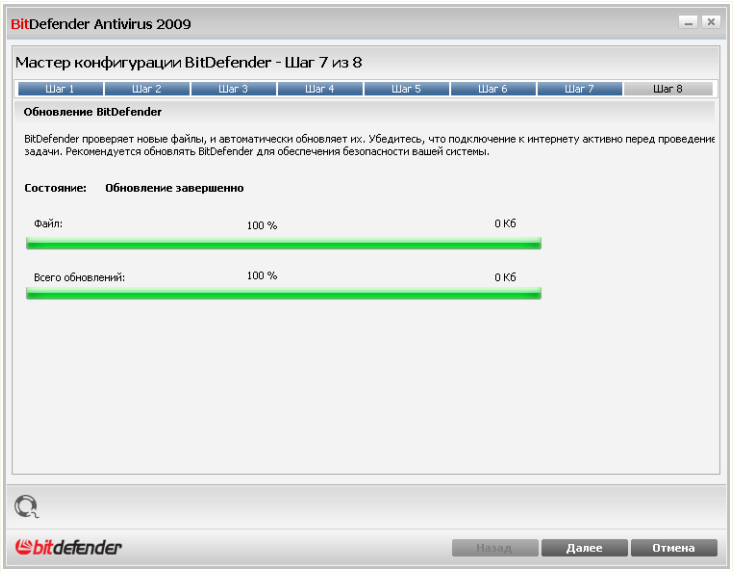
- **Обновить модули BitDefender (может потребоваться перезагрузка)** - на следующем шаге будет произведено обновление модулей BitDefender, чтобы обеспечить защиту Вашего компьютера от новых вирусов и угроз.
- **Запустить быструю проверку системы** - на следующем шаге будет проведена быстрая проверка системы, чтобы BitDefender мог убедиться, что файлы в папках `Windows` и `Program Files` не заражены.
- **Запускать полное сканирование системы ежедневно в 2:00 утра** - запускает полное сканирование системы ежедневно в 2:00 утра.

Важно
Рекомендуем Вам включить данные опции перед тем, как перейти к следующему шагу, чтобы обеспечить полную безопасность Вашей системы.

Если Вы выбрали только последнюю опцию или не выбрали ни одной, то следующий шаг будет пропущен.

Для продолжения нажмите **Далее**.

2.2.7. Шаг 7/8 - Ожидание завершения задач



Статус задачи

Подождите, пока задачи завершатся. Вы можете наблюдать статус выполнения задачи, выбранной на прошлом шаге.

Для продолжения нажмите **Далее**.

2.2.8. Шаг 8/8 - Конец

Завершить

Выберите **Открыть мою учетную запись BitDefender**, чтобы войти в Вашу учетную запись BitDefender. Необходимо соединение с интернетом.

Щелкните мышкой на кнопке **Завершить**.

3. Обновление

Чтобы обновить старую версию BitDefender до BitDefender Antivirus 2009, выполните следующую процедуру:

1. Удалите старую версию BitDefender со своего компьютера. Более подробную информацию смотрите в справке или руководстве пользователя к приложению.
2. Перезагрузите компьютер.
3. Установите BitDefender Antivirus 2009, как описано в разделе «*Установка BitDefender*» (p. 4) данного руководства пользователя.

4. Удаление или восстановление BitDefender.

Если Вы хотите удалить или восстановить **BitDefender Antivirus 2009**, выполните следующие действия, начиная с меню Пуск: **Пуск** → **Программы** → **BitDefender 2009** → **Восстановить или удалить**.

Подтвердите свой выбор, щелкнув по кнопке **Далее**. В появившемся окне выберите:

- **Восстановить** - переустановка всех установленных компонентов программы.

  Если Вы выбираете эту опцию, появится следующее окно: Нажмите **Восстановить**, чтобы начать процесс восстановления.

  Перегрузите компьютер после соответствующего предложения, а затем нажмите **Установить**, чтобы переустановить BitDefender Antivirus 2009.

  Как только процесс установки завершен, появится новое окно. Щелкните мышкой на кнопке **Завершить**.

- **Удалить** - удаление всех установленных компонентов.

  Замечание
  Рекомендуем вам выбрать**Удалить** для корректной переустановки.

  Если Вы выбираете удалить BitDefender, появится новое окно.

  Важно
  Только Windows Vista! Удаляя BitDefender, вы лишаетесь защиты от вредоносных программ, таких как вирусы и программы-шпионы. Если вы хотите активировать собственную защиту Windows после удаления BitDefender, отметьте соответствующее поле.

  Нажмите **Удалить**, чтобы начать удаление BitDefender Antivirus 2009 с Вашего компьютера.

  В процессе удаления Вам будет предложено оставить отзыв. Нажмите **OK**, чтобы перейти к странице он-лайн вопросов и ответить на некоторые короткие вопросы. Если Вы не хотите проходить опрос, нажмите **Завершить**.

  Как только процесс удаления закончится, появится новое окно. Щелкните мышкой на кнопке **Завершить**.

Замечание
После окончания процесса удаления, рекомендуем удалить папку `BitDefender` из директории `Program Files`.

При удалении BitDefender возникла проблема.

Если во время удаления BitDefender возникла ошибка, процесс будет отменен, и появится новое окно. Чтобы убедиться, что BitDefender полностью удален с Вашего компьютера, нажмите **Запустить инструмент удаления**. Он удалит все файлы и записи в реестре, которые не были удалены во время автоматического процесса.

Основны администрирования

5. Начало работы

Как только вы установите BitDefender, защита вашего компьютера будет обеспечена.

5.1. Запуск BitDefender Antivirus 2009

Чтобы начать использование функций BitDefender, сначала запустите приложение.

Чтобы открыть главный интерфейс BitDefender, воспользуйтесь меню "Пуск": **Пуск → Программы → BitDefender 2009 → BitDefender Antivirus 2009**, или более быстрым вариантом: дважды щелкните **значок BitDefender** на панели задач.

5.2. Режим просмотра пользовательского интерфейса

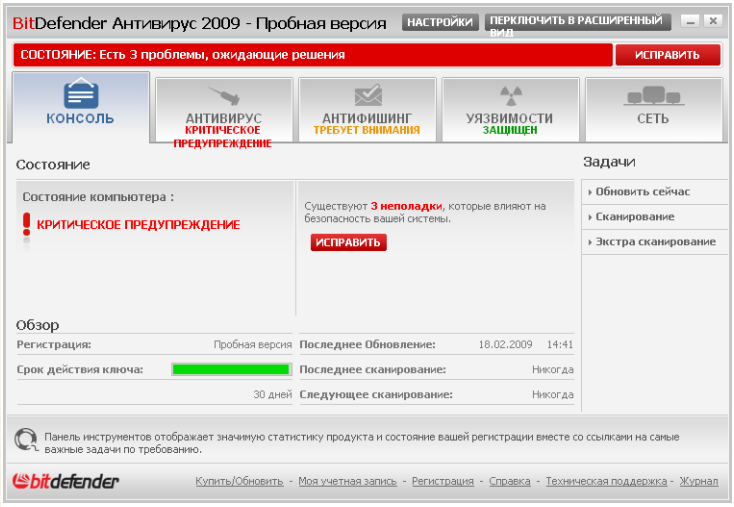
Приложение BitDefender Antivirus 2009 удовлетворяет требованиям как технически подкованных пользователей, так и новичков, так как его графический интерфейс удобен для любой категории пользователей.

Вы можете выбрать просмотр BitDefender в Базовом или Расширенном режиме, в зависимости от вашего опыта пользования нашим продуктом.

Замечание
Вы можете легко переключаться между этими окнами, нажимая кнопку **Переключить в основной вид** или **Переключить в расширенный вид** соответственно.

5.2.1. Основной вид

Основной вид является упрощенным интерфейсом, предоставляющим доступ ко всем модулям на базовом уровне. Вам придется отслеживать предупреждения и важные уведомления, а также исправлять возникающие проблемы.



Основной вид

- Как вы уже, наверное, заметили, в верхней части окна расположены две кнопки и строка состояния.

Элемент	*Описание*
Настройки	Открыть окно, где можно легко включить или отключить важные модули безопасности.
Переключить в расширенный вид	Открытие окна расширенного вида. В этом окне вы сможете увидеть полный список модулей и подробно настроить каждый компонент. BitDefender использует этот параметр в следующий раз при открытии интерфейса.
Состояние	Отображение информации о приложении и помощь в устранении уязвимостей в компьютере.

- Внутри окна расположены пять вкладок.

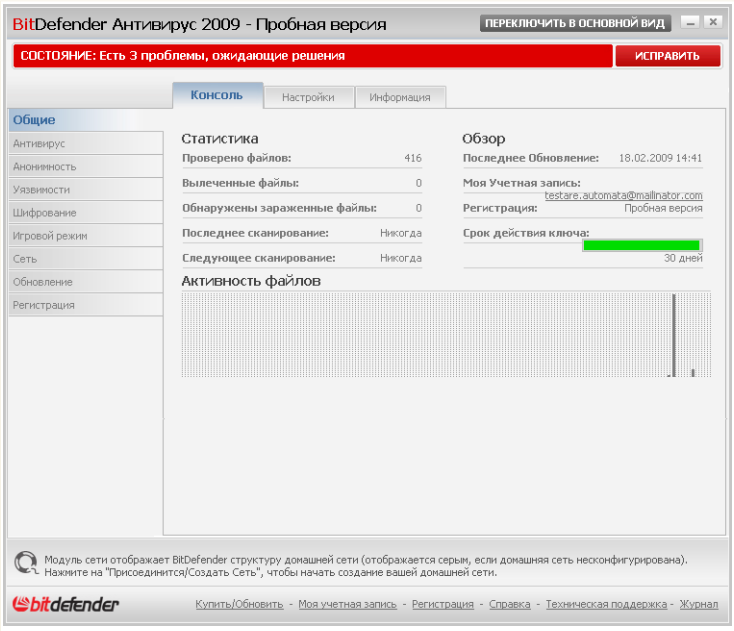
Вкладка	Описание
Консоль	Отобразить важную статистику по продукту и ваше состояние регистрации со ссылками на основные задачи, выполняемые по требованию.
Антивирус	Отображение состояния антивирусного модуля BitDefender, который помогает поддерживать BitDefender всегда в обновленном состоянии и надежно защищать компьютер от вирусов.
Антифишинг	Отображение состояния антифишингового модуля, который обеспечивает безопасный доступ ко всем веб-страницам, открываемым программами Internet Explorer или Firefox.
Уязвимости	Отображение состояния модуля сканирования уязвимостей, который помогает держать важные приложения на вашем компьютере в обновленном состоянии.
Сеть	Отображение структуры домашней сети BitDefender.

- Кроме того, основной вид окна BitDefender содержит несколько полезных ссылок.

Ссылка	Описание
Моя учетная запись	Создание или вход в учетную запись BitDefender. Учетная запись BitDefender предоставляет бесплатный доступ к службе техподдержки.
Регистрация	Ввод нового лицензионного ключа или отображение текущего лицензионного ключа и состояния регистрации.
Справка	Доступ к файлу справки о пользовании приложением BitDefender.
Техническая поддержка	Обращение в службу поддержки BitDefender.
Журнал	Просмотр подробного отчета о всех задачах, выполненных приложением BitDefender в вашей системе.

5.2.2. Расширенный вид

Расширенный вид обеспечивает доступ к каждому конкретному компоненту приложения BitDefender. Благодаря ему вы сможете настроить дополнительные параметры, а также отслеживать дополнительные функции.



Расширенный вид

- Как вы, наверное, уже заметили, в верхней части окна расположены кнопка и строка состояния.

Элемент	Описание
Переключить в основной вид	Открытие окна основного вида. В этом окне вы сможете увидеть базовый интерфейс BitDefender, включая основные модули (Безопасность, Настройка, Менеджер файлов, Сеть) и консоль. BitDefender использует этот параметр в следующий раз при открытии интерфейса.

Элемент	Описание
Состояние	Отображение информации о приложении и помощь в устранении уязвимостей в компьютере.

- В левой части окна расположено меню с перечнем всех модулей безопасности.

Модуль	Описание
Общие	Доступ к основным параметрам или просмотр консоли и подробных сведений о системе.
Антивирус	Подробная настройка антивирусных параметров и операций сканирования. Здесь также можно настроить исключения и модуль карантина.
Анонимность	Предотвращение кражи данных с вашего компьютера и защита вашей конфиденциальности, когда вы находитесь в режиме онлайн.
Шифрование	Шифрование обмена сообщениями между интернет-пейджерами Yahoo Messenger и Windows Live (MSN) Messenger.
Уязвимости	Этот параметр позволяет держать важные приложения на вашем ПК в обновленном состоянии.
Режим Игровой/Ноутбук	Позволяет отложить задачи BitDefender по расписанию, пока ноутбук работает от батареи, а также убрать все уведомления и всплывающие окна во время игры.
Сеть	Позволяет настраивать несколько компьютеров у вас дома и управлять ими.
Обновление	Получение сведений о последних обновлениях, собственно обновление и настройка процесса обновления продукта.
Регистрация	Регистрация продукта BitDefender Antivirus 2009, смена лицензионного ключа и создание учетной записи BitDefender.

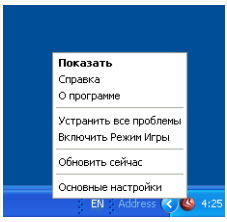
- Кроме того, расширенный вид окна BitDefender содержит несколько полезных ссылок.

Ссылка	Описание
Моя учетная запись	Создание или вход в учетную запись BitDefender. Учетная запись BitDefender предоставляет бесплатный доступ к службе техподдержки.
Регистрация	Ввод нового лицензионного ключа или отображение текущего лицензионного ключа и состояния регистрации.
Справка	Доступ к файлу справки о пользовании приложением BitDefender.
Техническая поддержка	Обращение в службу поддержки BitDefender.
Журнал	Просмотр подробного отчета о всех задачах, выполненных приложением BitDefender в вашей системе.

5.3. Значок BitDefender в системном трее.

Чтобы еще быстрее управлять всей программой, воспользуйтесь ярлыком BitDefender в панели задач.

Двойной щелчок по этому значку открывает приложение BitDefender. Кроме того, щелчок правой кнопкой мыши по значку открывает контекстное меню, которое обеспечивает быстрое управление приложением BitDefender.



Значок BitDefender

- **Показать** - открывает окно BitDefender.
- **Справка** - Открытие файла справки с подробными инструкциями к приложению BitDefender Antivirus 2009.
- **О компании** - открывает веб-страницу BitDefender
- **Исправить все проблемы** - помогает устранить имеющиеся уязвимости в безопасности компьютера.
- **Включить / выключить режим игры** - переключает Режим Игры вкл / выкл.
- **Обновить сейчас** - запускает немедленное обновление. Когда проверка завершится, откроется новое окно, где Вы можете увидеть результаты проверки.
- **Основные настройки** - Включение и выключение важнейших модулей безопасности. Появится новое окно, где вы сможете включать и выключать их одним щелчком.

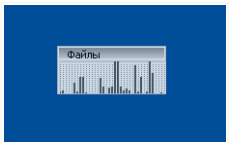
Всякий раз находясь в игровом режиме вы будете видеть букву G поверх значка BitDefender.

Если есть критические проблемы, которые затрагивают безопасность вашей системы, то на значке BitDefender будет отображен восклицательный знак. Вы можете подвести курсор мыши к значку, чтобы увидеть число проблем.

5.4. Полоса Активности Сканирования

В окне **График активности** графически показано, как проходит проверка Вашейсистемы на наличие вирусов.

Серые полоски (**Файловая зона**) показывают число проверенных файлов в секунду, по шкале от 0 до 50.



Строка состояния

Замечание
Если проверка в реальном времени отключена, то будет отображаться красный крест поверх **Файловой зоны**.

Вы можете использовать **Панель активной проверки** для проверки объектов. Для этого перетащите объекты, которые Вы желаете проверить, прямо на нее. Для дополнительной информации, перейдите к «*Проверка перетаскиванием*» (p. 122).

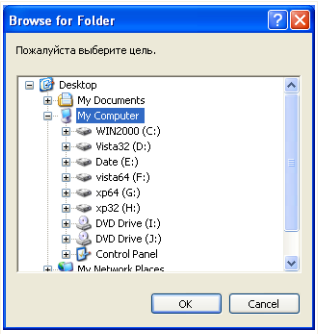
Чтобы убрать это окно с экрана, просто щелкните правой кнопкой мышки на нем и выберите пункт меню **Скрыть**. Чтобы полностью скрыть это окно, выполните следующую процедуру:

1. Нажмите **Переключить в расширенный вид** (если включен **Основной вид**).
2. Вызовите модуль **Общие** из левого бокового меню.
3. Щелкните на вкладке **Настройки**.
4. Снимите флажок **Включить строку состояния сканирования (на экранном графике активности продукта)**.

5.5. Ручная проверка BitDefender

Если Вы хотите быстро проверить содержимое какой-либо папки, Вы можете воспользоваться ручной проверкой BitDefender.

Чтобы открыть Ручное сканирование BitDefender, воспользуйтесь меню Пуск в Windows: **Пуск → Программы → BitDefender 2009 → BitDefender Manual Scan** Появится следующее окно:



Ручная проверка BitDefender

Необходимо найти нужную папку, которую Вы хотите просканировать, и нажать **OK**. Модуль BitDefender Scanner будет запущен и обеспечит процесс проверки.

5.6. Игровой режим

Новый Режим Игры изменяет параметры настроек системы защиты для того, чтобы снизить к минимуму воздействие на компьютер во время игры, при этом поддерживая безопасность на высоком уровне. Если вы находитесь в игровом режиме, применяется следующая процедура:

- Сводится к минимуму использование процессорного времени и оперативной памяти
- Откладываются автоматические задачи обновления и сканирования
- Отключаются все уведомления и всплывающие окна
- Сканируются только самые важные файлы

Всякий раз находясь в игровом режиме вы будете видеть букву G поверх значка BitDefender.

5.6.1. Использование Игрового режима

Если Вы хотите включить Режим игры можно воспользоваться одним из следующих способов:

- Кликните правой кнопкой мыши на иконке BitDefender в системном трее и установите **Включить Режим Игры**.

- Нажмите `Ctrl+Shift+Alt+G` (горячая клавиша по умолчанию).

Важно
Не забудьте отключить Режим Игры, когда закончите. Чтобы сделать это, используйте один из способов, каким Вы его включали.

5.6.2. Изменение Горячих клавиш Режима Игры

Чтобы изменить Горячие клавиши, необходимо выполнить следующие шаги:

1. Нажмите **Переключить в расширенный вид** (если включен **Основной вид**).
2. Выберите **Режим Игровой / Ноутбук** из бокового меню слева.
3. Щелкните на вкладке **Игровой режим**.
4. Нажмите кнопку **Дополнительно...**.
5. Под параметром **Использовать горячие клавиши** выберите горячую клавишу по умолчанию:
   - Выберите клавиши, которые Вы хотите изменить, используя следующие: клавиша Control (`Ctrl`), клавиша Shift (`Shift`) или клавиша Alternate (`Alt`).
   - В поле редактирования укажите букву с клавишей, которую Вы хотите использовать.

   Например, если Вы хотите использовать клавиши `Ctrl+Alt+D`, Вы должны указать только `Ctrl` и `Alt` и набрать `D`.

Замечание
Сняв флажок у параметра **Использовать горячие клавиши** вы отключите использование горячей клавиши.

5.7. Интегрирование в браузеры

BitDefender защищает Вас от попыток фишинга, когда Вы используете Интернет. Просматривает веб сайты, к которым получает доступ и сообщает Вам, если есть какие-нибудь фишинг угрозы. Белый Список веб-сайтов, которых не надо просматривать BitDefender, можно формировать.

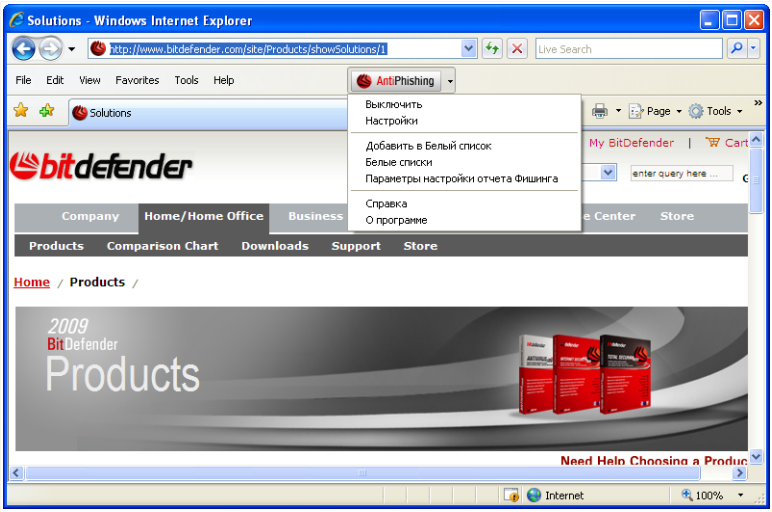
BitDefender интегрируется непосредственно через интуитивно-понятную панель инструментов в следующие веб-браузеры:

- Internet Explorer
- Mozilla Firefox

Вы можете легко и эффективно управлять настройками антифишинга и белым списком при помощи панели антифишинга BitDefender, интегрируемой в один из перечисленных браузеров.

Антифишинговая панель, представленная **значком BitDefender**, расположена в верхней части браузера. Нажмите на это, чтобы открыть меню панели инструментов.

Замечание
Если Вы не можете увидеть панель инструментов, то откройте меню **Просмотр**, укажите **Панель инструментов** и выберите **Панель инструментов BitDefender**.



Панель инструментов антифишинга

Следующие команды доступны в меню панели инструментов:

- **Включить / Выключить** - включить / выключить панель инструментов антифишинга BitDefender.

Замечание
Если вы хотите отключить панель инструментов антифишинга, Ваш компьютер не будет больше защищен от попыток фишинга.

- **Настройки** - открывает окно, где Вы можете определить настройки панели инструментов антифишинга.

  Доступными являются следующие варианты:
  - **Включено сканирование** - включено антифишинговое сканирование.
  - **Запрос перед добавлением в белый список** - спрашивает Вас перед добавлением веб сайта в Белый список.
- **Добавить в Белый список** - добовляет нормальные веб сайты в Белый список.

Замечание
Добавление сайта в Белый список означает, что BitDefender не будет проверять данный сайт на попытки фишинга. Рекомендуем добавлять в этот спиок только те сайты, в которых Вы полностью уверены.

- **Просмотр Белого списка** - открывает Белый список.

  Вы можете просмотреть полный список сайтов, которые не проходят проверку модулями антифишинга BitDefender.

  Если Вы хотите удалить сайт из Белого списка, т.е. впредь Вас будут уведомлять о всех существующих угрозах фишинга на данной странице, нажмите кнопку **Удалить** рядом с названием этого сайта.

  В Белом списке Вы можете добавлять те сайты, которым полностью доверяете, таким образом, модули антифишинга больше не будут проверять эти страницы. Чтобы добавить сайт в Белый список, введите этот адрес в соответствующее поле и нажмите **Добавить**.
- **Помощь** - открывает документацию к программе в электронном виде.
- **О программе** - открывает окно, где можно просмотреть информацию о BitDefender и о том, где искать помощь в случае непредвиденных обстоятельств.

5.8. Интеграция в интернет-пейджер

BitDefender предоставляет возможности защиты конфиденциальных документов и обмена сообщениями между интернет-пейджерами Yahoo Messenger и MSN Messenger.

По умолчанию BitDefender шифрует все сеансы обмена мгновенными сообщениями при условии, если:

- у вашего собеседника установлена версия BitDefender, которая поддерживает шифрование мгновенных сообщений, и эта функция включена в используемом интернет-пейджере;
- вы и ваш собеседник используете Yahoo Messenger или Windows Live (MSN) Messenger.

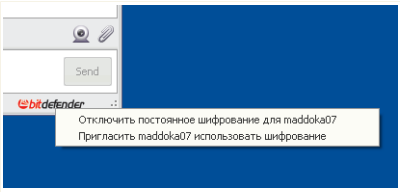
Важно

BitDefender не будет шифровать обмен сообщениями, если собеседник использует какой-либо веб-клиент, например Meebo, или другое приложения для чата, поддерживающее Yahoo Messenger или MSN.

Вы можете легко настроить шифрование мгновенного обмена сообщениями с помощью панели инструментов BitDefender из окна чата.

Правый щелчок на панели инструментов BitDefender вызывает следующие параметры:

- перманентное включение / выключение шифрования для определенного собеседника;
- предложение определенному собеседнику использовать шифрование;
- удаление определенного собеседника из черного списка Родительского контроля.

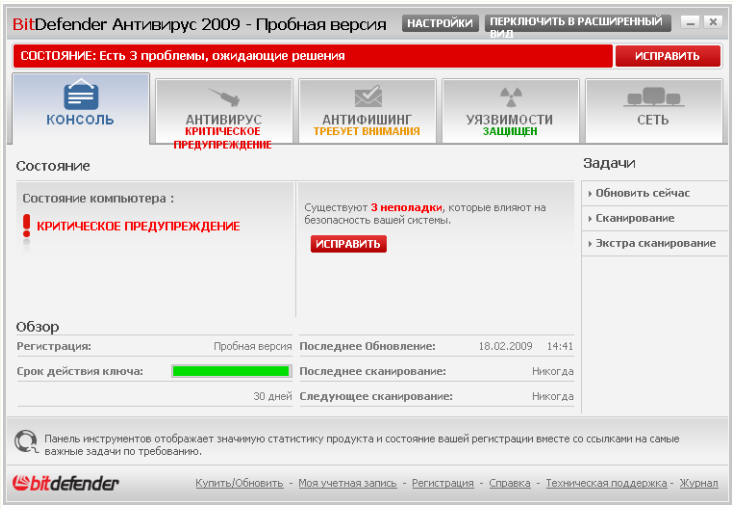


Параметры шифрования мгновенных сообщений

Выберите один из вышеперечисленных параметров, чтобы начать их использование.

6. Консоль

Щелчок на Консоли отображает значимую статистику продукта и состояние вашей регистрации вместе со ссылками на самые важные задачи по требованию.



Консоль

6.1. Обзор

Здесь вы можете видеть краткую статистику о состоянии обновлений, состоянии вашей учетной записи, регистрации и сведениях о лицензии.

Элемент	Описание
Последнее обновление	Отображает дату, когда ваш продукт BitDefender обновлялся в последний раз. Пожалуйста, проводите регулярные обновления, чтобы ваша система была полностью защищенной.
Моя учетная запись	Отображение адреса электронной почты, на который вы можете отправить запрос на получение доступа к вашей

Элемент	Описание
	оперативной учетной записи для восстановления своего лицензионного ключа BitDefender, а также воспользоваться услугами службы поддержки BitDefender или другими персонализированными услугами.
Регистрация	Отображает тип и состояние вашего лицензионного ключа. Чтобы поддерживать систему в безопасности, настойчиво рекомендуется обновлять BitDefender, если срок действия ключа вышел.
Срок действия ключа	Число дней до истечения срока действия лицензионного ключа.

Чтобы обновить BitDefender, просто нажмите кнопку **Обновить сейчас** в разделе задач.

Чтобы создать или войти в учетную запись BitDefender, используйте следующую процедуру.

1. Щелкните ссылку **Моя учетная запись** внизу окна. Откроется веб-страница.
2. Введите свое имя пользователя, пароль и нажмите кнопку **Вход**.
3. Для создания учетной записи BitDefender выберите **У вас нет учетной записи?** и введите требуемую информацию.

Замечание
Предоставленные Вами данные конфиденциальны.

Чтобы зарегистрировать BitDefender Antivirus 2009, выполните следующую процедуру.

1. Щелкните ссылку **Моя учетная запись** внизу окна. Откроется мастер регистрации за один шаг.
2. Выберите параметр **Я хочу зарегистрировать продукт с новым ключом**.
3. Введите новый лицензионный ключ в соответствующем текстовом поле.
4. Щелкните мышкой на кнопке **Завершить**.

Чтобы приобрести новый лицензионный ключ, выполните следующую процедуру.

1. Щелкните ссылку **Моя учетная запись** внизу окна. Откроется мастер регистрации за один шаг.

2. Щелкните на ссылке **Обновите ваш ключ на BitDefender**. Откроется веб-страница.
3. Нажмите кнопку **Купить**.

6.2. Задачи

Здесь вы найдете ссылки на наиболее важные задачи безопасности: полное сканирование системы, полное сканирование, обновление.

Доступны следующие варианты:

- **Полная проверка системы** - запускает полное сканирование компьютера (включая архивы).
- **Полное сканирование** - полное сканирование вашего компьютера (включая архивы).
- **Обновить сейчас** - запускает немедленное обновление.

6.2.1. Сканирование с помощью BitDefender

Чтобы просканировать ваш компьютер на malware, перейдите на соответствующую задачу сканирования, нажав соответствующую кнопку. Данная таблица содержит список задач сканирования с их описанием:

Задача	*Описание*
Полная проверка системы	Проверка всей системы кроме архивов. В конфигурации по умолчанию проверка производится на все виды вредоносных программ, угрожающих безопасности Вашей системы, а именно на наличие вирусов, программ-шпионов, рекламного ПО, руткитов и проч.
Полное сканирование	Проверка всей системы В конфигурации по умолчанию проверка производится на все виды вредоносных программ, угрожающих безопасности Вашей системы, а именно на наличие вирусов, программ-шпионов, рекламного ПО, руткитов и проч.

Замечание
Поскольку задания **Глубокая проверка системы** и **Полная проверка системы** проводят анализ всей системы, их выполнение может занять определенный

промежуток времени. Поэтому, рекомендуем выполнять эти задачи с небольшим приоритетом, либо когда Ваша система не загружена.

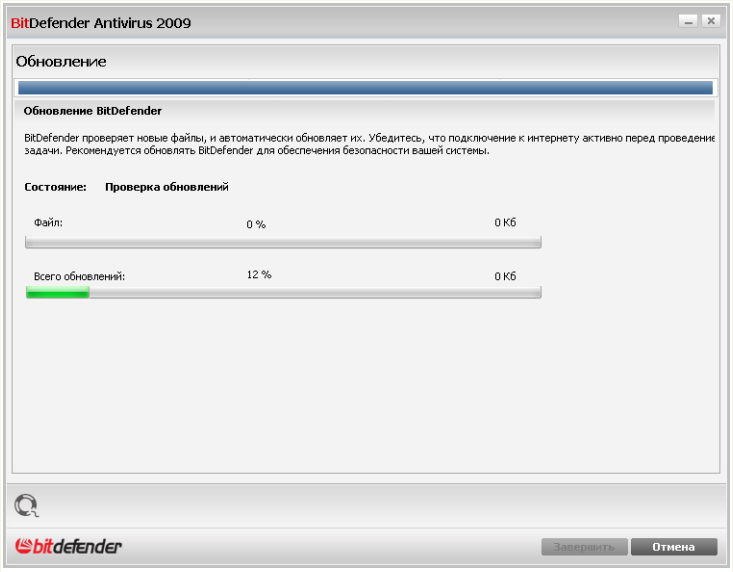
Каждый раз, когда Вы запускаете процесс проверки по требованию или быструю проверку, либо полную проверку, то запускается Сканер BitDefender.

Чтобы завершить процесс проверки выполните последовательность из трех шагов.

6.2.2. Обновление BitDefender

Каждый день появляются и обнаруживаются все новые вредоносные программы. Вот почему так важно постоянно обновлять сигнатурные базы Bitdefender новыми вредоносными программами.

По умолчанию, BitDefender проверяет наличие обновлений при запуске компьютера и **ежечасно** в дальнейшем. Если Вы хотите обновить BitDefender, нажмите **Обновить сейчас**. Процесс обновления будет инициирован, и появится соответствующее окно:



Обновление BitDefender

В этом окне Вы можете видеть статус процесса обновления.

Процесс обновления происходит "на лету", т.е. файлы заменяются по мере обновления. Таким образом, процесс обновления не влияет на работоспособность продукта, и, в то же время, исключается возможность возникновения уязвимости Вашего компьютера.

Если вы хотите закрыть это окно, просто нажмите **Отмена**. Это не будет останавливать процесс обновления.

Замечание

Если Вы подключаетесь к Интернету по телефонной линии, лучше всего регулярно обновлять BitDefender по требованию пользователя.

Если требуется, то перезагрузите компьютер. В случае основного обновления, Вас попросят перезагрузить компьютер.

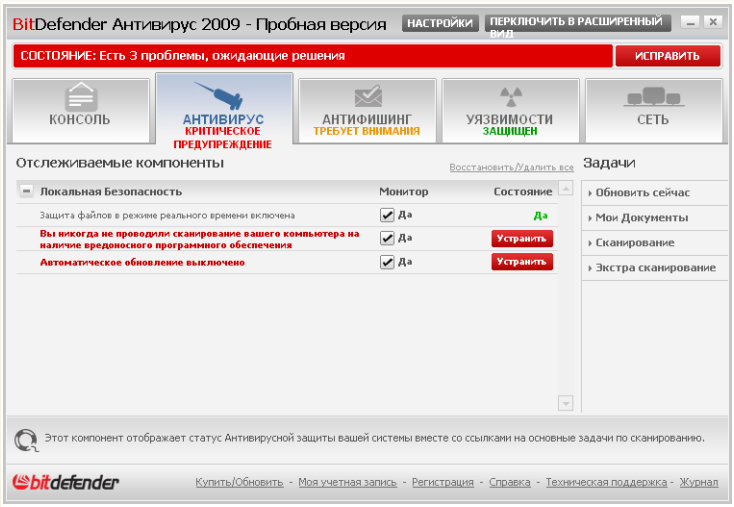
Нажмите **Перезагрузить**, чтобы сейчас перезагрузить Вашу систему.

Если Вы хотите перезагрузить Вашу систему позже, то нажмите **OK**. Мы рекомендуем перезагрузить Вашу систему так быстро, как это возможно.

7. Антивирус

BitDefender снабжен антивирусным модулем, который помогает поддерживать само приложение BitDefender всегда в обновленном состоянии и надежно защищать ваш компьютер от вирусов.

Чтобы войти в антивирусный модуль, нажмите вкладку **Антивирус**.



Антивирус

Антивирусный модель состоит из двух разделов:

- **Отслеживаемые компоненты** - Просмотр полного списка отслеживаемых компонентов для каждого модуля безопасности. Вы можете выбирать, какие модули следует отслеживать. Рекомендуется включать отслеживание всех компонентов.
- **Задачи** - Здесь вы найдете ссылки на наиболее важные задачи безопасности: полное сканирование системы, полное сканирование, обновление.

7.1. Отслеживаемые компоненты

Отслеживаемый компонент:

Категория	Описание
Локальная безопасность	С помощью этого компонента вы можете следить за состоянием каждого модуля безопасности, который защищает объекты, хранящиеся на вашем компьютере (файлы, реестр, память и т.п.).

Щелчок мыши на значке "+" открывает список настроек, а щелчок мыши на значке "-" закрывает его.

7.1.1. Локальная Безопасность

Мы знаем, что важно быть в курсе, когда какая-либо проблема может угрожать безопасности вашего компьютера. Путем отслеживания каждого модуля безопасности BitDefender Antivirus 2009 будет уведомлять вас не только при установке параметра, который может повлиять на безопасность вашего компьютера, но также когда вы забываете выполнить важные задачи.

Проблемы, связанные с локальной безопасностью, описываются развернутыми предложениями. Кроме этого, если что-то может повлиять на безопасность вашего компьютера, вы увидите красную кнопку состояния **Устранить**. В противном случае отображается кнопка **OK**.

Угрозы	Описание
Защита файлов в режиме реального времени включена	Обеспечение проверки всех файлов, когда они запускаются вами или приложением, работающим в вашей системе.
Вы проводили сканирование на наличие вирусоносного программного обеспечения сегодня	Настойчиво рекомендуется провести сканирование по требованию как можно быстрее для проверки всех файлов, хранящихся на вашем компьютере, на наличие вирусоносного программного обеспечения.

Угрозы	Описание
Автоматическое обновление включено	Пожалуйста, оставляйте автоматическое обновление аключенным, для обеспечения всех антивирусных сигнатур BitDefender обновлениями на постоянной базе.
Выполняется обновление	Проводится обновление подписей продуктов и антивирусных программ.

Когда кнопки состояния зеленые, безопасность вашей системы подвержена минимальному риску. Чтобы кнопки стали зелеными, выполните следующую процедуру:

1. Нажимайте кнопки **Устранить**, чтобы устранить уязвимости одну за другой.
2. Если проблему не удается решить сразу же, то выполните все действия мастера, чтобы исправить данную проблему.

Если вы хотите исключить компонент из списка отслеживания, просто снимите флажок **Да, отслеживать этот компонент**.

7.2. Задачи

Здесь вы найдете ссылки на наиболее важные задачи безопасности: полное сканирование системы, полное сканирование, обновление.

Доступны следующие варианты:

- **Полная проверка системы** - запускает полное сканирование компьютера (включая архивы).
- **Полное сканирование** - полное сканирование вашего компьютера (включая архивы).
- **Сканировать Мои Документы** - запускает быстрое сканирование документов и настроек.
- **Обновить сейчас** - запускает немедленное обновление.

7.2.1. Сканирование с помощью BitDefender

Чтобы просканировать ваш компьютер на malware, перейдите на соответствующую задачу сканирования, нажав соответствующую кнопку. Данная таблица содержит список задач сканирования с их описанием:

Задача	Описание
Полная проверка системы	Проверка всей системы кроме архивов. В конфигурации по умолчанию проверка производится на все виды вредоносных программ, угрожающих безопасности Вашей системы, а именно на наличие вирусов, программ-шпионов, рекламного ПО, руткитов и проч.
Полное сканирование	Проверка всей системы В конфигурации по умолчанию проверка производится на все виды вредоносных программ, угрожающих безопасности Вашей системы, а именно на наличие вирусов, программ-шпионов, рекламного ПО, руткитов и проч.
Сканировать Мои документы	Используйте данное задание для проверки основных папок пользователя: `Мои документы`, `Рабочий стол` и `Автозагрузка`. Это будет гарантировать безопасность ваших документов, безопасность рабочего пространства и загрузки безопасных приложений Автозагрузки.

Замечание

Поскольку задания **Глубокая проверка системы** и **Полная проверка системы** проводят анализ всей системы, их выполнение может занять определенный промежуток времени. Поэтому, рекомендуем выполнять эти задачи с небольшим приоритетом, либо когда Ваша система не загружена.

Каждый раз, когда Вы запускаете процесс проверки по требованию или быструю проверку, либо полную проверку, то запускается Сканер BitDefender.

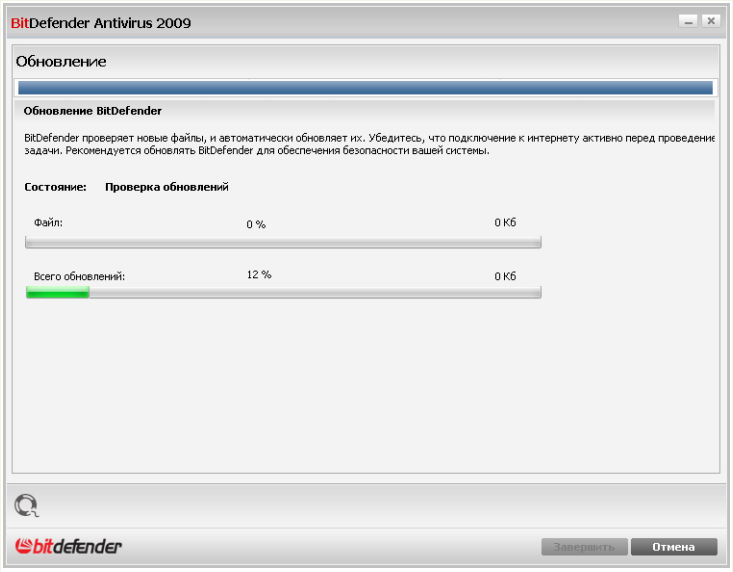
Чтобы завершить процесс проверки выполните последовательность из трех шагов.

7.2.2. Обновление BitDefender

Каждый день появляются и обнаруживаются все новые вредоносные программы. Вот почему так важно постоянно обновлять сигнатурные базы Bitdefender новыми вредоносными программами.

По умолчанию, BitDefender проверяет наличие обновлений при запуске компьютера и **ежечасно** в дальнейшем. Если Вы хотите обновить BitDefender,

нажмите **Обновить сейчас**. Процесс обновления будет инициирован, и появится соответствующее окно:



Обновление BitDefender

В этом окне Вы можете видеть статус процесса обновления.

Процесс обновления происходит "на лету", т.е. файлы заменяются по мере обновления. Таким образом, процесс обновления не влияет на работоспособность продукта, и, в то же время, исключается возможность возникновения уязвимости Вашего компьютера.

Если вы хотите закрыть это окно, просто нажмите **Отмена**. Это не будет останавливать процесс обновления.

Замечание
Если Вы подключаетесь к Интернету по телефонной линии, лучше всего регулярно обновлять BitDefender по требованию пользователя.

Если требуется, то перезагрузите компьютер. В случае основного обновления, Вас попросят перезагрузить компьютер.

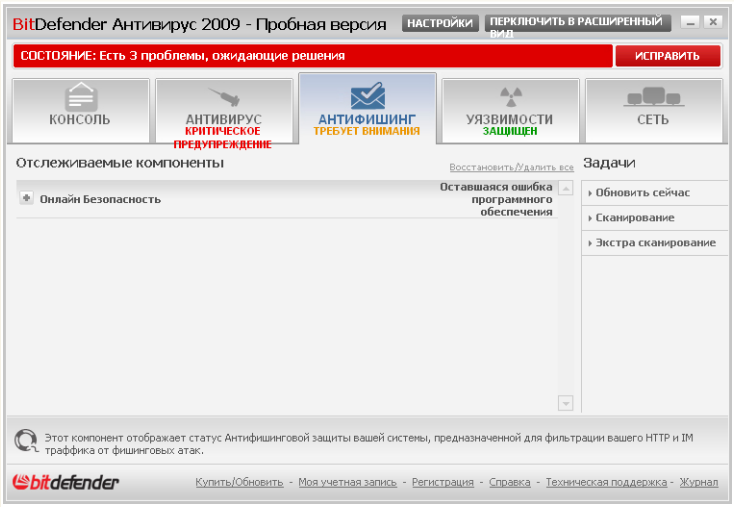
Нажмите **Перезагрузить**, чтобы сейчас перезагрузить Вашу систему.

Если Вы хотите перезагрузить Вашу систему позже, то нажмите **OK**. Мы рекомендуем перезагрузить Вашу систему так быстро, как это возможно.

8. Антифишинг

BitDefender поставляется с антифишинговым модулем, который обеспечивает безопасный доступ ко всем веб-страницам, открываемым программами Internet Explorer и Firefox.

Чтобы войти в антифишинговый модуль, нажмите вкладку **Антифишинг**.



Антифишинг

Антифишинговый модуль состоит из двух разделов:

- **Отслеживаемые компоненты** - Просмотр полного списка отслеживаемых компонентов для каждого модуля безопасности. Вы можете выбирать, какие модули следует отслеживать. Рекомендуется включать отслеживание всех компонентов.
- **Задачи** - Здесь вы найдете ссылки на наиболее важные задачи безопасности: полное сканирование системы, полное сканирование, обновление.

8.1. Отслеживаемые компоненты

Отслеживаемый компонент:

Категория	Описание
Онлайн безопасность	Здесь вы можете следить за состоянием каждого модуля безопасности, который защищает ваши онлайн-транзакции при подключении к Интернету.

Щелчок мыши на значке "+" открывает список настроек, а щелчок мыши на значке "-" закрывает его.

8.1.1. Онлайн Безопасность

Проблемы, связанные с онлайн-безопасностью, описываются развернутыми предложениями. Кроме этого, если что-то может повлиять на безопасность вашего компьютера, вы увидите красную кнопку состояния **Устранить**. В противном случае отображается кнопка **OK**.

Угрозы	Описание
Функция шифрования отправки сообщений для IM включена.	Если у ваших собеседников установлен BitDefender 2009, все беседы с помощью программ Yahoo! Messenger и Windows Live Messenger будут шифроваться. Рекомендуется включить шифрование обмена мгновенными сообщениями, чтобы сохранить конфиденциальность ваших бесед.
Антифишинговая защита для Firefox включена	BitDefender защищает Вас от попыток фишинга, когда Вы используете Интернет.
Антифишинговая защита для Internet Explorer включена	BitDefender защищает Вас от попыток фишинга, когда Вы используете Интернет.

Когда кнопки состояния зеленые, безопасность вашей системы подвержена минимальному риску. Чтобы кнопки стали зелеными, выполните следующую процедуру:

1. Нажимайте кнопки **Устранить**, чтобы устранить уязвимости одну за другой.
2. Если проблему не удается решить сразу же, то выполните все действия мастера, чтобы исправить данную проблему.

Если вы хотите исключить компонент из списка отслеживания, просто снимите флажок **Да, отслеживать этот компонент**.

8.2. Задачи

Здесь вы найдете ссылки на наиболее важные задачи безопасности: полное сканирование системы, полное сканирование, обновление.

Доступны следующие варианты:

- **Полная проверка системы** - запускает полное сканирование компьютера (включая архивы).
- **Полное сканирование** - полное сканирование вашего компьютера (включая архивы).
- **Сканировать Мои Документы** - запускает быстрое сканирование документов и настроек.
- **Обновить сейчас** - запускает немедленное обновление.

8.2.1. Сканирование с помощью BitDefender

Чтобы просканировать ваш компьютер на malware, перейдите на соответствующую задачу сканирования, нажав соответствующую кнопку. Данная таблица содержит список задач сканирования с их описанием:

Задача	*Описание*
Полная проверка системы	Проверка всей системы кроме архивов. В конфигурации по умолчанию проверка производится на все виды вредоносных программ, угрожающих безопасности Вашей системы, а именно на наличие вирусов, программ-шпионов, рекламного ПО, руткитов и проч.
Полное сканирование	Проверка всей системы В конфигурации по умолчанию проверка производится на все виды вредоносных программ, угрожающих безопасности

Задача	Описание
	Вашей системы, а именно на наличие вирусов, программ-шпионов, рекламного ПО, руткитов и проч.
Сканировать Мои документы	Используйте данное задание для проверки основных папок пользователя: `Мои документы`, `Рабочий стол` и `Автозагрузка`. Это будет гарантировать безопасность ваших документов, безопасность рабочего пространства и загрузки безопасных приложений Автозагрузки.

Замечание
Поскольку задания **Глубокая проверка системы** и **Полная проверка системы** проводят анализ всей системы, их выполнение может занять определенный промежуток времени. Поэтому, рекомендуем выполнять эти задачи с небольшим приоритетом, либо когда Ваша система не загружена.

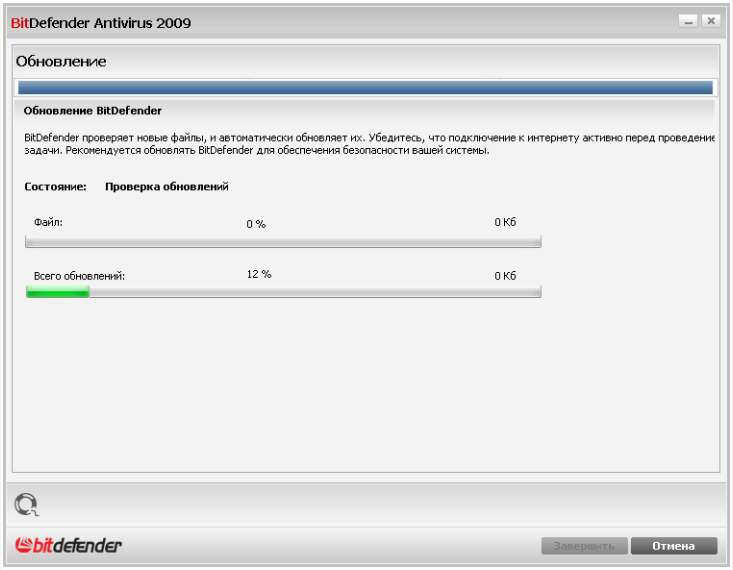
Каждый раз, когда Вы запускаете процесс проверки по требованию или быструю проверку, либо полную проверку, то запускается Сканер BitDefender.

Чтобы завершить процесс проверки выполните последовательность из трех шагов.

8.2.2. Обновление BitDefender

Каждый день появляются и обнаруживаются все новые вредоносные программы. Вот почему так важно постоянно обновлять сигнатурные базы Bitdefender новыми вредоносными программами.

По умолчанию, BitDefender проверяет наличие обновлений при запуске компьютера и **ежечасно** в дальнейшем. Если Вы хотите обновить BitDefender, нажмите **Обновить сейчас**. Процесс обновления будет инициирован, и появится соответствующее окно:



Обновление BitDefender

В этом окне Вы можете видеть статус процесса обновления.

Процесс обновления происходит "на лету", т.е. файлы заменяются по мере обновления. Таким образом, процесс обновления не влияет на работоспособность продукта, и, в то же время, исключается возможность возникновения уязвимости Вашего компьютера.

Если вы хотите закрыть это окно, просто нажмите **Отмена**. Это не будет останавливать процесс обновления.

Замечание
Если Вы подключаетесь к Интернету по телефонной линии, лучше всего регулярно обновлять BitDefender по требованию пользователя.

Если требуется, то перезагрузите компьютер. В случае основного обновления, Вас попросят перезагрузить компьютер.

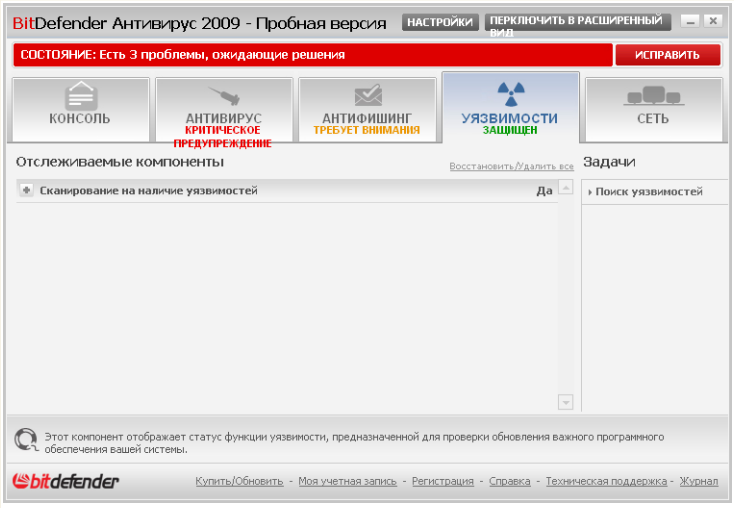
Нажмите **Перезагрузить**, чтобы сейчас перезагрузить Вашу систему.

Если Вы хотите перезагрузить Вашу систему позже, то нажмите **OK**. Мы рекомендуем перезагрузить Вашу систему так быстро, как это возможно.

9. Уязвимости

К BitDefender прилагается модуль сканирования уязвимостей, который помогает держать важные приложения на вашем компьютере в обновленном состоянии.

Чтобы войти в модуль сканирования уязвимостей, нажмите вкладку **Уязвимости**



Уязвимости

Модель сканирования уязвимостей состоит из двух разделов:

- **Отслеживаемые компоненты** - Просмотр полного списка отслеживаемых компонентов для каждого модуля безопасности. Вы можете выбирать, какие модули следует отслеживать. Рекомендуется включать отслеживание всех компонентов.
- **Задачи** - Здесь вы можете найти ссылки на наиважнейшие задачи безопасности.

9.1. Отслеживаемые компоненты

Отслеживаемый компонент:

Категория	Описание
Поиск уязвимостей	Здесь вы можете определить, все ли важное программное обеспечение на вашем компьютере обновлено. Пароли к учетным записям Windows проверяются согласно правилам безопасности.

Щелчок мыши на значке "+" открывает список настроек, а щелчок мыши на значке "-" закрывает его.

9.1.1. Сканирование на наличие уязвимостей

Проблемы, связанные с уязвимостями, описываются развернутыми предложениями. Кроме этого, если что-то может повлиять на безопасность вашего компьютера, вы увидите красную кнопку состояния **Устранить**. В противном случае отображается кнопка **OK**.

Угрозы	Описание
Служба проверки уязвимостей включена	Отслеживание обновлений Windows Updates, обновлений Microsoft Windows Office и паролей к учетным записям Microsoft Windows, чтобы ваша операционная система была обеспечена обновлениями, а защиту паролем невозможно было обойти.
Критичные обновления Microsoft	Установка доступных важных обновлений Microsoft.
Другие обновления Microsoft	Установка доступных второстепенных обновлений Microsoft.
Автоматические обновления Windows включены	Установка новых обновлений безопасности Windows по мере их доступности.
Администратор (Сильный пароль)	Уровень надежности пароля для определенных пользователей.

Когда кнопки состояния зеленые, безопасность вашей системы подвержена минимальному риску. Чтобы кнопки стали зелеными, выполните следующую процедуру:

1. Нажимайте кнопки **Устранить**, чтобы устранить уязвимости одну за другой.
2. Если проблему не удается решить сразу же, то выполните все действия мастера, чтобы исправить данную проблему.

Если вы хотите исключить компонент из списка отслеживания, просто снимите флажок **Да, отслеживать этот компонент**.

9.2. Задачи

Здесь вы можете найти ссылки на наиважнейшие задачи безопасности.

Доступна следующая кнопка:

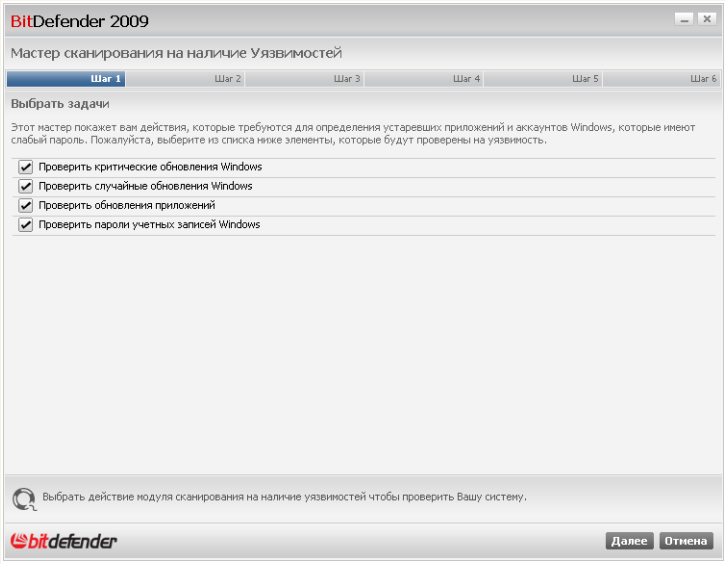
- **Поиск уязвимостей**

9.2.1. Поиск уязвимостей

Сканирование на уязвимость проверяет обновления Microsoft Windows, обновления Microsoft Windows Office и пароли ваших аккаунтов Microsoft Windows для гарантии того, что ваша операционная система обновлена и не содержит паролей, которые было бы легко обойти.

Чтобы проверить компьютер на наличие уязвимостей, выберите **Поиск уязвимостей** и выполняйте указания мастера.

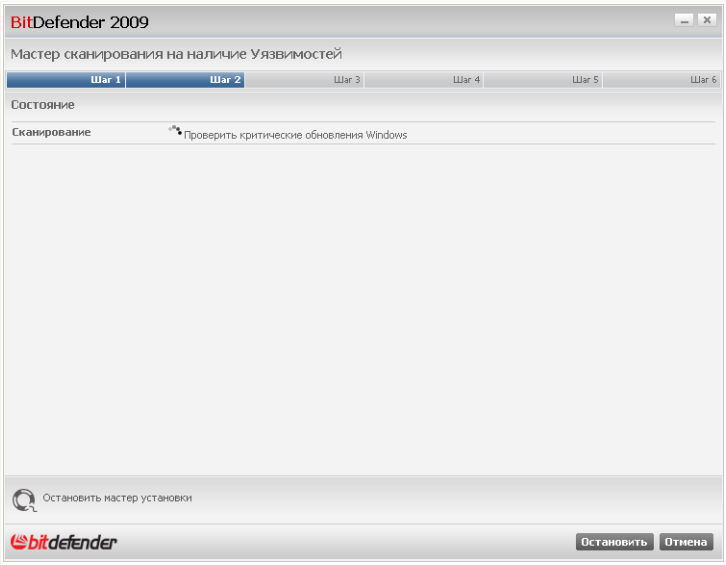
Шаг 1/6 - Выберите уязвимости для проверки



Уязвимости

Нажмите **Далее**, чтобы проверить систему на наличие выбранных уязвимостей.

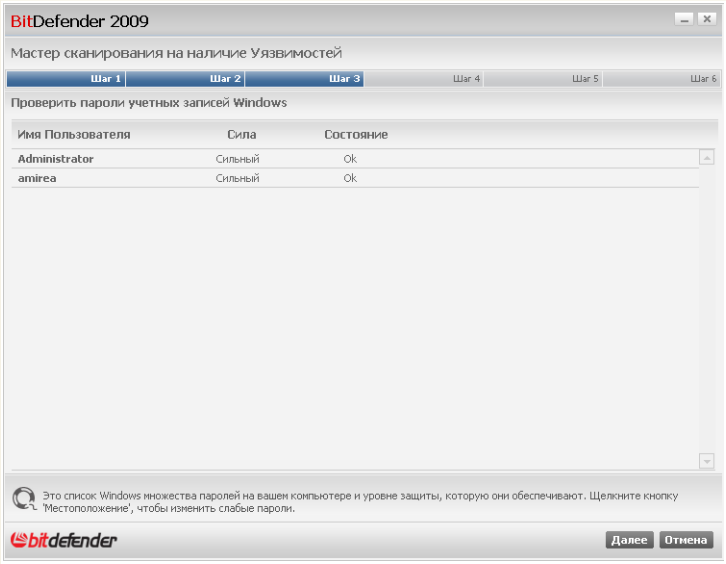
Шаг 2/6 - Проверка уязвимостей



Проверка уязвимостей

Подождите, пока BitDefender завершит проверку уязвимостей.

Шаг 3/6 - Смените слабые пароли



Пользовательские пароли

Вы можете просмотреть список учетных записей пользователей Windows, установленных на вашем компьютере, и уровень защиты, обеспечиваемый их паролями.

Нажмите **Устранить**, чтобы поменять все слабые пароли. Появится новое окно.

Изменить пароль

Выберите метод устранения проблемы:

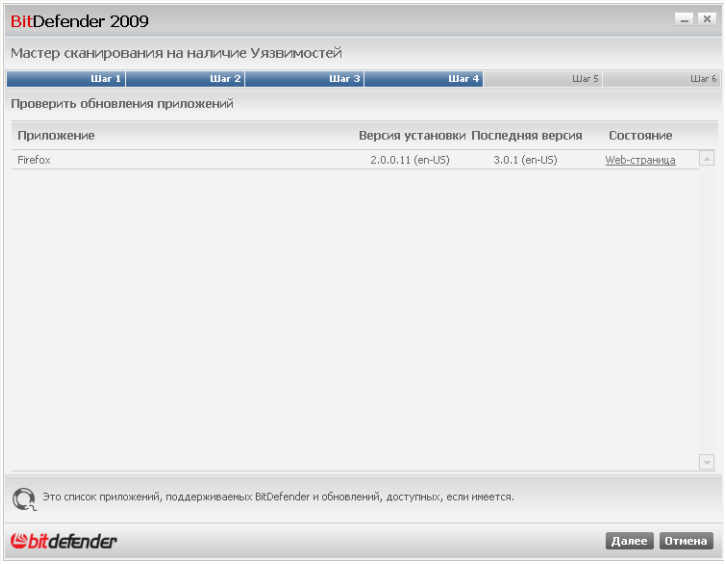
- **Пользователь может изменить пароль в следующем сеансе.** BitDefender выведет запрос на смену пароля в следующий раз при входе в Windows.
- **Изменить пароль.** Необходимо ввести пароль в поля ввода.

Замечание
Чтобы получить сильный пароль, используйте комбинации символов в верхнем и нижнем регистре, числа и специальные символы (такие как, например, #, $ или @).

Нажмите **OK**, чтобы сменить пароль.

Щелкните по кнопке **Далее**.

Шаг 4/6 - Обновите приложения

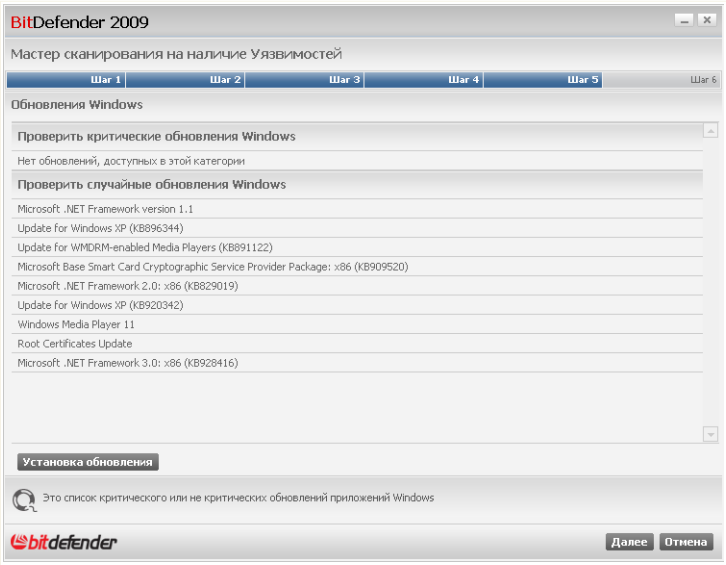


Приложения

Вы можете просмотреть список приложений, проверенных BitDefender, и проверить, нуждаются ли они в обновлениях. Если приложение нуждается в обновлении, щелкните появившуюся ссылку, чтобы загрузить последнюю версию.

Щелкните по кнопке **Далее**.

Шаг 5/6 - Обновите Windows



Обновления Windows

Вы можете просмотреть список важных и второстепенных обновлений Windows, которые в данный момент не установлены на вашем компьютере. Нажмите **Установка обновления**, чтобы установить все доступные обновления.

Щелкните по кнопке **Далее**.

Шаг 6/6 - Просмотрите результаты

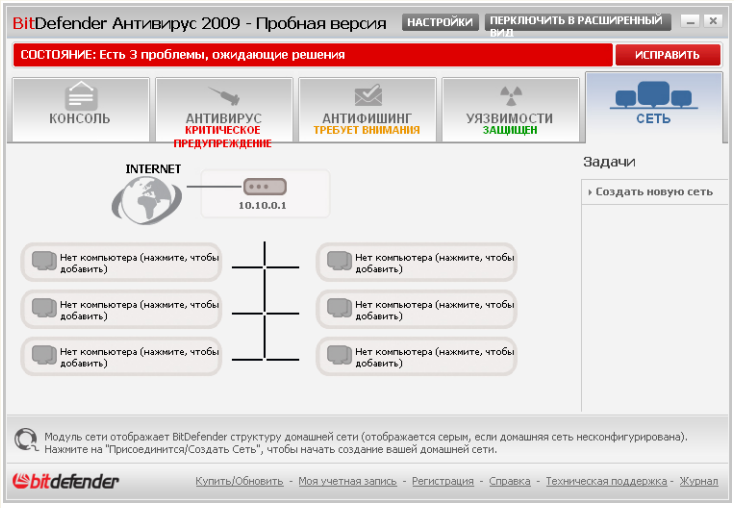
Результаты

Нажмите **Закрыть**.

10. Сеть

Модуль Сеть позволяет управлять обновлениями BitDefender, установленными на ваших домашних компьютерах, с одного компьютера.

Чтобы открыть модуль Сеть, нажмите вкладку **Менеджер файлов**.



Сеть

Для управления продуктами BitDefender, установленными на ваших домашних компьютерах, необходимо выполнить следующую процедуру:

1. Войдите в домашнюю сеть BitDefender на своем компьютере. Вход в сеть состоит из настройки административного пароля для управления домашней сетью.
2. Войдите в сеть с каждого компьютера, которым вы хотите управлять (установите пароль).
3. Вернитесь к своему компьютеру и добавьте те компьютеры, которыми вы хотите управлять.

10.1. Задачи

В самом начале доступна только одна кнопка.

- **Создать новую сеть** - Установка пароля для входа в сеть.

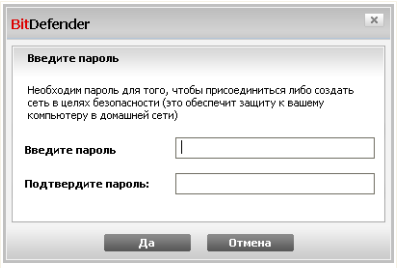
После входа в сеть появятся еще несколько кнопок.

- **Локальная сеть** - обеспечивает выход из сети.
- **Управление сетью** - Позволяет добавлять компьютеры в сеть.
- **Сканировать все файлы** - Позволяет сканировать все управляемые компьютеры одновременно.
- **Обновление файлов** - Позволяет обновлять все управляемые компьютеры одновременно.
- **Регистрация** - Позволяет зарегистрировать все управляемые компьютеры сразу.

10.1.1. Подключение к сети BitDefender

Чтобы подключиться к домашней сети BitDefender, выполните следующую процедуру:

1. Нажмите **Создать новую сеть**. Появится окно настройки пароля для управления домашней сетью.



Настройка пароля

2. Введите одинаковый пароль в каждом из полей ввода
3. В конце щелкните мышкой на кнопке **OK**.

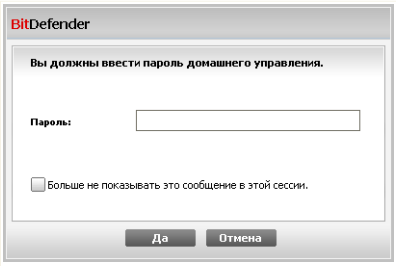
На карте сети будет отображаться имя компьютера.

10.1.2. Добавление компьютеров в сеть BitDefender.

Перед добавлением компьютера в домашнюю сеть BitDefender необходимо настроить пароль управления домашней сетью BitDefender на соответствующем компьютере.

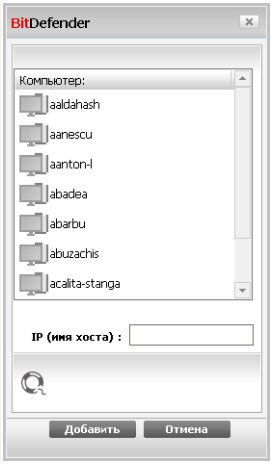
Чтобы добавить компьютер в домашнюю сеть BitDefender, выполните следующую процедуру:

1. Нажмите **Управление сетью**. Появится окно ввода пароля для управления локальной сетью.



Введите пароль

2. Введите пароль для управления домашней сетью и нажмите **OK**. Появится новое окно.

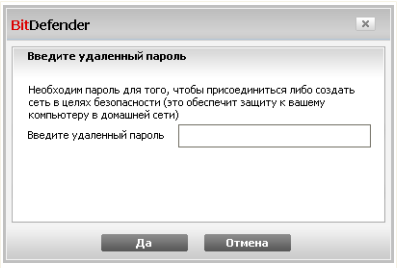


Добавить компьютер

Вы увидите список компьютеров, находящихся в сети. Значки имеют следующие значения:

- Указывает на находящийся в сети компьютер, на котором не установлены продукты BitDefender.
- Указывает на находящийся в сети компьютер, на котором установлен BitDefender.
- Указывает на автономный компьютер, на котором установлен BitDefender.

3. Сделайте одно из следующего:
   - Выберите из списка имя добавляемого компьютера.
   - Введите IP-адрес или имя добавляемого компьютера в соответствующем поле.
4. Нажмите **Добавить**. Появится окно ввода пароля управления домашней сетью для соответствующего компьютера.



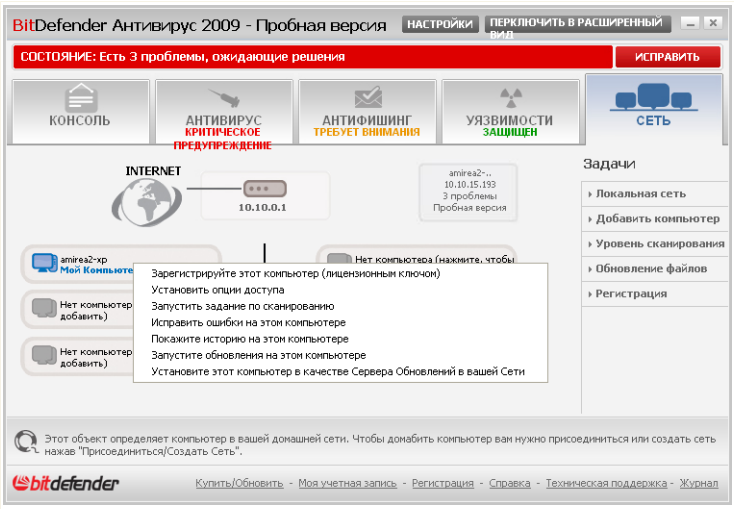
Авторизация

5. Введите пароль управления домашней сетью на соответствующем компьютере.
6. В конце щелкните мышкой на кнопке **OK**. Если вы ввели правильный пароль, имя выбранного компьютера появится на карте сети.

Замечание
На сетевую карту можно добавить до пяти компьютеров.

10.1.3. Управление сетью BitDefender

Как только домашняя сеть BitDefender будет создана, вы сможете управлять всеми продуктами BitDefender с одного компьютера.



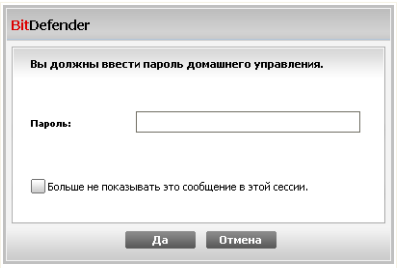
Карта сети

Если передвинуть курсор мыши поверх компьютера на карте сети, вы увидите краткие сведения о нем (имя, IP-адрес, число проблем, влияющих на безопасность системы, состояние регистрации BitDefender).

Если щелкнуть правой кнопкой мыши на имени компьютера на карте сети, вы увидите список управляющих заданий, которые можно выполнять с удаленным компьютером.

- **Зарегистрируйте этот компьютер**
- **Установить опции доступа**
- **Запустить задание по сканированию**
- **Исправить ошибки на этом компьютере**
- **Покажите историю на этом компьютере**
- **Запустите обновления на этом компьютере**
- **Профили**
- **Запустите панель настроек на этом компьютере**
- **Установите этот компьютер в качестве сервера обновлений в вашей сети**

Перед запуском задания на определенном компьютере появится окно ввода пароля управления домашней сетью.



Введите пароль

Введите пароль для управления домашней сетью и нажмите **OK**.

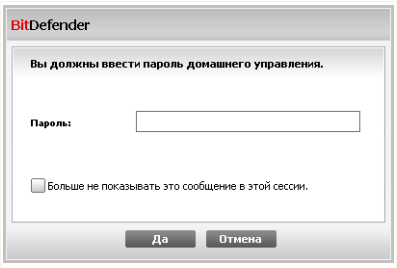
Замечание

Если вы планируете выполнить несколько заданий, можно выбрать параметр **Больше не показывать это сообщение в этой сессии**. Выбрав этот параметр, вы не будете видеть окно ввода пароля во время текущего сеанса.

10.1.4. Сканирование всех компьютеров

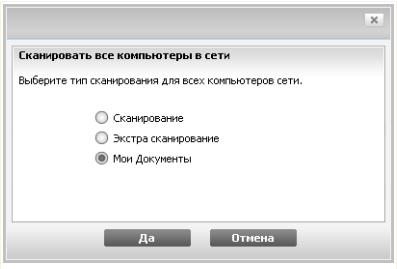
Для сканирования всех управляемых компьютеров выполните следующую процедуру:

1. Нажмите **Сканировать все файлы**. Появится окно ввода пароля для управления локальной сетью.



Введите пароль

2. Выберите тип сканирования.
   - **Полная проверка системы** - запускает полное сканирование компьютера (включая архивы).
   - **Полное сканирование** - полное сканирование вашего компьютера (включая архивы).
   - **Сканировать Мои Документы** - запускает быстрое сканирование документов и настроек.



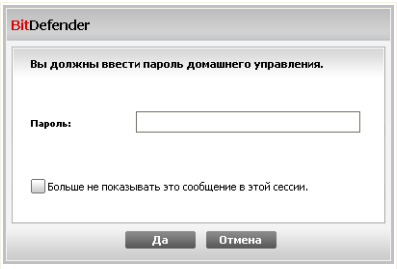
Выберите тип сканирования

3. В конце щелкните мышкой на кнопке **OK**.

10.1.5. Обновление всех компьютеров

Для обновления всех управляемых компьютеров выполните следующую процедуру:

1. Нажмите **Обновление файлов**. Появится окно ввода пароля для управления локальной сетью.



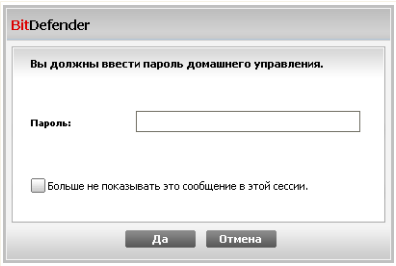
Введите пароль

2. В конце щелкните мышкой на кнопке **OK**.

10.1.6. Регистрация всех компьютеров

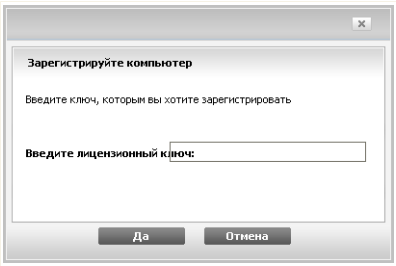
Для регистрации всех управляемых компьютеров выполните следующую процедуру:

1. Нажмите **Регистрация**. Появится окно ввода пароля для управления локальной сетью.



Введите пароль

2. Введите ключ, с помощью которого вы хотите выполнить регистрацию.



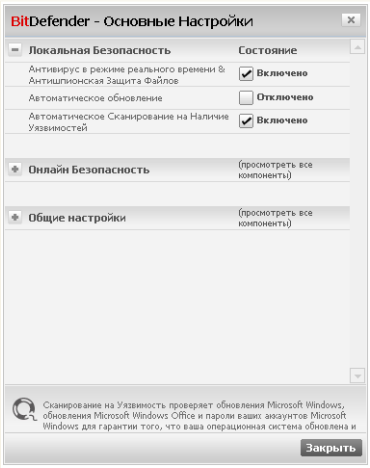
Регистрация

3. В конце щелкните мышкой на кнопке **OK**.

11. Основные настройки

В модуле основных настроек можно легко включить или отключить важные модули безопасности.

Для входа в модуль основных настроек нажмите кнопку **Настройки** вверху окна основного вида.



Основные настройки

Доступные модули безопасности сгруппированы в несколько категорий.

Категория	*Описание*
Локальная безопасность	Здесь вы можете включить/выключить защиту файлов в реальном времени или автоматическое обновление.
Онлайн безопасность	Здесь вы можете включить/выключить защиту почты и веба в реальном времени.
Основные настройки	Здесь вы можете включить/выключить игровой режим, режим ноутбука, пароли, полосу активности сканирования и т.п.

Щелчок мыши на значке "+" открывает список настроек, а щелчок мыши на значке "-" закрывает его.

11.1. Локальная Безопасность

Вы можете включить/выключить модули безопасности одним щелчком.

Модуль безопасности	Описание
Антивирус в режиме реального времени & антишпионская защита файлов	Защита файлов в режиме реального времени гарантирует их проверку, когда они запускаются вами или приложением, которое работает в вашей системе.
Автоматическое обновление	Автоматическое обновление гарантирует, что новейшие продукты BitDefender и файлы сигнатур загружаются и устанавливаются автоматически на регулярной основе.
Автоматическое сканирование на наличие уязвимостей	Автоматическое сканирование на наличие уязвимостей обеспечивает обновление важного программного обеспечения на вашем компьютере.

11.2. Онлайн Безопасность

Вы можете включить/выключить модули безопасности одним щелчком.

Модуль безопасности	Описание
Антифишинг веб защита в режиме реального времени	Антифишинговая защита веба в реальном времени обеспечивает сканирование всех файлов, загруженных через HTTP, на наличие попыток фишинга.
Защита данных	Служба Контроля Идентичности помогает хранить вашу конфиденциальную информацию, сканируя особенные строки в веб и почтовом траффике.

Модуль безопасности	Описание
Шифрование	Если у ваших IM контактов установлен BitDefender 2009, все передачи IM сообщений с помощью Yahoo! Messenger и Windows Live Messenger будут зашифрованы.

11.3. Общие настройки

Вы можете включить/выключить элементы, связанные с безопасностью, одним щелчком.

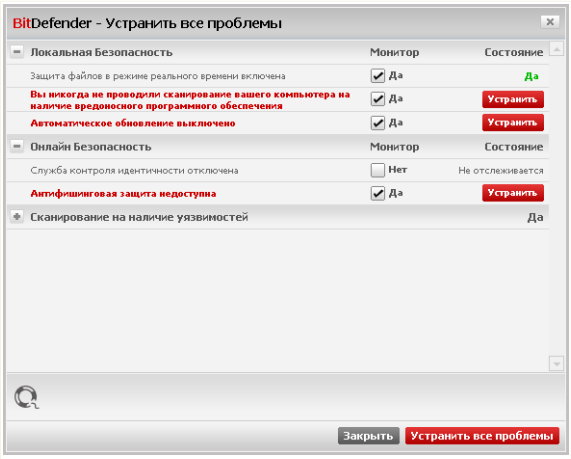
Элемент	Описание
Режим Игры	Режим Игры временно изменяет настройки защиты, чтобы минимизировать их влияние на деятельность системы во время игры.
Режим ноутбука	Режим Ноутбука временно изменяет настройки защиты, чтобы минимизировать их влияние на длительность работы батареи вашего ноутбука.
Пароль настроек	Благодаря этому настройки BitDefender могут быть изменены только теми, кто знает этот пароль.
Новости BitDefender	Включив этот параметр, вы будете получать важные новости компании, обновления продукта и список новых угроз от BitDefender.
Предупреждение об уведомлении продукта	Включив этот параметр, вы будете получать информационные уведомления.
Полоса активности сканирования	Полоса активности сканирования - это небольшая прозрачная панель, отображающая ход сканирования BitDefender. Зеленая полоса отображает активность сканирования на вашей локальной системе. Красная линия отображает активность сканирования вашего интернет-соединения.
Запускать BitDefender при загрузке	Включение этого параметра обеспечивает загрузку пользовательского интерфейса BitDefender при запуске. Этот параметр не повлияет на уровень защиты.

Элемент	Описание
Отправлять отчеты о вирусах	Включение этого параметра обеспечивает отправку отчетов о сканировании на вирусы в лаборатории BitDefender для анализа. Обратите внимание на то, что эти отчеты не будут содержать конфиденциальных данных, таких как, например, ваше имя или IP-адрес, и они не будут использоваться в коммерческих целях.
Определение атак	Включение этого параметра обеспечивает отправку отчетов о потенциальных вирусных атаках в лаборатории BitDefender для анализа. Обратите внимание на то, что эти отчеты не будут содержать конфиденциальных данных, таких как, например, ваше имя или IP-адрес, и они не будут использоваться в коммерческих целях.

12. Полоса состояния

Как вы уже, наверное заметили, в верхней части окна BitDefender Antivirus 2009 находится строка состояния, отображающая число проблем, ожидающих решения. Нажмите кнопку **Устранить все проблемы**, чтобы с легкостью устранить все угрозы безопасности компьютера. Появится окно состояния безопасности.

Окно состояния безопасности позволяет отображать и управлять систематизированным списком уязвимостей системы безопасности вашего компьютера. BitDefender Antivirus 2009 позволяет знать, повлияет ли существующая проблема на безопасность вашего компьютера.



Полоса состояния

12.1. Локальная Безопасность

Мы знаем, что важно быть в курсе, когда какая-либо проблема может угрожать безопасности вашего компьютера. Путем отслеживания каждого модуля безопасности BitDefender Antivirus 2009 будет уведомлять вас не только при установке параметра, который может повлиять на безопасность вашего компьютера, но также когда вы забываете выполнить важные задачи.

Проблемы, связанные с локальной безопасностью, описываются развернутыми предложениями. Кроме этого, если что-то может повлиять на безопасность вашего компьютера, вы увидите красную кнопку состояния **Устранить**. В противном случае отображается кнопка **OK**.

Угрозы	*Описание*
Защита файлов в режиме реального времени включена	Обеспечение проверки всех файлов, когда они запускаются вами или приложением, работающим в вашей системе.
Вы проводили сканирование на наличие вирусоносного программного обеспечения сегодня	Настойчиво рекомендуется провести сканирование по требованию как можно быстрее для проверки всех файлов, хранящихся на вашем компьютере, на наличие вирусоносного программного обеспечения.
Автоматическое обновление включено	Пожалуйста, оставляйте автоматическое обновление аключенным, для обеспечения всех антивирусных сигнатур BitDefender обновлениями на постоянной базе.
Выполняется обновление	Проводится обновление подписей продуктов и антивирусных программ.

Когда кнопки состояния зеленые, безопасность вашей системы подвержена минимальному риску. Чтобы кнопки стали зелеными, выполните следующую процедуру:

1. Нажимайте кнопки **Устранить**, чтобы устранить уязвимости одну за другой.
2. Если проблему не удается решить сразу же, то выполните все действия мастера, чтобы исправить данную проблему.

Если вы хотите исключить компонент из списка отслеживания, просто снимите флажок **Да, отслеживать этот компонент**.

12.2. Онлайн Безопасность

Проблемы, связанные с онлайн-безопасностью, описываются развернутыми предложениями. Кроме этого, если что-то может повлиять на безопасность

вашего компьютера, вы увидите красную кнопку состояния **Устранить**. В противном случае отображается кнопка **OK**.

Угрозы	*Описание*
Функция шифрования отправки сообщений для IM включена.	Если у ваших собеседников установлен BitDefender 2009, все беседы с помощью программ Yahoo! Messenger и Windows Live Messenger будут шифроваться. Рекомендуется включить шифрование обмена мгновенными сообщениями, чтобы сохранить конфиденциальность ваших бесед.
Антифишинговая защита для Firefox включена	BitDefender защищает Вас от попыток фишинга, когда Вы используете Интернет.
Антифишинговая защита для Internet Explorer включена	BitDefender защищает Вас от попыток фишинга, когда Вы используете Интернет.

Когда кнопки состояния зеленые, безопасность вашей системы подвержена минимальному риску. Чтобы кнопки стали зелеными, выполните следующую процедуру:

1. Нажимайте кнопки **Устранить**, чтобы устранить уязвимости одну за другой.
2. Если проблему не удается решить сразу же, то выполните все действия мастера, чтобы исправить данную проблему.

Если вы хотите исключить компонент из списка отслеживания, просто снимите флажок **Да, отслеживать этот компонент**.

12.3. Сканирование на наличие уязвимостей

Проблемы, связанные с уязвимостями, описываются развернутыми предложениями. Кроме этого, если что-то может повлиять на безопасность вашего компьютера, вы увидите красную кнопку состояния **Устранить**. В противном случае отображается кнопка **OK**.

Угрозы	*Описание*
Служба проверки уязвимостей включена	Отслеживание обновлений Windows Updates, обновлений Microsoft Windows Office и паролей к учетным записям Microsoft Windows, чтобы ваша операционная система была обеспечена обновлениями, а защиту паролем невозможно было обойти.
Критичные обновления Microsoft	Установка доступных важных обновлений Microsoft.
Другие обновления Microsoft	Установка доступных второстепенных обновлений Microsoft.
Автоматические обновления Windows включены	Установка новых обновлений безопасности Windows по мере их доступности.
Администратор (Сильный пароль)	Уровень надежности пароля для определенных пользователей.

Когда кнопки состояния зеленые, безопасность вашей системы подвержена минимальному риску. Чтобы кнопки стали зелеными, выполните следующую процедуру:

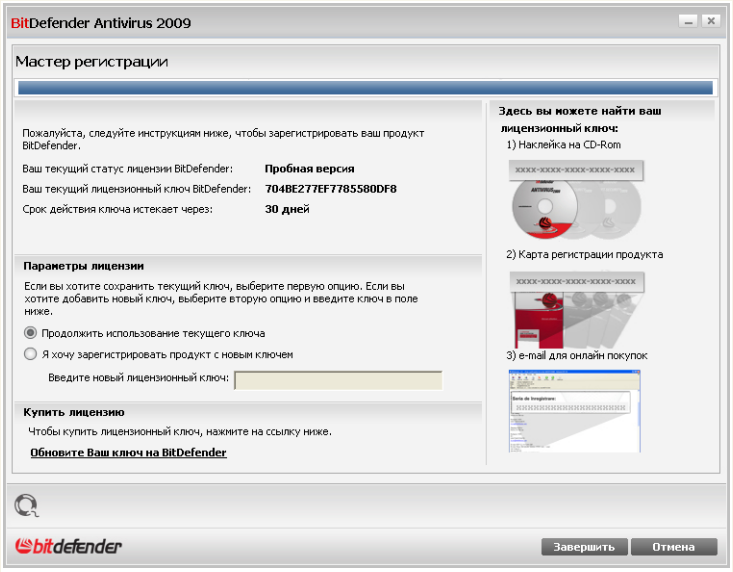
1. Нажимайте кнопки **Устранить**, чтобы устранить уязвимости одну за другой.
2. Если проблему не удается решить сразу же, то выполните все действия мастера, чтобы исправить данную проблему.

Если вы хотите исключить компонент из списка отслеживания, просто снимите флажок **Да, отслеживать этот компонент**.

13. Регистрация

BitDefender Antivirus 2009 устанавливается с 30-дневным периодом пробного использования. Если вы хотите зарегистрировать BitDefender Antivirus 2009, сменить лицензионный ключ или создать учетную запись BitDefender, щелкните ссылку **Регистрация**, которая находится в нижней части окна BitDefender. Появится Мастер регистрации.

13.1. Шаг 1/1 - Регистрация BitDefender Antivirus 2009



Регистрация

Вы можете просмотреть статус регистрации BitDefender, действующий лицензионный ключ, и количество дней, которые остались до окончания срока действия лицензии.

Для регистрации BitDefender Antivirus 2009:

1. Выберите **Я хочу зарегистрировать продукт с новым ключем**.
2. Введите лицензионный ключ в поле для редактирования.

Замечание

Вы можете найти ваш лицензионный ключ:

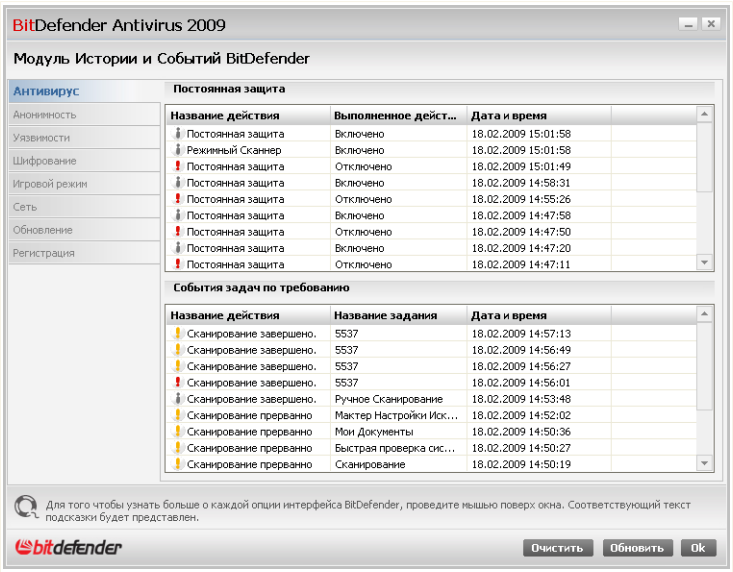
- на обложке CD.
- на регистрационной карточке продукта.
- в электронном письме о покупке.

Если у Вас нет лицензионного ключа BitDefender, нажмите соответствующую ссылку для перехода в онлайн-магазин BitDefender и приобретите лицензионный ключ.

Щелкните мышкой на кнопке **Завершить**.

14. Журнал

Ссылка **История** внизу окна центра безопасности BitDefender открывает окно с архивированными событиями BitDefender. Здесь представлен обзор всех событий, связанных с безопасностью. Например, вы можете проверить, было ли успешным последнее обновление, были ли найдены на вашем компьютере вредоносные программы и т.п.



События

Чтобы помочь Вам ориентироваться в архиве событий BitDefender, слева имеются следующие категории:

- **Антивирус**
- **Контроль личных данных**
- **Обновление**
- **Сеть**

Для каждой категории имеется список событий. Для каждого события отображается следующая информация: краткое описание, действие, выполненное BitDefender при появлении события, дата и время события. Если Вы хотите узнать больше о каком-то определенном событии, дважды нажмите на нем.

Нажмите **Очистить журнал**, если Вы хотите удалить старые записи в журнале событий, или **Обновить**, чтобы убедиться, что отображаются все записи, включая и самые последние.

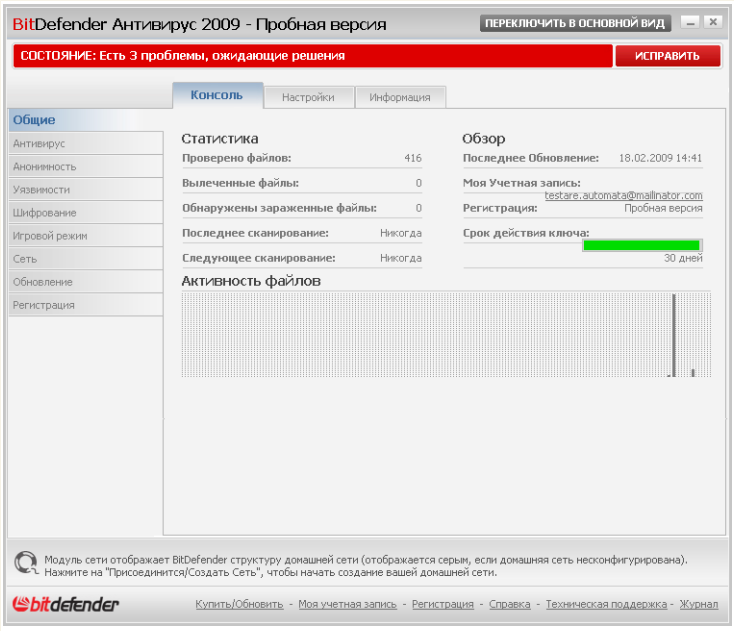
Расширенное Администрирование

15. Общие

Модуль Общие предоставляет сведения о системе и активности BitDefender. Здесь вы также можете изменить общее поведение BitDefender.

15.1. Консоль

Чтобы увидеть статистику активности и состояние вашей регистрации, перейдите в раздел **Основные>Консоль** в окне расширенного вида.



Консоль

Консоль состоит из нескольких разделов:

- **Статистика** - Важные сведения об активности BitDefender.

- **Обзор** - Отображение состояния обновления, состояния учетной записи и сведений о лицензии.
- **Файлы** - Счетчик объектов, проверенных сканером вредоносного ПО BitDefender. Высота панели указывает на интенсивность трафика во время данного интервала времени.

15.1.1. Статистика

Если вы хотите следить за активностью BitDefender, начните с раздела Статистика. Вы увидите следующие элементы:

Элемент	Описание
Проверено файлов	Отображает количество файлов, которые были проверены на наличие вредоносного кода во время последнего сканирования.
Вылеченные файлы	Отображает количество файлов, которые были вылечены BitDefender во время последнего сканирования.
Обнаружено вирусов	Отображает количество вирусов, которые были найдены во время последнего сканирования.

15.1.2. Обзор

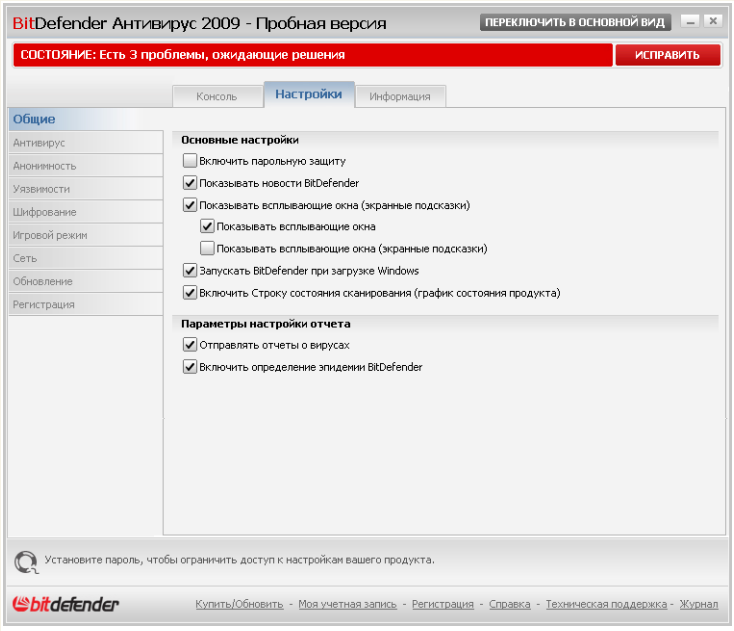
Здесь вы можете видеть краткую статистику о состоянии обновлений, состоянии вашей учетной записи, регистрации и сведениях о лицензии.

Элемент	Описание
Последнее обновление	Отображает дату, когда ваш продукт BitDefender обновлялся в последний раз. Пожалуйста, проводите регулярные обновления, чтобы ваша система была полностью защищенной.
Мой аккаунт	Отображение адреса электронной почты, на который вы можете отправить запрос на получение доступа к вашей оперативной учетной записи для восстановления своего лицензионного ключа BitDefender, а также воспользоваться услугами службы поддержки

Элемент	Описание
	BitDefender или другими персонализированными услугами.
Регистрация	Отображает тип и состояние вашего лицензионного ключа. Чтобы поддерживать систему в безопасности, настойчиво рекомендуется обновлять BitDefender, если срок действия ключа вышел.
Истечение срока	Число дней до истечения срока действия лицензионного ключа.

15.2. Настройки

Для настройки общих параметров BitDefender и управления его настройками перейдите в раздел **Общие>Настройки** в окне расширенного вида.



Основные настройки

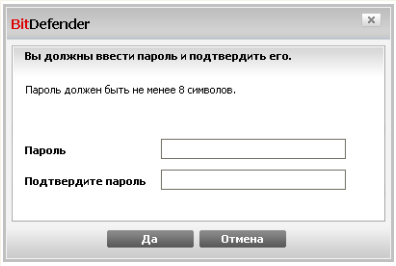
Здесь Вы можете настроить операции, выполняемые программой Bitdefender. По умолчанию, Bitdefender загружается при запуске операционной системы Windows и затем выполняется в свернутом виде – о его выполнении свидетельствует иконка в области уведомлений на панели задач.

15.2.1. Основные настройки

- **Включить защиту паролем настроек программы** - включает защиту паролем конфигурации консоли управления BitDefender.

  Замечание
  Если вы не единственный, кто имеет права администратора для данного компьютера, рекомендуется защитить настройки BitDefender паролем.

  Если Вы выбираете эту опцию, появится следующее окно:



Введите пароль

Введите пароль в поле **Пароль**, и еще раз в поле **Повторите пароль** и нажмите **OK**.

Если у Вас установленн пароль, то его будут запрашивать всякий раз при измении настроек BitDefender. Другие администраторы (если такие есть), также должны использовать этот пароль, чтобы изменить настройки BitDefender.

Важно
Если Вы забыли пароль, Вам придется провести восстановление программы, чтобы изменить настройки BitDefender.

- **Показывать новости BitDefender (уведомление на тему безопасности)** - время от времени показывает уведомления относительно новых вирусов, рассылаемые сервером BitDefender.
- **Показывать всплывающие окна** - включает функцию всплывающих окон, отображающих статус программы. Вы можете настроить BitDefender для отображения всплывающих окон только при использовании основного вида или расширенного вида.

- **Запуск BitDefender при загрузке Windows** - BitDefender автоматически запускается при загрузке системы. Мы настоятельно рекомендуем выбрать эту функцию!
- **Включить панель активности сканирования (экранный график активности программы)** - отображает панель Активность сканирования всегда, когда Вы произвели вход в Windows. Снимите галочку в этом поле, если больше не хотите, чтобы Панель активности сканирования отображалась.

Замечание
Эта настройка может быть сделана только для текущего пользователя Windows.

15.2.2. Параметры настройки отчета

- **Отправлять отчеты о вирусах** - отправляет в лаборатории BitDefender Labs отчет о вирусах, обнаруженных на Вашем компьютере. Это позволяет отслеживать эпидемии вирусов.

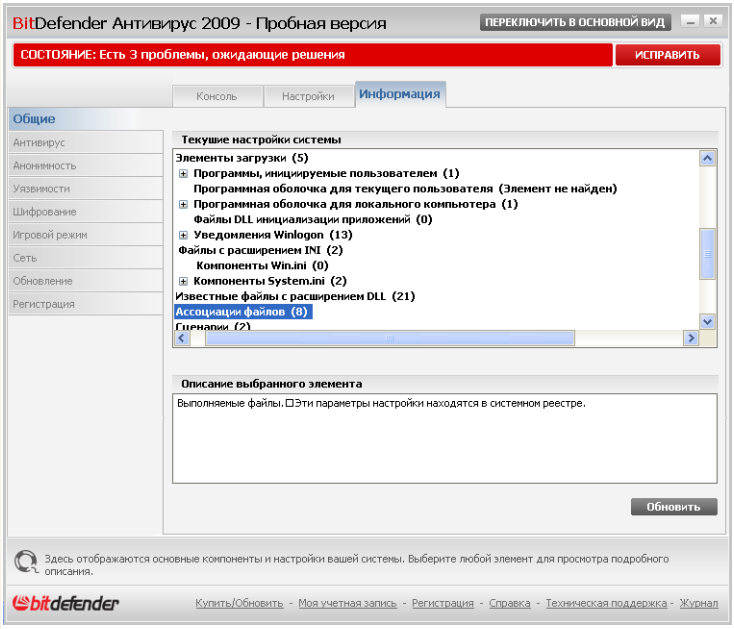
  Эти отчеты не содержат никакой конфиденциальной информации, например, Вашего имени, IP-адрес Вашего компьютера, и не используются в коммерческих целях. Отправляемая информация содержит только название вируса и используется исключительно для статистики.
- **Включить функцию BitDefender обнаружения эпидемий** - отправляет в лаборатории BitDefender Labs отчет о потенциальных вирусных эпидемиях.

  Эти отчеты не содержат никакой конфиденциальной информации, например, Вашего имени, IP-адрес Вашего компьютера, и не используются в коммерческих целях. Отправляемая информация содержит только возможный вирус и используется исключительно для статистики.

15.3. Системная информация

BitDefender позволяет просматривать все системные настройки и приложения, запускаемые при запуске системы. Таким образом, Вы можете отслеживать активность системы и установленных приложений, а также распознавать потенциально опасные объекты.

Чтобы получить информацию о системе, перейдите к разделу **Общие>Информация** в окне расширенного вида.



Системная информация

Информация о системе содержит перечень всех объектов, загруженных как при запуске системы, так и различными приложениями.

Три кнопки доступны:

- **Восстановить** - Смена текущих сопоставлений расширений файлов на значения по умолчанию. Доступно только для параметра **Ассоциации файлов**!
- **Перейти в** - открывается окно, в которое помещается выбранный объект (например, **Регистрация**).

> ***Замечание***
> В зависимости от выбранного элемента, кнопка **Перейти к** может не отображаться.

- **Обновить** - обновляется информация в окне **Информация о системе**.

16. Антивирус

BitDefender защищает Ваш компьютер от всех типов вредоносных программ (вирусов, троянов, программ-шпионов, руткитов и т.д.). Настройки защиты BitDefender разделены на две категории:

- Постоянная защита - Предотвращение попадания в систему нового вредоносного ПО. К примеру, BitDefender проверяет текстовый файл на наличие известных угроз при его открытии, а также электронные сообщение, когда Вы их получаете.

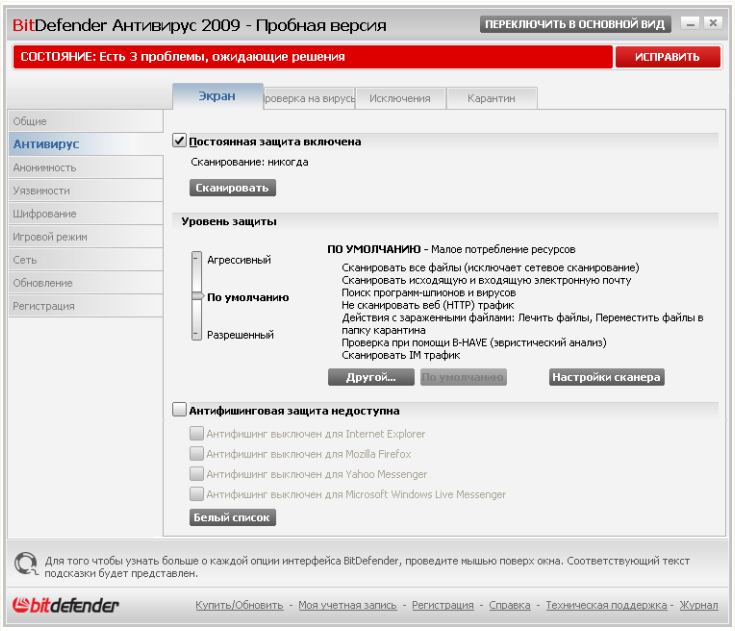
  Замечание
  Постоянная защита также называется сканированием на лету - файлы сканируются по мере доступа к ним.

- Сканирование по требованию - Обнаружение и удаление вредоносного ПО, которое уже попало в систему. Это классический тип проверки по желанию пользователя, когда Вы выбираете диск, папку, или файл для проверки BitDefender, а BitDefender проверяет их по Вашему требованию. Задачи проверки позволяют создавать распланированые действия, которые регулярно запускаются по расписанию.

16.1. Защита в режиме реального времени

BitDefender обеспечивает непрерывную защиту в реальном времени от множества угроз путем сканирования всех открытых файлов, почтовых сообщений, а также переписки с помощью Интернет-пейджеров (ICQ, NetMeeting, Yahoo Messenger, MSN Messenger). Антифишинговый модуль BitDefender предотвращает разглашение личной информации при просмотре интернет-страниц путем уведомления о потенциально опасных веб-страницах.

Для настройки постоянной защиты и антифишингового модуля BitDefender перейдите к разделу **Антивирус>Экран** в окне расширенного вида.



Защита в режиме реального времени

Здесь вы можете проверить, включена ли постоянная защита. Если вы хотите сменить состояние постоянной защиты, уберите или установите соответствующий флажок.

Важно
Чтобы предотвратить попадание вирусов на Вашем компьютере, включите **Постоянную защиту**.

Чтобы начать быстрое сканирование системы ,нажмите **Сканировать сейчас**.

16.1.1. Конфигурация уровня защиты

Вы можете выбрать уровень защиты согласно Вашим потребностям в безопасности. Передвиньте бегунок по шкале в соотвествующий уровень защиты.

Существует 3 уровня защиты:

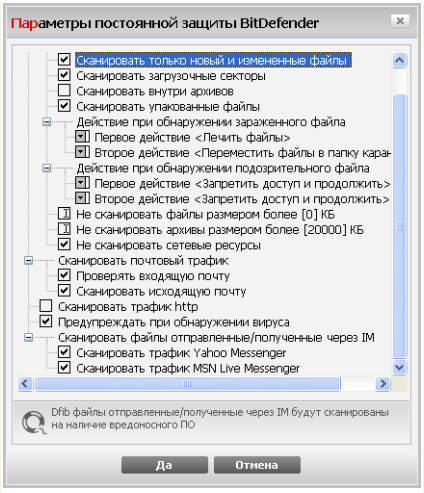
Уровень защиты	*Описание*
Разрешающий	Выполняет основные процессы безопасности. Потребляет малое количество ресурсов. Программы и входящие электронные сообщения проверяются только на наличие вирусов. Кроме классического сканирования при помощи базы образов, также используется эвристический анализ. К зараженным файлам могут применяться следующие действия: вылечить файл/запретить доступ.
Стандартный	Предлагает стандартный уровень безопасности. Потребляет малое количество ресурсов. Все файлы, входящие и исходящие электронные сообщения проверяются на вирусы и программы-шпионы. Кроме классического сканирования при помощи базы образов, также используется эвристический анализ. К зараженным файлам могут применяться следующие действия: вылечить файл/запретить доступ.
Агрессивный	Предлагает высокий уровень безопасности. Потребляет среднее количество ресурсов. Все файлы, входящие и исходящие электронные сообщения, а также веб-трафик проверяются на вирусы и программы-шпионы. Кроме классического сканирования при помощи базы образов, также используется эвристический анализ. К зараженным файлам могут применяться следующие действия: вылечить файл/запретить доступ.

Если Вы хотите вернуться к уровню по умолчанию нажмите **По умолчанию**.

16.1.2. Настройка уровня защиты

Опытные пользователи могут воспользоваться дополнительными настройками BitDefender, например, не проверять файлы с определенным расширением, определенные директории и архивы, которые точно безвредны. Это может значительно уменьшить время проверки и улучшить работу компьютера во время проверки.

Вы можете настроить **Постоянную защиту**, нажав **Настройка уровня**. Появится следующее окно:



Настройки защиты

Опции сканирования организованы как расширяемое меню, очень похожее на то, которое используется при поиски в Windows. Щелчок мышки на значке "+" разворачивает список, а на значке "-" – закрывает его.

Замечание

Вы можете заметить, что некоторые списки, даже помеченные значком "+" не открываются. Это означает, что эти настройки еще не выбраны. Выберите их и список откроется.

- Выберите настройку **Проверять открываемые и закачиваемые напрямую (P2P) файлы** - чтобы проверять все открываемые файлы и обмен данными с помощью служба мгновенной доставки сообщений, таких как ICQ, NetMeeting, Yahoo Messenger, MSN Messenger. Затем выберите типы файлов, которые необходимо проверить.

Настройка		*Описание*
Проверить открываемые файлы	**Проверить все файлы**	Проверяются все открываемые файлы, независимо от их формата.

Настройка		*Описание*
	Проверить только файлы программ	Проверяются только файлы программ, то есть файлы с расширением: .exe; .bat; .com; .dll; .ocx; .scr; .bin; .dat; .386; .vxd; .sys; .wdm; .cla; .class; .ovl; .ole; .exe; .hlp; .doc; .dot; .xls; .ppt; .wbk; .wiz; .pot; .ppa; .xla; .xlt; .vbs; .vbe; .mdb; .rtf; .htm; .hta; .html; .xml; .xtp; .php; .asp; .js; .shs; .chm; .lnk; .pif; .prc; .url; .smm; .pdf; .msi; .ini; .csc; .cmd; .bas; .eml; .nws.
	Проверить файлы с расширением	Проверяются только файлы с заданным расширением. Задаваемые расширения разделяются знаком ";".
	Проверка на наличие других угроз	Проверка на наличие других угроз. Обнаруженные файлы будут считаться зараженными. Программное обеспечение, которое включает компоненты рекламного ПО, может прекратить работу, если выбрана эта настройка. Поставьте значок в поле **Пропускать программы дозвона и приложения при сканировании**, если Вы хотите пропускать подобные файлы при сканировании.
Сканировать начальную загрузку		Проверка загрузочных секторов системы.
Проверять внутри архивов		Проверяются также архивы, к которым есть доступ.
Проверить запакованные файлы		Проверяются все запакованные файлы.
Первоначальное действие		Из выпадающего списка, Вы можете выбрать одно из следующих действий, которое будет выполнено при обнаружении зараженного и подозрительного файла.
	Запретить доступ и продолжать	При обнаружении зараженного файла доступ к нему будет запрещен.

Настройка		Описание
	Вылечить файл	Выполняется лечение зараженных файлов.
	Удалить файл	Зараженный файл удаляется немедленно, без предупреждения.
	Переместить файл в карантин	Зараженные файлы перемещаются в Карантин.
Второе действие		Из выпадающего списка, Вы можете выбрать второе действие, которое будет применено к зараженным файлам, если первое действие будет безуспешным.
	Запретить доступ и продолжать	При обнаружении зараженного файла доступ к нему будет запрещен.
	Удалить файл	Зараженный файл удаляется немедленно, без предупреждения.
	Переместить файл в карантин	Зараженные файлы перемещаются в Карантин.
Не проверять файлы, чей размер превышает [x] Kb		Введите максимальный размер файла для проверки. Если введен 0 Kb, будут проверены все фалы, независимо от их размера.
Не проверять архивы, чей размер превышает [20000] Кб		Введите максимальный размер сканируемых архивов в килобайтах (КБ). Если вы хотите, чтобы проверялись все архивы, независимо от их размера, введите 0.
Не проверять общие сетевые ресурсы		Если данная опция включена, BitDefender не будет осуществлять проверку сетевых ресурсов с общим доступом, что позволит ускорить работу сети. Рекомендуем включать данную опцию только тогда, когда Ваша сеть защищена каким-либо антивирусным продуктом.

- **Сканировать электронную почту** - сканирование электронных сообщений.

  Доступными являются следующие варианты:

Настройка	Описание
Сканировать входящие сообщения.	Сканировать все входящие электронные сообщения.
Сканировать исходящие сообщения	Сканировать все исходящие электронные сообщения.

- **Сканировать трафик http** - сканировать трафик http.
- **Предупреждать об обнаружении вируса** - при обнаружении вируса в файле или электронном письме появляется окно с предупреждением.

  Предупреждение об обнаружении зараженного вирусом файла содержит название вируса, путь к зараженному файлу, тип действия BitDefender, выполненного с этим файлом и ссылку на сайт BitDefender, где Вы сможете получить более подробную информацию об этом вирусе. В случае обнаружения вируса в электронной почте, в предупреждении будет также приведена информация об отправителе и получателе зараженного письма.

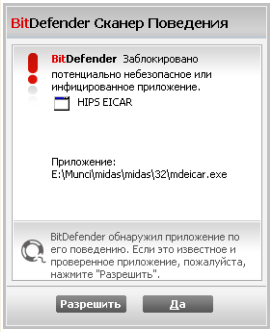
  В случае обнаружения подозрительного файла Вы можете запустить из окна предупреждений программу Мастер, которая поможет Вам посылать этот файл в лабораторию Bitdefender для дальнейшего анализа. При этом Вы можете указать свой адрес электронной почты, чтобы получить информацию относительно этого предупрежедния.
- **Сканирование файлов, полученных через интернет-пейджеры.** Для сканирования файлов, полученных или отправленных программами Yahoo Messenger или Windows Live Messenger, установите соответствующие флажки.

Нажмите **OK**, чтобы сохранить изменения и закройте окно.

16.1.3. Настройка Сканера поведения

Сканер поведения обеспечивает защиту против новых угроз, для которых еще не были выпущены сигнатуры. Он постоянно отслеживает и анализирует поведение приложений, запущенных на вашем компьютере, и предупреждает о подозрительном поведении приложений.

Сканер поведения выдает предупреждение, когда приложение пытается выполнить потенциально опасное действие, и запрашивает о действии пользователя.

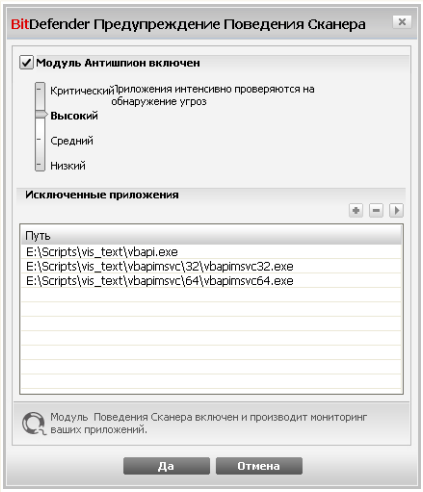


Уведомления Режимного сканера

Если вы знаете, что обнаруженному приложению можно доверять, нажмите **Разрешить**. Сканер поведения не будет проверять данное приложение на наличие потенциально опасного поведения.

Если вы хотите немедленно закрыть приложение, нажмите **OK**.

Чтобы настроить Сканер поведения, нажмите кнопку **Настройки сканера**.



Настройки Режимного Сканнера

Если вы хотите отключить Сканер поведения, снимите флажок **Модуль Антишпион включен**.

Важно
Рекомендуется держать Сканер поведения включенным, чтобы обеспечить защиту против неизвестных вирусов.

Настройка уровня защиты

Уровень защиты Сканера поведения автоматически меняется при установке нового уровня постоянной защиты. Если вас не устраивает значение по умолчанию, вы можете настроить уровень защиты вручную.

Замечание
Примите к сведению, что если вы смените текущий уровень постоянной защиты, уровень защиты Сканера поведения изменится соответственно.

Передвиньте бегунок, чтобы установить уровень защиты, наилучшем образом соответствующий вашим потребностям.

Уровень защиты	*Описание*
Критический	Приложения проверяются на наличие потенциально опасных действий с максимальной интенсивностью.
Высокий	Приложения проверяются на наличие потенциально опасных действий с высокой интенсивностью.
Средний	Приложения проверяются на наличие потенциально опасных действий с умеренной интенсивностью.
Низкий	Приложения проверяются на наличие потенциально опасных действий.

Управление исключенными приложениями

Вы можете настроить Сканер поведения так, чтобы он не проверял определенные приложения. Приложения, которые не проверяются Сканером поведения, отображаются в таблице **Исключенные приложения**.

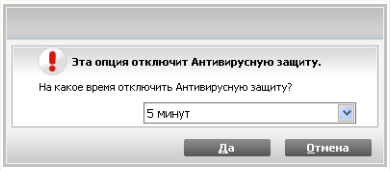
Для управления исключенными приложениями вы можете воспользоваться кнопками, находящимся вверху таблицы:

- **Add** - exclude a new application from scanning.
- **Remove** - remove an application from the list.

- **Edit** - edit an application path.

16.1.4. Отключение постоянной защиты

Если Вы захотите отключить постоянную защиту, то появится окно с предупреждением.



Включенная постоянная защита

Вы должны подтвердить свое намерение, выбрав промежуток времени, на который Вы хотите отключить постоянную защиту. Вы можете отключить постоянную защиту на 5, 15 или 30 минут, на час, навсегда или до следующей перезагрузки системы.

Внимание
Этот аспект является критическим с точки зрения безопасности. Рекомендуем Вам отключать постоянную защиту на как можно меньший промежуток времени. Если постоянная защита отключена, Вы не защищены от угроз вредоносных программ.

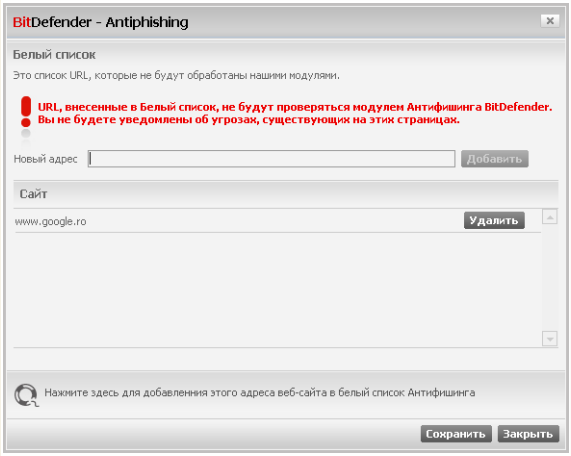
16.1.5. Настройка антифишинговой защиты

BitDefender обеспечивает постоянную антифишинговую защиту для следующих приложений:

- Internet Explorer
- Mozilla Firefox
- Yahoo! Messenger
- Windows Live (MSN) Messenger

Вы можете отключить антифишинговую защиту полностью или только для некоторых приложений.

Нажмите кнопку **Белый список** для настройки и управления списком вебсайтов, которые не следует сканировать антифишинговым модулем BitDefender.



Белый спиок антифишинга

Вы увидите список вебсайтов, которые BitDefender на данный момент не проверяет на наличие вредоносного содержания.

Чтобы добавить новый веб-сайт в белый список, введите его адрес URL в поле **Новый адрес** и нажмите **Добавить**. Белый список должен содержать только те вебсайты, которым вы полностью доверяете. Например, добавьте туда веб-сайты, где вы совершаете интернет-покупки.

Замечание

В белый список вебсайты можно добавлять из панели антифишингового модуля BitDefender, встроенного в ваш браузер.

Если вы хотите удалить вебсайт из белого списка, нажмите соответствующую кнопку **Удалить**.

Нажмите **Закрыть**, чтобы сохранить изменения и закрыть окно.

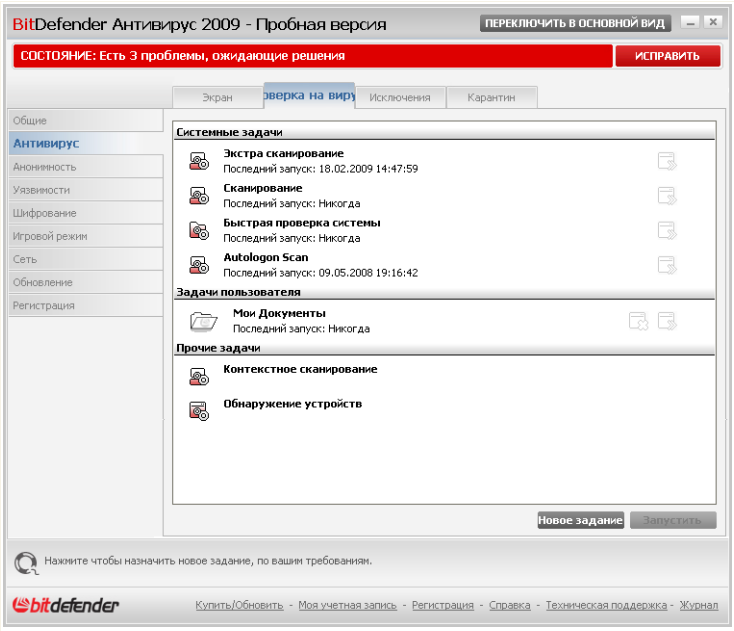
16.2. Сканирование по требованию

Главное назначение программного продукта BitDefender защищать Ваш компьютер от вирусов. В первую очередь BitDefender не позволяет новым вирусам

проникнуть на компьютер, проверяя электронные письма и новые загружаемые и копируемые файлы.

Однако есть вероятность того, что вирус проник в компьютер до установки BitDefender. Поэтому полезно проверить Ваш компьютер на наличие вирусов после установки программы, а также регулярно проверять компьютер.

Перейдите к разделу **Антивирус>Проверка** в окне расширенного вида, чтобы настроить и запустить проверку по требованию.



Задачи сканирования

Проверка по требованию производится согласно установленым задачам. Там указывают опции проверки, а также объекты, подлежащие проверке. Вы можете проверить компьютер в любое время, запуская задания по умолчанию, либо самостоятельно созданные Вами задачи. Вы также можете запланировать их регулярный запуск по расписанию или запуск, когда система не выполняет никаких задач, чтобы не оказывать влияния на Вашу работу.

16.2.1. Задачи сканирования

BitDefender имеет несколько заданий по умолчанию, которые учитывают основные задачи. Вы также можете создавать свои собственные задания.

У каждого задания есть окно **Свойства**, позволяющее Вам настроить данное задание и просматривать результаты его работы. Более подробную информацию можно найти здесь: «*Настройка задач проверки*» (p. 108).

Существует три категории задач сканирования:

- **Системные задачи** - содержат список стандартных системных задач. Есть следующие задачи:

Стандартные задачи	*Описание*
Глубокая проверка системы	Проверка всей системы В конфигурации по умолчанию проверка производится на все виды вредоносных программ, угрожающих безопасности Вашей системы, а именно на наличие вирусов, программ-шпионов, рекламного ПО, руткитов и проч.
Полная проверка системы	Проверка всей системы кроме архивов. В конфигурации по умолчанию проверка производится на все виды вредоносных программ, угрожающих безопасности Вашей системы, а именно на наличие вирусов, программ-шпионов, рекламного ПО, руткитов и проч.
Быстрая проверка системы	Сканирование `Windows`, `Program Files` и `Всех пользователей` папки. В конфигурации по умолчанию проверка производится на все виды вредоносных программ, кроме руткитов. Не производится проверка памяти, реестра и записей cookies.
Autologon Scan	Проверка элементов, запускающихся при входе пользователя в систему. По умолчанию проверка элементов автозапуска отключена. Если вы хотите воспользоваться этим заданием, щелкните на нем правой кнопкой мыши, выберите **Планировщик** и поставьте задание на выполнение

Стандартные задачи	Описание
	при запуске системы. Вы можете указать, сколько времени (в минутах) задание должно выполняться после запуска.

Замечание
Поскольку задания **Глубокая проверка системы** и **Полная проверка системы** проводят анализ всей системы, их выполнение может занять определенный промежуток времени. Поэтому, рекомендуем выполнять эти задачи с небольшим приоритетом, либо когда Ваша система не загружена.

- **Задачи пользователя** - содержит задачи, определенные пользователем.

  Задача под названием `Мои документы` обеспечивается. Используйте данное задание для проверки основных папок пользователя: `Мои документы`, `Рабочий стол` and `Автозагрузка`. Это позволит обеспечить безопасность Ваших документов, безопасность рабочего пространства и запуск незараженных программ при загрузке.

- **Прочие задачи** - содержит список мелких задач. Эти задачи проверки включают альтернативные типы сканирования, которые не могут быть запущены из данного окна. Вы можете только изменить их настройки или просмотреть отчеты о проверке.

Справа от каждой задачи доступны три кнопки:

- **Задачи по расписанию** - указывает на то, что выполнение данной задачи запланировано позднее. Нажмите эту кнопку, чтобы перейти к разделу Планировщик section в окне **Свойства**, где можно изменить данную настройку.
- **Удалить** - удаляет выбранное задание.

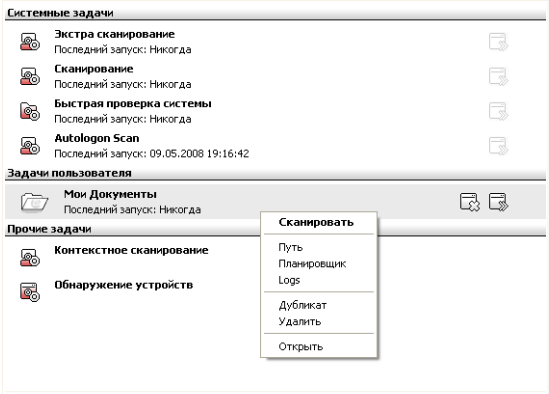
Замечание
Недоступно для системных задач. Вы не можете удалить системные задачи.

- **Проверить** - запускает соответствующее задание, запуская немедленную проверку.

Слева от каждого задания расположена кнопка **Свойства**, позволяющая настроить задание и просмотреть журналы проверок.

16.2.2. Использование Выпадающего меню

Для каждой задачи имеется выпадающее меню, открывающееся щелчком правой кнопки мыши по выбранной задаче.



Выпадающее меню

В выпадающем меню имеются следующие команды:

- **Проверить сейчас** - запуск выбранной задачи, немедленное начало процесса проверки.
- **Путь** - открытие окна **Параметры** и вкладки Путь, где вы можете сменить объект сканирования выбранного задания.

Замечание
В случае системных задач, эта кнопка меняется на **Показать путь задачи**, так что Вы можете только просмотреть объект проверки.

- **Планировщик** - открытие окна **Параметры** и вкладки Планировщик, где вы можете установить выполнение выбранного задания по расписанию.
- **Logs** - открытие окна **Параметры** и вкладки Logs, где вы можете просмотреть отчеты, созданные после выполнения выбранного задания.
- **Дубликат** - создание копии выбранной задачи. Данная функция полезна при создании новых задач, поскольку можно изменить настройки дубликата.
- **Удалить** - удаление выбранной задачи.

Замечание
Недоступно для системных задач. Вы не можете удалить системные задачи.

- **Открыть** - открытие окна **Параметры** и вкладки Обзор, где вы можете изменить параметры выбранного задания.

Замечание
Из-за их особенных свойств для категории **Прочие задачи** доступны только параметры **Logs** и **Открыть**.

16.2.3. Создание задач сканирования

Создать задачу сканирования, используя один из следующих способов:

- Создать копию существующего задания, переименовать его и внести необходимые изменения в окне Свойства;
- Нажмите **Новое задание**, чтобы создать новое задание и настроить его.

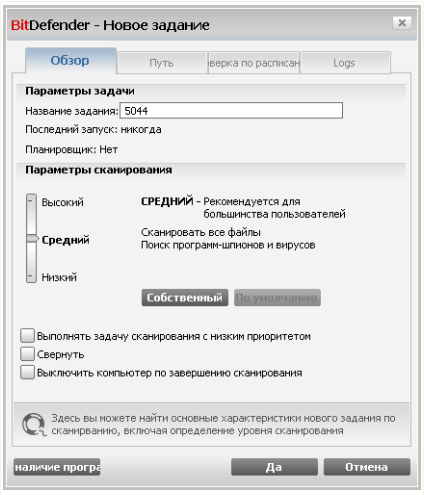
16.2.4. Настройка задач проверки

Каждая задача имеет собтсвенное окно **Свойства**, где можно настроить опции проверки, установить объект проверки, запланировать задачу или просмотреть отчеты. Открыть это окно нажав кнопку **Открыть**, расположенный с права от задачи **Открыть**).

Замечание
Чтобы получить больше информации, просмотрите журналы и таблицу **Журналы**, обратитесь к «*Просмотр журнала проверок*» (p. 128).

Конфигурация настроек сканирования

Формировать опции сканирования для определенной задачи **Настройки**. Появится следующее окно:



Обзор

Здесь можно просмотреть информацию о задаче (название, последний запуск и планирование), а также установить параметры проверки.

Выбор уровеня проверки

Прежде всего, необходимо выбрать уровень проверки. Переместите бегунок вдоль шкалы, чтобы установить соответствующий уровень проверки.

Существует 3 уровня проверки:

Уровень защиты	*Описание*
Низкий	Подразумевает среднюю эффективность выявления. Потребляет небольшое количество ресурсов. Программы проверяются только на наличие вирусов. Кроме классической проверки при помощи базы образов, также используется эвристический анализ.
Средний	Подразумевает высокую эффективность выявления. Потребляет среднее количество ресурсов.

Уровень защиты	*Описание*
	Все файлы проверяются на наличие вирусов и программ-шпионов. Кроме классической проверки при помощи базы образов, также используется эвристический анализ.
Высокий	Подразумевает очень высокую эффективность выявления. Потребляет значительное количество ресурсов. Все файлы и архивы проверяются на наличие вирусов и программ-шпионов. Кроме классической проверки при помощи базы образов, также используется эвристический анализ.

Имеется ряд общих настроект для процесса проверки:

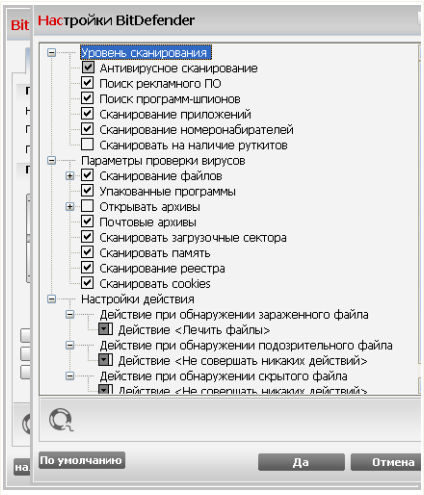
- **Выполнить задачу с низким приоритетом.** Уменьшается приоритет процесса проверки. Таким способом Вы ускоряете работу других программ, но увеличиваете время, необходимое для завершения процесса проверки.
- **Свернуть окно проверки в панель задач при запуске.** Окно проверки свертывается в системный трей. Чтобы открыть его, следует дважды щелкнуть на значке BitDefender.
- **Прекратить работу компьютера после сканирования, если никакие угрозы не найдены**

Нажмите **ОК** чтобы сохранить изменения и закройте окно. Чтобы запустить задачу, нажмите **Проверить**.

Настройка уровеня проверки

Опытные пользователи могут воспользоваться дополнительными настройками BitDefender, например, не проверять файлы с определенным расширением, определенные директории и архивы, которые точно безвредны. Это может значительно уменьшить время проверки и улучшить работу компьютера во время проверки.

Нажмите **Личный уровень**, чтобы установить Ваши настройки проверки. Откроется новое окно.



Настройки проверки

Опции сканирования организованы как расширяемое меню, очень похожее на то, которое используется при поиски в Windows. Щелчок мышки на значке "+" разворачивает список, а на значке "-" – закрывает его.

Настройки проверки разделены на 3 категории:

- **Уровень проверки.** Укажите тип вредоносной программы, поиск которой Вы хотите организовать при помощи BitDefender, указывая соответствующие опции в категории **Уровень проверки**.

Настройка	*Описание*
Проверка на вирусы	Сканирование на известные вирусы. BitDefender также обнаруживает неполные или поврежденные тела вирусов, удаляя любую потенциально опасную угрозу безопасности Вашей системы.
Проверка на вредоносное рекламное ПО	Проверка на вредоносное рекламное ПО. Эти файлы будут считаться зараженными. Программное обеспечение, которое включает

Настройка	Описание
	компоненты этого ПО, может прекратить работу, если выбрана эта настройка.
Проверка на наличие программ-шпионов	Проверка на известные программы-шпионы. Обнаруженные файлы будут считаться инфицированными.
Проверка на приложения	Сканирование допустимых приложений, которые могут быть использованы как инструмент злоумышленника с целью скрытия вредоносного ПО или с другим злым умыслом.
Проверка на номеронабирателей	Проверка на приложения, набирающие дорогие телефонные номера. Обнаруженные файлы будут считаться инфицированными. Программное обеспечение, включающее в себя компоненты, осуществляющие набор номеров, могут перестать работать при включении данной опции.
Проверка на руткиты	Проверка на скрытые объекты (файлы и процессы), известные как руткиты.

- **Опции проверки на вирусы.** Укажите тип сканируемых объектов (типы файлов, архивы и т.д.), выбрав соответствующие параметры из категории **Параметры проверки вирусов**.

Настройка		Описание
Проверка файлов	**Проверить все файлы**	Сканируются все файлы независимо от их типа.
	Проверить только файлы программ	Проверяются только файлы программ, то есть файлы с расширением: `exe`; `bat`; `com`; `dll`; `ocx`; `scr`; `bin`; `dat`; `386`; `vxd`; `sys`; `wdm`; `cla`; `class`; `ovl`; `ole`; `exe`; `hlp`; `doc`; `dot`; `xls`; `ppt`; `wbk`; `wiz`; `pot`; `ppa`; `xla`; `xlt`; `vbs`; `vbe`; `mdb`; `rtf`; `htm`; `hta`; `html`; `xml`; `xtp`; `php`; `asp`; `js`; `shs`; `chm`; `lnk`; `pif`; `prc`; `url`; `smm`; `pdf`; `msi`; `ini`; `csc`; `cmd`; `bas`; `eml`; `nws`.

Настройка		Описание
	Проверить файлы с расширением	Проверяются только файлы с заданным расширением. Задаваемые расширения разделяются знаком ";".
Открыть запакованные программы		Проверяются запакованные файлы.
Открыть архивы		Проверяются файлы внутри архивов. Сканирование архивных файлов увеличивает время проверки и требует большего объема системных ресурсов. Вы можете щелкнуть мышью в поле **Карантин ограничен** и ввести максимальный размер сканируемых архивов в килобайтах (КБ).
Открыть почтовые архивы		Проверяются файлы внутри почтовых архивов.
Проверить загрузочные секторы		Проверка загрузочных секторов системы.
Проверка памяти		Проверка памяти на вирусы и прочие вредоносные программы.
Проверка записей системного реестра		проверка записей системного реестра.
Проверка файлов Cookies		проверка файлов Cookies.

- **Настройки действий.** Укажите действие, которое следует предпринять над каждой категорией обнаруженных файлов с помощью параметра в категории **Настройки действия**.

  Замечание
  Чтобы установить новое действие, щелкните на текущем действии и выберите желаемый параметр из меню.

  - Выбрерите действие, которое будет применено над зараженными файлами. Доступными являются следующие варианты:

Действие	Описание
Только отчет	Не выполняются никакие действия с зараженными файлами. Названия этих файлов появятся в файле отчета.
Вылечить файлы	Удалите вредоносный код из обнаруженных инфицированных файлов.
Удалить файлы	Зараженный файл удаляется немедленно, без предупреждения.
Переместить файлы в карантин	Зараженные файлы перемещаются в Карантин. Добавленные в карантин файлы нельзя выполнять или открывать; таким образом, риск заражения сводится к нулю.

- Выберите действие, которое будет применено к обнаруженным подозрительным файлам. Доступными являются следующие варианты:

Действие	Описание
Только отчет	Не выполняются никакие действия с подозрительными файлами. Названия этих файлов появятся в файле отчета.
Удалить файлы	Подозрительные файлы удаляются немедленно, без предупреждения.
Переместить файлы в карантин	Подозрительные файлы перемещаются в Карантин. Добавленные в карантин файлы нельзя выполнять или открывать; таким образом, риск заражения сводится к нулю.

Замечание
Подозрительные файлы обнаруживаются при помощи эвристического анализа. Рекомендуем отправлять их на изучение в Лабораторию BitDefender.

- Выберите действие, которое будет применено к обнаруженным скрытым объектам (руткитам). Доступными являются следующие варианты:

Действие	Описание
Только отчет	Не выполняются никакие действия со скрытыми файлами. Названия этих файлов появятся в файле отчета.
Переместить файлы в карантин	Скрытые файлы перемещаются в Карантин. Добавленные в карантин файлы нельзя выполнять или открывать; таким образом, риск заражения сводится к нулю.
Сделать видимым	Выявить скрытые файлы, так что Вы сможете их просмотреть.

- **Опции действий над архивированными файлами.** Сканирование файлов внутри архивов и действия над ними связаны с определенными ограничениями. Защищенные паролем архивы нельзя сканировать, не предоставив пароль. В зависимости от формата (типа) архива, BitDefender может оказаться неспособен вылечить, изолировать или удалить зараженные архивированные файлы. Настройте действия, которые должны предприниматься над обнаруженными архивированными файлами с помощью соответствующих параметров из категории **Опции действий над архивированными файлами**.
  - Выбрерите действие, которое будет применено над зараженными файлами. Доступными являются следующие варианты:

Действие	Описание
Не совершать никаких действий	Только вести учет инфицированных архивированных файлов в отчете о сканировании. После завершения сканирования вы можете открыть отчет о проверке, чтобы просмотреть сведения об этих файлах.
Вылечить файлы	Удалите вредоносный код из обнаруженных инфицированных файлов. В некоторых случаях лечение будет невозможно, например, когда инфицированный файл находится внутри особого почтового архива.

Действие	Описание
Удалить файлы	Немедленно удалять инфицированные файлы с диска без предупреждения.
Переместить файлы в карантин	Переместить инфицированные файлы из исходного места в папку карантина. Добавленные в карантин файлы нельзя выполнять или открывать; таким образом, риск заражения сводится к нулю.

○ Выберите действие, которое будет применено к обнаруженным подозрительным файлам. Доступными являются следующие варианты:

Действие	Описание
Не совершать никаких действий	Вести учет только подозрительных архивированных файлов в отчете о сканировании. После завершения сканирования вы можете открыть отчет о проверке, чтобы просмотреть сведения об этих файлах.
Удалить файлы	Подозрительные файлы удаляются немедленно, без предупреждения.
Переместить файлы в карантин	Подозрительные файлы перемещаются в Карантин. Добавленные в карантин файлы нельзя выполнять или открывать; таким образом, риск заражения сводится к нулю.

○ Выберите действие, которое будет применено над защищенными паролем файлами. Доступными являются следующие варианты:

Действие	Описание
Отчет: не сканированный	Вести учет только защищенных паролем файлов в отчете о проверке. После завершения сканирования вы можете открыть отчет о проверке, чтобы просмотреть сведения об этих файлах.

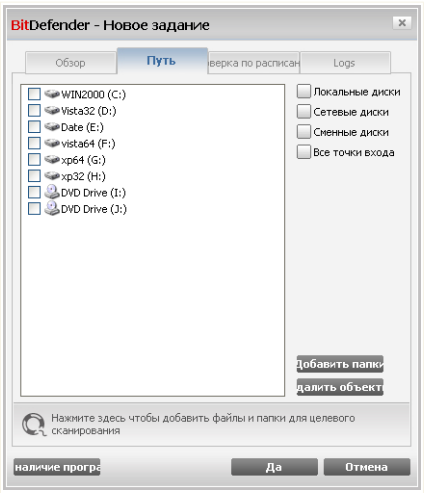
Действие	Описание
Подсказка для пароля	Запрашивать у пользователя пароль для сканирования обнаруженного файла, защищенного паролем.

Замечание
Если Вы выберите опцию игнорировать обнаруженные файлы, или выбранное Вами действие не будет выполнено, Вам будет предложено выбрать действие при помощи мастера проверки.

Чтобы загрузить настройки по умолчанию, щелкните мышкой на кнопке **По умолчанию**. Нажмите **OK**, чтобы сохранить изменения и закройте окно.

Настройка сканирования

Чтобы увидеть результаты сканирования после запуска, щелкните правой кнопкой на задании и выберите **Путь**. Появится следующее окно:



Поиск цели

Будет отображен список локальных, сетевых и сменных дисков, а также список файлов и каталогов, добавленных ранее, если такие есть. Все объекты, отмеченные галочкой, будут проверены при запуске задания.

В этом разделе находятся следующие кнопки:

- **Добавить список** - открывает окно обзора, где можно выбрать файлы, которые необходимо проверить.

  Замечание
  Вы можете также перетаскивать файлы или папки в список,чтобы добавить их в список.

- **Удалить объект** - удаляет файлы и папки из списка объектов для сканирования.

  Замечание
  Удалить можно только тот файл(ы) или ту папку(и), которые были добавлены. Объекты, обнаруженные программой автоматически, не могут быть удалены.

Помимо кнопок, описанных выше, есть также некоторые опции, которые позволяют осуществить быстрый выбор объектов для проверки.

- **Жесткие диски** - проверка жестких дисков.
- **Сетевые диски** - проверка всех сетевых дисков.
- **Съемные диски** - проверка съемных дисков (CD-ROM, гибкий диск).
- **Все объекты** - проверка всех дисков: жестких, сетевых и съемных.

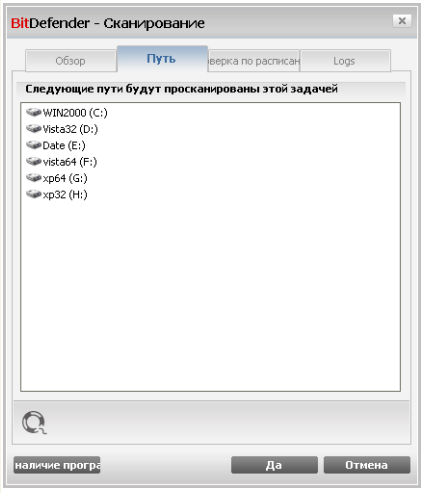
Замечание
Если Вы хотите проверить на наличие вирусов весь компьютер, поставьте значок в поле **Все объекты**.

Нажмите **ОК** чтобы сохранить изменения и закройте окно. Чтобы запустить задачу, нажмите **Проверить**.

Просмотр цели сканирования системных задач

Вы не можете изменять объект проверки для заданий проверки из категории **Системные задания**. Вы можете только видеть цель сканирования.

Чтобы просмотреть цели сканирования из определенной системной задачи, щелкните правой кнопкой мыши по задаче и выберите**Показать пути задачи**. **Полное сканирование системы**, например, появится окно следующего вида:



Цель сканирования из задачи "Полное сканирование системы"

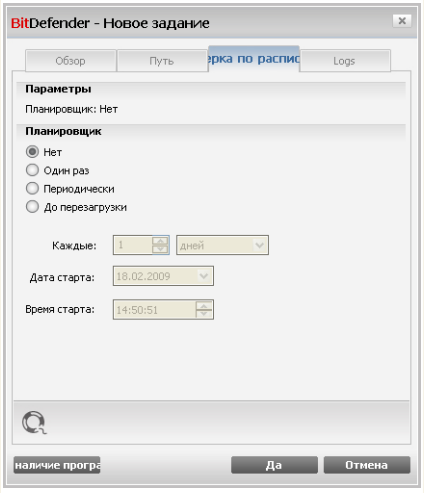
Полное сканирование системы и **Глубокое сканирование системы** просканирует все локальные диски, в то время как **Быстрое сканирование системы** просканирует только папки `Windows` и `Program Files`.

Щелкните мышкой на кнопке **OK** и закройте окно. Чтобы запустить задачу, нажмите **Сканировать**.

Планирование задач сканирования

Работая с комплексными задачами, процесс сканирования займет некоторое количество времени, и он будет более эффективным, если все другие программы будут закрыты. Поэтому лучше запланировать на такое время, когда вы не используете Ваш компьютер и он находится в режиме ожидания.

Чтобы просмотреть расписание запуска конкретного задания или изменить его, нажмите правой клавишей мыши и выберите пункт **Расписание задания**. Появится следующее окно:



Проверка по расписанию

Вы можете просмотреть запланированные задачи, если такие есть.

Когда запланируете задачу, вы должны выбрать один из следующих опций:

- **Не запланировано** - запуск задания только по команде пользователя.
- **Единоразово** - запуск проверки единоразово в определенный момент. Укажите дату и время в полях **Дата/Время запуска**.
- **Периодически** - процедура проверки запускается многократно, периодически через определенные промежутки времени (часы, дни, недели, месяцы, годы), начиная с заданной даты и в определенное время.

  Если Вы хотите повторять процесс проверки через определенные интервалы времени, выберите **Периодически** и в поле **Каждые** введите число минут/часов/дней/недель/месяцев/лет, соотвествующих необходимому интервалу. Также необходимо указать дату и время первого запуска в полях **Дата/Время запуска**.
- **До перезагрузки** - запуск сканирования спустя заданное количество минут после того, как пользователь вошел в систему.

Нажмите **ОК** чтобы сохранить изменения и закройте окно. Чтобы запустить задачу, нажмите **Проверить**.

16.2.5. Сканирование объектов

Перед тем, как запустить процесс проверки, Вы должны убедиться, что базы BitDefender находятся в актуальном состоянии. Проверка Вашего компьютера при помощи устаревшей бызы сигнатур может привести к тому, что BitDefender не сможет обнаружить новые вредоносные программы, выявленные с момента последнего обновления. Чтобы узнать, когда было произведено последнее обновление, в консоли настроек нажмите **Обновление>Обновление**.

Замечание
Чтобы BitDefender полностью проверил все Ваши файлы, необходимо закрыть все запущенные приложения, особенно почтовые программы, например, Outlook,Outlook Express или Eudora.

Методы сканирования

BitDefender имеет четыре типа сканирования по требованию:

- Немедленная проверка - запуск задачи проверки из списка системных / определенных пользователем.
- Контекстная проверка - щелкните правой клавишей мыши на файле или папке и выберите BitDefender Antivirus 2009.
- Проверка с перетаскиванием - перетащите файл или папку на Панель состояния проверки;
- Ручная проверка - непосредственный выбор файлов и папок для сканирования.

Немедленная проверка

Для проверки Вашего компьютера или его части можно воспользоваться заданиями проверки по умолчанию, либо можно создать собственные задания. Это называют немедленным сканированием.

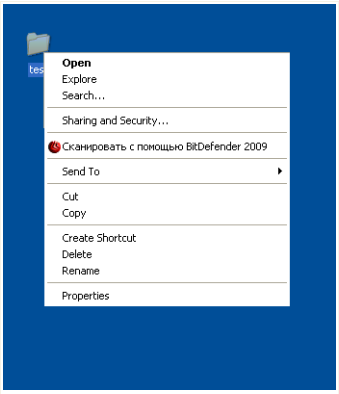
Чтобы запустить задачу сканирования, используйте один из следующих методов:

- дважды щелкните на нужной задаче в списке.
- нажмите **Проверить сейчас** для выполнения задачи.
- выберите задачу и нажмите **Запустить задачу**.

Появится Сканер BitDefender и начется сканирование. Больше информации найдете «*Сканер BitDefender*» (p. 124).

Проверка через контекстное меню

Чтобы проверить файл или папку без создания нового задания проверки, можно воспользоваться контекстным меню. Этоназывается сканирование через контекстное меню.



Контекстное сканирование

Щелкните правой кнопкой мышки на файле или папке, которые необходимо проверить, и выберите **BitDefender Antivirus 2009**.

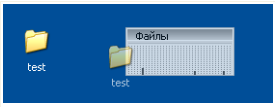
Появится Сканер BitDefender и начется сканирование. Больше информации найдете «*Сканер BitDefender*» (p. 124).

Вы можете изменить настройки проверки и просмотреть файл отчета с помощью **Свойств** в окне задачи **Проверка через контекстное меню**.

Проверка перетаскиванием

Перетащите файл или папку, которую вы хотите проверить, в **Панель активной проверки**, как показано ниже.

Тяните Файл



Переместите файл

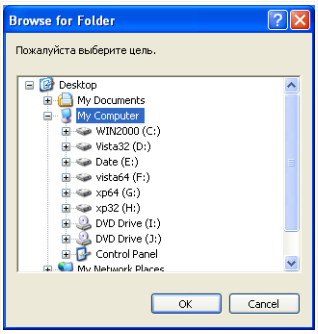
Появится Сканер BitDefender и начется сканирование. Больше информации найдете «*Сканер BitDefender*» (p. 124).

Ручное сканирование

Проверка вручную состоит в том, чтобы непосредственно выбрать объект проверки при помощи опции Ручная проверка BitDefender в группе задач BitDefender в меню Пуск.

Замечание
Ручная проверка также полезна потому, что ее можно выполнить даже когда Windows работает в Безопасном режиме.

Чтобы выбрать объект, который будет проверен BitDefender, надо зайти в **Пуск → Программы → BitDefender 2009 → BitDefender Manual Scan**. Появится следующее окно:



Ручное сканирование

Выберите объект, который необходимо проверить, и нажмите **OK**.

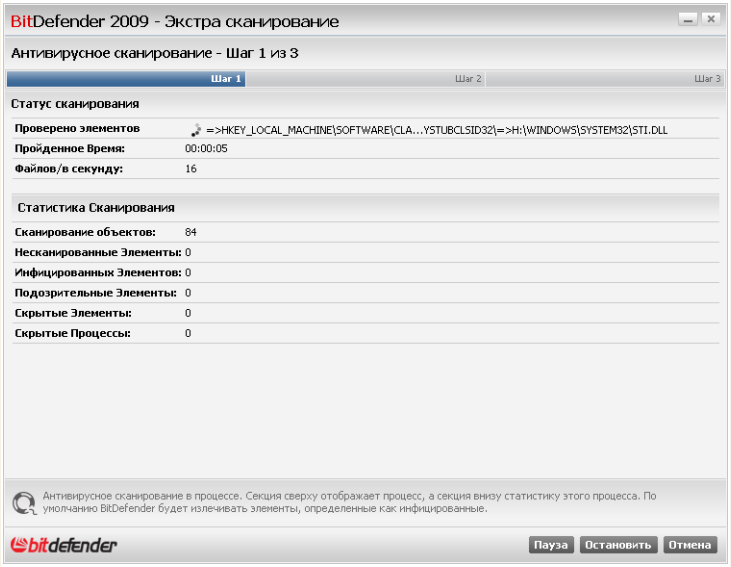
Появится Сканер BitDefender и начется сканирование. Больше информации найдете «*Сканер BitDefender*» (p. 124).

Сканер BitDefender

Когда Вы начнете процесс сканирования по требованию, то появится BitDefender Сканер. Чтобы завершить процесс проверки выполните последовательность из трех шагов.

Шаг 1/3 - Сканирование

BitDefender начнет проверку выбранных объектов.



Сканирование

Вы можете просматривать состояние проверки и статистику (скорость сканирования, время до окончания, количество проверенных / зараженных / подозрительных / скрытых объектов и проч.).

Замечание
В зависимости от сложности задач проверки, процесс сканирования может занять некоторое время.

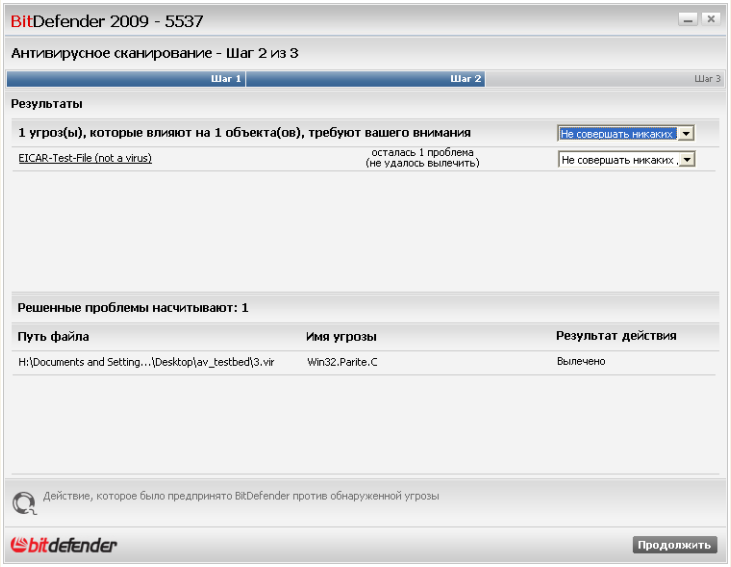
Чтобы временно приостановить процесс проверки, нажмите **Пауза**. Чтобы продолжить проверку, нажмите **Возобновить**.

Вы можете остановить процесс проверки в любое время, нажав **Стоп& Да**. При этом вы попадете на самый последний шаг мастера.

Дождитесь окончания сканирования BitDefender

Шаг 2/3 - Выберите Действия

Когда проверка завершится, откроется новое окно, где Вы можете просмотреть результаты проверки.



Действия

Вы можете просмотреть количество проблем, влияющих на безопасность Вашей системы.

Зараженные объекты разделены на группы, в зависимости от вредоносной программы, которой они были инфицированы. Кликните на ссылку, чтобы найти больше информации о зараженных объектах.

Для всех проблем вы можете выбрать общее действие, либо есть возможность выбрать отдельное действие для каждой группы проблем.

Доступны следующие варианты:

Действие	*Описание*
Ни чего не делать	Над обнаруженными файлами не будет производиться никаких действий.
Вылечить	Выполняется лечение зараженных файлов.
Удалить	Удаление обнаруженных файлов.

Действие	Описание
Раскрыть	Сделать скрытые объекты видимыми.

Нажмите **Продолжить**, чтобы применить выбранные действия.

Шаг 3/3 - Просмотр результатов

Когда BitDefender завершит исправление проблем, результаты проверки будут отображены в новом окне.

Резюме

Здесь Вы можете просмотреть краткий обзор. Щелкните **Показать файл отчета** для просмотра файла отчета.

Важно
Если потребуется, перезагрузите Вашу систему для завершения процесса очистки.

Нажмите **Закрыть**, чтобы закрыть окно.

BitDefender не может исправить некоторые проблемы

В большинстве случаев BitDefender успешно лечит зараженные файлы, которые обнаруживает, или изолирует инфекцию. Однако, есть проблемы, которые не могут быть исправлены.

В это случае рекомендуем Вам обратиться в Службу поддержки BitDefender на сайте www.bitdef.ru. Представители технической поддержки помогут Вам решить возникшие проблемы.

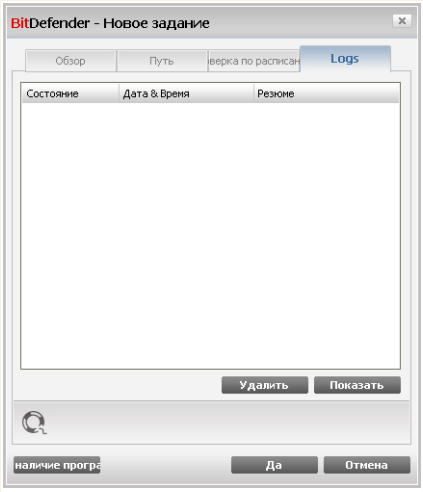
Обнаруженные BitDefender подозрительные файлы

Подозрительные файлы - файлы обнаруженные при эвристическом анализе и они могут быть зараженны вредоносным ПО, описания которого еще нет в вирусных сигнатурах.

Если в процессе проверки были найдены подозрительные файлы, Вам будет предложено отправить их в Лабораторию BitDefender. Нажмите **OK**, чтобы отправить эти файлы в Лабораторию BitDefender для дальнейшего анализа.

16.2.6. Просмотр журнала проверок

Чтобы увидеть результаты сканирования после запуска задания, щелкните правой кнопкой на задании и выберите **Logs**. Появится следующее окно:



Журнал отчета

Здесь Вы можете увидеть файлы отчетов, которые генерировались каждый раз, когда выполнялась задача. Для каждого файла Вам предоставляют информацию, относительно состояния записанного процесса сканирования, даты и времени, из отчета результатов сканирования.

Доступны две кнопки:

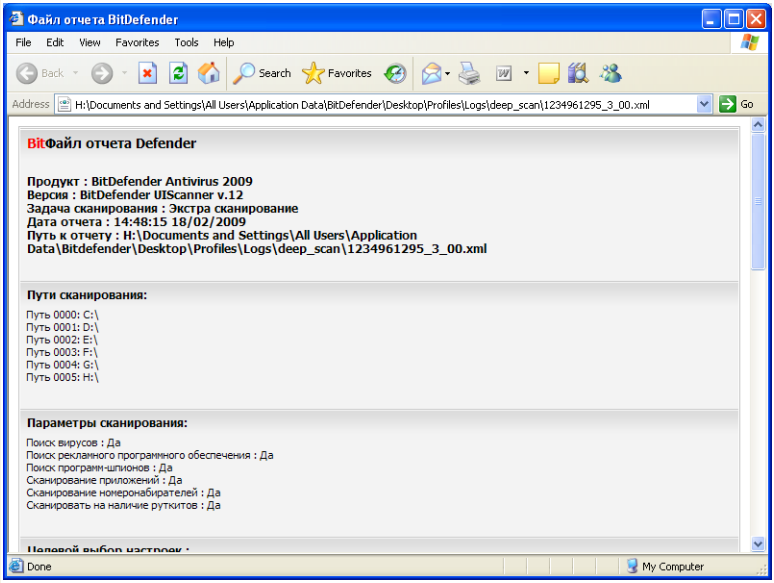
- **Удалить** - удаление выбранного файла отчета.
- **Показать** - просмотр выбранного файла отчета. Отчет сканирования откроется в вашем web-браузере по умолчанию.

Замечание
Для просмотра или удаления файла можно воспользоваться щелчком правой кнопки мыши на выбранном файле и выбрать соответствующее действие из открывшегося меню.

Нажмите **ОК** чтобы сохранить изменения и закройте окно. Чтобы запустить задачу, нажмите **Проверить**.

Пример отчета проверок

Следующий рисунок представляет собой пример файла отчета сканирования:



Пример отчета проверок

Отчет сканирования содержит подробную информацию о записанном процессе сканирования, такое как сканирование опций, сканирование цели, найденные угрозы и действия совершенные над ними.

16.3. Объекты исключены из резидентного сканирования и из сканирования по требованию

Иногда бывают случаи, когда необходимо исключить определенные файлы из сканирования. К примеру, возможно, Вы захотите исключить тестовый файл EICAR из объектов входной проверки или файлы с расширением `.avi`.

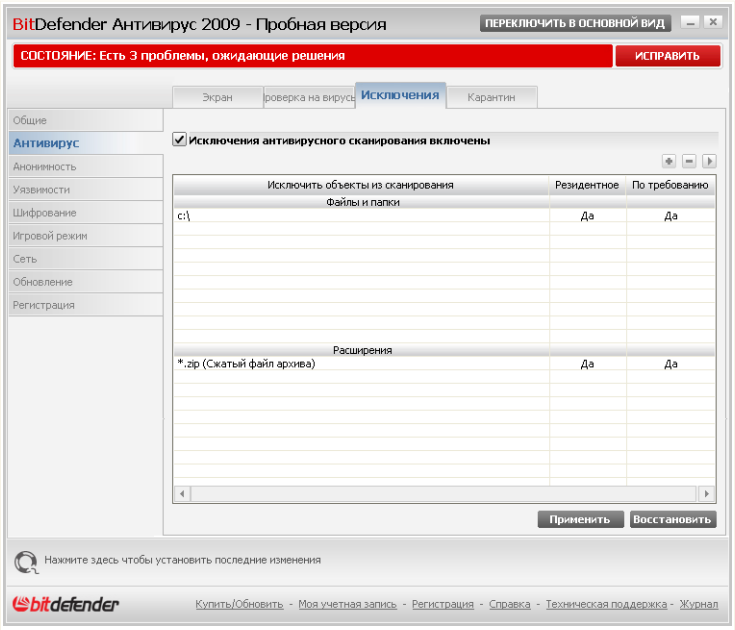
BitDefender позволяет исключать объекты при входной проверке и/или проверки по требованию. Данная функция предназначена для уменьшения времени на проверку и исключения вмешательства в процесс Вашей работы.

Два типа объектов могуть быть исключены из сканирования:

- **Пути** - файл или папка (включая все объекты, которые она содержит), обозначенные путем в системе, которые будут исключены из проверки.
- **Расширения** - все файлы, имеющие определенное расширение будут исключены из просмотра.

Замечание
Объекты не будут проверяться, если они исключенны из списка входного сканирования, причем независимо от того, запрашиваются ли они Вами, либо другим приложением.

Перейдите к разделу **Антивирус>Исключения** в окне расширенного вида для просмотра и управления объектами, исключенными из списка проверки.



Исключения

Вы можете просмотреть объекты (файлы, папки, файлы с определенным расширением), которые исключаются из процесса сканирования. Для каждого объекта можно узнать, исключен ли он из входной проверки, проверки по требованию или др.

Замечание
Указанные здесь исключения НЕ распространяются на контекстную проверку.

Чтобы удалить вход из стола, выберите и нажмите на кнопку **Удалить**.

Чтобы редактировать вход, выбрети и нажмите кнопку **Редактировать**. Откроется новое окно, где Вы можете изменить расширение или путь к исключению и тип сканирования, из которой Вы необходимо исключить. Внесите необходимые изменения и нажмите **OK**.

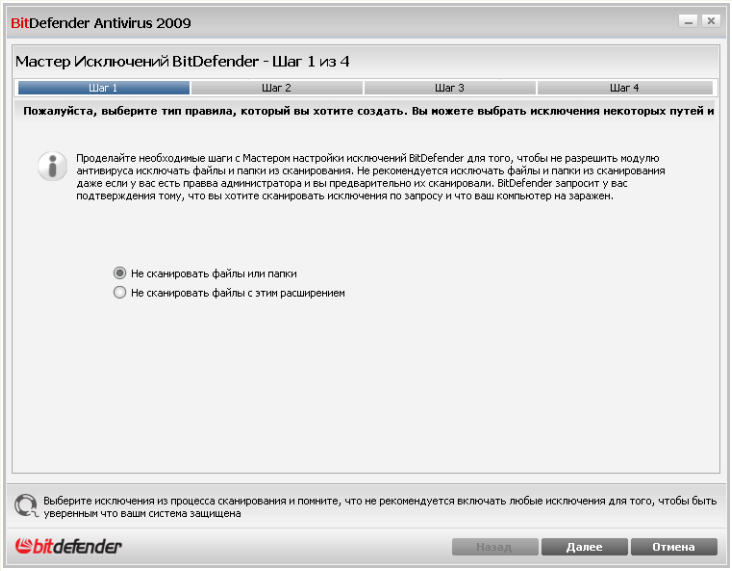
Замечание
Вы также можете нажать правой кнопкой мыши на объекте и воспользоваться пунктами меню для его редактирования или удаления.

Вы можете нажать на **Сброс** вернув изменения сделанные к правилам, при условии, Вы не сохранили их нажав **Применить**.

16.3.1. Исключение путей для сканирования

Чтобы исключить пути для сканирования, нажмите на кнопку **Добавить**. Вам дадут указания относительно процесса исключения определенных путей при помощи открывшегося мастера настройки.

Шаг 1/4 - Выберите тип объекта

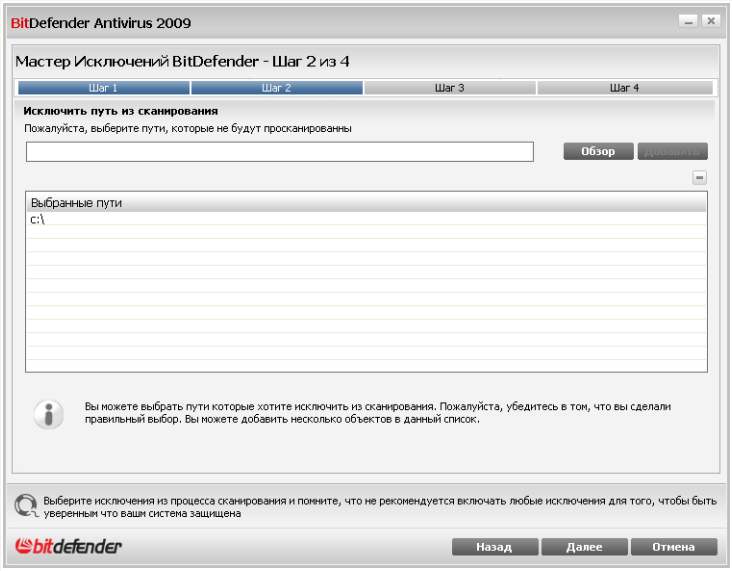


Тип объекта

Выберите опцию для исключения пути из сканирования.

Щелкните по кнопке **Далее**.

Шаг 2/4 - Укажите пути исключения



Пути исключения

Определить пути, которые будут исключены из сканирования, используя любой из следующих методов:

- Нажмите **Обзор**, выберите файл или папку для исключения из сканирования и нажмите **Добавить**.
- Введите путь, который Вы хотите исключить из проверки, в соответствующее поле и нажмите **Добавить**.

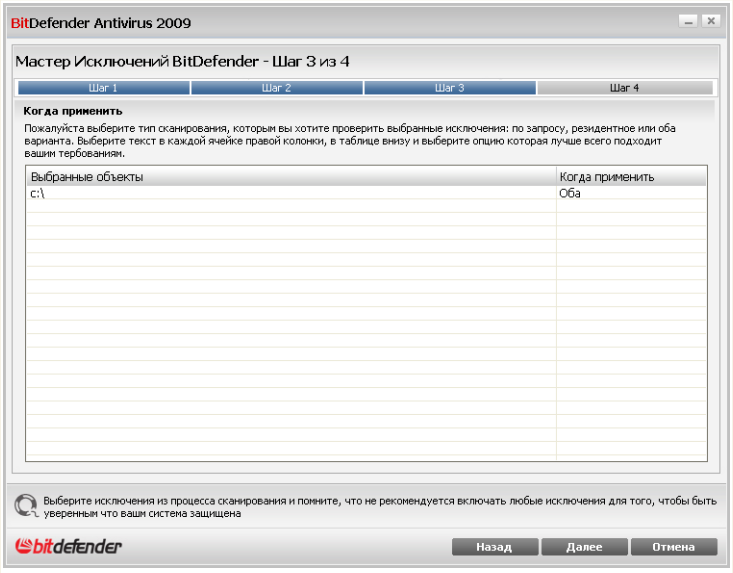
> ***Замечание***
> Если указанный путь не существует, появится сообщение об ошибке. Нажмите **OK** и проверьте правильность пути.

По мере добавления, пути будут отображаться в таблице. Вы можете добавлять любое количество путей.

Чтобы удалить вход из стола, выберите и нажмите на кнопку **Удалить**.

Щелкните по кнопке **Далее**.

Шаг 3/4 - Выберите тип проверки



Тип сканирования

Вы можете просмотреть таблицу, содержащую все исключаемые пути, а также тип проверки.

По умолчанию, введенные пути исключаются как из входной проверки, так и из проверки по указанию. Чтобы изменить эту настройку, нажмите на правую колонку и выберите необходимый пункт из списка.

Щелкните по кнопке **Далее**.

Шаг 4/4 - Проверьте исключенные файлы

Проверка исключенных файлов

Настоятельно рекомендуется проверять файлы в указанных папках, чтобы убедиться, что они не заражены. Поставьте данный флажок для сканирования этих файлов перед исключением их из списка проверки.

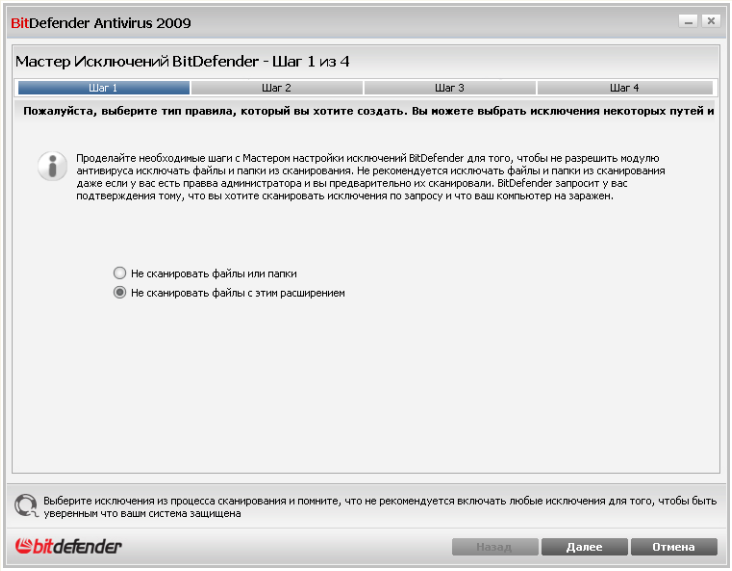
Щелкните мышкой на кнопке **Завершить**.

Щелкните мышкой на **Применить** чтобы сохранить сделанные изменения.

16.3.2. Исключение расширений из сканирования

Чтобы исключить расширения из сканирования, нажмите **Добавить**. Вам дадут указания относительно процесса исключения определенных расширений из проверки при помощи открывшегося мастера настройки.

Шаг 1/4 - Выберите тип объекта

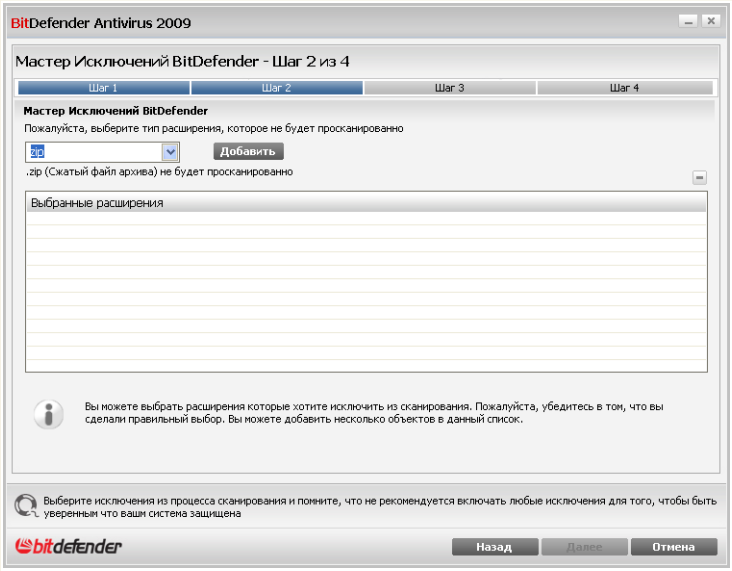


Тип объекта

Выберите опцию, которая исключает расширение из сканирования.

Щелкните по кнопке **Далее**.

Шаг 2/4 - Задайте расширения, которые необходимо исключить



Исключение расширений

Задать расширения, которые должны быть исключены из сканирования можно следующими методами:

- Из меню выберите расширение, которое Вы хотите исключить из проверки, и нажмите **Добавить**.

> ***Замечание***
> Меню содержит список расширений файлов, зарегистрированных в Вашей системе. При выборе расширения, вы увидите его описание, если есть.

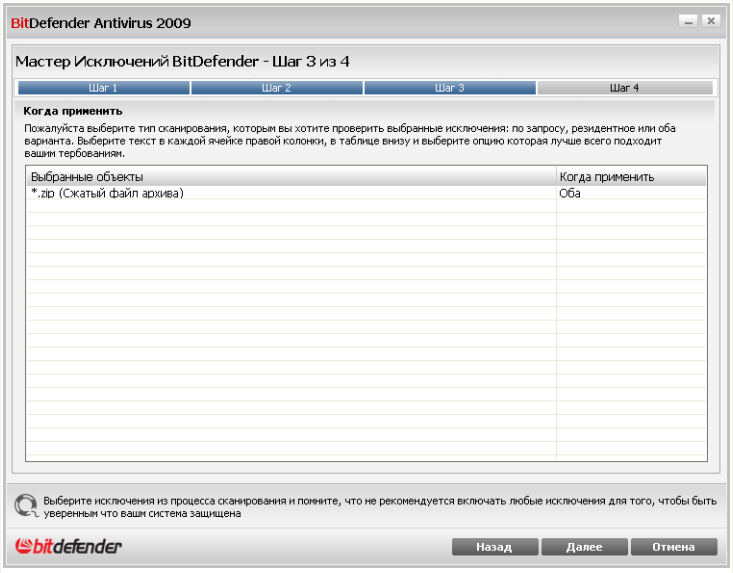
- Тип расширения, которое должно быть исключенно из сканирования, в редактирующей области и нажмите **Добавить**.

По мере добавления, расширения будут отображаться в таблице. Вы можете добавлять любое количество расширений.

Чтобы удалить вход из стола, выберите и нажмите на кнопку **Удалить**.

Щелкните по кнопке **Далее**.

Шаг 3/4 - Выберите тип проверки



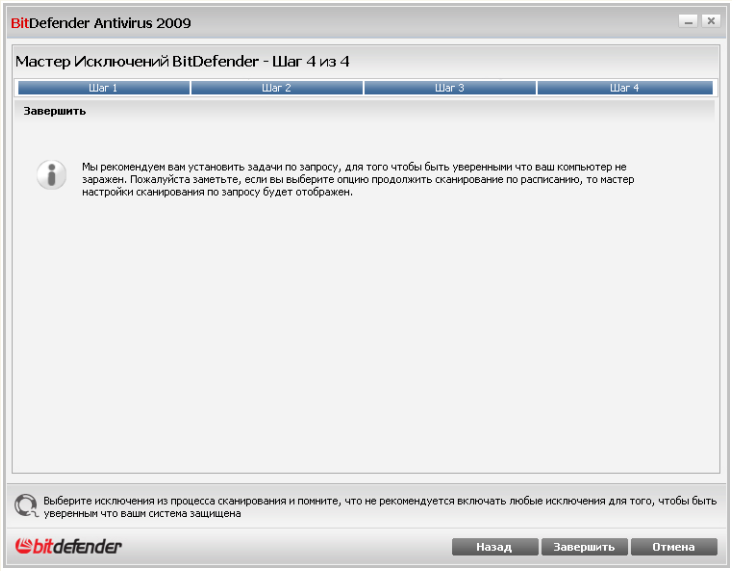
Тип сканирования

Вы можете просмотреть таблицу, содержащую все исключаемые расширения, а также тип проверки.

По умолчанию, выбранные расширения исключаются как из входной проверки, так и из проверки по указанию. Чтобы изменить эту настройку, нажмите на правой колонке и выберите необходимый пункт из списка.

Щелкните по кнопке **Далее**.

Шаг 4/4 - Выберите тип проверки



Тип сканирования

Настоятельно рекомендуется проверять файлы с указанными расширениями, чтобы убедиться, что они не заражены.

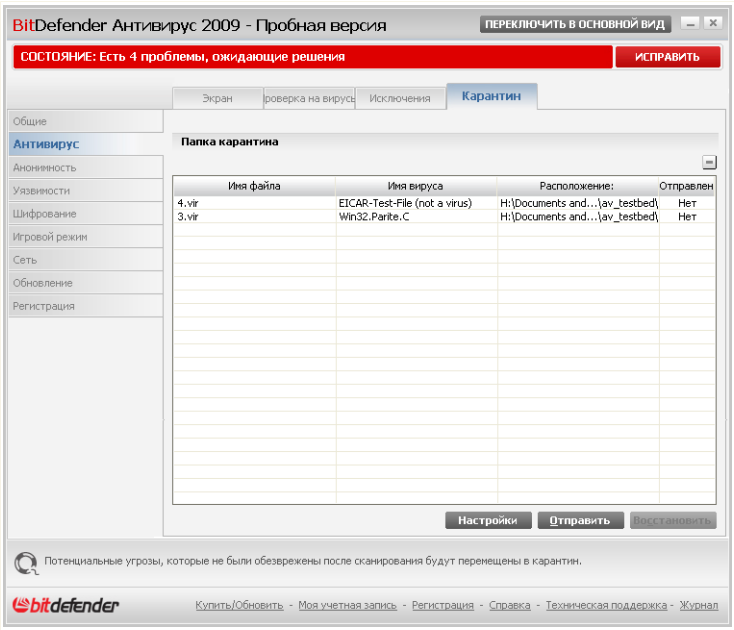
Щелкните мышкой на кнопке **Завершить**.

Щелкните мышкой на **Применить** чтобы сохранить сделанные изменения.

16.4. Область Карантина

BitDefender позволяет изолировать зараженные и подозрительные файлы в области, названной карантином. Благодаря этому другие файлы не могут быть заражены, и в то же время, Вы всегда можете отправить эти файлы в лабораторию BitDefender на анализ.

Перейдите к разделу **Антивирус>Карантин** в окне расширенного вида, чтобы просмотреть и выполнить действия над файлами в карантине, а также настроить параметры карантина.



Карантин

В разделе Карантин отображаются файлы, изолированные в данный момент в папке Карантин. Для каждого файла в карантине отображается его имя, имя обнаруженного вируса, путь к его исходному местонахождению и дата занесения.

Замечание
Вирус, изолированный в карантинной зоне, не может причинить никакого вреда, так как его нельзя запустить или открыть для чтения.

16.4.1. Управление изолированными файлами

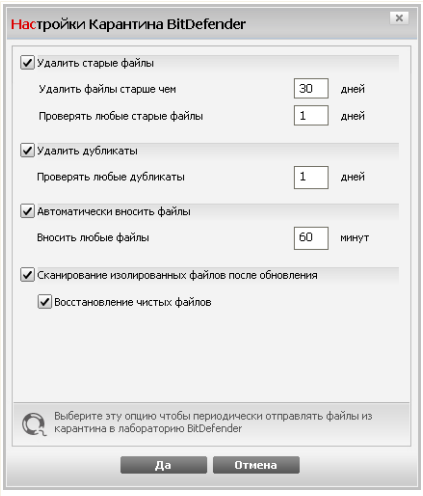
Чтобы удалить выбранный файл из карантина, нажмите кнопку **Удалить**. Если Вы хотите восстановить выбранный файл в его первоначальное местоположение, нажмите **Восстановить**.

Вы можете отослать любые файлы из карантина в лабораторию BitDefender, нажав **Отправить**.

Контекстное меню. Имеется контекстное меню, которое легко позволяет выполнять действия над файлами в карантине. Доступны те же функции, аналогичные описанным ранее. Вы также можете нажать **Обновить**, чтобы обновить содержимое раздела Карантин.

16.4.2. Конфигурация настроек Карантина

Чтобы настроить Карантин, нажмите **Настройки**. Появится новое окно.



Настройки Карантина

Использую настройки Карантина, Вы можете сделать, чтобы BitDefender выполнял следующие действия:

Удаление старых файлов. Чтобы автоматически удалить старые файлы в карантине, включите соответствующую опцию. Вы должны указать количество дней, после которого файлы в карантине должны быть удалены и частоту, с которой BitDefender должен проверять старые файлы.

Замечание
По умолчанию, BitDefender ежедневно проверяет старые файлы и удаляет файлы, старше 30 дней.

Удаление дубликатов. Чтобы автоматически удалить дублирующие файлы в карантине, включите соответствующую опцию. Вы должны указать количество дней между двумя последующими проверками дубликатов.

Замечание
По умолчанию, BitDefender ежедневно проверяет дубликаты файлов и удаляет каждый день.

Автоматически предлагать на рассмотрение файлы. Чтобы автоматически предлагать на рассмотрение изолированные файлы, провертье соответствующую опцию. Вы должны указать частоту с которой предлагать на расмотрение файлы.

Замечание
По умолчанию, BitDefender автоматически предлагает на рассмотрение каждые 60 минут.

Сканирование изолированных файлов после обновления. Для автоматического сканирования изолированных файлов после каждого выполненного обновления установите соответствующий флажок. Вы можете включить автоматическое перемещение вылеченных файлов в исходную папку, выбрав **Восстановление чистых файлов**.

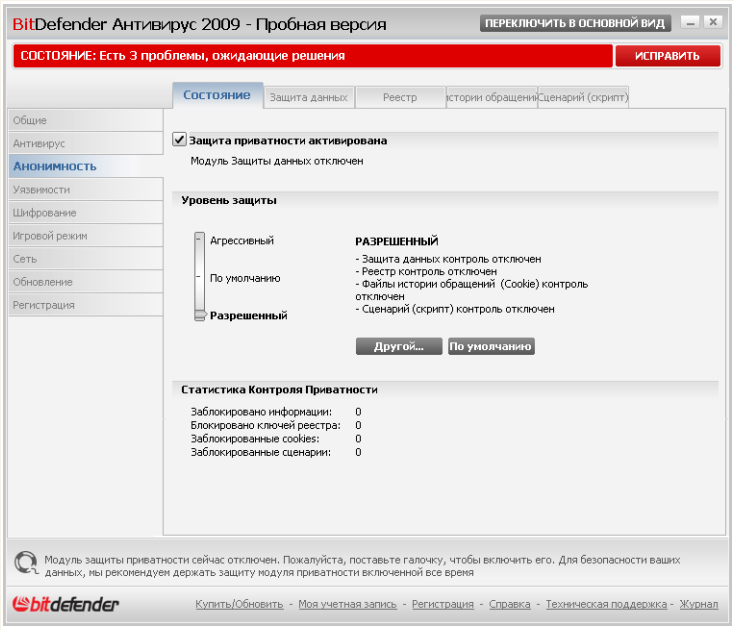
Нажмите **OK**, чтобы сохранить изменения и закройте окно.

17. Анонимность

Bitdefender контролирует множество потенциальных "горячих точек" в вашей системе, где могут действовать программы-шпионы, и также проверяет любые изменения в вашей системе и программном обеспечении. Он эффективно блокирует "трояны" и прочие программы, устанавливаемые хакерами, пытающимися нарушить конфиденциальность Вашей информации и выслать Вашу личную информацию, например, номер кредитной карты, с Вашего компьютера хакеру.

17.1. Настройка Статуса Анонимности

Чтобы настроить и следить за работой модуля Контроля личных данных, перейдите в раздел **Контроль личных данных>Состояние** в окне расширенного вида.



Настройка Статуса Анонимности

Здесь вы можете проверить, включен ли модуль анонимности. Если вы хотите сменить состояние модуля Анонимности, уберите или установите соответствующий флажок.

Важно
Чтобы защитить Ваш компьютер от воровства данных и обеспечить защиту конфиденциальной информации **Контроль личных данных** должен быть включен.

Модуль Анонимности защищает ваш компьютер, используя эти важные элементы управления защитой:

- Защита данных - защита конфиденциальных данных путем фильтрации всего исходящего трафика веба (HTTP), электронной почты (SMTP) и мгновенных сообщений согласно правил, указанных в разделе Защита данных.
- Управление реестром - спрашивает разрешения всякий раз, когда какая-либо программа будет пытаться менять запись в реестре для загрузки при запуске системы.
- Контроль cookies - запрашивает разрешение всякий раз, когда новый вебсайт пытается записать файл cookie.
- Контроль сценариев - запрашивает разрешение всякий раз, когда вебсайт пытается инициировать выполнение сценария или другого активного контента.

В нижней части данного раздела можно просмотреть **Статистику Контроля Конфиденциальности**.

17.1.1. Конфигурация уровня защиты

Вы можете выбрать уровень защиты согласно Вашим потребностям в безопасности. Передвиньте бегунок по шкале в соотвествующий уровень защиты.

Существует 3 уровня защиты:

Уровень защиты	*Описание*
Разрешающий	Включен только **Контроль регистра**
Стандартный	Включены только **Контроль регистра** и **Контроль конфиденциальности**.
Агрессивный	Включены только **Контроль регистра**, **Контроль сценариев** и **Контроль конфиденциальности**.

Вы можете настроить уровень защиты, нажмите **Настроить уровень**. В появившемся окне, выберите директивы защиты, которые Вы хотите включить и нажмите **OK**.

Нажмите **По умолчанию**, чтобы установить бегунок в уровень по умолчанию.

17.2. Контроль Идентичности

Обеспечение безопасности конфиденциальной информации - это волнующий всех вопрос. С развитием Интернет коммуникаций, развиваются и методы кражи информации, а также новые методы введения людей в заблуждение с целью выманивания частной информации.

Независимо от того, адрес ли это Вашей электронной почты или номер Вашей кредитной карты, если они попадут в плохие руки, то Вам может быть нанесен значительный ущерб: Вас могут засыпать спамовыми сообщениями или удивить нулевой баланс на Вашей карте.

Контроль конфиденциальности защищает вас от кражи уязвимых данных, когда вы в режиме онлайн. Основываясь на созданные вами правила, Контроль Конфиденциальности сканирует веб-траффик, электронную почту и траффик мгновенных сообщений, которые требуют от вашего компьютера особых строк символов (например, номер вашей кредитной карточки). Если есть совпадение, соответствующая веб-страница, адрес электронной почты или мгновенное сообщение блокируется.

Вы можете создать правила для зашиты какой-либо информации, которую вы считаете личной или конфиденциальной, от своего телефонного номера или адреса электронной почты до сведений о своем банковском счете. Приложение обеспечивает многопользовательскую поддержку, таким образом пользователи, входящие в различные учетные записи Windows, могли настраивать и использовать свои личные правила защиты данных. Создаваемые вами правила применяются и могут быть использованы только в случае если вы вошли в свою учетную запись Windows.

Зачем нужна защита данных?

- Функция защиты данных очень эффективна при блокировании логгеров клавиатуры. Этот тип вредоносного ПО записывает все ваши нажатия клавиш и отправляет их по интернету злоумышленнику (хакеру) В украденных данных хакер может найти личную информацию, такую как, например, номера банковских счетов и пароли, а также использовать ее в личных целях.

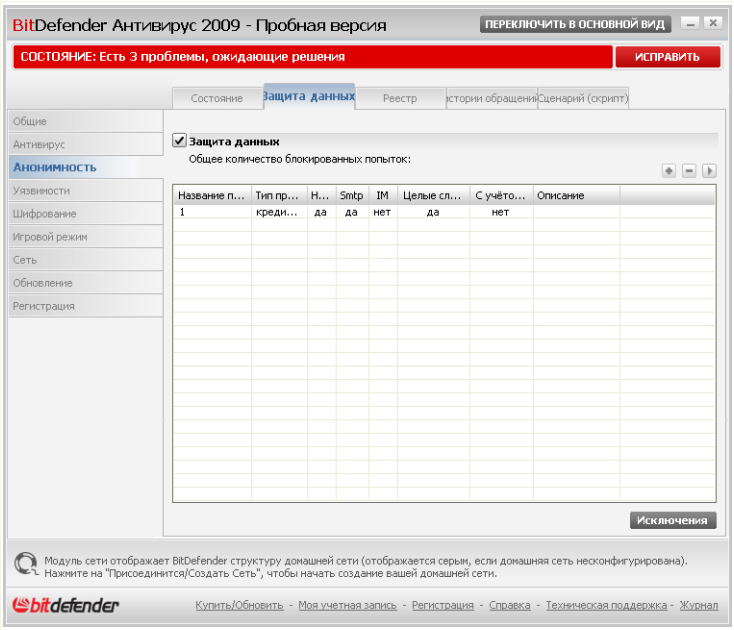
Даже если такому приложению удастся избежать обнаружение антивирусом, оно не сможет отправлять украденные данные по электронной почте, через веб или в мгновенных сообщениях, если вы создали соответствующие правила защиты.

- Функция защиты данных может защитить вас от попыток фишинга (попыток похитить персональную информацию). Самые распространенные попытки фишинга используют фальсификацию адреса электронной почты, провоцируя вас отсылать информацию на поддельную веб-страницу.

  Например, вы можете получить электронное сообщение якобы от вашего банка с просьбой срочно обновить вашу банковскую информацию. В этом сообщении будет находится ссылка на веб-страницу, где вы должны будете ввести свою личную информацию. Хотя все будет выглядеть вполне правдоподобно, и электронное сообщение, и веб-страница, на которую указывает ссылка, будут поддельными. Если перейти по ссылке в электронном сообщении и ввести свою личную информацию на поддельной веб-странице, эта информация попадет к злоумышленнику, который предпринял попытку фишинга.

  Если действуют соответствующие правила защиты данных, вы не сможете отправить личную информацию (такую как номер кредитной карты) на веб-странице, если вы явно не укажите исключение для этой веб-страницы.

Для настройки функции защиты данных перейдите к разделу **Анонимность>Защита данных** в окне расширенного вида.



Контроль Идентичности

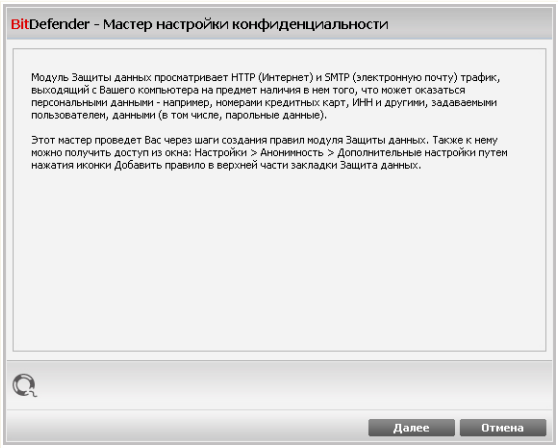
Если вы хотите использовать Контроль конфиденциальности, необходимо выполнить следующие шаги:

1. Установите флажок **Защита данных**.
2. Создавайте правила для защиты ваших уязвимых данных. Более подробные сведения вы найдете по ссылке «*Создание правил конфиденциальности*» (р. 148).
3. При необходимости, определите особые исключения для правил, которые вы создали. Более подробные сведения вы найдете по ссылке «*Определение исключений*» (р. 152).

17.2.1. Создание правил конфиденциальности

Чтобы создать новое правило защиты данных, нажмите кнопку **Добавить** и следуйте указаниям мастера настройки.

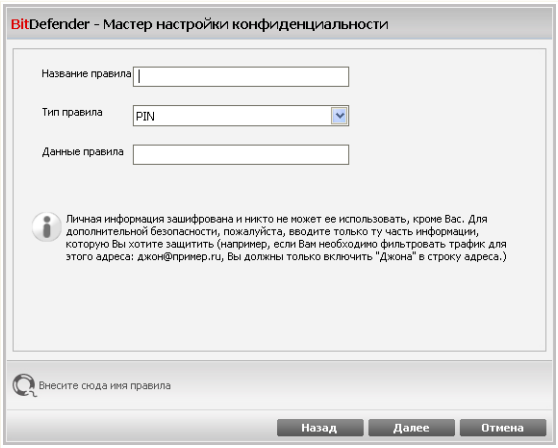
Шаг 1/4 - Окно приветствия



Окно приветствия

Щелкните по кнопке **Далее**.

Шаг 2/4 - Задать тип правила и данные



Установить тип правила и данных

Вам необходимо настроить следующие параметры:

- **Имя правила** - введите имя правила в поле для редактирования.
- **Тип правила** - выберите тип правила (адрес, имя, кредитная карта, PIN-код и т.д.).
- **Данные Правила** - введите данные, которые вы хотите защитить, в это поле для редактирования. К примеру, если вы хотите защитить номер вашей кредитной карточки, введите его частично или весь здесь.

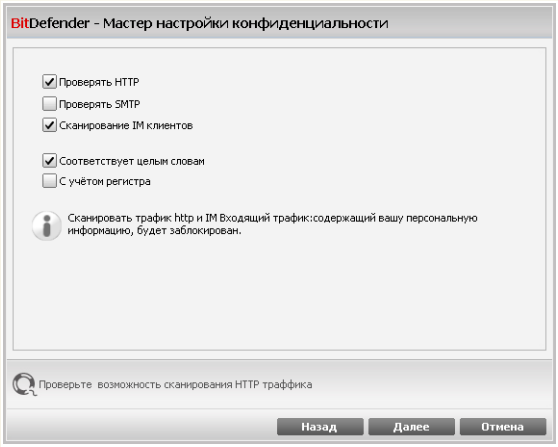
Замечание

Если Вы введете менее трех символов, Вам будет предложено уточнить данные. Рекомендуем Вам ввести минимум три символа, чтобы избежать блокирования по ошибке сообщений и веб-страниц.

Все введенные Вами данные шифруются. Для дополнительной безопасности не вводите полностью данные, которые Вы хотите защитить.

Щелкните по кнопке **Далее**.

Шаг 3/4 - Выберите трафик



Выберите трафик

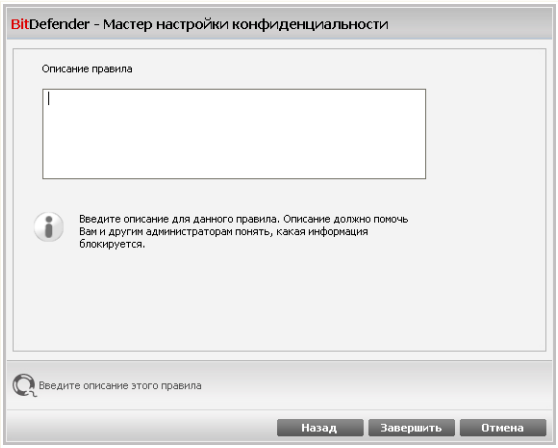
Выберите трафик, который будет проверяться BitDefender. Доступными являются следующие варианты:

- **Проверять HTTP** - поверяет HTTP (веб) трафик и блокирует исходящие данные, содержащие данные правила.
- **Проверять SMTP** - поверяет SMTP (почта) трафик и блокирует исходящие электронные сообщения, содержащие данные правила.
- **Проверка мгновенных сообщений** - поверяет трафик мгновенных сообщений и блокирует исходящие сообщения в чатах, содержащие данные правила.

Вы можете применять правило только в случае, если совпадение произойдет по целому слову, или же если совпадение произойдет по вхождению искомой строки.

Щелкните по кнопке **Далее**.

Шаг 4/4 - Введите описание правила



Опишите правило

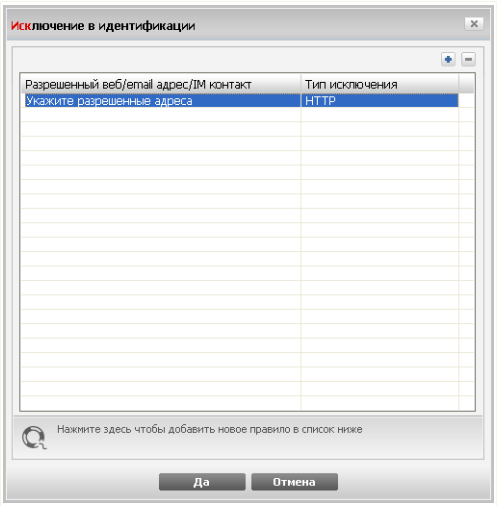
Введите краткое описание правила в поле редактирования. Так как заблокированные данные (символьные строки) не отображаются в виде простого текста при доступе к правилу, описание должно помочь вам легко идентифицировать их.

Щелкните мышкой на кнопке **Завершить**. Правило будет отображаться в таблице.

17.2.2. Определение исключений

Есть случаи, когда Вы должны определить исключения к определенным правилам конфиденциальности. Давайте рассмотрим пример, когда Вы хотите создать правило, предотвращающее отсылание номера Вашей кредитной карты через HTTP (веб). Каждый раз, когда номер Вашей кредитной карты будет отправлен с веб-сайта со страницы Вашей учетной записи, соответствующая страница будет заблокирована. Если, например, вы хотите совершить покупку в Интернет-магазине (в безопасности которого Вы уверены), Вам необходимо будет создать исключение из соответствующего правила.

Откройте окно где вы можете управлять исключениями, нажмите **Исключения**.



Исключения

Добавить исключение, следуя по этим шагам:

1. Нажмите **Добавить** добавить новый вход.
2. Щелкните дважды на кнопке **Указать допустимые адреса** и укажите веб-сайт, адрес электронной почты или контакт интернет-пейджера, который вы хотите добавить в качестве исключения.
3. Двойной щелчок на **Выберите тип** и выберите в меню соответствующий тип ранее указанного адреса.
   - Если у Вас есть определенный веб адрес, выберите **HTTP**.
   - Если у Вас есть определенный почтовый адрес, выберите **SMTP**.
   - Если вы указали контакт интернет-пейджера, выберите **IM**.

Чтобы удалить исключение из списка, то выбери его и нажми **Удалить**.

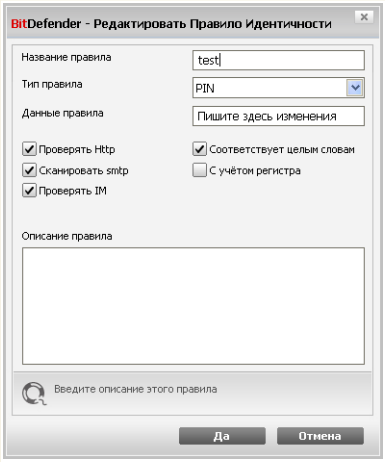
Щелкните мышкой на **Применить** чтобы сохранить сделанные изменения.

17.2.3. Управление правилами

В этом окне Вы видите список правил в таблице.

Чтобы удалить правило, выберите его и нажмите кнопку **Удалить**.

Чтобы редактировать правило, надо выбрать его и нажать кнопку **Редактировать** или дважды щелкнуть на правиле. Появится новое окно.



Редактировать правило

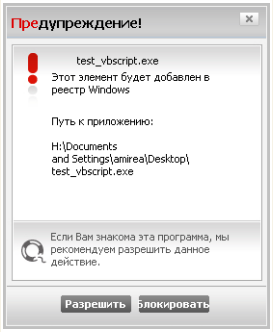
Здесь вы можете изменять название, описание и параметры правила (тип, данные и вид трафика). Нажмите **OK**, чтобы сохранить изменения.

17.3. Управление реестром

Реестр – важнейший компонент операционной системы Windows. Там хранятся настройки, установленные программы, информация пользователя и тому подобное.

В **Реестре** также определяется, какие программы необходимо автоматически загружать при запуске Windows. Многие программы-шпионы пользуются этим, чтобы автоматически запускаться при включении компьютера.

Функция **Управление реестром** позволяет следить за реестром операционной системы Windows. Это очень полезно для обнаружения программ класса Троян. Вы будете получать сообщение всякий раз, когда какая-либо программа будет менять запись в реестре, для того чтобы загружаться при запуске системы.



Предупреждение реестра

Вы можете посмотреть, какая программа пытается внести изменения в системный реестр Windows.

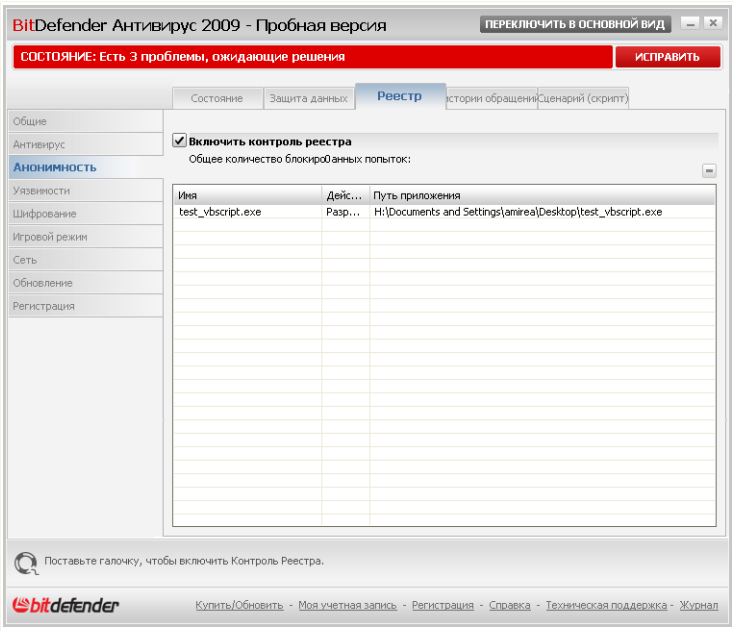
Если вы не узнаете, что это за программа и если одна выглядит подозрительно, нажмите **Блокировать**, чтобы не позволить ей вносить изменения в системный реестр. Иначе нажмите кнопку **Разрешить**, чтобы позволить ей вносить изменения.

На основании вашего ответа создастся правило и появится в списке правил. То же действие будет применяться, когда эта программа попытается внести изменения в запись реестра.

Замечание

Обычно BitDefender предупреждает Вас, когда Вы устанавливаете программу, запускающуюся после следующей перезагрузки компьютера. В большинстве случаев эти программы официальные и им можно доверять

Для настройки функции контроля реестра перейдите к разделу **Анонимность>Реестр** в окне расширенного вида.



Управление реестром

В этом окне Вы видите список правил в таблице.

Чтобы удалить правило, выберите его и нажмите кнопку **Удалить**.

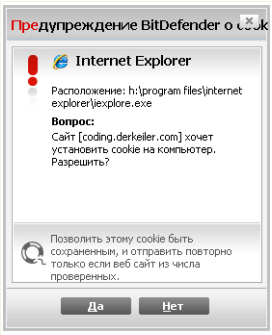
17.4. Контроль файлов истории обращений (Cookies)

Файлы истории обращений (Cookies) встречаются в Интернете очень часто. Это небольшие файлы, хранящиеся на Вашем компьютере. Сайты в сети создают такие файлы, чтобы отслеживать некоторую особенную информацию о Вас.

Файлы Cookies созданы, чтобы сделать жизнь пользователя легче. Например, с их помощью веб-сайт «запоминает» Ваше имя и Ваши настройки, и Вам не нужно вводить их при каждом посещении.

Но файлы истории обращений могут и раскрывать определенную информацию о Вас, отслеживая Ваши «перемещения» в сети.

Вот здесь и помогает функция **Контроль cookie**. Когда активно, **Контроль cookie**у Вас спрашивается разрешение всякий раз, когда новый сайт пытается создать файл cookie:



Cookie Предупреждение

В этом окне Вы видите название приложения, которое пытается создать файл cookie.

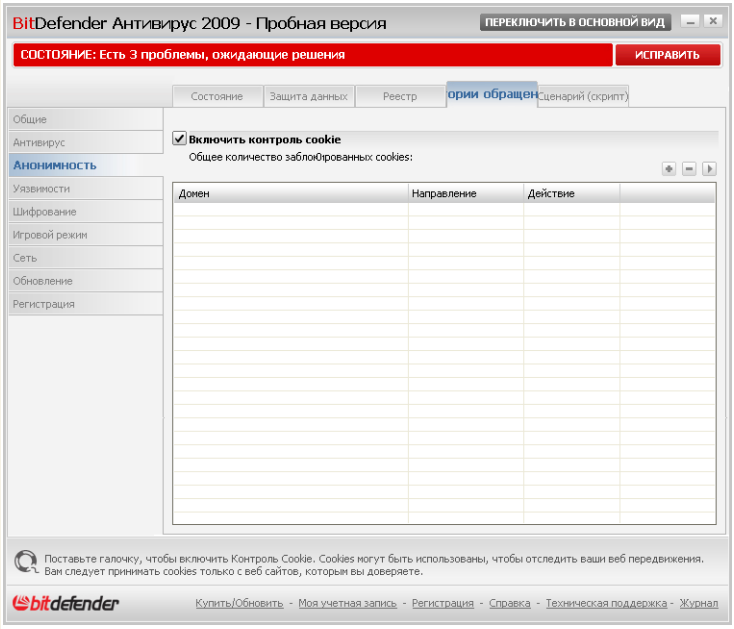
Поставьте значок в поле **Запомнить этот ответ** и щелкните мышкой на кнопке **Да** или **Нет**. Будет создано новое правило, которое будет занесено в таблицу правил.При подключении к этому же сайту в следующий раз Вы уже не получите предупреждения.

Это поможет Вам решить, каким веб-сайтам стоит доверять, а каким – нет.

Замечание

Так как на сегодняшний день используется множество файлов cookie, в самом начале Вам будет трудно работать с функцией **Контроль Cookie**: Вы слишком часто будете получать предупреждения. Как только Вы занесете регулярно посещаемые сайты в список правил, работать в Интернете будет так же легко, как и раньше.

Для настройки функции контроля файлов cookies перейдите к разделу **Анонимность>Cookie** в окне расширенного вида.



Контроль файлов истории обращений (Cookies)

В этом окне Вы видите список правил в таблице.

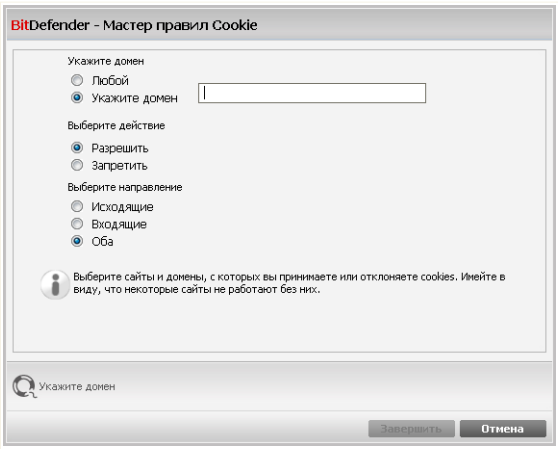
Важно
Значимость правил нарастает снизу вверх. То есть, последнее правило наиболее важное –оно имеет самый высокий приоритет. Чтобы изменить приоритет правил, перетаскивайте их по вверх-вниз по списку.

Чтобы удалить правило, выберите его и нажмите кнопку **Удалить**. Для изменения параметров правил дважды щелкните на правиле и выполните желаемые изменения в окне настройки.

Чтобы добавить новое правило вручную, нажмите кнопку **Добавить** и настройте параметры правила в окне конфигурации.

17.4.1. Окно конфигурации

При редактировании или добавления правила вручную, появится окно конфигурации.



Выберите адрес, действие и направление

Вы можете установить следующие настройки:

- **Адрес домена** - введите адрес домена, к которому будет применяться правило.
- **Действие** - выбрать действие для правила.

Действие	*Описание*
Разрешить	Сценарии в этом домене будут выполняться.
Запретить	Сценарии в этом домене не будут выполняться.

- **Направление** - выбор направления передачи данных.

Тип	*Описание*
Исходящие	Правило применяется только для файлов истории обращений cookies, которые отсылаются обратно к подключенному сайту.

Тип	Описание
Входящие	Правило применяется только для файлов истории обращений cookies, которые поступают от подключенного сайта.
Входящие и исходящие	Правило применяется и ко входящему, и к исходящему трафику.

Замечание
Вы можете принимать файлы cookies, но никогда не возвращать их, выбрав настройку **Запрещать** и направление **Исходящие**.

Щелкните мышкой на кнопке **Завершить**.

17.5. Контроль сценариев

Сценарии и другие приложения, такие как управляющие элементы ActiveX и Java приложения, которые обычно используются для создания страниц в Интернете, могут также быть запрограммированы на нанесение ущерба пользователю. Например, элементы ActiveX могут получить полный доступ к данным на вашем компьютере и считывать информацию, удалять ее, получать пароли и перехватывать сообщения, пока Вы работаете в режиме online. Вы должны работать с содержимым только тех сайтов, которые Вы хорошо знаете и которым полностью доверяете.

BitDefender позволяет Вам разрешить или заблокировать выполнение данных элементов.

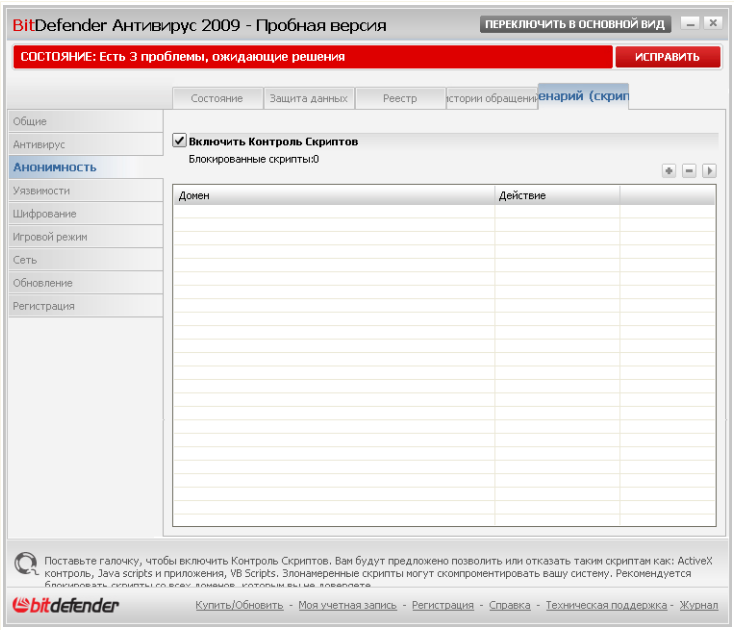
Используя функцию **Контроль сценариев** Вы всегда будете знать, каким сайтам в сети можно доверять, а каким нельзя. BitDefender будет запрашивать Ваше разрешение всякий раз, когда веб-сайт попробует использовать сценарий или другой активный контент:

Предупреждение о сценариях

В этом окне Вы видите название ресурса.

Поставьте галочку в поле **Запомнить этот ответ** и щелкните мышкой на кнопке **Да** или **Нет** Будет создано новое правило, которое будет занесено в таблицу правил. Когда этот же ресурс будет пытаться отправить Вам активный контент, Вы уже не получите предупреждения.

Для настройки функции контроля сценариев перейдите к разделу **Анонимность>Сценарий** в окне расширенного вида.



Контроль сценариев

В этом окне Вы видите список правил в таблице.

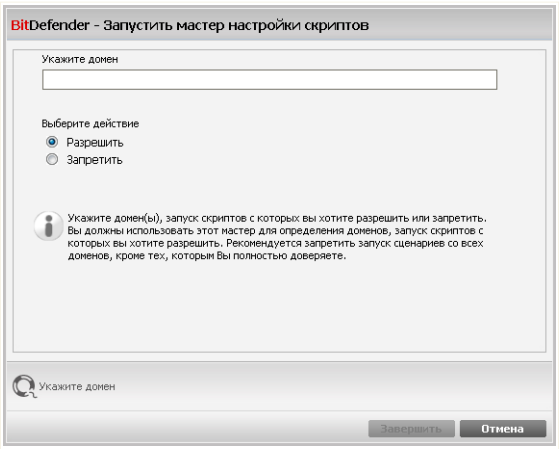
Важно
Значимость правил нарастает снизу вверх. То есть, последнее правило наиболее важное –оно имеет самый высокий приоритет. Чтобы изменить приоритет правил, перетаскивайте их по вверх-вниз по списку.

Чтобы удалить правило, выберите его и нажмите кнопку **Удалить**. Для изменения параметров правил дважды щелкните на правиле и выполните желаемые изменения в окне настройки.

Чтобы создать новое правило вручную, нажмите кнопку **Добавить** и настройте параметры правила в окне конфигурации.

17.5.1. Окно конфигурации

При редактировании или добавления правила вручную, появится окно конфигурации.



Выберите адрес и действие

Вы можете установить следующие настройки:

- **Адрес домена** - введите адрес домена, к которому будет применяться правило.
- **Действие** - выбрать действие для правила.

Действие	*Описание*
Разрешить	Сценарии в этом домене будут выполняться.
Запретить	Сценарии в этом домене не будут выполняться.

Щелкните мышкой на кнопке **Завершить**.

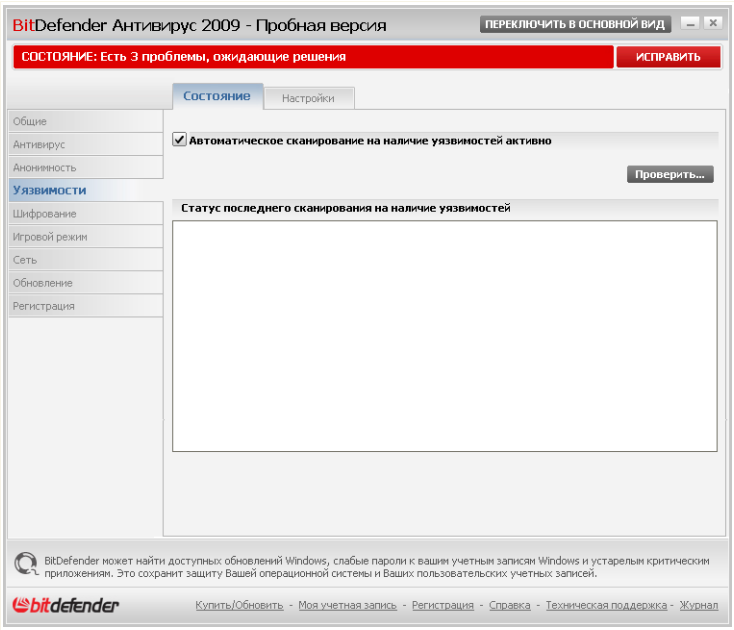
18. Уязвимости

Важный шаг в защите вашего компьютера против злоумышленников и вредоносного ПО состоит в том, чтобы держать операционную систему и используемые приложения в обновленном состоянии. Более того, чтобы предотвратить несанкционированный физический доступ к компьютеру, каждую учетную запись Windows необходимо снабдить сильным паролем (паролем, который трудно угадать).

BitDefender регулярно проверяет систему на наличие уязвимостей и уведомляет о существующих проблемах.

18.1. Состояние

Для настройки автоматической проверки на наличие уязвимостей или запуска проверки перейдите к разделу **Уязвимости>Состояние** в окне расширенного вида.



Сканирование на наличие уязвимостей

В таблице отображаются проблемы, обнаруженные во время последней проверки на наличие уязвимостей, а также их состояние Вы увидите действие, которое необходимо выполнить для устранения каждой уязвимости, если таковые будут обнаружены. Если вместо действия отображается **Отсутствует**, значит данная проблема не является уязвимостью.

Важно
Чтобы автоматически получать уведомления об уязвимостях системы или приложений, параметр **Автоматическое сканирование на наличие уязвимостей** должен быть включен.

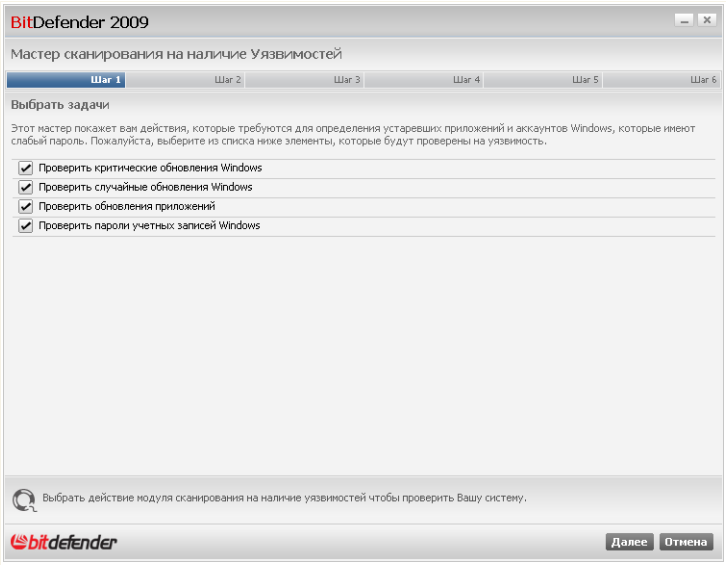
18.1.1. Устранение уязвимостей

Для устранения обнаруженной уязвимости необходимо дважды щелкнуть мышью на ней, и, в зависимости от проблемы, выполнить следующие действия:

- Если доступны обновления Windows, нажмите кнопку **Установка обновления** для их установки.
- Если версия приложения устарела, воспользуйтесь ссылкой **Web-страница** для загрузки и установки последней версии данного приложения.
- Если учетная запись Windows снабжена слабым паролем, настоятельно рекомендуйте пользователю сменить пароль при следующем входе в систему или смените его сами.

Вы можете нажать кнопку **Проверить...** и следовать указаниям мастера для пошагового устранения уязвимостей.

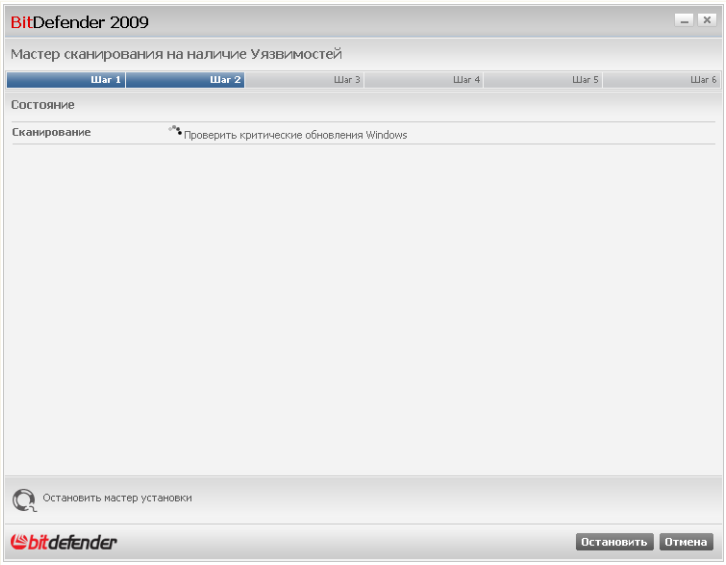
Шаг 1/6 - Выберите уязвимости для проверки



Уязвимости

Нажмите **Далее**, чтобы проверить систему на наличие выбранных уязвимостей.

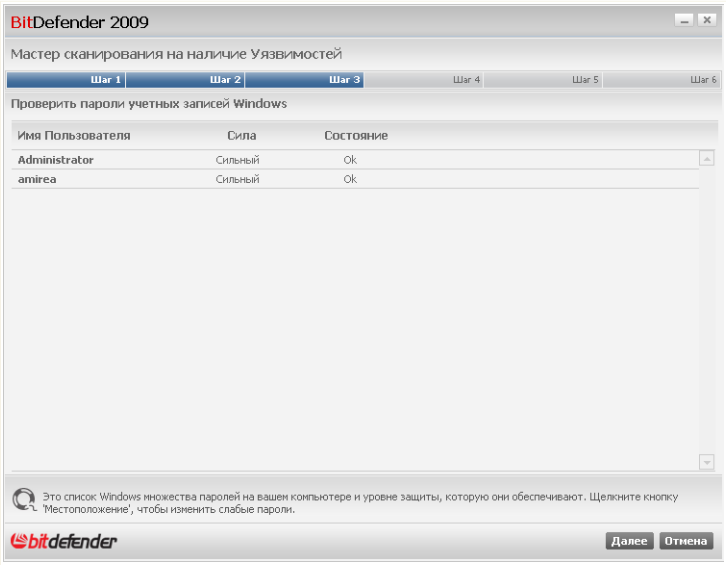
Шаг 2/6 - Проверка уязвимостей



Проверка уязвимостей

Подождите, пока BitDefender завершит проверку уязвимостей.

Шаг 3/6 - Смените слабые пароли



Пользовательские пароли

Вы можете просмотреть список учетных записей пользователей Windows, установленных на вашем компьютере, и уровень защиты, обеспечиваемый их паролями.

Нажмите **Устранить**, чтобы поменять все слабые пароли. Появится новое окно.

Изменить пароль

Выберите метод устранения проблемы:

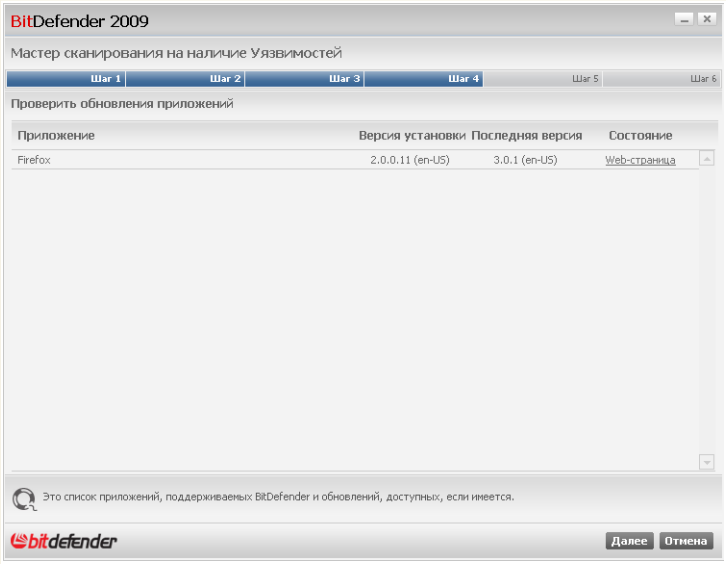
- **Пользователь может изменить пароль в следующем сеансе.** BitDefender выведет запрос на смену пароля в следующий раз при входе в Windows.
- **Изменить пароль.** Необходимо ввести пароль в поля ввода.

Замечание
Чтобы получить сильный пароль, используйте комбинации символов в верхнем и нижнем регистре, числа и специальные символы (такие как, например, #, $ или @).

Нажмите **OK**, чтобы сменить пароль.

Щелкните по кнопке **Далее**.

Шаг 4/6 - Обновите приложения

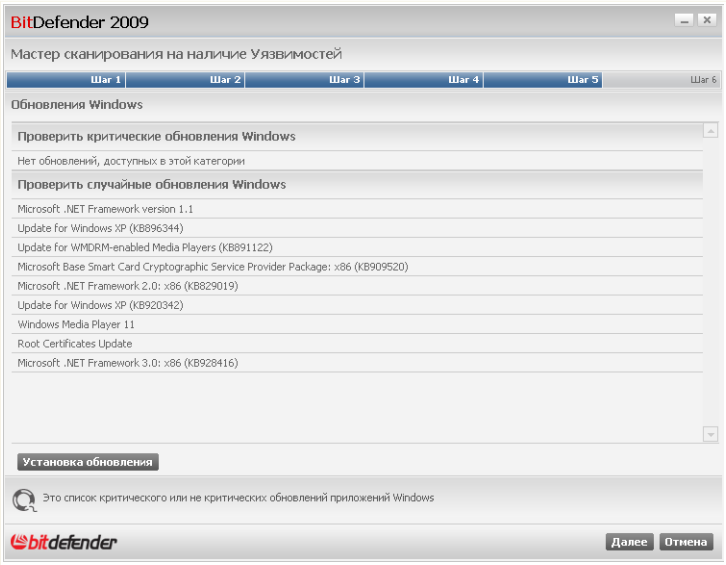


Приложения

Вы можете просмотреть список приложений, проверенных BitDefender, и проверить, нуждаются ли они в обновлениях. Если приложение нуждается в обновлении, щелкните появившуюся ссылку, чтобы загрузить последнюю версию.

Щелкните по кнопке **Далее**.

Шаг 5/6 - Обновите Windows



Обновления Windows

Вы можете просмотреть список важных и второстепенных обновлений Windows, которые в данный момент не установлены на вашем компьютере. Нажмите **Установка обновления**, чтобы установить все доступные обновления.

Щелкните по кнопке **Далее**.

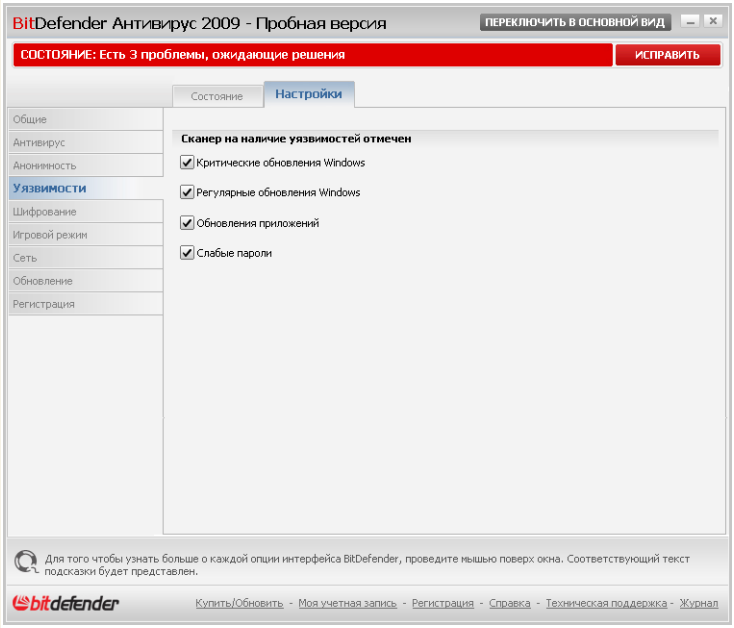
Шаг 6/6 - Просмотрите результаты

Результаты

Нажмите **Закрыть**.

18.2. Настройки

Для настройки параметров автоматической проверки на наличие уязвимостей перейдите к разделу **Уязвимости>Настройки** в окне расширенного вида.



Автоматическое сканирование на наличие уязвимостей

Установите флажки, соответствующие системным уязвимостям, наличие которых должно регулярно проверяться.

- **Критические обновления Windows**
- **Регулярные обновления Windows**
- **Слабые пароли**
- **Обновления приложений**

Замечание
Если снять флажок, соответствующий определенной уязвимости, BitDefender больше не будет уведомлять вас о связанных с ней проблемах.

19. Шифрование приложений мгновенного обмена сообщениями

По умолчанию BitDefender шифрует все сеансы обмена мгновенными сообщениями при условии, если:

- у вашего собеседника установлена версия BitDefender, которая поддерживает шифрование мгновенных сообщений, и эта функция включена в используемом интернет-пейджере;
- вы и ваш собеседник используете Yahoo Messenger или Windows Live (MSN) Messenger.

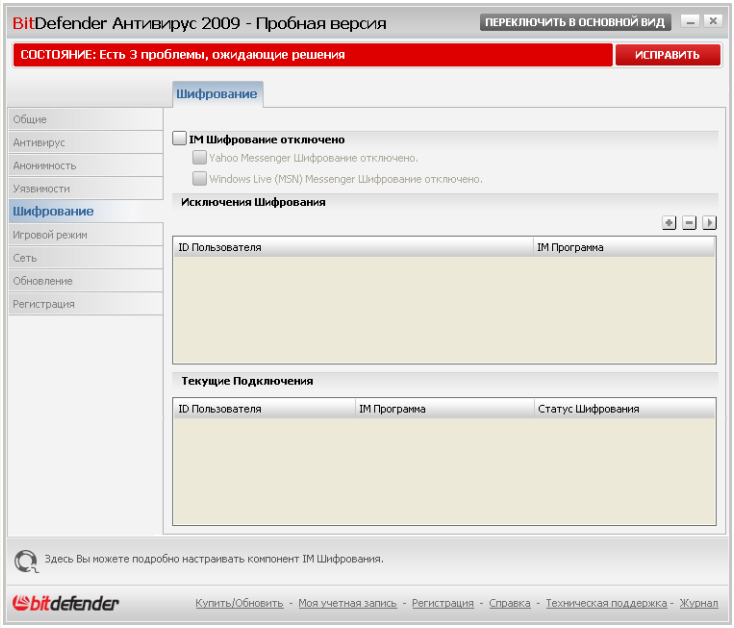
Важно

BitDefender не будет шифровать обмен сообщениями, если собеседник использует какой-либо веб-клиент, например Meebo, или другое приложения для чата, поддерживающее Yahoo Messenger или MSN.

Для настройки шифрования мгновенных сообщений перейдите в раздел **Шифрование>Шифрование IM** в окне расширенного вида.

Замечание

Вы можете легко настроить шифрование мгновенного обмена сообщениями с помощью панели инструментов BitDefender из окна чата. Для получения дополнительной информации перейдите к «*Интеграция в интернет-пейджер*» (p. 36).



Шифрование приложений мгновенной пересылки сообщений

По умолчанию шифрование мгновенных сообщений включено как для Yahoo Messenger, так и для Windows Live (MSN) Messenger. Вы можете выключить шифрование мгновенных сообщений полностью или только для определенной программы обмена сообщениями.

Отобразятся две таблицы:

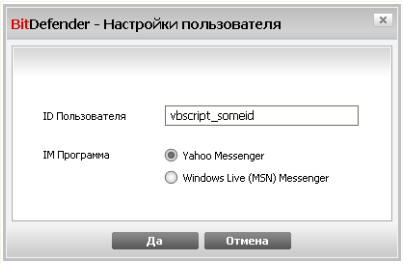
- **Исключения шифрования** - список всех идентификаторов пользователей и используемых ими интернет-пейджеров, для которых шифрование выключено. Чтобы удалить контакт из списка, выберите и нажмите кнопку **Удалить**.
- **Текущие подключения** - список текущих соединений обмена сообщениями (идентификаторы пользователей и соответствующие интернет-пейджеры), а также наличие или отсутствие шифрования. Соединение может быть не зашифровано по следующим причинам:
  - Шифрование соответствующего контакта следует отключить явно.

- У вашего контакта не установлена версия BitDefender, которая поддерживает шифрование мгновенных сообщений.

19.1. Отключение шифрования для отдельных пользователей

Для отключения шифрования для отдельного пользователя выполните следующую процедуру:

1. Нажмите кнопку **Добавить**, чтобы открыть окно настройки.



Добавление контактов

2. Введите в поле ввода идентификатор вашего контакта.
3. Выберите интернет-пейджер, связанный с данным контактом.
4. В конце щелкните мышкой на кнопке **OK**.

20. Игровой режим

Модуль игрового режима позволяет настраивать специальные режимы работы BitDefender:

- Игровой режим временно изменяет параметры продукта с целью минимизации потребления ресурсов при игре.
- Режим невидимости предотвращает выполнение запланированных заданий при работе от батареи с целью экономии заряда батареи.

20.1. Игровой режим

Игровой режим изменяет параметры настроек системы защиты для того, чтобы снизить к минимуму воздействие на компьютер во время игры. Если вы находитесь в игровом режиме, применяется следующая процедура:

- Все предупреждения и всплывающие окна BitDefender будут отключены.
- Режим защиты BitDefender в реальном времени будет установлен, как **Разрешен**.
- По умолчанию обновления не выполняются.

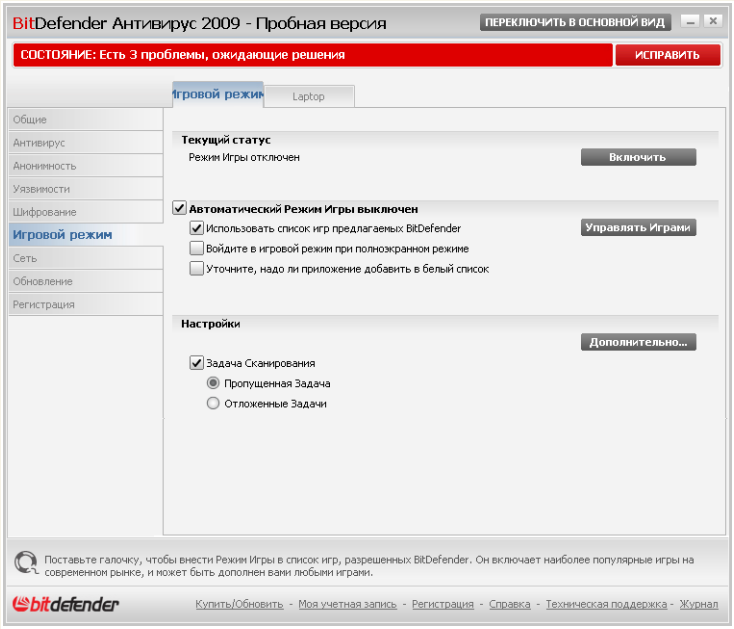
Замечание
Чтобы изменить этот параметр, перейдите к разделу Обновление>Настройки и снимите флажок **Не обновлять, если Режим игры включен**.

- Запланированные задания проверки отключены по умолчанию

По умолчанию BitDefender автоматически входит в Игровой режим при запуске игры, находящейся в списке известных игр BitDefender, или когда приложение разворачивается на полный экран. Вы можете войти в Игровой режим вручную с помощью горячей клавиши по умолчанию `Ctrl+Alt+Shift+G`. Настоятельно рекомендуется выходить из Игрового режима по завершении игры (вы можете воспользоваться той же самой горячей клавишей `Ctrl+Alt+Shift+G`).

Замечание
Всякий раз находясь в игровом режиме вы будете видеть букву `G` поверх значка BitDefender.

Для настройки игрового режима перейдите в раздел **Игра/Режим ноутбука>Игровой режим** в окне расширенного вида.



Игровой режим

Вверху раздела отображается состояние Игрового режима. Щелкните **Включить** или **Выйти** для смены текущего состояния.

20.1.1. Настройка автоматического перехода в Игровой режим

Функция автоматического перехода в Игровой режим позволяет программе BitDefender автоматически переходить в Игровой режим при обнаружении игры. Вы можете установить следующие параметры:

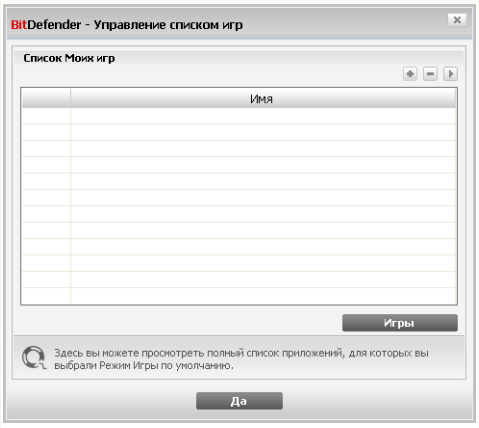
- **Использовать список игр предлагаемых BitDefender** - для автоматического входа в игровой режим при запуске игры из списка известных игр BitDefender. Для просмотра этого списка нажмите **Управлять играми**, а затем **Игры**.

- **Войдите в игровой режим при полноэкранном режиме** - для автоматического перехода в игровой режим при разворачивании приложения на полный экран.
- **Добавить приложение в список игр?** - вывод запроса на добавление нового приложения в список игр при выходе из полноэкранного режима. Если добавить новое приложение в список игр, то при следующем его запуске BitDefender автоматически перейдет в Игровой режим.

Замечание
Если вы не хотите, чтобы BitDefender автоматически переходил в Игровой режим, снимите флажок **Автоматический нежим bгры**.

20.1.2. Управление списком игр

BitDefender автоматически переходит в Игровой режим при запуске приложения из списка игр. Для просмотра и управления списком игр нажмите **Управлять играми**. Появится новое окно.



Список игр

Новые приложения автоматически добавляются в список при следующих условиях:

- Вы запускаете игру из списка игр, известных программе BitDefender. Для просмотра этого списка нажмите **Игры**.

- Выйдя из полноэкранного режима, вы добавляете приложение в список игр из появившегося окна.

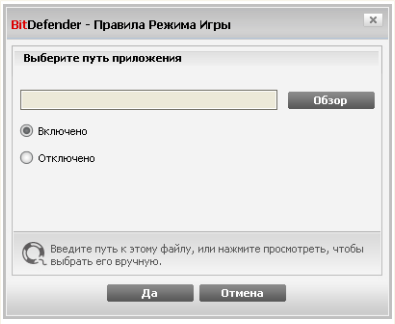
Если вы хотите отключить Автоматический режим игры для отдельного приложения из списка, снимите соответствующий флажок. Следует отключить Автоматический игровой режим для обычных приложений, которые переходят в полноэкранный режим, таких как, например, веб-браузеры и проигрыватели видео.

Для управления списка игр вы можете воспользоваться кнопками, находящимся вверху таблицы:

- **Добавить** - добавление нового приложения в список игр.
- **Удалить** - удаление приложения из списка игр.
- **Редактировать** - редактирование существующего приложения в списке игр.

Добавление и редактирование игр в списке

При добавлении и редактировании игр в списке появляется следующее окно:



Добавить игру

Нажмите **Обзор**, чтобы выбрать приложение, или введите полный путь к приложению в поле ввода.

Если вы не хотите автоматически переходить в игровой режим при запуске выбранного приложения, нажмите **Выключить**.

Нажмите **OK**, чтобы добавить добавить новую запись в список игр.

20.1.3. Настройка параметров игрового режима

Для настройки поведения при запланированных заданиях воспользуйтесь следующими параметрами:

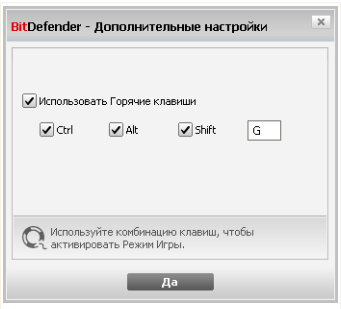
- **Задача сканирования** - для предотвращения выполнения запланированных заданий в игровом режиме. Вы можете выбрать один из следующих параметров:

Настройка	Описание
Пропущенная задача	Никогда не запускать запланированное задание.
Отложенные задачи	Выполнять запланированное задание сразу после выхода из игрового режима.

20.1.4. Изменение Горячих клавиш Режима Игры

Вы можете войти в Игровой режим вручную с помощью горячей клавиши по умолчанию `Ctrl+Alt+Shift+G`. Чтобы изменить Горячие клавиши, необходимо выполнить следующие шаги:

1. Нажмите **Дополнительно...**. Появится новое окно.



Дополнительно...

2. Под параметром **Использовать горячие клавиши** выберите горячую клавишу по умолчанию:

- Выберите клавиши, которые Вы хотите изменить, используя следующие: клавиша Control (`Ctrl`), клавиша Shift (`Shift`) или клавиша Alternate (`Alt`).
- В поле редактирования укажите букву с клавишей, которую Вы хотите использовать.

Например, если Вы хотите использовать клавиши `Ctrl+Alt+D`, Вы должны указать только `Ctrl` и `Alt` и набрать `D`.

3. Щелкните мышкой на **Применить** чтобы сохранить сделанные изменения.

Замечание
Сняв флажок **Использовать горячие клавиши** вы отключите использование данной горячей клавиши.

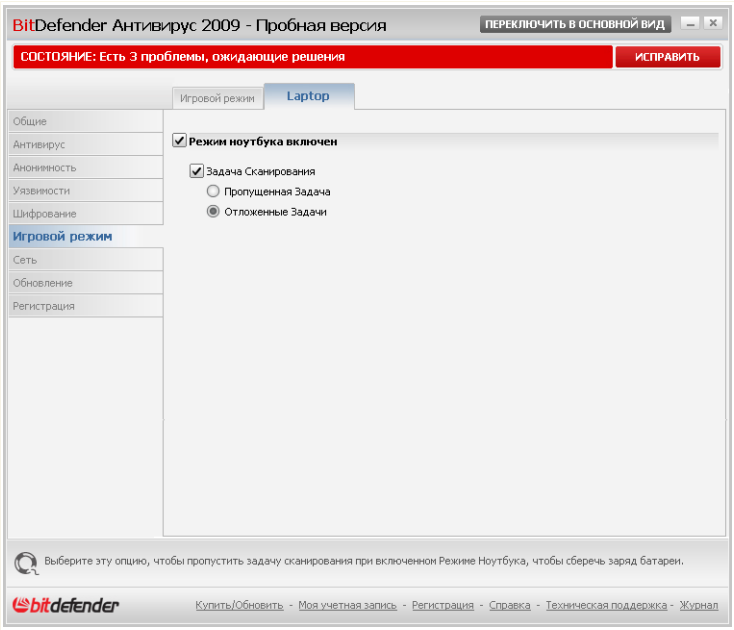
20.2. Laptop

Режим ноутбука специально предназначен для пользователей портативных компьютеров. Его цель - минимизировать влияние работы BitDefender на энергопотребление, когда эти устройства работают от батареи.

В режиме ноутбука запланированные задания не выполняются по умолчанию.

BitDefender замечает, когда ваш ноутбук переключается на питание от батареи, и автоматически переходит в Режим ноутбука. Таким же образом, BitDefender автоматически выходит из Режима ноутбука, когда он обнаруживает, что ноутбук уже не работает от батареи.

Для настройки Режима ноутбука перейдите в раздел **Игра/Режим ноутбука>Игровой режим** в окне расширенного вида.



Laptop

Здесь вы будете видеть, включен Режим ноутбука или нет. Если режим ноутбука включен, BitDefender применит новые параметры, когда ноутбук перейдет на питание от батареи.

20.2.1. Настройка параметров Режима ноутбука

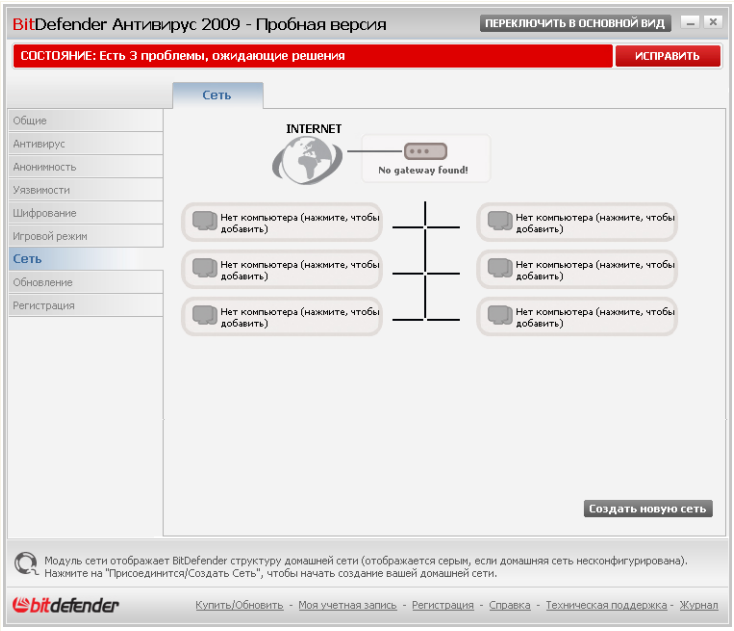
Для настройки поведения при запланированных заданиях воспользуйтесь следующими параметрами:

- **Задача сканирования** - для предотвращения выполнения запланированных заданий в Режиме ноутбука. Вы можете выбрать один из следующих параметров:

Настройка	*Описание*
Пропущенная задача	Никогда не запускать запланированное задание.
Отложенные задачи	Выполнять запланированное задание сразу после выхода из Режима ноутбука.

21. Сеть

Модуль Сеть позволяет управлять обновлениями BitDefender, установленными на ваших домашних компьютерах, с одного компьютера.



Карта сети

Для управления продуктами BitDefender, установленными на ваших домашних компьютерах, необходимо выполнить следующую процедуру:

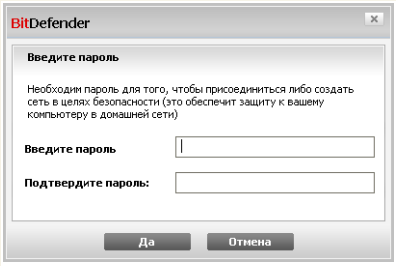
1. Войдите в домашнюю сеть BitDefender на своем компьютере. Вход в сеть состоит из настройки административного пароля для управления домашней сетью.
2. Войдите в сеть с каждого компьютера, которым вы хотите управлять (установите пароль).

3. Вернитесь к своему компьютеру и добавьте те компьютеры, которыми вы хотите управлять.

21.1. Подключение к сети BitDefender

Чтобы подключиться к домашней сети BitDefender, выполните следующую процедуру:

1. Нажмите **Создать новую сеть**. Появится окно настройки пароля для управления домашней сетью.



Настройка пароля

2. Введите одинаковый пароль в каждом из полей ввода
3. В конце щелкните мышкой на кнопке **OK**.

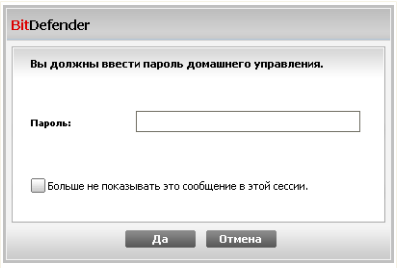
На карте сети будет отображаться имя компьютера.

21.2. Добавление компьютеров в сеть BitDefender.

Перед добавлением компьютера в домашнюю сеть BitDefender необходимо настроить пароль управления домашней сетью BitDefender на соответствующем компьютере.

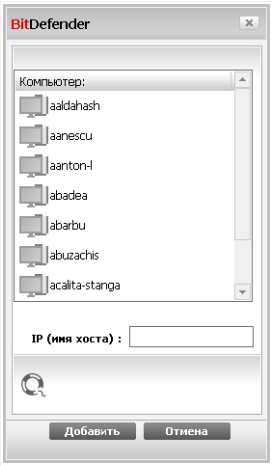
Чтобы добавить компьютер в домашнюю сеть BitDefender, выполните следующую процедуру:

1. Нажмите **Управление сетью**. Появится окно ввода пароля для управления локальной сетью.



Введите пароль

2. Введите пароль для управления домашней сетью и нажмите **OK**. Появится новое окно.



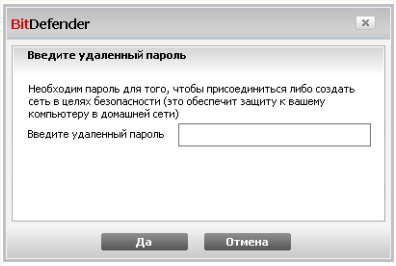
Добавить компьютер

Вы увидите список компьютеров, находящихся в сети. Значки имеют следующие значения:

- Указывает на находящийся в сети компьютер, на котором не установлены продукты BitDefender.

- Указывает на находящийся в сети компьютер, на котором установлен BitDefender.
- Указывает на автономный компьютер, на котором установлен BitDefender.

3. Сделайте одно из следующего:
   - Выберите из списка имя добавляемого компьютера.
   - Введите IP-адрес или имя добавляемого компьютера в соответствующем поле.
4. Нажмите **Добавить**. Появится окно ввода пароля управления домашней сетью для соответствующего компьютера.



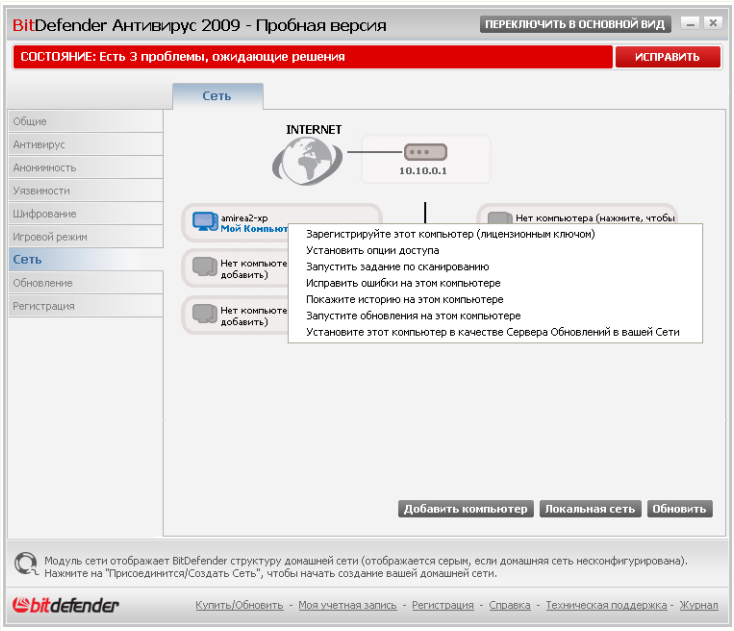
Авторизация

5. Введите пароль управления домашней сетью на соответствующем компьютере.
6. В конце щелкните мышкой на кнопке **OK**. Если вы ввели правильный пароль, имя выбранного компьютера появится на карте сети.

Замечание
На сетевую карту можно добавить до пяти компьютеров.

21.3. Управление сетью BitDefender

Как только домашняя сеть BitDefender будет создана, вы сможете управлять всеми продуктами BitDefender с одного компьютера.



Карта сети

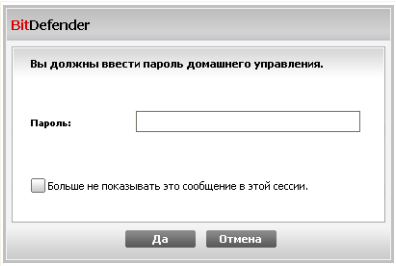
Если передвинуть курсор мыши поверх компьютера на карте сети, вы увидите краткие сведения о нем (имя, IP-адрес, число проблем, влияющих на безопасность системы, состояние регистрации BitDefender).

Если щелкнуть правой кнопкой мыши на имени компьютера на карте сети, вы увидите список управляющих заданий, которые можно выполнять с удаленным компьютером.

- **Зарегистрируйте этот компьютер**
- **Установить опции доступа**
- **Запустить задание по сканированию**
- **Исправить ошибки на этом компьютере**
- **Покажите историю на этом компьютере**
- **Запустите обновления на этом компьютере**

- **Профили**
- **Запустите панель настроек на этом компьютере**
- **Установите этот компьютер в качестве сервера обновлений в вашей сети**

Перед запуском задания на определенном компьютере появится окно ввода пароля управления домашней сетью.



Введите пароль

Введите пароль для управления домашней сетью и нажмите **OK**.

Замечание

Если вы планируете выполнить несколько заданий, можно выбрать параметр **Больше не показывать это сообщение в этой сессии**. Выбрав этот параметр, вы не будете видеть окно ввода пароля во время текущего сеанса.

22. Обновление

Каждый день появляются и обнаруживаются все новые вредоносные программы. Вот почему так важно постоянно обновлять сигнатурные базы Bitdefender новыми вредоносными программами.

Если Вы подключаетесь к Интернет через широкополосное соединения или DSL, BitDefender возьмет на себя решение вопросов безопасности: проверит появление новых образов вирусов сразу же при подключении, и затем будет проверять каждый **час**.

Если будет обнаружено обновление, вы, возможно, увидите сообщение с просьбой подтвердить обновление, или же обновление начнется автоматически, в зависимости от настроек автоматического обновления.

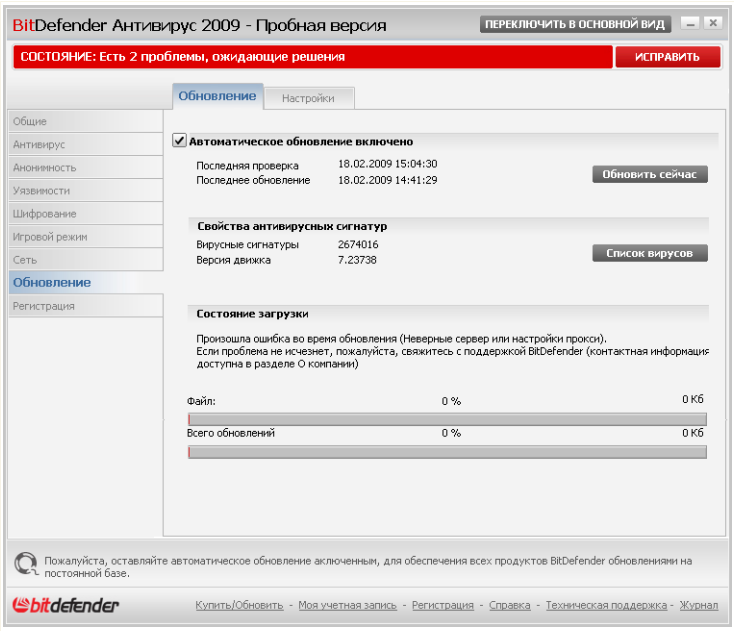
Процесс обновления происходит "на лету", т.е. файлы заменяются по мере обновления. Таким образом, процесс обновления не влияет на работоспособность продукта, и, в то же время, исключается возможность возникновения уязвимости Вашего компьютера.

Имеются следующие варианты обновления:

- **Обновления защиты от вирусов** - как только появляется новая угроза, необходимо обновить файл с образами вирусов, чтобы гарантировать постоянную современную защиту от них. Этот тип обновления также известен как **Обновление образов вирусов**.
- **Обновление защиты от программ-шпионов** - образы новых программ-шпионов будут добавлены в базу данных. Этот тип обновления также известен как **Обновление Антишпиона**.
- **Обновление программного продукта** - когда выпускается новая версия программы, в новую версию добавляются новые функции и методы проверки, что только улучшает работу программы. Этот тип обновления также известен как **Обновление программы**.

22.1. Автоматическое обновление

Для просмотра сведений, связанных с обновлением, и выполнения автоматических обновлений перейдите в раздел **Обновление>Обновление** в окне расширенного вида.



Автоматическое обновление

Здесь Вы можете просмотреть, когда была последняя проверка на наличие обновлений и информацию о последнем обновлении (было ли оно успешным, возникли ли какие-либо ошибки в процессе). Здесь также отображается информация о текущей версии программы и количество образов вредоносных программ.

Если Вы откроете это окно в течение обновления, то увидете статус загрузки.

Важно
Чтобы обезопасить компьютер от атак через Интернет, **Автоматическое обновление** должно быть включено.

Вы можете получить сигнатуры вредоносного ПО для вашего продукта BitDefender, нажав кнопку **Список вирусов**. При этом будет создан и открыт в браузере файл HTML, который будет содержать все доступные сигнатуры. После этого вы сможете выполнять поиск сигнатуры определенного вредоносного ПО

по базе или нажатием кнопки **BitDefender Virus List** переходить к онлайн-версии базы сигнатур BitDefender.

22.1.1. Требование к обновлению

Кроме того, вы можете выполнять автоматическое обновление в любое время, нажав кнопку **Обновить сейчас**. Этот тип обновления также именуется **Обновление по требованию**.

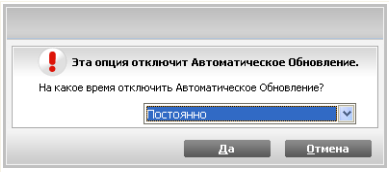
Модуль **Обновления** подключится к серверу обновления BitDefender и проверит наличие обновлений. Если программа обнаруживает новое обновление, то, в зависимости от настроек, установленных в разделе Опции обновления вручную. Вам будет предложено подтвердить загрузку обновления или обновление будет производиться автоматически.

Важно
Вам может потребоваться перезагрузить компьютер, чтобы завершить обновление. Мы рекомендуем сделать это как можно раньше.

Замечание
Если Вы подключаетесь к Интернету по телефонной линии, лучше всего регулярно обновлять BitDefender по требованию пользователя.

22.1.2. Отключение автоматического обновления

Если Вы выберите эту опцию, то появится окно с предупреждением:



Отключить автоматическое обновление

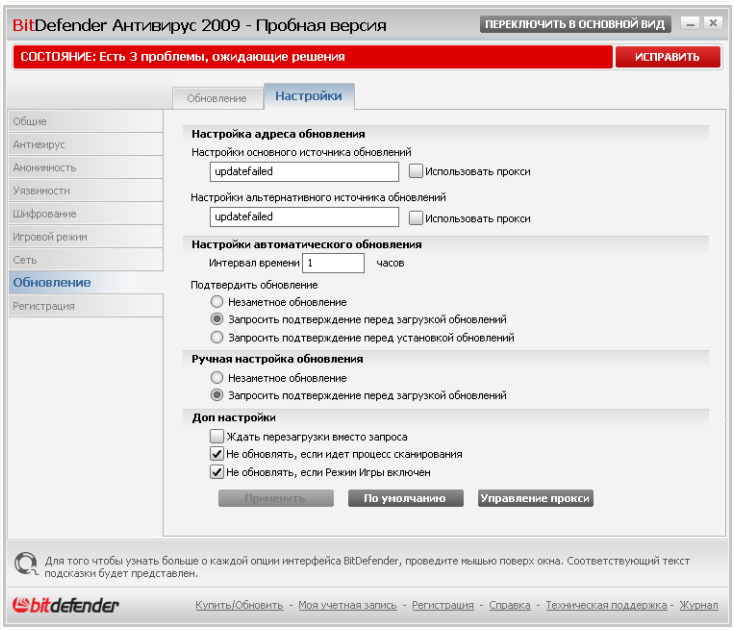
Вы должны подтвердить свое намерение, выбрав промежуток времени, на который Вы хотите отключить автоматическое обновление. Вы можете отключить на 5, 15 или 30 минут, на час, навсегда или до следующей перезагрузки системы.

Внимание
Этот аспект является критическим с точки зрения безопасности. Рекомендуем Вам отключать автоматическое обновление на как можно меньший промежуток времени. Если автоматическое обновление отключено, Вы не защищены от самых последних угроз.

22.2. Параметры обновления

Обновление может быть выполнено через локальную сеть, через Интернет напрямую или через прокси-сервер. По умолчанию BitDefender проверяет на наличие обновлений ежечасно через Интернет и устанавливает необходимые обновления без уведомления.

Чтобы установить настройки обновлений и настроить прокси, перейдите в раздел **Обновления>Настройки** окне расширенного вида.



Параметры обновления

В окне Настройки обновления Вы можете увидеть четыре типа настроек: (**Настройки местоположения обновления**, **Настройки автоматического обновления**, **Обновления вручную** и **Настройки интерфейса**).

22.2.1. Настройки местоположения обновления

Чтобы настроить местоположение обновлений, используйте опции для категории **Настройки местоположения обновления**.

Замечание
Изменять данные настройки нужно лишь в том случае, если Вы подключены к локальной сети, в которой хранятся обновления BitDefender, или если Вы осуществляете соединение с Интернет через прокси сервер.

Для более надежных и быстрых обновлений, Вы можете настроить 2 места обновления:**Основное местоположение обновлений** и **Альтернативное местоположение обновлений**. По умолчанию, это: `http://upgrade.bitdefender.com`.

Чтобы изменить адрес источника, откуда берутся обновления, введите URL адрес локального зеркала в поле **URL**, соответствующем месту, которое Вы хотите изменить.

Замечание
Рекомендуем установить местное зеркало в качестве первоначального источника обновления и оставить альтернативный источник без изменений, в качестве запасного на случай, если местное зеркало станет недоступным.

Если компания использует прокси сервер для выхода в Интернет, поставьте отметку в поле **использовать прокси**, а затем нажмите **Настроить прокси**. Больше информации Вы найдете здесь «*Управление прокси*» (p. 197)

22.2.2. Конфигурирование автоматического обновления

Чтобы настроить автоматическое обновление, ииспользуйте опции в разделе **Настройки автомотического обновления**.

Вы можете указать количество часов между запросами на наличие обновлений в поле **Интервал времени**. По умолчанию интервал составляет 1 час.

Чтобы указать, как необходимо проводить процесс автоматического обновления, выберите одну из следующих опций:

- **Обновление без предупреждения** - BitDefender автоматически скачивает и устанавливает обновления.
- **Запрос перед загрузкой обновлений** - каждый раз, когда появится новое обновление, BitDefender будет запрашивать ваше подтверждение перед загрузкой.
- **Запрос перед установкой обновлений** - каждый раз, когда будет загружено обновление, Вам будет запрос об их загрузке.

22.2.3. Конфигурация обновлений вручную

Чтобы указать, как необходимо проводить процесс ручного обновления (обновления по запросу пользователя), выберите одну из следующих опций в категории **Настройки ручного обновления**:

- **Обновление без предупреждения** - обновление вручную будет выполняться автоматически в фоновом режиме.
- **Запрос перед загрузкой обновлений** - каждый раз, когда появится новое обновление, BitDefender будет запрашивать ваше подтверждение перед загрузкой.

22.2.4. Дополнительные настройки

Чтобы избежать того, когда процесс обновления BitDefender мешает Вашей работе на компьютере, настройте опции в категории **Дополнительные настройки**:

- **Ожидать перезагрузки без запроса** - Если для завершения установки обновления необходимо выполнитьб перезапуск компьютера, программное обеспечение будет при выборе данной опции продложать работу со старыми файлами до перезагрузки системы. При этом не будет появляться сообщение с запросом пользователя о необходимости перезапуска системы, в связи с чем процесс обновления BitDefender не будет мешать работе пользователя.
- **Не выполнять обновление пока идет проверка** - BitDefender не будет выполнять обновление пока идет проверка. Таким образом, BitDefender процесс обновления не будет мешать задачам сканирования.

Замечание
Если BitDefender обновлен, во время сканирования, этот процесс будет прерван.

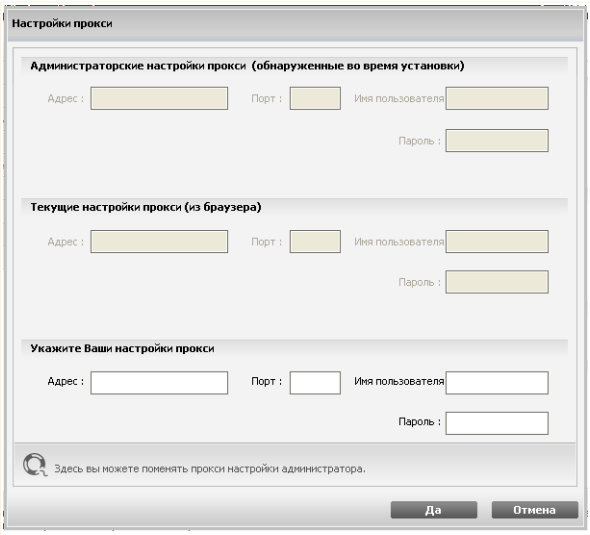
- **Не выполнять обновление, когда включен режим игры** - BitDefender не обновиться, пока включен режим игры. Таким образом, Вы можете минимизировать влияние продукта на работу системы в течение игр.

22.2.5. Управление прокси

Если Ваша компания использует прокси сервер для подсоединения к Интернет, Вам необходимо указать настройки прокси сервера, чтобы BitDefender имел возможность обновляться. В противном случае, он будет использовать настройки прокси администратора, устанавливавшего программу или настройки прокси текущего браузера, если таковые имеются.

Замечание
Настройки прокси сервера могут изменяться только пользователями с правами администратора компьютера или же пользователями, знающими пароль к настройкам программы.

Чтобы настроить прокси сервер, нажмите **Настроить прокси**. Откроется окно **Прокси менеджера**.



Управление прокси

Есть три параметра настройки для прокси:

- **Настройки прокси администратора (определены в процессе установки)** - настройки прокси сервера, определенные в процессе установки программы в учетной записи администратора, эти настройки могут быть изменены, только если Вы работаете под данной учетной записью. Если прокси сервер требует указания имени пользователя и пароля, укажите их в соответствующих полях.
- **Текущие настройки прокси (из браузера, используемого по умолчанию)** - настройки прокси сервера для текущего пользователя, полученные из браузера, используемого по умолчанию. Если прокси сервер требует указания имени пользователя и пароля, укажите их в соответствующих полях.

  Замечание
  Поддерживаемыми браузерами являются Internet Explorer, Mozilla Firefox и Opera. Если по умолчанию Вы используете другой браузер, BitDefender не сможет получить настройки прокси сервера для текущего пользователя.

- **Ваши собственные настройки прокси** - вы можете изменять настройки прокси, если зашли как администратор.

  Следующие настройки должны быть определены:
  - **Адрес** - введите IP-адрес к прокси серверу.
  - **Порт** - введите порт использующий BitDefender для подсоединения к прокси серверу.
  - **Пользователь** - введите имя пользователя, опознаваемого прокси-сервером.
  - **Пароль** - введите пароль пользователя, указанного ранее.

При попытке соединения к Интернет, будет поочередно пробоваться каждый набор настроек прокси, пока BitDefender не удастся установить соединение.

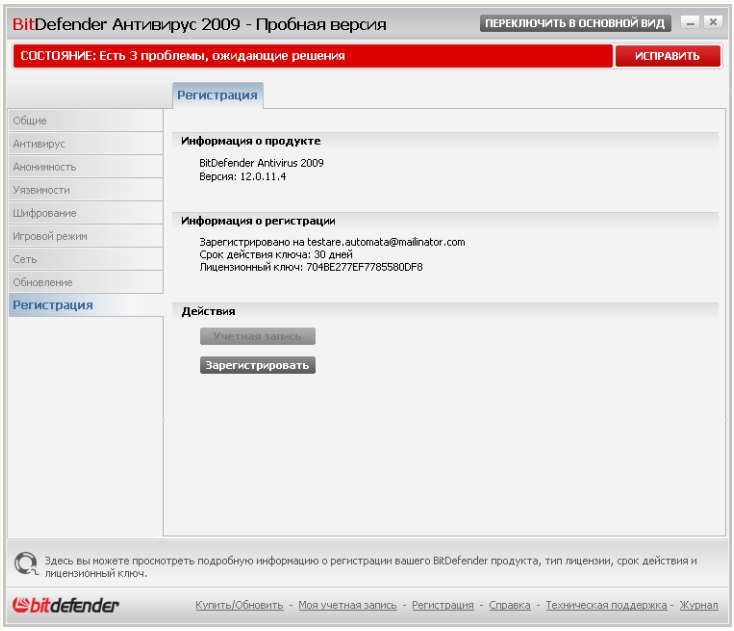
Прежде всего, для соединения к Интернет будет использованы Ваши собственные настройки прокси. Если это не поможет, следующими будут использованы настройки сервера, обнаруженные при установке продукта. В конце концов, если ни один из вариантов не сработает, будут использованы настройки прокси сервера, который использует браузер по умолчанию для соединения с Интернет.

Нажмите **OK**, чтобы сохранить изменения и закройте окно.

Щелкните мышкой на кнопке **Применить** чтобы сохранить изменения или щелкните мышкой на кнопке **По умолчанию** чтобы загрузить настройки по умолчанию.

23. Регистрация

Чтобы найти полные сведения по вашему продукту BitDefender и состояние регистрации, перейдите в раздел **Регистрация** в окне расширенного вида.



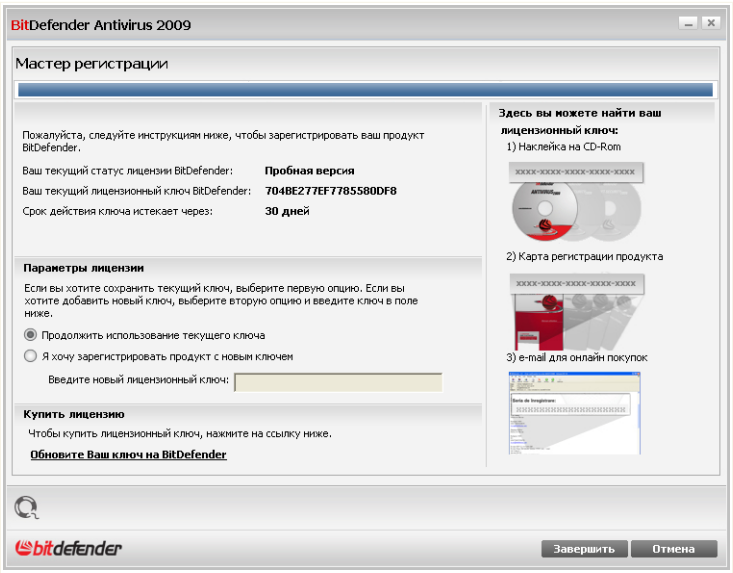
Регистрация

В данном разделе отображаются:

- **Информация о продукте**: продукт BitDefender и его версия.
- **Информация о регистрации**: адрес электронной почты, который используется для входа в учетную запись BitDefender (если она настроена), текущий лицензионный ключ и количество дней до истечения срока действия лицензии.

23.1. Регистрация BitDefender Antivirus 2009

Нажмите **Зарегистрировать** для открытия окна регистрации продукта.



Регистрация

Вы можете просмотреть статус регистрации BitDefender, действующий лицензионный ключ, и количество дней, которые остались до окончания срока действия лицензии.

Для регистрации BitDefender Antivirus 2009:

1. Выберите **Я хочу зарегистрировать продукт с новым ключем**.
2. Введите лицензионный ключ в поле для редактирования.

Замечание

Вы можете найти ваш лицензионный ключ:

- на обложке CD.
- на регистрационной карточке продукта.
- в электронном письме о покупке.

Если у Вас нет лицензионного ключа BitDefender, нажмите соответствующую ссылку для перехода в онлайн-магазин BitDefender и приобретите лицензионный ключ.

Щелкните мышкой на кнопке **Завершить**.

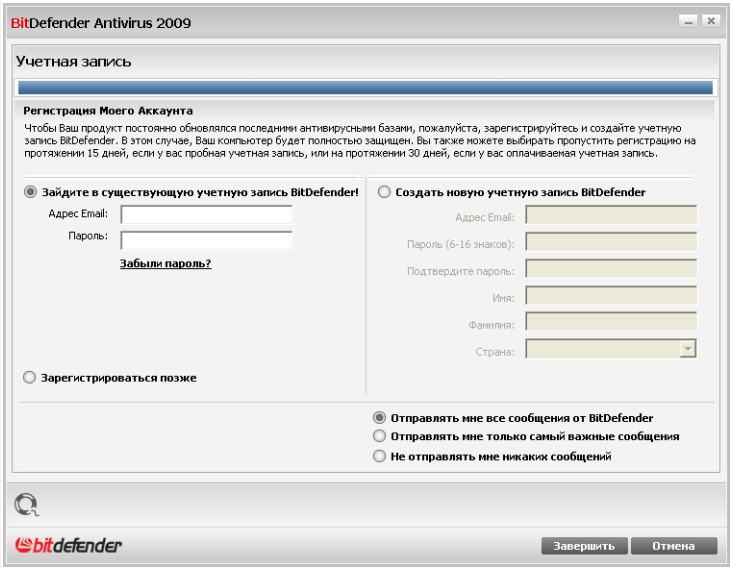
23.2. Создание учетной записи BitDefender

Создание учетной записи BitDefender является обязательной частью процесса регистрации. Учетная запись BitDefender даст вам доступ к обновлениям, специальным предложениям и поощрениям. Если вы утеряете BitDefender лицензионный ключ, вы сможете зайти в свою учетную запись по ссылке http://myaccount.bitdefender.com, чтобы восстановить его.

Важно

Вам необходимо создать учетную запись в течении 15 дней со дня установки BitDefender (если вы его зарегистрировали, в течении 30 дней). В противном случае, BitDefender не будет обновляться.

Если вы еще не создали учетную запись BitDefender, нажмите **Учетная запись**, чтобы открыть окно регистрации учетной записи.



Создание учетной записи

Если Вы не хотите создавать учетную запись BitDefender, выберите **Пропустить регистрацию** и нажмите **Завершить**. В другом случае, действуйте исходя из вашей ситуации:

- «У меня нет учетной записи BitDefender» (p. 202)
- «У меня уже есть учетная запись BitDefender» (p. 203)

У меня нет учетной записи BitDefender

Для создания учетной записи BitDefender выберите **Создать новую учетную запись BitDefender** и введите требуемую информацию. Предоставленные Вами данные конфиденциальны.

- **Адрес электронной почты** - введите адрес своей электронной почты.
- **Пароль** - введите пароль Вашей учетной записи BitDefender. Длина пароля должна быть не менее шести символов.
- **Повторите пароль** - снова введите набранный ранее пароль.

- **Имя** - введите Ваше имя.
- **Фамилия** - введите Вашу фамилию.
- **Страна** - выберите страну, в которой находитесь.

Замечание
Используйте указанные адрес электронной почты и пароль для доступа к своей учетной записи на http://myaccount.bitdefender.com.

Чтобы успешно создать учетную запись, Вы должны прежде всего активировать свой электронный адрес. Проверьте электронную почту и следуйте инструкциям в письме, которое будет выслано Вам службой регистрации BitDefender.

Дополнительно, BitDefender может информировать вас о специальных предложениях и поощрениях, через адрес электронной почты, указанной в вашей учетной записи. Выберите одну из доступных функций:

- **Отправлять мне все сообщения от BitDefender**
- **Отправлять мне наиболее важные сообщения**
- **Не отправлять мне сообщения**

Щелкните мышкой на кнопке **Завершить**.

У меня уже есть учетная запись BitDefender

BitDefender автоматически определит, если вы решистрировали учетную запись BitDefender ранее на этом компьютере. В этом случае, предоставьте пароль вашей учетной записи.

Если у Вас уже есть активная учетная запись, но BitDefender не определяет ее, выберите **Использовать существующую учетную запись BitDefender** и укажите e-mail и пароль Вашей учетной записи.

Если Вы забыли пароль, нажмите **Забыли пароль?** и следуйте инструкциям.

Дополнительно, BitDefender может информировать вас о специальных предложениях и поощрениях, через адрес электронной почты, указанной в вашей учетной записи. Выберите одну из доступных функций:

- **Отправлять мне все сообщения от BitDefender**
- **Отправлять мне наиболее важные сообщения**
- **Не отправлять мне сообщения**

Щелкните мышкой на кнопке **Завершить**.

Получение справки

24. Техническая поддержка

Являясь ценимым поставщиком, BitDefender стремится предоставлять своим клиентам беспрецедентный уровень быстрой и полной поддержки. Центр Поддержки (с которым можно связаться по следующему адресу) постоянно проинформирован о самых последних угрозах. Именно здесь вы можете получить быстрый ответ на все Ваши вопросы.

Стремление сохранить время и деньги клиентов, предоставляя им самые последние продукты по самым оптимальным ценам, всегда было приоритетом BitDefender.

Вы можете в любое время обратиться за поддержкой по адресу support@bitdef.ru. Чтобы получить оперативный ответ пожалуйста, укажите в Вашем письме как можно больше подробностей о Вашем BitDefender, системе, опишите проблему, с которой Вы столкнулись как можно подробнее.

24.1. База знаний BitDefender

Так называемая «База знаний» BitDefender - это хранилище информации о продуктах BitDefender с открытым доступом для клиентов в режиме реального времени (”on-line”). В ней накапливаются, в виде отчетов, имеющих легкодоступный формат, результаты всей деятельности по оказанию технической поддержки и устранению ошибок в программе группами технической поддержки и разработчиками компании, а также имеются статьи более общего характера об обезвреживании вирусов, управлению внедрением решений BitDefender и подробными пояснениями различных проблем, равно как и множество других материалов.

База знаний BitDefender открыта для всех и снабжена поисковыми средствами, позволяющими легко найти ответ на интересующую Вас проблему. Этот ценный массив информации является еще одним источником технических знаний и экспертных решений для клиентов BitDefender. Все обоснованные информационные запросы и отзывы о найденных программных ошибках, поступившие от клиентов BitDefender своевременно находят свое место в базе знаний BitDefender: в виде отчетов об устранении программных ошибок, обновлениях для максимального устранения недоделок и информационных материалов/статей, дополняющих файлы справки программного продукта.

База знаний BitDefender открыта круглосуточно по адресу http://kb.bitdefender.com.

24.2. Просьба помощи

24.2.1. Перейти к самообслуживанию через веб

Возник вопрос? Наши специалисты готовы круглосуточно оказать Вам помощь по телефону, электронной почте или при помощи чата.

Перейдите по нижеследующим ссылкам:

Английский

http://www.bitdefender.com/site/KnowledgeBase/

Немецкий

http://www.bitdefender.com/de/KnowledgeBase/

Французский

http://www.bitdefender.com/fr/KnowledgeBase/

Румынский

http://www.bitdefender.com/ro/KnowledgeBase/

Испанский

http://www.bitdefender.com/es/KnowledgeBase/

24.2.2. Откройте тикет техподдержки

Если Вы хотите создать уведомление для службы поддержки или получить помощь по электронной почте, просто перейдите по одной из этих ссылок:

Английский: http://www.bitdefender.com/site/Main/contact/1/
Немецкий: http://www.bitdefender.de/site/Main/contact/1/
Французский: http://www.bitdefender.fr/site/Main/contact/1/
Румынский: http://www.bitdefender.ro/site/Main/contact/1/
Испанский: http://www.bitdefender.es/site/Main/contact/1/

24.3. Контактная информация:

Эффективная связь является залогом успешного бизнеса. За последние 10 лет компании BITDEFENDER удалось завоевать непререкаемый авторитет среди своих клинтов и партнеров за счет предвосхищения их ожиданий и постоянного улучшения связи с ними. Мы будем рады ответить на все ваши вопросы и решить ваши проблемы – не колеблясь, обращайтесь к нам за помошью.

24.3.1. Адреса веб-сайтов

Отдел продаж: sales@bitdefender.com
Техническая поддержка: support@bitdefender.com
Документация: documentation@bitdefender.com
Партнерские программы: partners@bitdefender.com
Маркетинг: marketing@bitdefender.com
Отдел по связям со СМИ: pr@bitdefender.com
Вакансии: jobs@bitdefender.com
Лаборатория – для вирусов: virus_submission@bitdefender.com
Лаборатория - для спама: spam_submission@bitdefender.com
Жалобы: abuse@bitdefender.com
Веб-сайт: http://www.bitdefender.com/ru
ftp архив продукта: ftp://ftp.bitdefender.com/pub
Локальные дистрибьюторы: http://www.bitdefender.com/partner_list
База знаний BitDefender: http://kb.bitdefender.com

24.3.2. Офисы филиалов

Офисный персонал компании, ответственный за продукт BitDefende, ответит на ваши запросы коммерческого и общего характера, относящейся к сфере их деятельности и географической привязке. Ниже приведены адреса и контактная информация этих офисов.

Россия и страны СНГ (кроме Украины)

BITDEFENDER
West Gate Park, Building H2, 24 Preciziei Street, sector 6
Bucharest, Romania
Э-мейл: sales@bitdefender.com
Телефон: +40 21 2063470
Веб-сайт: http://www.bitdefender.com/ru

BitDefender Rescue CD

25. Обзор

BitDefender Antivirus 2009 поставляется вместе с загрузочным компакт-диском (Реаниматор BitDefender), который может проверить и вылечить все существующие жесткие диски до загрузки операционной системы.

Вы должны использовать компакт-диск BitDefender Реаниматор в любое время, когда операционная система не работает должным образом из-за заражения вирусом. Это обычно случается, когда не используется антивирусная программа.

Обновление базы данных вирусных образов осуществляется автоматически без вмешательства пользователя каждый раз, когда Вы запускаете компакт-диск BitDefender Реаниматор.

BitDefender Rescue CD (диск-реаниматор BitDefender) - это измененный дистрибутив Knoppix, с интегрированным решением BitDefender для Linux на носителе GNU/Linux Knoppix Live CD, который представляет собой готовое к использованию антивирусное решение, которое можно использовать для проверки и "дезинфекции" жестких дисков (включая и разделы Windows NTFS). В то же время, диск-реаниматор BitDefender можно использовать для восстановления ценных данных в случаях, когда не возможно загрузить ОС Windows.

Замечание
Вы можете скачать BitDefender Rescue CD отсюда: http://download.bitdefender.com/rescue_cd/

25.1. Системные требования

Перед загрузкой BitDefender Rescue CD, необходимо сначала проверить соответствие вашей системы следующим требованиям.

Тип процессора
x86-совместимый процессор с минимальной тактовой частотой 166 МГц, что, однако, не гарантирует устойчивой работы программы. Предпочтительно выбирать процессор поколения i686, с тактовой частотой 800МГц.

Память
Минимум 512 Мб оперативной памяти (рекомендуется 1 Гб)

CD-ROM
BitDefender Rescue CD запускается с компакт-диска, поэтому необходимыми является наличие дисковода CD-ROM и настройка BIOS на загрузку системы с компакт-диска.

Подключение к сети Интернет
Хотя программа BitDefender Rescue CD выполняется без подключения к сети Интернет, для процедур обновления необходим доступ к активной ссылке HTTP, хотя бы через прокси-сервер. Поэтому для установки последнего обновления, подключение к сети Интернет является ОБЯЗАТЕЛЬНЫМ.

Графическая разрешающая способность
Стандартная SVGA-совместимая карта.

25.2. Включенное программное обеспечение

В компакт-диск BitDefender Реаниматор входят следующие пакеты программ.

Xedit
Это текстовый редактор.

Vim
Это мощный текстовый редактор, поддерживающий подсветку синтаксиса, графический интерфейс пользователя (GUI) и многое другое. Для более подробной информации смотрите Домашнюю страницу Vim .

Xcalc
Это калькулятор.

RoxFiler
RoxFiler - быстрый и мощный пакет для работы с графическими файлами.

Больше информации Вы найдете домашняя страница RoxFiler.

MidnightCommander
GNU Midnight Commander (mc) - файловый менеджер.

Более подробная информация домашняя страница MC.

Pstree
Pstree - показывает запущенные процессы.

Top
Top - показывает Linux задачи.

Xkill

Xkill - убивает клиента его X ресурсами.

Partition Image

Partition Image помогает сохранить разделы системных форматов EXT2, Reiserfs, NTFS, HPFS, FAT16 и FAT32 в файлы образов. Данная программа очень полезна при осуществлении резервного копирования данных.

Более подробная информация домашняя страница Partimage.

GtkRecover

GtkRecover - GTK версия консольной программы восстановления. Она помогает восстановить Ваши файлы.

Более подробная информация домашняя страница GtkRecover.

ChkRootKit

ChkRootKit - инструмент, который помогает Вам просматривать ваш компьютер на наличие руткитов.

Более подробная информация домашняя страница ChkRootKit.

Nessus Network Scanner

Nessus - сканер безопасности для Linux, Solaris, FreeBSD и Mac OS X.

Более подробная информация домашняя страница Nessus.

Iptraf

Iptraf – консольная утилита для сбора сетевой статистики.

Более подробная информациядомашняя страница Iptraf.

Iftop

Iftop - утилита позволяющая мониторить трафик в реальном времени.

Более подробная информация домашняя страница Iftop.

MTR

MTR - диагностический инструмент сети.

Более подробная информация домашняя страница MTR.

PPPStatus

PPPStatus отображает статистическую информацию о входящих и исходящих потоках трафика по TCP/IP.

Более подробная информация домашняя страница PPPStatus.

Wavemon

Wavemon - программа мониторинга для беспроводных сетевых устройств.

Более подробная информация домашняя страница Wavemon.

USBView

USBView показывает информацию об устройствах, связанных с USB.

Более подробная информация домашняя страница USBView.

Pppconfig

Pppconfig помогает автоматически настраивать dial-up ppp-соединение.

DSL/PPPoe

DSL/PPPoe настраивает PPPoE (ADSL) соединение.

I810rotate

I810rotate - переключатель видео сигналов на i810 аппаратном оборудование используя i810switch(1).

Более подробная информация домашняя страница I810rotate.

Mutt

Mutt - мощный почтовый клиент на текстовой основе MIME.

Более подробная информация домашняя страница Mutt.

Mozilla Firefox

Mozilla Firefox - один из лучших веб браузеров.

Более подробная информация домашняя страница Mozilla Firefox.

Elinks

Elinks - текстовый веб браузер.

Более подробная информация домашняя страница Elinks.

26. Реаниматор BitDefender

Данный раздел содержит информацию о том, как запускать и останавливать работу диска-реаниматора BitDefender, проверять Ваш компьютер на наличие вредоносных программ, а также сохранять данные с неработающей системы Windows на сменные носители. Однако, при помощи программ, имеющихся на данном диске, Вы можете выполнять гораздо больше действий, чем описано в данном руководстве.

26.1. Запуск BitDefender Rescue CD

Чтобы запустить компакт-диск с данным программным продуктом, установите настройки BIOS вашего компьютера на загрузку с дисковода компакт-дисков, поместите компакт-диск с продуктом в дисковод и перезагрузите компьютер. Убедитесь в том, что ваш компьютер настроен на загрузку с компакт-диска.

Подождите, пока на экране монитора появится информация и выполняйте соответствующие инструкции для запуска BitDefender Rescue CD.

Замечание
Перед использованием Реаниматора выберите язык, который вы хотите использовать, из списка доступных языков.

Экран загрузки

При загрузке обновление базы данных вирусных сигнатур осуществляется автоматически без вмешательства пользователя.

После окончания загрузки на экране появится новый интерфейс - рабочий стол. Теперь Можно начинать работу с BitDefender Rescue CD.

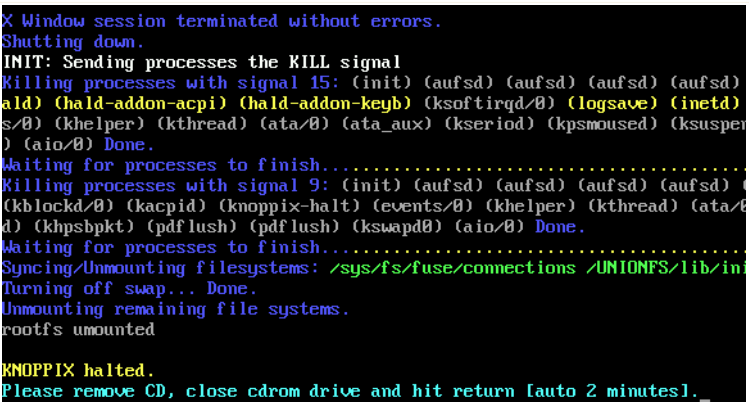
Рабочий стол

26.2. Остановка BitDefender Rescue CD

Вы можете выполнить безопасное отключение компьютера, для чего следует выбрать команду **Exit** в контекстном меню BitDefender Rescue CD (открывающееся после щелчка правой кнопкой мыши), либо использовать команду **halt** в терминале.

Выберите команду "EXIT"

Когда BitDefender Rescue благополучно закроет все программы, на экране появится новое изображение, соответствующее показанному на следующем рисунке. Теперь можно извлечь CD, чтобы последующую загрузку компьютера выполнить уже с жесткого диска. Теперь ваш компьютер можно выключить или перезагрузить.



Ожидайте появления этого сообщения на экране, сигнализирующего о завершении работы программы

26.3. Как выполнить антивирусную проверку?

Когда процесс загрузки завершен, откроется мастер, позволяющий произвести полную проверку Вашего компьютера. Все, что необходимо сделать для этого, - нажать кнопку **Старт**.

Замечание
Если разрешения вашего экрана недостаточно для корректного отображения, Вам будет предложено запустить проверку в текстовом режиме.

Чтобы завершить процесс проверки выполните последовательность из трех шагов.

1. Вы можете просматривать состояние проверки и статистику (скорость сканирования, время до окончания, количество проверенных / зараженных / подозрительных / скрытых объектов и проч.).

   Замечание
   В зависимости от сложности задач проверки, процесс сканирования может занять некоторое время.

2. Вы можете просмотреть количество проблем, влияющих на безопасность Вашей системы.

   Проблемы отображаются группами. Щелчок мышки на значке "+" разворачивает список, а на значке "-" – закрывает его.

   Для каждой группы проблем Вы можете выбрать общее действие, либо есть возможность выбрать отдельное действие для каждой проблемы.
3. Здесь Вы можете просмотреть краткий обзор.

Если Вы хотите просканировать только определенную директорию, тогда необходимо:

Просмотрите ваши папки, щелкните правой кнопкой мышки на названии файла или каталога и выберите команду **Послать**. Затем выберите **BitDefender Scanner**.

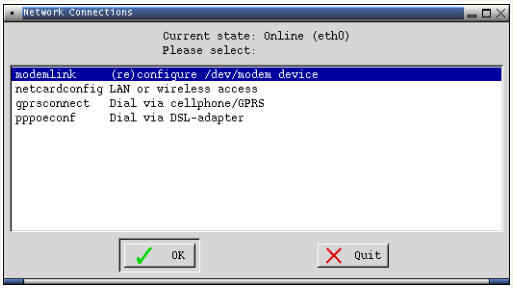
Вместо этого, Вы можете запустить командную сроку с терминала. **BitDefender Antivirus Scanner** начнет проверку выбранного Вами файла или папки с заданным по умолчанию местоположением.

```
# bdscan /path/to/scan/
```

26.4. Как настроить соединение с интернетом?

Если Вы находитесь в сети DHCP (использующей протокол динамического выбора хост-машины), и в вашем компьютере установлена сетевая карта стандарта Ethernet, то в этом случае связь с Internet должна обнаруживаться и устанавливаться автоматически. Для настройки сети вручную, Вам следует выполнить следующие инструкции.

1. Дважды щелкните на ярлыке Сетевые подключения на рабочем столе. Появится следующее окно.



Сетевые подключения

2. Выберите тип подключения, который вы используете, и нажмите OK.

Подключение	Описание
modemlink	Выберите этот тип подключения, если для доступа в Интернет вы используете модем и телефонную линию.
netcardconfig	Выберите этот тип подключения, если для доступа в Интернет вы используете локальную сеть (Local Area Network). Она также пригодна для беспроводных соединений.
gprsconnect	Выберите этот тип подключения, если вы выходите в Интернет через мобильную сеть с помощью GPRS (General Packet Radio Service), со своего компьютера.

Подключение	Описание
	Конечно же, вы можете также воспользоваться GPRS-модемом вместо мобильного телефона.
pppoeconf	Выберите этот тип подключения, если для доступа в Интернет вы используете модем DSL (Цифровая абонентская линия).

3. Следуйте указаниям на экране. Если вы не уверены в своем ответе, посоветуйтесь с системным или сетевым администратором.

Важно
Имейте в виду, что только вы активируете модем, выбрав описанные выше параметры. Для настройки сетевого подключения выполните следующие шаги.

1. Щелкните правой кнопкой мыши по рабочей области. Появится контекстное меню BitDefender реаниматор CD.
2. Выберите опцию **Терминал (как root)**.
3. Попробуйте ввести следующие команды:

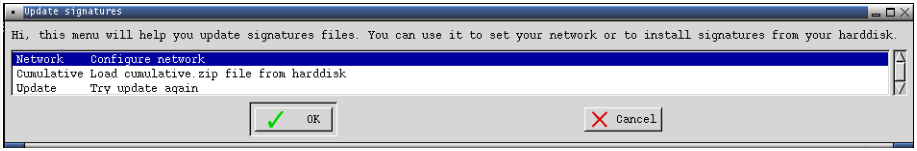
```
# pppconfig
```

4. Следуйте указаниям на экране. Если вы не уверены в своем ответе, посоветуйтесь с системным или сетевым администратором.

26.5. Как обновлять BitDefender?

Во время загрузки системы обновление вирусных сигнатур происходит автоматически. Однако если вы пропустите этот шаг, здесь описывается процедура обновления BitDefender.

1. Дважды щелкните на ярлыке Обновить сигнатуры на рабочем столе. Появится следующее окно.



Обновление сигнатур

2. Сделайте одно из следующего:
   - Выберите **Кумулятивная** для установки сигнатур, уже сохраненных на жестком диске, найдя и загрузив файл `cumulative.zip` на вашем компьютере.
   - Выберите **Обновить**, чтобы сразу подключиться к интернету и загрузить последние сигнатуры вирусов.
3. В конце щелкните мышкой на кнопке **OK**.

26.5.1. Как я делаю обновление BitDefender через прокси?

Если есть прокси-сервер между вашим компьютером и Интернет, то необходимо сделать некоторые настройки конфигурации, чтобы обновить вирусные сигнатуры.

Чтобы выполнить обновление BitDefender через прокси-сервер, необходимо выполнить следующие шаги:

1. Щелкните правой кнопкой мыши по рабочей области. Появится контекстное меню BitDefender реаниматор CD.
2. Выберите опцию **Терминал (как root)**.
3. Тип команды: **cd /ramdisk/BitDefender-scanner/etc**.
4. Тип команды: **mcedit bdscan.conf**, чтобы редактировать этот файл используя GNU Midnight Commander (mc).
5. Раскомментируйте следующую строку: `#HttpProxy =` (просто удалите символ `#`) и задайте домен, имя пользователя, пароль и порт порт прокси-сервера. Например, эта строка может выглядеть так:

   ```
   HttpProxy = myuser:mypassword@proxy.company.com:8080
   ```
6. Нажмите **F2**, чтобы сохранить правильный файл, подтвердите сохранение и тогда нажмите **F10**, чтобы закрыть это.
7. Тип команды: **bdscan update**.

26.6. Как мне сохранить мои данные?

Предположим, Вы не можете запустить Ваш компьютер с ОС Windows из-за неизвестных проблем. В тоже время, Вам очень нужно получить доступ к данным на Вашем компьютере. Именно здесь пригодится диск-реаниматор BitDefender.

Выполните следующие шаги для того, чтобы скопировать данные с Вашего компьютера на сменный носитель, например, на модуль памяти USB:

1. Поместите диск-реаниматор BitDefender в привод, а модуль памяти подсоедините к USB порту, и перегрузите компьютер.

   Замечание

   Если подключить запоминающее устройство позже, нужно будет смонтировать его с помощью следующей процедуры:

   a. Дважды щелкните на ярлыке Terminal Emulator (Эмулятор консоли) на рабочем столе.

   b. Введите следующую команду:

   ```
   # mount  /media/sdb1
   ```

   Примите во внимание, что в зависимости от конфигурации вашего компьютера вместо `sdb1` вам понадобится ввести `sda1`.

2. Ждите, пока BitDefender Rescue CD не загрузится. Появится следующее окно.

Экран рабочего стола

3. Нажмите два раза на раздел, где расположены данные, которые Вы хотите сохранить (например `[sda3]`).

Замечание

При работе с реаниматором BitDefender Вам придется столкнуться с обозначениями дисков, принятыми в Linux, Таким образом, `[sda1]` будет скорее всего соответствовать разделу `(C:)` диска в ОС Windows, `[sda3]` - `(F:)`, а `[sdb1]` - модулю памяти.

Важно

Если работа компьютера была неправильно завершена, возможно, причина в том, что некоторые разделы не были смонтированы автоматически. Чтобы смонтировать раздел, выполните следующую процедуру.

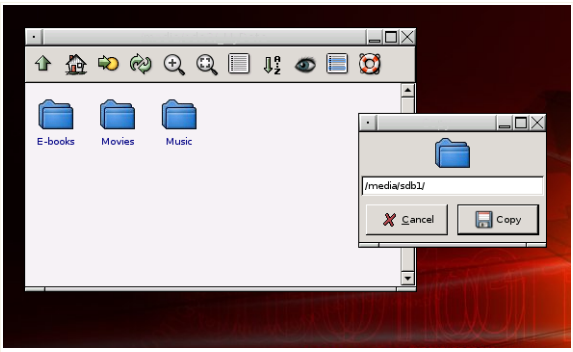
a. Дважды щелкните на ярлыке Terminal Emulator (Эмулятор консоли) на рабочем столе.

b. Введите следующую команду:

```
# mount  /media/partition_name
```

4. Просмотрите ваши папки и откройте желательную директорию. Например, `MyData` который содержит поддиректории `Видео`, `Музыка` и `Книги`.

5. Нажмите правой кнопкой мыши на выбранной папки и выберите **Копировать**. Появится следующее окно.



Сохранение данных

6. Введите `/media/sdb1/` в соответствующее текстовое поле и нажмите **Копировать**.

   Примите во внимание, что в зависимости от конфигурации вашего компьютера вместо `sdb1` вам понадобится ввести `sda1`.

Глоссарий

ActiveX

ActiveX – это компоненты, которые могут использоваться другими программами и операционными системами вызывающими их. Технология ActiveX используется вместе с программой Microsoft Internet Explorer для создания интерактивных страниц, которые выглядят и работают скорее как компьютерные программы, нежели как простые страницы. С помощью ActiveX пользователь может задавать и отвечать на вопросы, «нажимать» на кнопки и другим способом взаимодействовать с веб-страницей. Элементы ActiveX часто пишутся на языке Visual Basic.

Главный недостаток технологии ActiveX – полное отсутствие какой-либо защиты. Поэтому эксперты по компьютерной безопасности не одобряют их использование в сети Интернет.

Программы сбора рекламной информации о пользователе (Adware)

Программы Adware часто устанавливаются «в качестве нагрузки» к основным приложениям, которые предоставляются бесплатно, при условии что пользователь соглашается установить программу-adware. Поскольку adware-приложения обычно устанавливаются только после того, как пользователь принимает условия, указанные в соответствующем лицензионном соглашении, где указывается функция приложения, то их функционирование не является каким-либо нарушением прав пользователя.

Однако, всплывающие рекламные объявления могут причинять неудобства пользователю, а в некоторых случаях и ухудшать операционные характеристики системы. Кроме того, пользовательская информация, собираемой некоторыми из этих приложений, может показаться недопустимой для разглашения теми пользователями, которые недостаточно полно изучили условия лицензионного соглашения.

Архивировать

Диск или директория, содержащие запасные файлы.

Файл, содержащий один или несколько файлов в сжатом формате.

Брешь в системе (Backdoor)

Брешь в защите системы, специально оставленная разработчиками. Это не всегда делается со злым умыслом: например, в некоторых операционных системах предусмотрены учетные записи, которые могут использоваться персоналом службы технической поддержки или программистами разработчика.

Загрузочный сектор

Сектор в начале каждого диска, в котором хранится информация об архитектуре диска: размер сектора, размер папки и т.д. Загрузочный сектор загрузочного диска содержит еще и программу, загружающую операционную систему.

Загрузочный вирус

Вирус, заражающий загрузочный сектор жесткого или гибкого диска. Попытка загрузиться с зараженной дискеты приводит к тому, что вирус активируется в памяти. Всякий раз, когда Вы загружаете систему с этого места, вирус будет активироваться в памяти.

Браузер

Сокращение от Web browser – приложение, которое ищет и показывает на экране Веб-страницы. Два самых популярных браузера - это Netscape Navigator и Microsoft Internet Explorer. Это графические браузеры, то есть, они показывают и рисунки, и текст. Кроме того, большинство современных браузеров могут отображать мультимедийную информацию, включая звук и видеоизображение, хотя они и требуют установки дополнительных программ и оборудования (plug-ins).

Командная строка

В командной строке пользователь вводит в специальном поле нужные команды на специальном командном языке.

Файлы истории обращений (Cookie)

В сфере Интернет технологий под названием «файлы истории обращений (cookies)» понимаются маленькие файлы, содержащие информацию о компьютере, которую можно проанализировать и использовать для того, чтобы выяснить Ваши интересы и предпочтения. Поэтому технология создания таких файлов процветает, и сейчас Вы можете получить рекламу товаров, основанную на Ваших интересах. Это палка о двух концах. С одной стороны, Вы видите именно то, что Вам может пригодиться. Но с другой – за Вами постоянно следят, и знают, на какой странице Вы находитесь, и на какой кнопке щелкаете мышкой. Понятно, почему сейчас так широко обсуждается конфиденциальность данных пользователей, и многие чувствуют себя ущемленными в своих правах, будучи уверенными, что их «считывают» как кассир в магазине считывает штрих-код на этикетке. Порой эта точка зрения кажется крайностью, но иногда она полностью отражает действительность.

Дисковод

Это оборудование, считывающее данные с диска и записывающее их на диск.

Накопитель на жестких дисках (hard disk drive) считывает данные и записывает их на жесткие диски.

Накопитель на гибких магнитных дисках (floppy drive) работает с гибкими дисками.

Дисковод может быть встроенным, то есть находиться в корпусе компьютера, или же внешним, то есть находиться в отдельном корпусе и подключаться к компьютеру.

Загрузка

Копирование данных (обычно целых файлов) из основного местоположения (источника) на периферийное (внешнее) устройство. Обычно этот термин используется по отношению к копированию файла из источника в сети на свой компьютер. Загрузкой также называют копирование файла с сетевого файлового сервера на компьютер в сети.

Электронная почта

Электронная почта. Отправка сообщений на другие компьютеры через локальную или глобальную сеть.

События

Действие или событие, обнаруженное программой. Событиями могут быть действия пользователя, например щелчок кнопки мыши, или нажатие на клавишу, или системные события, например, переполнение памяти.

Ложная тревога

Событие «ложная тревога» появляется, когда программа считает зараженным файл, который таковым на самом деле не является.

Расширение (имени) файла

Часть названия файла после точки, обозначающая тип данных, хранящихся в нем.

Многие операционные системы, такие как Unix, VMS, и MSDOS, используют расширения имени файла. Обычно они состоят из трех букв, потому что старые ОС не поддерживают более длинные расширения. Например, "c" текст программы на языке C (C source code), "ps" – язык PostScript, а "txt" – любой текстовый файл.

Эвристический (метод)

Способ обнаружения новых вирусов, основанный на правилах. Этот способ проверки не связан напрямую с определенными образами вирусов. Преимущество эвристической проверки состоит в том, что новый вирус не может обмануть фильтр. Однако он может принять подозрительный код в обычных программах за вирус и выдать так называемую «ложную тревогу».

IP

Сокращение от Internet Protocol – Интернет Протокол – маршрутизируемый протокол семейства TCP/IP, отвечающий за адресацию, маршрутизацию, фрагментацию и повторную компоновку IP пакетов.

Прикладная минипрограмма Java апплет

Программа, написанная на языке Java, работающая только на страницах в сети. Чтобы использовать апплет на странице, Вы должны указать его название и размер (длину и ширину в пикселях), которые он может использовать. При открывании страницы браузер загружает эту программу с сервера и запускает ее на компьютере пользователя (который в этом случае называется «клиент»). Апплеты отличаются от приложений, которыми они управляются, более строгим протоколом обеспечения безопасности.

Например, даже если минипрограмма запускается на компьютере-клиенте, она не может считывать или записывать данные на этот компьютер. Кроме того, апплеты могут считывать и записывать данные только с того домена, которым они обслуживаются.

Макро-вирус

Компьютерный вирус, который кодируется как встроенный в документ макрос. Многие приложения, такие как Microsoft Word и Excel поддерживают сложные макроязыки.

Эти приложения позволяют встраивать макросы в документ, и эти макросы выполняются всякий раз, когда ВЫ открываете документ.

Почтовая программа (клиент)

Приложение, которое позволяет Вам отправлять и получать электронную почту.

Память

Внутренние устройства хранения информации. Термин «Память» относится к запоминающему устройству, например, микросхеме. Термин «Накопитель» относится к таким устройствам, как диски. В каждом компьютере изначально есть физическая память, называемая оперативная (основная) память или RAM.

Не- эвристический (метод)

Этот метод проверки основан на использовании определенных образов вирусов (сигнатур). Основное преимущество этого метода состоит в том, что его нельзя обмануть похожей на вирус программой, а следовательно, не возникает ложная тревога.

Запакованные программы

Файл в сжатом формате. Многие операционные системы и приложения содержать команды, позволяющие запаковать файл, и он будет занимать меньше места. Например, у вас есть текстовый файл, состоящий из десяти последовательных символов пробела. В нормальном состоянии этот файл занимает десять байт памяти.

Однако программа, запаковывающая файлы (архиватор), может заменить эти пробелы специальным символом пробелов и количеством замененных пробелов. В этом случае десять пробелов займут всего лишь два байта. И это только один из многих методов архивации файлов.

Путь

Точное местоположение файла на компьютере. Это местоположение обычно описывается средствами иерархической файловой системы сверху вниз, указывая диск, каталог и подкаталоги, сам файл и расширение файла, приблизительно так : c:jobscompany/resume.txt. Эта подробная информация и есть полный путь.

Маршрут между двумя объектами, например, канал связи между двумя компьютерами.

Фишинг (Phishing)

Действие, сводящееся к отправке пользователю электронного письма якобы от имени реально существующей организации с целью получения обманным путем конфиденциальной информации о пользователе и ее последующего присвоения в корыстных целях. В получаемом пользователем сообщении по электронной почте его с помощью ссылки приглашают посетить якобы официальный веб-сайт реально существующей организации, где его просят подтвердить или обновить личные данные (например, пароли и номера банковского счета, кредитной карточки, карточки социального обеспечения). Однако на самом деле такого рода веб-сайт является поддельным и создается для кражи конфиденциальной информации пользователей.

Полиморфный вирус

Вирус, изменяющий свою форму всякий раз, заражая новый файл. Поскольку у таких вирусов нет бинарной закономерности, их трудно обнаружить.

Порт

Компьютерный интерфейс, с помощью которого подключается внешнее устройство. У персональных компьютеров есть несколько видов портов. Внутри корпуса есть несколько портов для подключения дисководов, монитора и клавиатуры. Снаружи есть порты для подключения модемов, принтеров, мыши и других внешних устройств.

В сетях на базе протоколов TCP/IP и UDP порт – это конечная точка логического подключения. Номер порта указывает на его тип. Например, порт номер 80 используется для HTTP трафика.

Файл отчета

Файл, содержащий список совершенных действий. BitDefender включает в отчеты путь к проверенным файлам, папки, количество проверенных архивов и файлов, а также сколько подозрительных и зараженных файлов обнаружено.

Руткит

Руткиты - это набор программных инструментов, позволяющих получить доступ к системе на уровне администратора. Термин впервые использовался для операционных систем UNIX и относился к инструментам перекомпиляции, которые позволяли получить права администратора, при этом их присутствие оставалось скрытым для системных администраторов.

Основной целью руткитов является скрывать процессы, файлы, логины и журналы. Они также могут перехватывать данные с терминалов, сетевых соединений или перифирийных устройств, если их встроить в соотвествующее программное обеспечение.

По своей природе руткиты не вредоносны. Например, системы и даже некоторые приложения скывают важные файлы при помощи руткитов. Однако, чаще всего их все-таки используют как вредоносные порграммы, либо чтобы скрыть присутствие в системе. При совмещении с вредоносными программами, руткиты представляют значительную угрозу для целостности и безопасности системы. Они могут отслеживать трафик, создавать бреши в системе, изменять файлы и журналы, избегая выявления.

Сценарий (скрипт)

Еще один термин, обозначающий макрос или командный файл. Сценарий – это набор команд, выполняющихся без участия пользователя.

Спам

Рекламное сообщение или новостная рассылка по электронной почте. Обычно под спамом понимают незаконную рассылку электронных писем, часто коммерческого содержания.

Программа-шпион (Spyware)

Любого рода программа-шпион, которая тайно и без ведома пользователя (чаще всего в рекламных целях) собирает информацию о пользователе во время его с соединения с Интернетом,. Шпионские программы обычно маскируют как скрытые компоненты бесплатных или условно бесплатных (shareware) приложений, которые можно скачать с Интернета, хотя следует отметить, что большинство бесплатных или условно бесплатных приложений не содержит программ-шпионов. Программа-шпион после своей установки отслеживает адреса в Интернете, к которым обращается пользователь и тайно пересылает эту информацию третьим лицам. Кроме того, программы-шпионы могут собирать информацию об адресах электронной почты, паролях и даже номерах кредитных карточек пользователей.

Программы-шпионы аналогичны вирусам-троянам в том смысле, что и те и другие устанавливаются самими пользователями во время установки других программ. Жертвами программ-шпионом обычно становятся при скачивании известных программных продуктов из файлообменных сетей.

Действия программ-шпионы являются не только нарушением этики и конфиденциальности, но и кражей ресурсов компьютерной памяти пользователей и ресурсов канала соединения с Интернетом за счет передачи информации программой-шпионом своему источнику при подключении пользователя к Интернету. За счет потребления памяти и системных ресурсов программами-шпионами, работа последних в фоновом режиме может приводить к неустойчивой работы системы и ее сбоям.

Элементы запуска

Все файлы, помещенные в эту папку будут открываться при запуске компьютера. Это могут быть, например, экран запуска, звуковой файл, проигрываемый при первом запуске компьютера, ежедневник с напоминаниями или другие приложения. Обычно в эту папку помещается не сам файл, а его ярлык.

Системный трей (область уведомлений на панели задач)

Область уведомлений впервые появилась в операционной системе Windows 95. Она расположена на панели задач Windows, обычно в нижней части экрана, рядом с часами и содержит маленькие иконки, обеспечивающие быстрый доступ к таким функциям, как факс, принтер, модем, регулировка

громкости и т.д. Чтобы просмотреть подробную информацию о программе и ее настройки, просто дважды щелкните мышкой на иконке.

TCP/IP

Протокол управления передачей/Интернет протокол (Transmission Control Protocol/Internet Protocol) – набор сетевых протоколов, широко используемых в Интернете. Они объединяют в одну большую сеть множество взаимосвязанных сетей, состоящих из компьютеров с различной архитектурой и с различными операционными системами. Протокол TCP/IP включает в себя стандарты связи между компьютерами и общепринятые правила объединения сетей и трафик маршрутизации.

Вирус класса Троян

Вредоносная программа, маскирующаяся под безвредное приложение. В отличие от обычных вирусов, вирус класса Троян не копирует себя, однако, он может быть не менее разрушительным. Вирусы одного из наиболее опасных типов обещают избавить Ваш компьютер от всех вирусов, но на самом деле загружают вирусы на компьютер.

Этот термин взят из поэмы Гомера «Илиада», где в одной из глав описывается, как греки подарили своим врагам, жителям Трои, огромного деревянного коня, якобы в знак мира. Но после того, как троянцы втащили статую в город, греческие солдаты выскочили из полости в теле коня и открыли городские врата, после чего их соратники ворвались в Трою и захватили город.

Обновление

Новая версия программного обеспечения или оборудования, разработанная на замену устаревшей версии этого продукта. Кроме того, многие обновления часто определяют, установлена ли на компьютере старая версия данного программного продукта. Если нет – обновление невозможно.

У программы BitDefender есть свой собственный модуль обновления, который позволяет вручную проверять наличие или автоматически обновлять программный продукт.

Вирус

Программа или часть кода, которая загружается на Ваш компьютер без Вашего ведома и запускается против Вашего желания. Многие вирусы также могут копировать себя. Все компьютерные вирусы созданы людьми. Очень легко написать простой вирус, который копирует себя снова и снова. Даже такой простой вирус очень опасен, так как он быстро использует всю свободную память и система зависает. Более опасные вирусы могут передавать себя по сети и прорываться через системы защиты.

Образ вируса

Двоичный образец вируса, используемый программой защиты от вирусов для обнаружения и уничтожения этого вируса.

Вирус класса червь

Программа, которая распространяется по сети, копируя и отправляя себя дальше. Она не может присоединяться к другим программам.