bitdefender

antivirus 2010

Руководство пользователя

BitDefender Antivirus 2010
Руководство пользователя

Опубликовано 2009.09.22

Правовые положения

Содержание

Лицензионное соглашение 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 условия настоящего Соглашения, Вы соглашаетесь зарегистрировать ваше программное обеспечение, используя "Мой аккаунт", в качестве условия Вашего использования Программного Обеспечения (получение обновлений) и вашего права на сервисное обслуживание. Такой контроль помогает гарантировать, что программное обеспечение работает только на законных основаниях на должным образом лицензированных компьютеров и что должным образом пролицензированные конечные пользователи получат сервисное обслуживание. Для регистрации необходим действительный серийный номер и адрес электронной почты, для уведомлениях о обновлении версий ПО и других уведомлений.

Данные условия относятся ко всем продуктам и услугам BitDefender для домашних пользователей, установленных на вашем компьютере, 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, включающих программное обеспечение и услуги, а также возможные сопутствующие физические носители, 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. BITDEFENDER предоставляет вам и только вам следующую неисключительную, ограниченную, без права передачи, непереносимую, несублицензируемую и предусматривающую оплату роялти лицензию на использование BitDefender.

ПРИКЛАДНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ. Вы можете установить и использовать BitDefender на необходимом количестве компьютеров, 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 сетевых функций. Каждый пользователь может установить данный программный продукт на персональном компьютере, а также может сделать дополнительную резервную копию на другом устройстве. Количество разрешенных пользователей - это количество лицензированных пользователей.

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 действия 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 все предыдущие 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 передавать право на лицензию, сдавать в аренду или продавать BitDefender. Вы не имеете права воспроизводить

недокументируемый продукт, вносить изменения, раскодировать, создавать свои продукты на основе BitDefender, 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, ЯВНЫХ ИЛИ ПОДРАЗУМЕВАЕМЫХ, В ОТНОШЕНИИ ПРОГРАММНОГО ПРОДУКТА, УСОВЕРШЕНСТВОВАНИЙ, ПОДДЕРЖКИ И ПРОЧИХ УСЛУГ (МАТЕРИАЛЬНЫХ ИЛИ НЕМАТЕРИАЛЬНЫХ). 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, COOKIES, 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 косвенный ущерб, возникший в результате использования, работы или установки BitDefender, даже если компания BITDEFENDER предупреждала о такой возможности.

В НЕКОТОРЫХ СТРАНАХ НЕ ДОПУСКАЕТСЯ 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 согласия на использование, оценку или тестирование BitDefender.

ВАЖНАЯ ИНФОРМАЦИЯ 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.

СОГЛАСИЕ НА ЭЛЕКТРОННЫЕ СООБЩЕНИЯ. BitDefender может потребоваться отправить вам уведомления и другие сообщения о программном обеспечении и услугах поддержки или использовать предоставленную вами информацию для связи. ("Коммуникационные сообщения"). BitDefender будет отправлять Коммуникационные сообщения через уведомления внутри продукта или по электронной почте на первичные адреса электронной почты зарегистрированных пользователей, или размещать на своих сайтах. Принимая условия настоящего Соглашения, вы даете согласие на получение всех Коммуникационных сообщений через эти электронные средства, и подтверждаете и демонстрируете, что вы можете получить доступ к Коммуникационным сообщениям на сайтах.

ТЕХНОЛОГИЯ СБОРА ДАННЫХ -BitDefender сообщает вам, что в определенных программах или продуктах, он может использовать технологию сбора данных для сбора технической информации (в том числе подозрительных файлов), для усовершенствования своих продуктов, предоставления соответствующих услуг, с целью их адаптации и предотвращения нелицензированного или незаконного использования продукта или убытков в результате вредоносной продукции. Вы подтверждаете, что BitDefender может использовать такую информацию как часть услуг, предоставляемых вместе с продуктом, и для предотвращения и прекращения деятельности вредоносных программ, запущенных на вашем компьютере.

Вы осознаете и подтверждаете что BitDefender может предоставлять обновления или дополнения к программе или продукту, которые автоматически загружаются на ваш компьютер.

Принимая условия настоящего Соглашения, Вы соглашаетесь загрузить исполняемые файлы для сканирования на серверах BitDefender. Аналогичным образом, для заключения договора и использования программы, вы можете предоставить BitDefender определенные личные данные. BitDefender сообщает вам, что он будет использовать ваши персональные данные в соответствии с действующим законодательством и установленной политикой конфиденциальности.

СБОР ДАННЫХ. Доступ пользователей к сайту и приобретение продуктов и услуг и использование инструментов или информации через веб-сайт,

подразумевает обработку персональных данных. Соблюдение законодательства, регулирующего обработку персональных данных и информационных услуг, электронную торговлю, имеет важнейшее значение для BitDefender. Иногда, для доступа к продуктам, содержимому услуг или инструментам, вам необходимо предоставить некоторые личные данные. BitDefender гарантирует, что эти данные будут обрабатываться конфиденциально и в соответствии с законодательством, регулирующим защиту персональных данных и информационных услуг и электронной торговли.

BitDefender действует в соответствии с принятым законодательством о защите данных, и принял административные и технические меры, необходимые для обеспечения безопасности персональных данных, которые он собирает.

Вы заявляете, что все данные, которые вы предоставляете, будут достоверными и точными и обязуетесь информировать BitDefender о любых изменениях в указанных данных. Вы имеете право возражать против обработки своих данных, которая не является необходимой для выполнения этого соглашения и его использования для иных целей, кроме поддержания договорных отношений.

В случае, если вы предоставите подробную информацию о третьей стороне, BitDefender не несет ответственность за соблюдение принципов информирования и получения согласия, в следствии этого вы должны гарантировать что заранее проинформировали и получили согласие владельца предоставленных данных, на передачу такой информации.

BitDefender, его филиалы и партнеры будут отправлять маркетинговую информацию по электронной почте или другими электронными средствами только тем пользователям, которые дали свое прямое согласие на получение сообщений, касающихся продуктов BitDefender или новостных услуг.

Политика конфиденциальности BitDefender гарантирует Вам право на доступ, исправление, ликвидацию и обработку данных с помощью уведомлений BitDefender по электронной почте, по адресу: juridic@bitdefender.com.

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.

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 окончания срока действия лицензии.

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 2010** для обеспечения защиты персональных компьютеров. Информация, представленная в этой книге, доступна не только для опытных пользователей, но и для любого пользователя, знакомого с операционной системой Windows.

Эта книга расскажет вам о продукте BitDefender Antivirus 2010, проведет вас через весь процесс установки, покажет вам, как его настроить. Вы узнаете, как пользоватся BitDefender Antivirus 2010, обновлять, тестировать и настраивать. Вы узнаете, как наилучшим образом использовать BitDefender.

Надеемся, что чтение будет увлекательным и полезным для Вас.

1. Обозначения, используемые в данной книге

1.1. Типографские обозначения

Для удобства читателей в этой книге используется несколько различных текстовых стилей. Их значения приведены в следующей таблице.

Виды шрифтов и стилей	Описание
`sample syntax`	Образцы написания напечатаны с моноширинными символами.
http://www.bitdefender.com	Ссылки URL на внешние источники (http или ftp серверы).
sales@bdef.ru	Адреса электронной почты в тексте приводятся в качестве контактной информации.
«Предисловие» (p. xvi)	В кавычках приводятся внутренние ссылки на другие материалы в пределах этого документа.
`filename`	Названия файлов и каталогов приводятся с использованием шрифтов моноширинных.
option	Все варианты продукта напечатаны **жирным** шрифтом.
`sample code listing`	Программные коды указаны моноширинным шрифтом.

1.2. Примечания

Примечания – это текстовая информация, выделенная в основном тексте различными средствами, целью которой является привлечение вашего внимания к дополнительной информации, имеющей отношение к содержанию текущего раздела руководства.

Замечание

Заметка – это краткое замечание. Вы можете пропустить её, но в ней может содержаться ценная информация, например, определенная особенность или ссылка на источник, имеющий отношение к данному материалу.

Важно

Эта информация требует вашего внимания, не рекомендуется пропускать ее. Как правило, она содержит не-критическую, но значимоую информацию.

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 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 и удаление. Следуйте пошаговой инструкции, для установки BitDefender на вашем компьютере. Начиная требований необходимых для успешной установки, вы пройдете через весь процесс установки. В конце, описывается процедура удаления, в случае необходимости удалить BitDefender.

Начало работы. Содержит всю необходимую вам информацию для начала работы с BitDefender. Представлено: интерфейс BitDefender, как решать проблемы, настройка основных параметров и регистрация вашего продукта.

Средний Уровень. Представляет Промежуточный Интерфейс BitDefender.

Режим Опытного Пользователя. Детальная презентация Интерфейса Опытного Пользователя 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.).

Интеграция в Windows и стороннее ПО. Показывает вам, как использовать опции BitDefender в контекстном меню Windows и панели инструментов BitDefender интегрированные в в поддерживаемые сторонние программы.

Как? Содержание процедур для быстрого выполнения наиболее распространенных задач в BitDefender.

Устранение неполадок и получение справки. Где искать и куда обращаться за помощью в случае возникновения неожиданных проблем.

Диск-реаниматор BitDefender. Описание диска-реаниматора BitDefender. Этот материал поможет Вам изучить и использовать возможности этого загрузочного диска.

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

3. Ваши комментарии

Мы будем рады вашим замечаниям по улучшению этой книги. Мы тщательно проверили информацию, изложенную в ней. Пожалуйста, напишите нам об ошибках, найденных Вами в этой книге, а также ваши рекомендации по ее улучшению. Ваши замечания помогут нам обеспечивать Вас максимально достоверной документацией.

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

Важно

Пожалуйста, присылайте все замечания относительно документации на английском языке, чтобы мы могли оперативно их обработать.

Установка и удаление

1. Системные требования

Вы можете устанавливать BitDefender Antivirus 2010 только на компьютерах, работающих под следующими операционными системами:

- Windows XP (32/64 bit) with Service Pack 2 или выше
- Windows Vista (32/64 bit) или Windows Vista with Service Pack 1 или выше
- Windows 7 (32/64 bit)

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. Минимальные системные требования

- 450 MB свободного пространства на жестком диске
- Процессор 800 MHz
- Память RAM:
  - 512 MB для Windows XP
  - 1 GB для Windows Vista и Windows 7
- Internet Explorer 6.0
- .NET Framework 1.1 (также доступен в установочном наборе)

1.2. Рекомендуемые системные требования:

- 600 MB доступно свободного пространства на жестком диске
- Intel CORE Duo (1.66 GHz) или эквивалентный процессор
- Память RAM:
  - 1 GB для Windows XP и Windows 7
  - 1.5 GB для Windows Vista
- Internet Explorer 7 (или выше)
- .NET Framework 1.1 (также доступен в установочном наборе)

1.3. Поддерживаемое ПО

Защита от антифишинга предоставляется только для:

- Internet Explorer 6.0 или выше
- Mozilla Firefox 2.5
- Yahoo Messenger 8.5
- Windows Live Messenger 8

Шифрование мгновенных сообщений (IM) осуществляется только для:

- Yahoo Messenger 8.5
- Windows Live Messenger 8

2. Подготовка к установке

Перед тем как установить BitDefender Antivirus 2010, завершите эту подготовку для обеспечения гладкого хода установки:

- Убедитесь, что компьютер, на котором вы собираетесь установить BitDefender, подходит под минимальные системные требования. Если компьютер не подходит под минимальные системные требования, BitDefender не будет установлен или если установлен, то не будет работать корректно, замедляя работу и вызывая нестабильность системы. За полным списком системных требований, обратитесь к «*Системные требования*» (p. 2).
- Войдите в систему под аккаунтом Администратора.
- Удалите любые другие программы безопасности с компьютера. Одновременный запуск двух программ безопасности может повлиять на их работу и вызвать серьезные проблемы с системой. Windows Defender будет отключен по умолчанию, перед началом установки.

3. Установка BitDefender

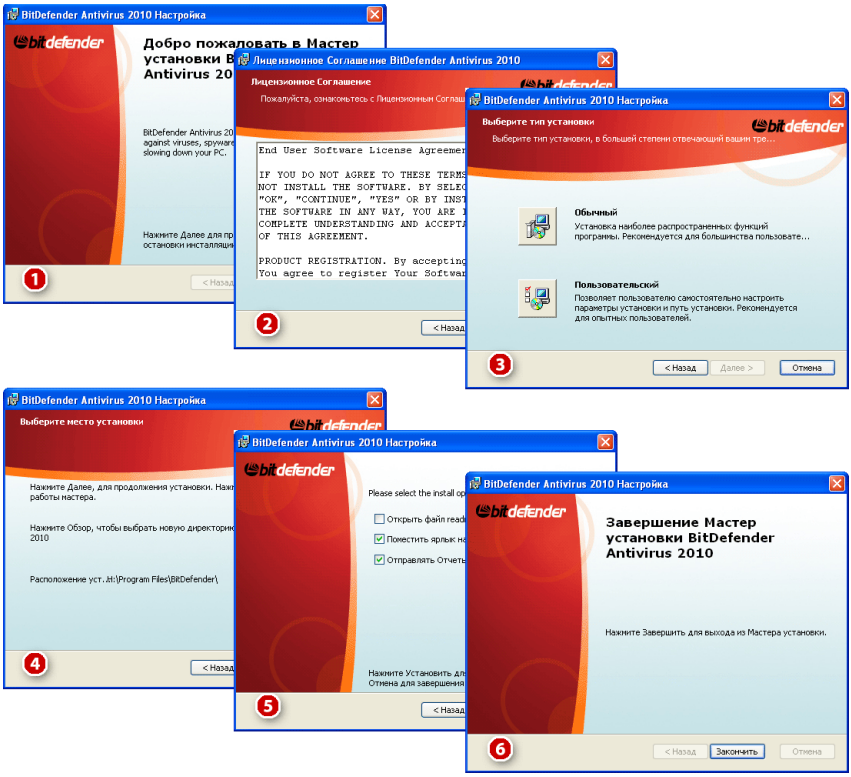
Вы можете установить BitDefender с установочного диска или с помощью установочного файла, загруженного на ваш компьютер с сайта BitDefender или других авторизованных сайтов (например, сайтов партнеров BitDefender или онлайн магазинов). Вы можете загрузить установочный файл BitDefender с сайта, пройдя по следующей ссылке: http://www.bitdefender.com/site/Downloads/.

- Для установки BitDefender с CD-диска, вставьте CD диск в дисковод. Появится экран приветствия. Для начала установки следуйте инструкциям.

  Если экран приветствия не появляется, проследуйте по этому пути `Products\Antivirus\install\ru\` из корня CD диска, и дважды кликните `runsetup.exe`.

- Чтобы установить BitDefender с помощью установочного файла загруженного на ваш компьютер, найдите этот файл и дважды щелкните по нему.

Сначала программа установки проверит вашу систему для подтверждения установки. Если установка прошла проверку, появится мастер установки. Следующее изображение показывает шаги мастера установки.



Пошаговая установка

Выполните следующие шаги для установки BitDefender Antivirus 2010:

1. Щелкните **Далее**. Вы можете отменить установку в любое время, нажав **Отмена**.

   BitDefender Antivirus 2010 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. Одновременный запуск двух или нескольких антивирусных продуктов обычно делает систему неработоспособной.

2. 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.

3. Выберите тип установки.

   - **Обычный** - для установки программы незамедлительно, используя настройки по умолчанию. Если вы выберите эту опцию, вы пропустите шаг 6.
   - **Пользовательский** - для настройки опций инсталляции и последующей установки программы. Эта опция позволяет изменить путь инсталляции.

4. По-умолчанию, BitDefender Antivirus 2010 будет установлен в директорию `C:\Program Files\BitDefender\BitDefender 2010`. Если вы хотите выбрать другую папку для установки, нажмите **Обзор**, а затем в открывшемся окне выберите папку, куда хотите установить BitDefender.

   Щелкните **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 2010 на вашем 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.
   - **Отключить Кеширование DNS Запросов** - для отключения Кеширования DNS Запросов. Сервис DNS-клиента может быть использован различными приложениями для отправки по сети информации без вашего ведома.
   - **Выключить Защиту Windows** - выключает Защиту Windows (доступна только для Windows Vista).

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

6. Дождитесь окончания установки и нажмите **Завершить**. Может появиться сообщение с просьбой перезагрузить вашу систему для того, чтобы мастер установки мог завершить процесс установки. Мы рекомендуем сделать это сразу.

Важно

После окончания установки и перезагрузки компьютера, появятся мастер регистрации и мастер настроек. Запустите эти мастера для регистрации и настройки BitDefender Antivirus 2010 и для создания учетной записи BitDefender.

Если вы приняли настройки установки по умолчанию при установке, вы можете увидеть в `Program Files` новую папку `BitDefender`, в которой будет находиться подкаталог `BitDefender 2010`.

3.1. Мастер регистрации

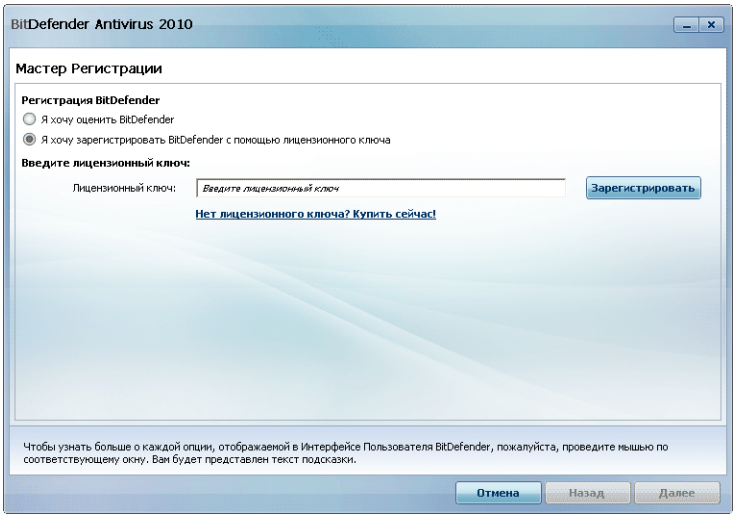
Когда вы перезагрузите компьютер после установки, появится мастер регистрации. Этот мастер поможет вам зарегистрировать BitDefender и настроить учетную запись BitDefender.

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 потеряете лицензионный ключ BitDefender, 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**, расположенную внизу пользовательского интерфейса.

3.1.1. Шаг 1 - Регистрация BitDefender Antivirus 2010



Регистрация

BitDefender Antivirus 2010 устанавливается с 30-дневным периодом пробного использования. Что бы продолжить оценивать продукт, выберите **Я хочу оценить BitDefender** и нажмите **Далее**.

Для регистрации BitDefender Antivirus 2010:

1. выберите **Я хочу зарегистрировать BitDefender с помощью лицензионного ключа**.
2. Введите лицензионный ключ в поле для редактирования.

Замечание

Вы можете найти ваш лицензионный ключ:

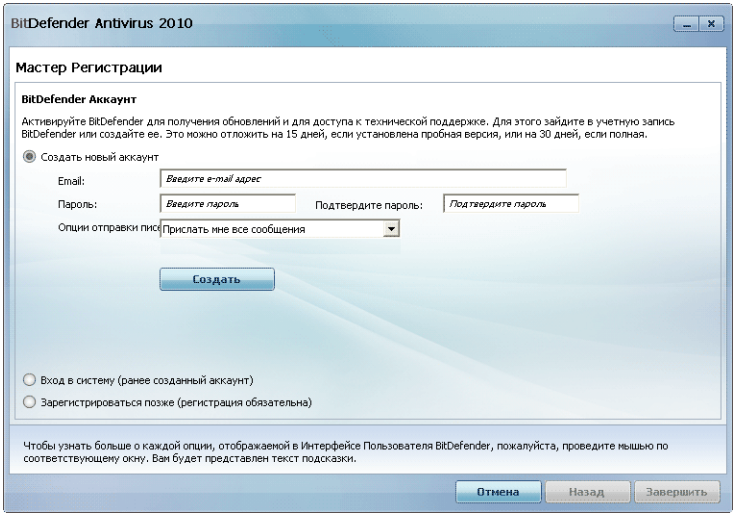
- на обложке CD.
- на регистрационной карточке продукта.
- в электронном письме о покупке.

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

3. Нажмите **зарегистрировать Сейчас**.
4. Щелкните **Далее**.

В вашей система обнаружен действительный лицензионный ключ BitDefender, вы можете продолжать использовать этот ключ нажав **Далее**.

3.1.2. Шаг 2 - Создание учетной записи BitDefender



Создание учетной записи

Если Вы не хотите создавать учетную запись BitDefender прямо сейчас, выберите **Зарегистрировать позже** и нажмите **Завершить**. В ином случае, действуйте исходя из вашей ситуации:

- «У меня нет учетной записи BitDefender» (p. 10)
- «У меня уже есть учетная запись BitDefender» (p. 11)

Важно

Вам необходимо создать аккаунт в течении 15 дней со дня установки BitDefender (если вы его зарегистрировали, срок пробного периода становится равным 30 дней). В противном случае, BitDefender не будет обновляться.

У меня нет учетной записи BitDefender

Для успешного создания аккаунта BitDefender, следуйте этим шагам:

1. Выберите **Создать новый аккаунт**.4564 messages remaining
2. Напечатайте необходимую информацию в соответствующих полях. Предоставленные Вами данные конфиденциальны.

- **Адрес электронной почты** - введите адрес своей электронной почты.
- **Пароль** - введите пароль Вашей учетной записи BitDefender. Пароль должен содержать не менее 6 и не более 16 символов.
- **Повторите пароль** - снова введите набранный ранее пароль.

Замечание
После активации учетной записи, вы можете использовать имеющийся адрес электронной почты и пароль, чтобы войти в свой аккаунт на http://myaccount.bitdefender.com.

3. Дополнительно, BitDefender может информировать вас о специальных предложениях и поощрениях по электронной почте, указанной в вашей учетной записи. Выберите одну из доступных опций из меню:
   - **Отправлять мне все сообщения**
   - **Отправлять мне только сообщения, связанные с продуктом**
   - **Не отправлять мне сообщения**
4. Нажмите **Создать**.
5. Нажмите **Завершить** для завершения работы мастера.
6. **Активируйте ваш аккаунт.** Чтобы использовать аккаунт вы должны его активировать. Проверьте почту и следуйте инструкциям в письме, отправленном вам сервисом регистрации BitDefender.

У меня уже есть учетная запись BitDefender

BitDefender автоматически определит, если вы решистрировали учетную запись BitDefender ранее на этом компьютере. В этом случае, введите пароль от вашего аккаунта и нажмите **Вход в Систему**. Нажмите **Завершить** для завершения работы мастера.

Если у вас уже есть активный аккаунт, но BitDefender не может его обнаружить, следуйте этим шагам что бы привязать продукт к этому аккаунту:

1. Выберите **Вход в систему (ранее созданный аккаунт)**.
2. Напечатайте e-mail адрес и пароль вашего аккаунта в соответствующих полях.

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

3. Дополнительно, BitDefender может информировать вас о специальных предложениях и поощрениях по электронной почте, указанной в вашей учетной записи. Выберите одну из доступных опций из меню:
   - **Отправлять мне все сообщения**

- **Отправлять мне только сообщения, связанные с продуктом**
- **Не отправлять мне сообщения**

4. Нажмите **Вход в Систему**.
5. Нажмите **Завершить** для завершения работы мастера.

3.2. Мастер Настроек

Когда вы закончите работу с мастером регистрации, появится мастер настроек. Этот мастер помогает сконфигурировать главные настройки BitDefender и интерфейс пользователя, лучшим образом подходящий под ваши требования. В конце работы Мастера, вы сможете обновить файлы программы и сигнатуры вредоносного ПО, и просканировать системные файлы и приложения, что бы убедиться что они не заражены.

Мастер состоит из нескольких простых шагов. Количество шагов зависит от вашего выбора. Здесь представлены все шаги, но вы будете предупреждены, если ваш выбор будет влиять на их количество.

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 2010. Если Вы не хотите запускать этот мастер, нажмите **Отмена**. BitDefender уведомит вас о необходимости настройки компонентов, когда вы откроете пользовательский интерфейс.

3.2.1. Шаг 1 - Выберите Используемость Профиля

Используемость Профилей

Нажмите кнопку которая лучшим образом отражает выполняемые на этом компьютере действия (используемость профиля).

Настройка	Описание
Обычный	Нажмите здесь, если этот компьютер в основном используется для просмотра веб страниц и мультимедийных целей.
Геймер	Нажмите здесь, если этот компьютер используется в основном для игр.
Пользовательский	Нажмите здесь, если хотите сконфигурировать все главные настройки BitDefender.

Позднее вы сможете сбросить Используемость профиля из интерфейса продукта.

3.2.2. Шаг 2 - Опишите Компьютер

Описание Компьютера

Выберите параметры, которые применяются к вашему компьютеру:

- **Этот компьютер находится в домашней сети.** выберите эту опцию, если хотите удаленно (с другого компьютера) управлять продуктом BitDefender установленным на этом компьютере. Дополнительный шаг мастера позволит вам настроить Модуль Управления Домашней Сетью.
- **Этот компьютер - Ноутбук .** Выберите эту опцию, если хотите что бы Режим Ноутбука был включен по умолчанию. Находясь в режиме ноутбука, запланированные задачи не выполняются, поскольку они требуют больше системных ресурсов и, увеличивают потребление энергии.

Для продолжения нажмите **Далее**.

3.2.3. Шаг 3 - Выберите Интерфейс Пользователя

Режимы просмотра пользовательского интерфейса

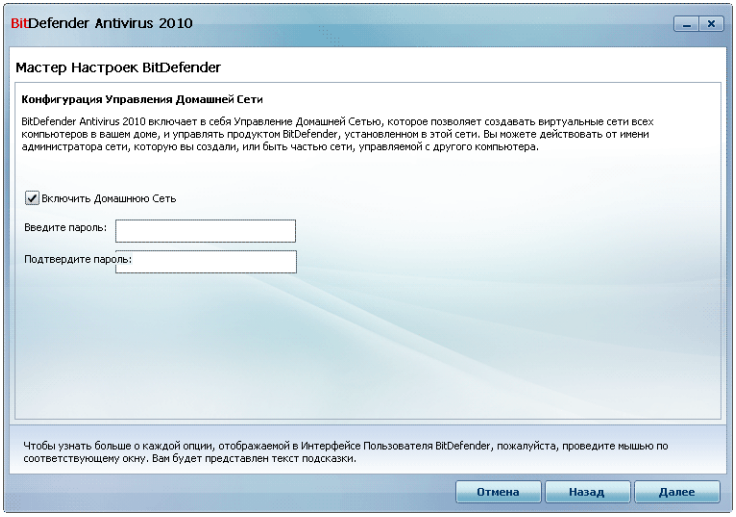
Нажмите на кнопку, которая наиболее точно описывает навыки работы на компьютере, чтобы выбрать соответствующий пользовательский интерфейс режима просмотра. Вы можете выбрать один из трех режимов для просмотра пользовательского интерфейса, в зависимости от ваших навыков работы на компьютере и своего предыдущего опыта работы с BitDefender.

Режим	Описание
Режим Новичка	Подходит для начинающих. Этот режим является простым в использовании и требует минимального взаимодействия с вашей стороны. Все, что требуетя от вас, - устранить существующие проблемы, обнаруженные BitDefender. Пошаговый Мастер поможет вам в их решении. Кроме того, вы можете выполнять общие задачи, такие как обновления сигнатур вирусов и файлов продукта или сканирование компьютера.
Режим Пользователя	Предназначенный для пользователей со средними навыками работы на компьютере, это режим расширят возможности того, что вы можете сделать Режиме Новичка.

Режим	Описание
	Вы можете устранять проблемы по выбору и решать, какие вопросы контролировать. Более того, вы можете удаленно управлять продктами BitDefender, установленными на компьютерах в вашем доме.
Режим опытного пользователя	Режим подходит для технически подкованных пользователей и позволяет полностью настроить каждую функцию BitDefender. Вы можете также использовать все задачи, предусмотренные для защиты вашего компьютера и данных.

3.2.4. Шаг 4 - Настроить Сеть BitDefender

Замечание
Этот шаг появится только если вы выставили в шаге 2, что этот компьютер подключен к домашней сети.



Конфигурация сети BitDefender

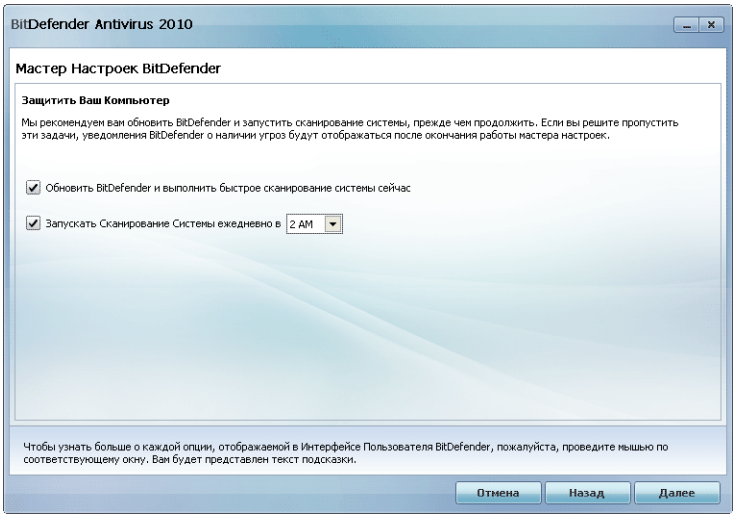
BitDefender позволяет вам создать виртуальную сеть компьютеров для домашнего использования и управлять продуктами BitDefender, установленными в этой сети.

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

1. Выберите **Включить Домашнюю Сеть**.
2. Введите один и тот же пароль администратора в каждое поле. Пароль позволяет администратору управлять этим продуктом BitDefender с другого компьютера.

Для продолжения нажмите **Далее**.

3.2.5. Шаг 5 - Выбор задач для запуска



Выбор задачи

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

- **Обновить BitDefender и выполнить быстрое сканирование сейчас** - в ходе следующего шага, будут обновлены сигнатуры вирусов и программные файлы BitDefender, для защиты вашего компьютера от новейших угроз. Также, незамедлительно после завершения обновления, BitDefender начнет сканирование файлов из папок `Windows` и `Program Files`, что бы удостовериться в том что они не заражены. Эти папки содержат файлы операционной системы и установленных приложений. Обычно, данные папки первые подлежат угрозе заражения.

- **Запускать Сканирование Системы каждый день в 2 часа ночи** - устанавливает запуск стандартного сканирования вашего компьютера на каждый день в 2 часа ночи. Для изменения времени запуска сканирования, нажмите меню и выберите желаемое время запуска. Если ваш компьютер выключен в запланированное время, сканирование запустится когда вы включите компьютер.

Замечание

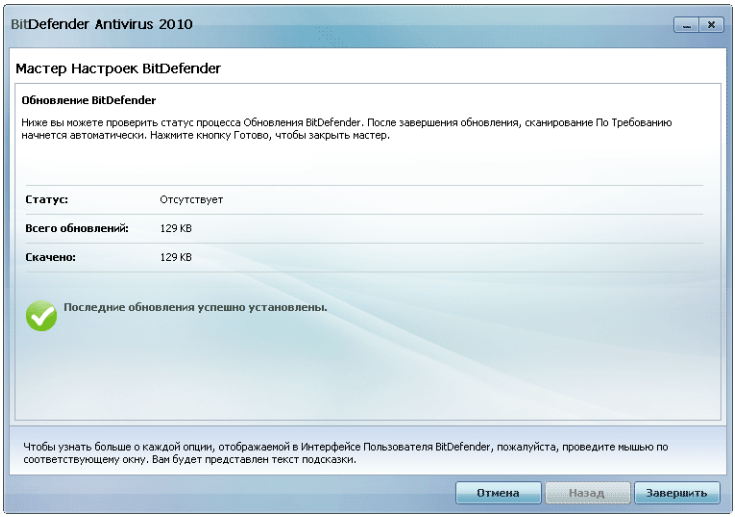
Если, позднее, вы захотите поменять время на которое запланировано сканирование, следуйте этим шагам.

1. Откройте BitDefender и установите пользовательский интерфейс в Режим опытного пользователя.
2. Нажмите **Антивирус** в левом меню.
3. Нажмите на вкладку **Сканирование Вирусов**.
4. Правой кнопкой мыши кликните на задаче **Сканирование Системы** и выберите **Планировать**. Появится новое окно.
5. По необходимости измените частоту и время начала.
6. Нажмите **OK** чтобы сохранить сделанные изменения.

Рекомендуем Вам включить данные опции перед тем, как перейти к следующему шагу, чтобы обеспечить полную безопасность Вашей системы. Для продолжения нажмите **Далее**.

Если вы снимите первый флажок, не будет никаких задач, выполняемых в последнем шаге мастера. Нажмите **Завершить** для завершения работы мастера.

3.2.6. Шаг 6 - Процедура завершена



Статус задачи

Дождитесь пока BitDefender обновит сигнатуры вирусов и модули сканирования. Как только обновление завершится, начнется быстрое системное сканирование. Проверка будет выполняться незаметно для пользователя, в фоновом режиме. Обратите внимание на иконку состояния сканирования в системном трее. Вы можете кликнуть в эту иконку, чтобы открыть окно сканирования и наблюдать прогресс проверки.

Нажмите **Завершить** для завершения работы мастера. Вам не придется ждать, когда сканирование будет завершено.

Замечание

Сканирование займет некоторое время. Когда оно закончится, откройте окно сканирования и оцените результаты проверки, чтобы убедиться, что ваша система чиста. Если во время проверки были обнаружены вирусы, Вам следует немедленно открыть BitDefender и запустить полное сканирование системы.

4. Обновление

Вы можете обновить до BitDefender Antivirus 2010, если используете BitDefender Antivirus 2010 beta или 2008 или 2009 версии.

Есть 2 способа выполнения обновлений:

- Установка BitDefender Antivirus 2010 непосредственно поверх устаревшей версии. Если вы устанавливаете непосредственно поверх 2009ой версии, Карантин буде импортирован автоматически.
- Удалите предыдущую версию, затем перегрузите компьютер и установите новую, следуя указаниям раздела «*Установка BitDefender*» (p. 5). Настройки продукта сохранены не будут. Используйте этот метод Обновления, в случае если остальные не удались.

5. Восстановление или удаление BitDefender.

Если хотите восстановить или удалить BitDefender Antivirus 2010, проделайте следующее: **Пуск → Программы → BitDefender 2010 → Восстановить или удалить**.

Подтвердите свой выбор, нажав **Далее**. В появившемся окне выберите:

- **Восстановить** - переустановка всех установленных компонентов программы, установленных на предыдущем этапе.

  Если выбираете опцию восстановления BitDefender, появится новое окно. Нажмите **Восстановить**, чтобы начать процесс восстановления.

  Перегрузите компьютер после соответствующего предложения, а затем нажмите **Установить**, чтобы переустановить BitDefender Antivirus 2010.

  По завершению процесса установки появится новое окно. Нажмите **Завершить**.

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

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

  Если Вы выбираете опцию удаления 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 2010 с Вашего компьютера.

  Как только процесс удаления закончится, появится новое окно. Нажмите **Завершить**.

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

Начало работы

6. Обзор

Как только вы установите BitDefender, защита вашего компьютера будет обеспечена. Если вы не завершили мастер настроек, вам надо открыть BitDefender как можно скорее и исправить все неполадки. Возможно, вам придется настроить отдельные элементы BitDefender или принимать превентивные меры для защиты вашего компьютера и данных. При желании Вы можете настроить BitDefender так, чтобы не получать уведомления об определенных событиях.

Если Вы не зарегистрировали продукт (в том числе не создали учетную запись BitDefender), не забудьте сделать это до конца испытательного срока. Вам необходимо создать аккаунт в течении 15 дней со дня установки BitDefender (если вы его зарегистрировали, срок пробного периода становится равным 30 дней). В противном случае, BitDefender не будет обновляться. Для получения дополнительной информации о процессе регистрации перейдите к «*Регистрация и Мой Аккаунт*» (p. 51).

6.1. Открытие BitDefender

Чтобы открыть главный интерфейс BitDefender Antivirus 2010, воспользуйтесь меню "Пуск": **Пуск → Программы → BitDefender 2010 → BitDefender Antivirus 2010** или для ускорения процесса дважды нажмите иконку BitDefender на панели задач.

6.2. Режимы 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 один из трех режимов для просмотра пользовательского интерфейса, в зависимости от ваших навыков работы на компьютере и своего предыдущего опыта работы с BitDefender.

Режим	Описание
Режим Новичка	Подходит для начинающих. Этот режим является простым в использовании и требует минимального взаимодействия с вашей стороны. Все, что требуетя от вас, - устранить существующие проблемы, обнаруженные BitDefender. Пошаговый Мастер поможет вам в их решении. Кроме того, вы можете выполнять общие задачи, такие как

Режим	Описание
	обновления сигнатур вирусов и файлов продукта или сканирование компьютера.
Режим Пользователя	Предназначенный для пользователей со средними навыками работы на компьютере, это режим расширят возможности того, что вы можете сделать Режиме Новичка. Вы можете устранять проблемы по выбору и решать, какие вопросы контролировать. Более того, вы можете удаленно управлять продктами BitDefender, установленными на компьютерах в вашем доме.
Режим опытного пользователя	Режим подходит для технически подкованных пользователей и позволяет полностью настроить каждую функцию BitDefender. Вы можете также использовать все задачи, предусмотренные для защиты вашего компьютера и данных.

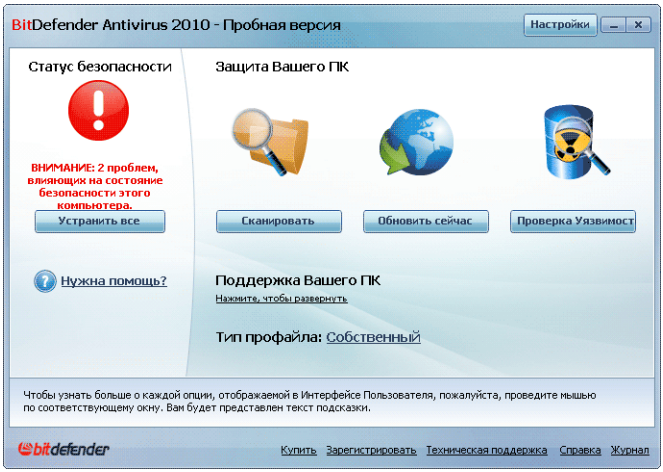
Режим пользовательского интерфейса выбирается в мастере настроек. Этот мастер появляется после мастера регистрации во время первого запуска компьютера после установки продукта. Если вы отмените мастер настроек, режим пользователя по умолчанию перейдет в Промежуточный.

Для изменения режима пользовательского интерфейса следуйте инструкции:

1. Откройте BitDefender.
2. Нажмите **Настройки** в вверхнем правом углу окна.
3. В катергоии Установки Пользовательского Интерфейса нажмите стрелку на кнопке и выберите желаемый режим.
4. Нажмите **OK**, чтобы применить изменения.

6.2.1. Режим Новичка

Если вы начинащий пользователь, Режим Новичка может быть более подходящим для вас. Этот режим проств использовании и практически не требует вмешательства с вашей стороны.



Режим Новичка

Окно состоит из 4х главных секций:

- **Статус Безопасности** информирует вас о пробемах, угрожающих безопасности вашего компьютера, и помогает решить их. При нажатии **Устранить Все Угрозы**, Мастер поможет вам легко удалить все угрозы и обеспечить безопасность данных. Для получения дополнительной информации перейдите «*Устранение Угроз(Проблем)*» (p. 40).
- **Защита ПК** - здесь вы можете найти необходимые задачи для защиты вашего компьютера и данных. Доступные задачи различаются в зависимости от используемости профиля.
  - Кнопка **Сканировать Сейчас** запускает стандартное сканирование вашей системы на наличие вирусов, шпионского ПО и других вредоносных программ. Мастер Сканирования на антивирусы появится и проведет вас через процесс сканирования. Для получения дополнительной информации перейдите к «*Мастер антивирусного сканирования*» (p. 56).
  - Кнопка **Обновить Сейчас** помогает вам обновить сигнатуры вирусов и программные файлы BitDefender. Откроется новое окно, где Вы можете увидеть результаты проверки. Если обнаружены обновления, они будут автоматически загружены и установлены на ваш компьютер.
  - Когда выбран **Обычный** профиль, кнопка **Проверка на Наличие Уязвимостей** запускает мастер помогающий вам найти уязвимости вашей системы, такие как устаревшее ПО или пропущенные обновления Windows.

Для получения дополнительной информации перейдите к *«Мастер Проверки на Наличие Уязвимостей»* (p. 68).

- При выборе профиля**Геймер**, кнопка **Включить /Выключить Режи Игры** позволяет вам включить/выключаитьРежим Игры. Режим Игры изменяет параметры настроек системы защиты для того, чтобы снизить к минимуму воздействие на компьютер во время игры.

- **Поддержка Вашего ПК** здесь вы можете найти дополнительные задачи для защиты вашего компьютера и данных.
  - **глубокое Сканирование Системы** запускает полную проверку вашей системы на наличие всех видов вредоносного ПО.
  - **Сканирование Моих Документов** сканирует на вирусы и другие вредоносные программы наиболее часто используемые папки : Мои Документы и Рабочий стол. Это позволит обеспечить безопасность ваших документов, безопасную рабочую среду и чистые приложения выполняющиеся при запуске системы.
  - **Сканирование при входе в систему** сканирует элементы запускаемые при входе в Windows.
- **Используемость Профиля** показывает тип использования выбранного в данный момент профиля. Используемость профилей отражает основные действия выполняющиеся на компьютере. В зависимости от используемости профиля, интерфейс продукта организуется с целью обеспечения легкого доступа к нужным задачам.

  Если вы хотите переключиться на другой профиль или редактировать текущий, нажмите на профиль и следуйте Мастеру настроек.

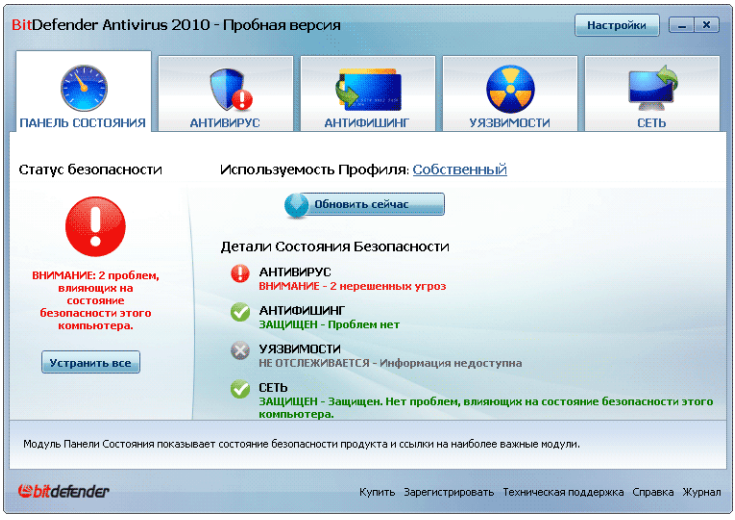
В правом верхнем углу окна находится кнопка **Настройки**. Она открывает окно, в котором вы можете изменить режим пользовательского интерфейса и включить или отключить основные настройки BitDefender. Для получения дополнительной информации перейдите *«Настройка общих параметров»* (p. 44).

В вверхнем нижнем углу окна находится несколько полезных ссылок.

Ссылка	Описание
Купить/Продлить	Открывает веб-сайт где вы можете купить лицензионный ключ для вашего BitDefender Antivirus 2010.
Регистрация	Ввод нового лицензионного ключа или отображение текущего лицензионного ключа и состояния регистрации.
Помощь & Поддержка	Дает доступ к файлу справки об использовании BitDefender.

6.2.2. Средний Уровень

Режим Пользователя - простой интерфейс, предназначенный для пользователей со средним навыком работы на компьютере, который позволяет получить доступ ко всем модулям на базовом уровне. Вам придется отслеживать предупреждения и критические оповещения и решать нежелательные проблемы.



Средний Уровень

Окно Режима Пользователя состоит из пяти вкладок. В следующей таблице кратко описывается каждая вкладка. Для получения дополнительной информации перейдите к «Средний Уровень» (p. 75) части руководства пользователя.

Вкладка	Описание
Панель инструментов	Отображает состояние безопасности вашей системы и позволяет сбросить используемость профиля.
Антивирус	Показывает состояние антивирусного модуля BitDefender, который помогает обновлять BitDefender и надежно защищать компьютер от вирусов.
Антифишинг	Показывает статус модулей, которые защищают вас от фишинга (кражи личной информации), когда вы в сети.

Вкладка	Описание
Уязвимости	Показывает состояние модуля сканирования на уязвимости, помогающего обновлять важнейшее программное обеспечение вашего ПК. Тут вы можете с легкостью исправить любую уязвимость, которая может повлиять на безопасность вашего компьютера.
Сеть	Показывает структуру домашней сети BitDefender. Тут вы можете настраивать и управлять продуктами BitDefender, установленными в вашей домашней сети. Таким образом вы можете управлять безопасностью вашей домашней сети с одного компьютера.

В правом верхнем углу окна находится кнопка **Настройки**. Она открывает окно, в котором вы можете изменить режим пользовательского интерфейса и включить или отключить основные настройки BitDefender. Для получения дополнительной информации перейдите *«Настройка общих параметров»* (p. 44).

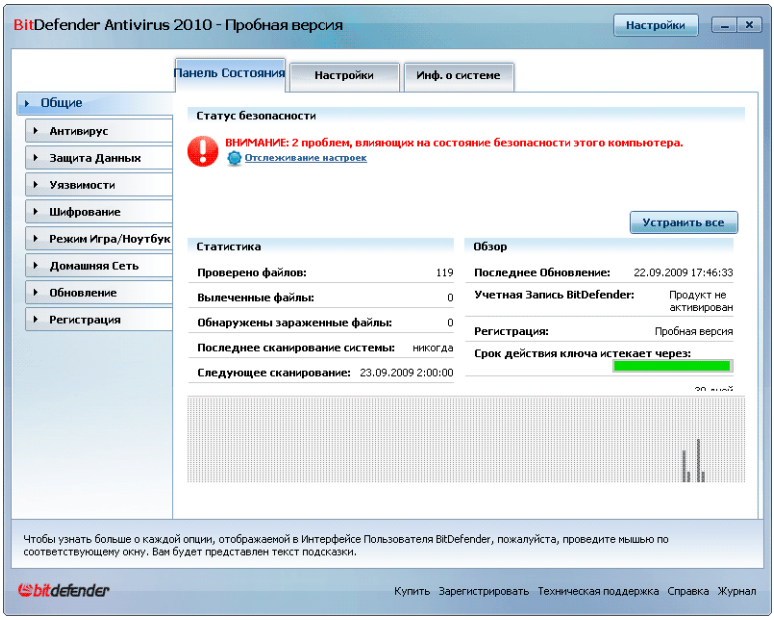
В вверхнем нижнем углу окна находится несколько полезных ссылок.

Ссылка	Описание
Купить/Продлить	Открывает веб-сайт где вы можете купить лицензионный ключ для вашего BitDefender Antivirus 2010.
Регистрация	Ввод нового лицензионного ключа или отображение текущего лицензионного ключа и состояния регистрации.
Техническая поддержка	Обращение в службу поддержки BitDefender.
Справка	Дает доступ к файлу справки об использовании BitDefender.
Просмотр журнала	Просмотр подробного отчета о всех задачах, выполненных приложением BitDefender в вашей системе.

6.2.3. Режим Опытного Пользователя

Режим опытного пользователя дает вам доступ к специфическим компонентам BitDefender. Тут вы можете детально настроить BitDefender.

Замечание
Режим Опытного Пользователя подходит для пользователей, с опытом работы на компьютере выше среднего, которые знакомы с разновидностями угроз, которым подвергается компьютер, а также с тем, как работают программы безопасности.



Режим Опытного Пользователя

В левой части окна расположено меню с перечнем всех модулей безопасности. Каждый модуль имеет несколько закладок, где вы можете настроить соответствующие параметры безопасности или задавать задачи безопасности и административные задачи. В следующей таблице кратко описывается каждый модуль. Для получения дополнительной информации перейдите к «Режим Опытного Пользователя» (p. 98) части руководства пользователя.

Модуль	Описание
Общие	Доступ к основным параметрам или просмотр консоли и подробных сведений о системе.
Антивирус	Подробная настройка параметров антивируса и операций сканирования, установка исключений и настройка модуля карантина.
Контроль Личных Данных	Предотвращение кражи данных с вашего компьютера и защита вашей конфиденциальности, когда вы находитесь в режиме онлайн.

Модуль	Описание
Уязвимости	Этот параметр позволяет держать важные приложения на вашем ПК в обновленном состоянии.
Шифрование	Позволяет зашифровать сообщения Yahoo Messenger и Windows Live (MSN) Messenger.
Режим Игровой/Ноутбук	Позволяет отложить задачи BitDefender по расписанию во время работы ноутбука 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	Позволяет регистрировать BitDefender Antivirus 2010, изменять лицензионный ключ или создавать учетную запись BitDefender.

В правом верхнем углу окна находится кнопка **Настройки**. Она открывает окно, в котором вы можете изменить режим пользовательского интерфейса и включить или отключить основные настройки BitDefender. Для получения дополнительной информации перейдите «*Настройка общих параметров*» (p. 44).

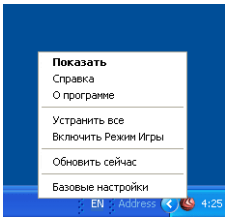
В вверхнем нижнем углу окна находится несколько полезных ссылок.

Ссылка	Описание
Купить/Продлить	Открывает веб-сайт где вы можете купить лицензионный ключ для вашего BitDefender Antivirus 2010.
Регистрация	Ввод нового лицензионного ключа или отображение текущего лицензионного ключа и состояния регистрации.
Техническая поддержка	Обращение в службу поддержки BitDefender.
Справка	Дает доступ к файлу справки об использовании BitDefender.
Просмотр журнала	Просмотр подробного отчета о всех задачах, выполненных приложением BitDefender в вашей системе.

6.3. Иконка Панели Задач

Для более быстрого доступа к управлению продуктом используйте иконку BitDefender на 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.



Панель задач

- **Показать** - открывает основной интерфейс BitDefender.
- **Помощь** - открывает файл Справка, в котором подробно описано как настроить и пользоваться BitDefender Antivirus 2010.
- **О программе** - открывает окно, где можно просмотреть информацию о BitDefender и о том, где искать помощь в случае непредвиденных обстоятельств.
- **Устранить все угрозы** - помогает устранить имеющиеся уязвимости в безопасности компьютера. Если опция недоступна, значит проблем. требующих решения, нет. Для получения дополнительной информации перейдите *«Устранение Угроз(Проблем)»* (p. 40).
- **Включить/Выключить Режим Игры** - activates / deactivates Режим Игры.
- **Обновить сейчас** - запускает немедленное обновление. Откроется новое окно, где Вы можете увидеть результаты проверки.
- **Основные Настройки** открывает окно, в котором вы можете изменить режим пользовательского интерфейса и включить или отключить основные параметры продукта. Для получения дополнительной информации перейдите *«Настройка общих параметров»* (p. 44).

Иконка панели задач BitDefender информирует вас, когда вашему компьютеру что-о угрожает, или о том, как работает продукт, сигнализируя следующим образом:

Красный треугольник с восклицательным знаком: Существуют критические угрозы безопасности системы. Они требуют немедленного вмешательства и решения.

Желтый треугольник с восклицательным знаком: Некритические проблемы влияют на безопасность вашей системы. Вы должны проверить и исправить их в ближайшее время.

БуквaG: Продукт работает в Режиме Игры.

Если BitDefender не работает, иконка на панели задач отмечена серым цветом. Обычно происходит, когда истекает срок действия лицензионного ключа. Также может произойти, когда BitDefender не отвечает или когда другие ошибки влияют на нормальную работу BitDefender.

6.4. Панель Активности Сканирования

В окне **График активности** графически показано, как проходит проверка Вашей системы на наличие вирусов. Это маленькое окошко по умолчанию доступно только в Режиме опытного пользователя.

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

Панель Активности Сканирования

Замечание
Если проверка в реальном времени отключена, то будет отображаться красный крест поверх знака **Файловая зона**.

6.4.1. Сканировать файлы и папки

Вы можете использовать панель активности сканирования чтобы быстро сканирования файлов и папкок. Перетащите файл или папку, которую вы хотите проверить, в **Панель Активности Сканирования**, как показано ниже.

Перетащить Файл

Переместите файл

Мастер Сканирования на антивирусы появится и проведет вас через процесс сканирования. Для получения дополнительной информации перейдите к *«Мастер антивирусного сканирования»* (p. 56).

Параметры сканирования. Опции сканирования предварительно настроены для достижения наилучших результатов обнаружения. При обнаружении инФицированных файлов, BitDefender попробует их излечить (удалить вредоносные коды). Если это не получится, то Мастер сканирования даст вам возможность определить что с ними делать. Опции сканирования стандартны и вы не можете их изменить.

6.4.2. Убрать/Восстановить панель активности сканирования

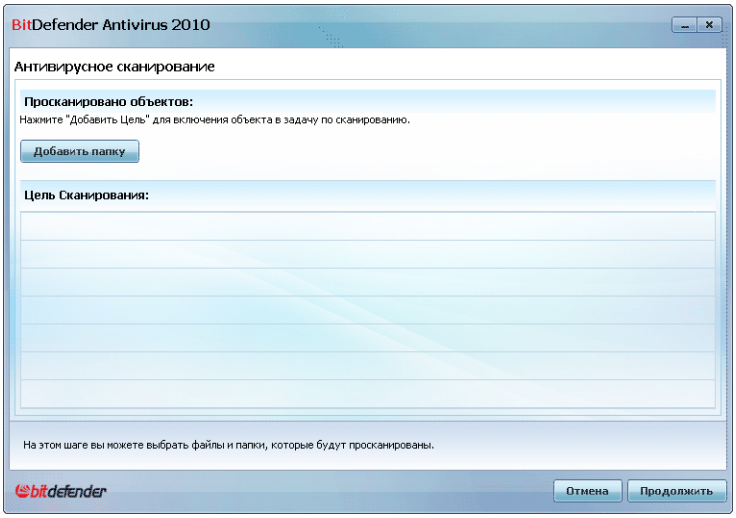
Чтобы убрать это окно с экрана, просто щелкните правой кнопкой мышки на нем и выберите пункт меню **Скрыть**. Выполните эти шаги чтобы восстановить панель активности сканирования:

1. Откройте BitDefender.
2. Нажмите **Настройки** в вверхнем правом углу окна.
3. В категории "Общие настройки", установите флажок в поле, соответствующем **Панель Активности Сканирования**.
4. Нажмите **OK**, чтобы применить изменения.

6.5. Ручное сканирование BitDefender

Ручное сканирование BitDefender дает вам возможность сканировать конкретную папку или диск не создавая задания сканирования. Эта функция разработана для использования в Безопасном режиме Windows Если ваша система заражена устойчивым вирусом попробуйте удалить его, запустив Безопасный режим Windows и просканировав все жесткие диски используя ручное сканирование BitDefender.

Чтобы открыть Ручное сканирование BitDefender, воспользуйтесь меню Пуск в Windows: **Пуск → Программы → BitDefender 2010 → BitDefender Ручное сканирование** Появится следующее окно:



Ручное сканирование BitDefender

Нажмите **Добавить Папку**, выберите местоположение которое вы хотите просканировать и нажмите **OK**. Если вы хотите просканировать многочисленные папки, повторите это действие для каждого дополнительного местоположения.

Пути к выбранным местоположениям появятся в колонке **Цель Сканирования**. Если вы передумали насчет пути, нажмите кнопку **Удалить**, которая находится рядом. Нажмите кнопку **Удалить все пути**, для удаления всех местоположений добавленных в список.

Когда вы закончите выбирать месторасположения, нажмите **Продолжить**. Мастер Сканирования на антивирусы появится и проведет вас через процесс сканирования. Для получения дополнительной информации перейдите к *«Мастер антивирусного сканирования»* (p. 56).

Параметры сканирования. Опции сканирования предварительно настроены для достижения наилучших результатов обнаружения. При обнаружении инФицированных файлов, BitDefender попробует их излечить (удалить вредоносные коды). Если это не получится, то Мастер сканирования даст вам возможность определить что с ними делать. Опции сканирования стандартны и вы не можете их изменить.

Что такое Безопасный режим?
Безопасный режим - особый способ запуска Windows, используемый главным образом для устранения проблем, влияющих на нормальной режим работы

Windows: от конфликтующих драйверов до вирусов, мешающим запусу Windows в нормальном режиме. В Безопасном режиме Windows загружает только самые необходимые компоненты и драйверы, способные работать в Безопасном Режиме. По этой причине большинство программ, в том числе и вирусов, не могут работать в этом режиме и легко могут быть удалены.
Чтобы запустить систему в Безопасном режиме, перезапустите ваш компьютер и нажмите F8 до появления меню доплнительных опций загрузки Windows. Вам необходимо выбрать **Безопасный Режим с Поддержкой Сети** , чтобы иметь доступ к интернету.

Замечание

Чтобы получить более подробную информацию о безопасном режиме обратитесь к справочной системе Windows (**Справка и поддержка** в меню Пуск). Также вы можете найти полезную информацию поискав в интернет.

6.6. Реим Игры и режим Ноутбука

Некоторые режимы работы компьютера, такие как игры или презентации, требуют повышенной бесперебойной реакции и производительности системы. Если ваш ноутбук работает от батареи, лучше отложить ненужные операции, требующие дополнительной электроэнергии, до подключения ноутбука к источнику бесперебойного питания.

Для адаптирования к этим особым ситуациям BitDefender Antivirus 2010 имеет два специальных режима работы:

- Режим Игры
- Режим Ноутбука

6.6.1. Режим Игры

Режим Игры изменяет параметры настроек системы защиты для того, чтобы снизить к минимуму воздействие на компьютер во время игры. При включении Режима Игры, применяются следующие настройки:

- Минимизировать использование процессорного времени и оперативной памяти
- Отложить автоматические задачи обновления и сканирования
- Отключить все уведомления и всплывающие окна
- Сканировать только самые важные файлы

Находясь в Режиме Игры, вы будете видеть букву G поверх значка BitDefender.

Использование Режима Игры

По умолчанию BitDefender автоматически входит в Игровой режим при запуске игры, находящейся в списке известных игр BitDefender, или когда приложение разворачивается на полный экран. BitDefender автоматически вернется в нормальный режим работы, когда вы закрываете игру или при выходе приложения из полноэкранного режима.

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

- Кликните правой кнопкой мыши на иконке BitDefender на панели задач 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.

Изменение Горячих клавиш Режима Игры

Чтобы изменить Горячие клавиши, необходимо выполнить следующие шаги:

1. Откройте BitDefender и установите пользовательский интерфейс в Режим опытного пользователя.
2. Выберите **Режим Игры/ Режим Ноутбука** из бокового меню слева.
3. Щелкните на вкладке **Режим Игры**.
4. Нажмите кнопку **Дополнительные Настройки**.
5. Используя парамер **Использовать Горячие Клавиши**, задайте желаемую горячую клавишу :
   - 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.

6. Нажмите **OK** чтобы сохранить сделанные изменения.

6.6.2. Режим Ноутбука

Режим ноутбука специально предназначен для пользователей портативных компьютеров. Его цель - минимизировать влияние работы BitDefender на энергопотребление, когда эти устройства работают от батареи. Находясь в режиме ноутбука, запланированные задачи не выполняются, поскольку они требуют больше системных ресурсов и, увеличивают потребление энергии.

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 использования Режима ноутбука вам нужно указать в Мастер настроек, что вы используете ноутбук. Если вы не выберите соответствующую опцию при запуске Мастера, вы можете включить Режим ноутбука следующим образом:

1. Откройте BitDefender.
2. Нажмите **Настройки** в вверхнем правом углу окна.
3. В категории "Общие настройки", установите флажок в поле, соответствующем **Обнаружение Режима Ноутбука**.
4. Нажмите **OK**, чтобы применить изменения.

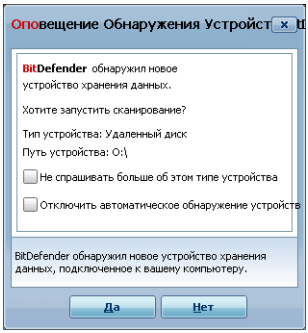
6.7. Автоматическое обнаружение устройств

BitDefender автоматически определяет подключение съемного запоминающего устройства к компьютеру и предлагает просканировать его, прежде чем получить доступ к его файлам. Этот режим рекомендуется для защиты компьютера от вирусов и других вредоносных программ.

Обнаруженные устройства разделяются на следующие категории:

- CD/DVD
- USB устройства хранения данных, таких как флэш-носители и внешние жесткие диски
- Удаленные сетевые диски

При обнаружении такого устройства, отображается окно предупреждения.



Предупреждение об обнаружении устройства

Для сканирования устройства хранения данных, просто нажмите **Да**. Мастер Сканирования на антивирусы появится и проведет вас через процесс сканирования. Для получения дополнительной информации перейдите к *«Мастер антивирусного сканирования»* (p. 56).

Если вы не хотите сканировать устройство, необходимо нажать кнопку **Нет**. В этом случае, одна из данных функций будет полезна:

- **Не спрашивать об этом типе устройства** - BitDefender больше не будет предлагать сканировать устройства хранения данных этого типа при подключении их к компьютеру.
- **Отключить автоматическое обнаружение устройств** - вам больше не будет предложено сканирование новых устройств хранения информации при их подключении к компьютеру.

Если вы случайно отключили автоматическое обнаружение устройств и хотите его включить, или если хотите настроить его параметры, выполните следующие действия:

1. Откройте BitDefender и установите пользовательский интерфейс в Режим опытного пользователя.
2. Перейдите **Антивирус>Сканировать вирусы**
3. В списке задач проверки усановите задачу **Обнаружение устройства сканирования**.
4. Щелкните правой кнопкой на задачу и выберите **Открыть**. Появится новое окно.
5. В закладке **Обзор** настройте требуемые параметры сканирования. Для получения дополнительной информации перейдите к *«Изменение настроек сканирования»* (p. 124).

6. В закладке **Detection** выберите типы устройств, которые необходимо обнаружить.
7. Нажмите **OK**, чтобы применить изменения.

7. Устранение Угроз(Проблем)

BitDefender использует систему слежения за угрозами для их выявления и оповещения. По умолчанию он отслеживает только ряд угроз, которые считаются наиболее опасными, но вы можете настроить BitDefender так, как вам требуется, выбирая, о каких именно угрозах вы хотели бы быь уведомлены.

Уведомления о текущих проблемах:

- Над иконкой BitDefender в системном трее появляется специальный знак, указывающий на нерешенные вопросы.

  Красный треугольник с восклицательным знаком: Существуют критические угрозы безопасности системы. Они требуют немедленного вмешательства и решения.

  Желтый треугольник с восклицательным знаком: Некритические проблемы влияют на безопасность вашей системы. Вы должны проверить и исправить их в ближайшее время.

  Также, если Вы наведете курсор на иконку, всплывающее окно подтвердит наличие имеющихся проблем.

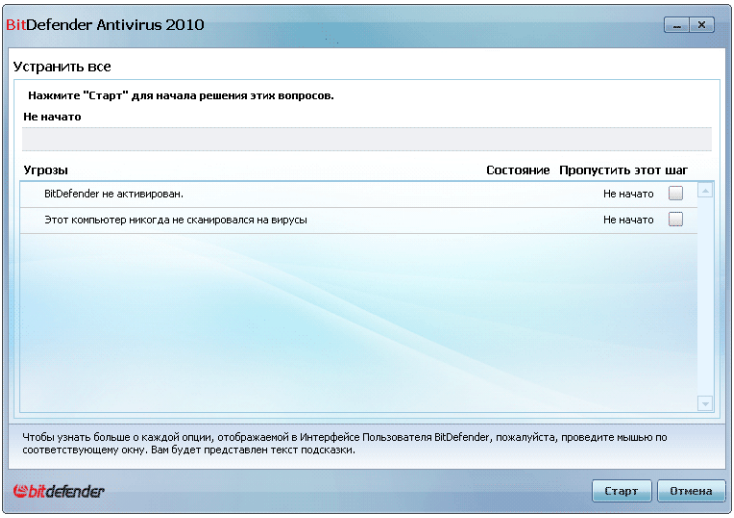
- При открытии BitDefender область Состояния Безопасности покажет количество проблем, влияющих на систему.

  - В Режиме Пользователя состояните безопасности показано в закладке **Панель Управления**.
  - Находясь в Режиме Опытного Пользователя, перейдите в **Общие>Панель Управления** , чтобы проверить статус безопасности.

7.1. Мастер Устранения Угроз

Самый простой путь устарнения проблем - следовать пошаговой инструкции мастера **Устанить Все Угрозы** . Мастер поможет вам легко удалить угрозы и обеспечить безопасность данных. Для того, чтобы запустить мастер, сделайте следующее:

- Нажмите правой кнопкой мыши на иконку BitDefender в панели задач и выберите **Устранить Все Угрозы**.
- Откройте BitDefender. В зависимости от режима пользовательского интерфейса, сделайте следующие шаги:
  - В Режиме Новичка нажмите **Устранить Все Угрозы**.
  - В Режиме Пользователя перейдите во вкладку **Панель Управления** и нажмите **Устранить Все Проблемы**.
  - В Режиме Опытного Пользователя перейдите **Общие>Панель Управления** и нажмите **Устранить Все Угрозы**.



Мастер Устранения Угроз

Мастер показывает список существующих на вашем компьютере уязвимостей безопасности.

Все текущие текущие проблемы выбраны для устранения. Если есть проблемы которые вы не хотите устранять, просто выберите соответствующий флажок. Если вы так поступите, их состояние поменяется на **Пропустить**.

Замечание
Если вы не хотите получать уведомления о определенных проблемах, вы должны настроить систему отслеживания так, как описано в следующей секции.

Для устранения выбранных проблем, нажмите **Пуск**. Некоторые проблемы устранятся незамедлительно. Остальные вам поможет устранить мастер.

Проблемы, которые помогает устранить этот мастер, могут быть сгруппированы в эти главные категории:

- **Отключенные настройки безопасности.** Такие проблемы устраняются незамедлительно, включением соответствующих настроек.
- **Профилактические задачи безопасности, которые необходимо выполнить.** Примером такой задачи является сканирование вашего компьютера. Рекомендовано сканировать компьютер, хотя бы 1 раз в неделю. В большинстве случаев BitDefender будет делать это автоматически. Как бы то ни было, если вы меняли график сканирования, вы будете предупреждены об этой проблеме.

При устранении таких проблем, мастер поможет вам успешно завершить задачу.

- **Системные уязвимости.** BitDefender автоматически проверяет ваше систему на наличие уязвимостей и предупреждает вас о них. Системные Уязвимости включают следующее:
  - ненадежные пароли аккаунтов Windows.
  - устаревшее ПО на вашем компьютере.
  - отсутствующие обновления Windows.
  - Автоматические обновления Windows отключены.

  Когда появляются такие проблемы, запускается Мастер Сканирования на Наличие Уязвимостей. Этот мастер поможет вам в устранении обнаруженных системных уязвимостей. Для получения дополнительной информации перейдите к *«Мастер Проверки на Наличие Уязвимостей»* (p. 68).

7.2. Настройка Отслеживания Угроз

Система отслеживания проблем, настроена на контроль и выдачу предупреждений о наиболее важных проблемах, которые могут затронуть безопасность вашего компьютера и ваших данных. Дополнительные проблемы могут контролироваться на основе сделанного вами выбора в Мастер Настроек (при настройке вашего профиля). Кроме проблем контролируемых по умолчанию, есть несколько других проблем о которых вы можете быть проинформированы.

вы можете настроить отслеживание системы, для лучшего обслуживания нужд безопасности, выбрав определенные проблемы, о которых вы хотите узнавать. Вы можете сделать это в Промежуточном Режиме или Режиме опытного Пользователя.

- В промежуточном Режиме, отслеживание системы может быть настроено из отдельных местоположений. Следуйте инструкции:
  1. Перейдите к вкладке **Антивирус**, **Антифишинг** или **Уязвимости**.
  2. Нажмите **Настройка Отслеживания Состояния**.
  3. Отметьте флажки соответствующие элементам, которые вы хотите контролировать.

  Для получения дополнительной информации перейдите к «Средний Уровень» (p. 75) части руководства пользователя.
- В Режиме Опытного Пользователя, отслеживание системы может быть настроено из центрального местоположения. Следуйте инструкции:
  1. Перейдите к**Общие>Панель Инструментов**.
  2. Нажмите **Настройка Отслеживания Состояния**.

3. Отметьте флажки соответствующие элементам, которые вы хотите контролировать.

Для получения дополнительной информации перейдите к главе *«Панель управления»* (p. 99).

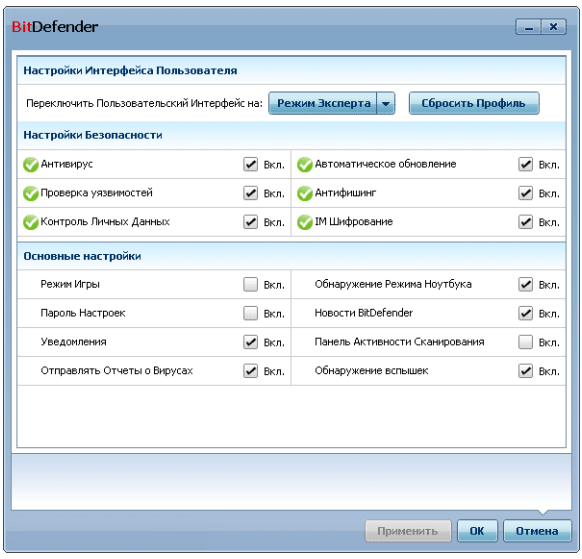
8. Настройка общих параметров

Вы можете настроить основные параметры продукта (в том числе изменить режим пользовательского интерфейса) из основного окна настроек. Чтобы открыть его, сделайте следующие:

- Откройте BitDefender и нажмите **Настройки** в верхнем правом углу окна.
- Щелкните правой кнопкой мыши на иконку BitDefender на панели задач и выбирите**Основные Настройки**.

Замечание

Для детального изменения настроек продукта используйте интерфейс Режима Опытного Пользователя. Для получения дополнительной информации перейдите к «Режим Опытного Пользователя» (p. 98) части руководства пользователя.



Основные настройки

Настройки организованы в три категории:

- Настройки Пользовательского Интерфейса
- Настройки Безопасности
- Основные Настройки

Чтобы применить и сохранить изменения в настройках, нажмите**OK**. Чтобы закрыть окно без сохранения изменений, нажмите**Cancel**.

8.1. Настройки Пользовательского Интерфейса

В этой области, вы можете переключить режим интерфейса пользователя и сбросить используемость профиля.

Переключение режима интерфейса пользователя. Как описано в разделе *«Режимы просмотра пользовательского интерфейса »* (p. 23),существует три режима отображения пользовательского интерфейса. Каждый режим пользовательского интерфейса предназначен для определенной категории пользователей, обусловленный их навыками работы с компьютером. Таким образом, существует пользовательский интерфейс для всех категорий пользователей, от начинающих до технически подготовленных.

Первая кнопка показывает Режим Интерфейса текущего пользователя. Для изменения режима пользовательского интерфейса, нажмите стрелку и выберите желаемый режим.

Режим	Описание
Режим Новичка	Подходит для начинающих. Этот режим является простым в использовании и требует минимального взаимодействия с вашей стороны. Все, что требуетя от вас, - устранить существующие проблемы, обнаруженные BitDefender. Пошаговый Мастер поможет вам в их решении. Кроме того, вы можете выполнять общие задачи, такие как обновления сигнатур вирусов и файлов продукта или сканирование компьютера.
Режим Пользователя	Предназначенный для пользователей со средними навыками работы на компьютере, это режим расширят возможности того, что вы можете сделать Режиме Новичка. Вы можете устранять проблемы по выбору и решать, какие вопросы контролировать. Более того, вы можете удаленно управлять продктами BitDefender, установленными на компьютерах в вашем доме.
Режим Опытного Пользователя	Режим подходит для технически подкованных пользователей и позволяет полностью настроить каждую функцию BitDefender. Вы можете также использовать все задачи, предусмотренные для защиты вашего компьютера и данных.

Сброс используемости профиля. Используемость профилей отражает основные действия выполняющиеся на компьютере. В зависимости от используемости профиля, интерфейс продукта организуется с целью обеспечения легкого доступа к нужным задачам.

Для перенастройки Используемости профиля, нажмите **Сбросить Используемость Профиля** и следуйте мастеру настроек.

8.2. Настройки Безопасности

В этой области, вы можете включить или отключить настройки продуктов, касающиеся различных аспектов компьютерной и информационной безопасности. При использовании одной из данных иконок указывается статус настроек:

Зеленый круг с галочкой: Настройка включена.

Красный кружок с восклицательным знаком: Настройка отключена.

Чтобы включить/отключить настройку, выбрать/очистить поставьте соответствующую галочку **Включить**.

Внимание

Будьте осторожны, когда отключаете постоянную защиту или автоматические обновление. Выключение этих функций может резко снизить безопасность компьютера. Если их действительно необходимо отключить, не забудьте включить их как можно скорее.

Весь список параметров и их описание приводится в следующей таблице:

Настройки	Описание
Антивирус	Защита файлов в режиме реального времени гарантирует их проверку при запуске вами или приложением, работающем в этой системе.
Автоматическое обновление	Автоматическое Обновление гарантирует, что новейшие продукты BitDefender и файлы сигнатур регулярно автоматически загружаются и устанавливаются.
Проверка Уязвимостей	Автоматическое сканирование на наличие уязвимостей обеспечивает обновление важного программного обеспечения на вашем компьютере.
Антифишинг	Защита от фишинга распознает страницу, созданную для кражи личной информации, и сообщает от этом пользователю.

Настройки	Описание
Контроль Конфиденциальных Данных	Контроль Конфиденцтальных Данных помогает предотвратить отправку ваших личных данных без вашего согласия. Он блокирует любые мгновенные сообщения, сообщения электронной почты или или другие формы передачи данных, которые передают данные, определенные как личные.
IM Шифрование	IM (Instant Messaging) шифрование защищает ваши разговоры через Yahoo! Messenger и Windows Live Messenger при условии, что ваши контакты используют совместимый продукт BitDefender и IM приложения.

Состояние некоторых из этих настроек может быть проконтролировано с помощью системы отслеживания проблем BitDefender. Если вы отключаете контролируемые настройки, BitDefender обозначит их, как проблему которую необходимо устранить.

Если вы не хотите что бы отключенные настройки отображались как проблемы, вы должны соответственно сконфигурировать систему отслеживания. Вы можете сделать это либо в Промежуточной Режиме, либо в Режиме Опытного Пользователя.

- В промежуточном Режиме, отслеживание системы можно настроить из отдельных местоположений, на основе категорий параметров. Для получения дополнительной информации перейдите к «Средний Уровень» (p. 75) части руководства пользователя.
- В Режиме Опытного Пользователя, отслеживание системы может быть настроено из центрального местоположения. Следуйте инструкции:
  1. Перейдите к**Общие>Панель Инструментов**.
  2. Нажмите **Настройка Отслеживания Состояния**.
  3. Отметьте галочкой соответствующие элементы, которые вы хотите отслеживать.

  Для получения дополнительной информации перейдите к главе *«Панель управления»* (p. 99).

8.3. Общие настройки

Здесь вы можете включить или отключить параметры, связанные с характеристиками продукта и опытом пользователя. Чтобы включить/отключить настройку, выбрать/очистить поставьте соответствующую галочку **Включить**.

Весь список параметров и их описание приводится в следующей таблице:

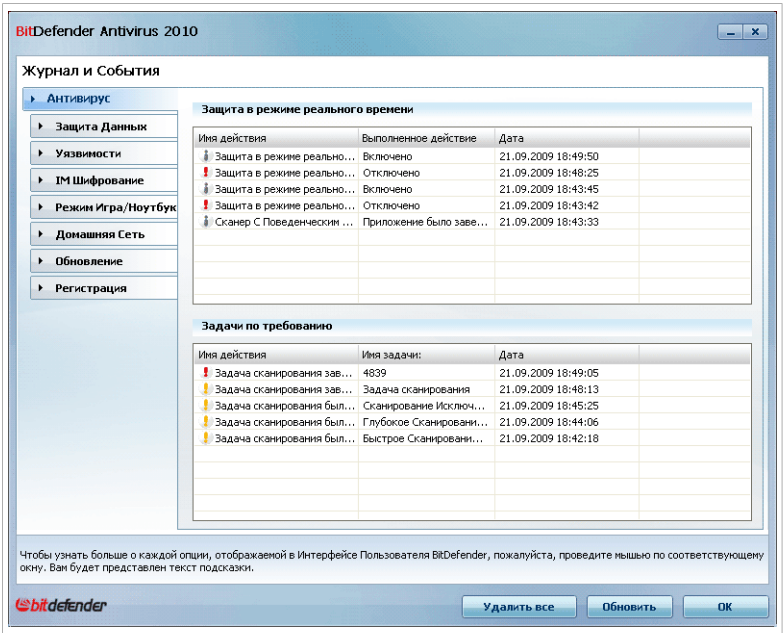
Настройки	Описание
Режим Игры	Режим Игры временно изменяет настройки защиты, чтобы минимизировать их влияние на деятельность системы во время игры.
Обнаружение Режима Ноутбука	Режим Ноутбука временно изменяет настройки защиты, чтобы минимизировать их влияние на длительность работы батареи вашего ноутбука.
Пароль настроек	Благодаря этому настройки BitDefender могут быть изменены только теми, кто знает этот пароль. Когда вы включите эту опцию, вам будет предложено установить пароль настроек. Введите пароль в оба поля и нажмите **OK** для его установки.
Новости BitDefender	Включив этот параметр, вы будете получать важные новости компании, обновления продукта и список новых угроз от BitDefender.
Сигналы Уведомлений Продукта	Включив этот параметр, вы будете получать информационные уведомления.
Панель Активности Сканирования	Панель активности сканирования - это мальенькое прозрачное окно, отображающее прогресс сканирования BitDefender. Для получения дополнительной информации перейдите к *«Панель Активности Сканирования»* (p. 32).
Отправлять отчеты о вирусах	Включение этого параметра обеспечивает отправку отчетов о сканировании на вирусы в лаборатории BitDefender для анализа. Обратите внимание, что эти отчеты не будут содержать конфиденциальных данных, таких как, например, ваше имя или IP-адрес, и они не будут использоваться в коммерческих целях.
Обнаружение 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.

9. Журнал и События

Ссылка **История** в нижней части главного окна BitDefender открывает другое окно с журналом событий 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.

Замечание

Ссылка доступна только в Промежуточном Режиме или Режиме Опытного Пользователя.



События

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

- **Антивирус**
- **Контроль конфиденциальных данных**
- **Уязвимости**
- **Шифрование IM**
- **Режим Игры/Режим Ноутбука**

- **Домашняя Сеть**
- **Обновление**
- **Регистрация**
- **Журнал**

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 него.

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

10. Регистрация и Мой Аккаунт

BitDefender Antivirus 2010 устанавливается с 30-дневным периодом пробного использования. Во время оценочного периода продукт полнофункционален и вы можете удостовериться в том, что он соответствует вашим ожиданиям. Заметьте, что после 15 дней пробного перида, продукт перестанет автоматически обновляться до тех пор, пока вы не создадите аккаунт. Создание учетной записи BitDefender - обязательная часть процесса регистрации.

До того как оценочный период истечет вы должны зарегистрировать продукт чтобы сохранить ваш компьютер защищенным. Регистрация состоит из двух шагов:

1. **Активация (регистрация аккаунта BitDefender).** Вы должны создать аккаунт BitDefender чтобы получать обновления и доступ к бесплатной техподдержке. Если у вас уже есть аккаунт BitDefender, зарегистрируйте ваш продукт в этом аккаунте. BitDefender сообщит, о необходимости активации и поможет решить этот вопрос.

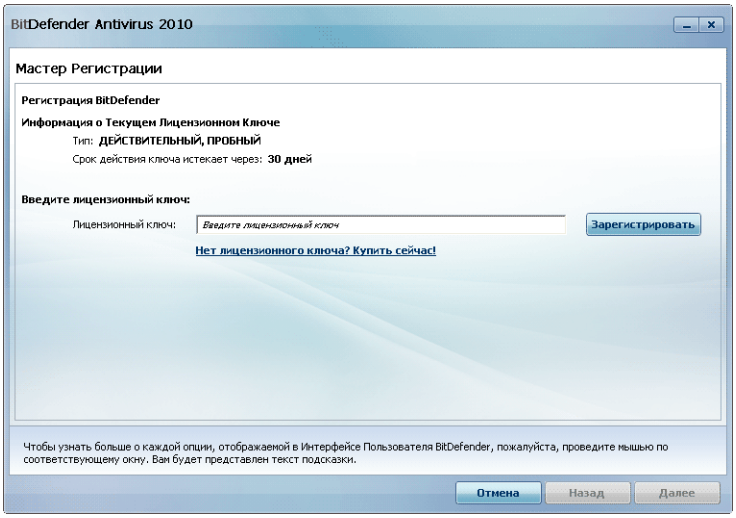
   Важно

   Вам необходимо создать аккаунт в течении 15 дней со дня установки BitDefender (если вы его зарегистрировали, срок пробного периода становится равным 30 дней). В противном случае, BitDefender не будет обновляться.

2. **Регистрация с лицензионным ключом.** Лицензионный ключ определяет как долго вы можете использовать продукт. Как только лицензионный ключ истек, BitDefender перестает защищать ваш компьютер. Вы должны зарегистрировать продукт, по истечении оценочного периода. Вам следует приобрести лицензионный ключ или продлить вашу лицензию за несколько дней истечения ключа.

10.1. Регистрация BitDefender Antivirus 2010

Если вы хотите зарегистрировать продукт с помощью лицензионного ключа или изменить существующий лицензионный ключ, нажмите ссылку **Зарегистрировать Сейчас**, расположенную в нижней части окна BitDefender. Появится окно 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 2010:

1. 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.

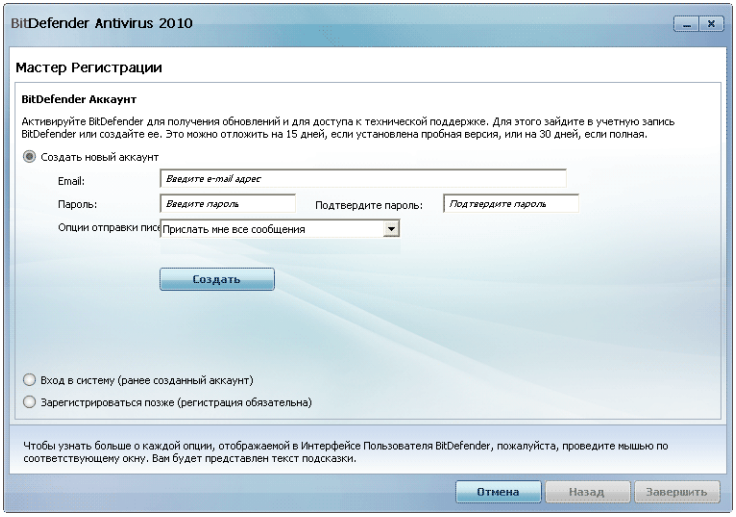
2. Нажмите **зарегистрировать Сейчас**.
3. Нажмите **Завершить**.

10.2. Активация BitDefender

Для Активации BitDefender, вы должны создать или войти в аккаунт BitDefender. Если вы не зарегистрировали аккаунт BitDefender в ходе первоначального мастера регистрации, сделайте как показано далее:

- В Режиме Новичка нажмите **Устранить Все Угрозы**. Этот мастер поможет вам устранить все ожидающие проблемы, включая активацию продукта.
- В Промежуточном режиме, перейдите к вкладке **Безопасность** и нажмите кнопку **Устранить** соответствующую вопросу активации продукта.
- В режиме Опытного пользователя, перейдите к **Регистрация** и нажмите кнопку **Активировать Продукт**.

Откроется окно регистрации аккаунта. Здесь вы можете создать или войти в аккаунт BitDefender, для активации вашего продукта.



Создание учетной записи

Если Вы не хотите создавать учетную запись BitDefender прямо сейчас, выберите **Зарегистрировать позже** и нажмите **Завершить**. В ином случае, действуйте исходя из вашей ситуации:

- «У меня нет учетной записи BitDefender» (p. 54)
- «У меня уже есть учетная запись BitDefender» (p. 54)

Важно

Вам необходимо создать аккаунт в течении 15 дней со дня установки BitDefender (если вы его зарегистрировали, срок пробного периода становится равным 30 дней). В противном случае, BitDefender не будет обновляться.

У меня нет учетной записи BitDefender

Для успешного создания аккаунта BitDefender, следуйте этим шагам:

1. Выберите **Создать новый аккаунт**.4564 messages remaining
2. Напечатайте необходимую информацию в соответствующих полях. Предоставленные Вами данные конфиденциальны.
   - **Адрес электронной почты** - введите адрес своей электронной почты.
   - **Пароль** - введите пароль Вашей учетной записи BitDefender. Пароль должен содержать не менее 6 и не более 16 символов.
   - **Повторите пароль** - снова введите набранный ранее пароль.

   Замечание

   После активации учетной записи, вы можете использовать имеющийся адрес электронной почты и пароль, чтобы войти в свой аккаунт на http://myaccount.bitdefender.com.

3. Дополнительно, BitDefender может информировать вас о специальных предложениях и поощрениях по электронной почте, указанной в вашей учетной записи. Выберите одну из доступных опций из меню:
   - **Отправлять мне все сообщения**
   - **Отправлять мне только сообщения, связанные с продуктом**
   - **Не отправлять мне сообщения**
4. Нажмите **Создать**.
5. Нажмите **Завершить** для завершения работы мастера.
6. **Активируйте ваш аккаунт.** Чтобы использовать аккаунт вы должны его активировать. Проверьте почту и следуйте инструкциям в письме, отправленном вам сервисом регистрации BitDefender.

У меня уже есть учетная запись BitDefender

BitDefender автоматически определит, если вы решистрировали учетную запись BitDefender ранее на этом компьютере. В этом случае, введите пароль от вашего аккаунта и нажмите **Вход в Систему**. Нажмите **Завершить** для завершения работы мастера.

Если у вас уже есть активный аккаунт, но BitDefender не может его обнаружить, следуйте этим шагам что бы привязать продукт к этому аккаунту:

1. Выберите **Вход в систему (ранее созданный аккаунт)**.
2. Напечатайте e-mail адрес и пароль вашего аккаунта в соответствующих полях.

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

3. Дополнительно, BitDefender может информировать вас о специальных предложениях и поощрениях по электронной почте, указанной в вашей учетной записи. Выберите одну из доступных опций из меню:
   - **Отправлять мне все сообщения**
   - **Отправлять мне только сообщения, связанные с продуктом**
   - **Не отправлять мне сообщения**
4. Нажмите **Вход в Систему**.
5. Нажмите **Завершить** для завершения работы мастера.

10.3. Покупка лицензионных ключей

Если оценочный период скоро завершается, вам стоит купить лицензионный ключ и зарегистрировать продукт. Откройте BitDefender и нажмите на кнопку **Купить/Обновить** в нижней части окна. Ссылка приведет вас на страницу, где вы сможете приобрести лицензионный ключ для BitDefender.

10.4. Обновление лицензии

Как клиент BitDefender вы имеете право на скидку на продление вашей лицензии. Вы также можете со скидкой или бесплатно обновить продукт до текущей версии.

Если ваш ключ скоро истекает, продлите лицензию. Откройте BitDefender и нажмите на кнопку **Купить/Обновить** в нижней части окна. Ссылка приведет вас на страницу, где вы сможете продлить лицензию.

11. Мастера

Чтобы облегчить использоваине BitDefender, несколько Мастеров помогут Вам выпольнить определенные задачи по обеспечению безопасности или изменить более сложные настройки продукта. Эта глава описывает мастеров, которые могут появиться при решении проблем ли выполнении определенных задач с BitDefender. Другие мастера настоек описаны отдельно в части «Режим Опытного Пользователя» (p. 98).

11.1. Мастер антивирусного сканирования

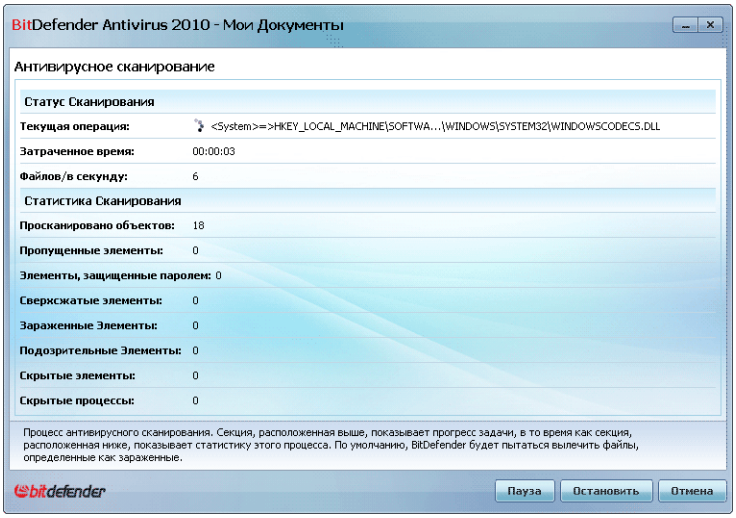
Когда бы вы не начали сканирование по требованию (к примеру, кликнув правой кнопкой мыши по папке и выбрав **Сканировать с помощью BitDefender**), появится мастер Антивирусного Сканера BitDefender. Чтобы завершить процесс проверки выполните последовательность из трех шагов.

Замечание

Если мастер сканирования не появился, возможно сканирование настроено проходить в тихом фоновом режиме. Найдите иконку состояния сканирования на панели задач. Вы можете кликнуть в эту иконку, чтобы открыть окно сканирования и наблюдать прогресс проверки.

11.1.1. 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.).

Дождитесь окончания сканирования BitDefender

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

Архивы, защищенные паролем. Если BitDefender во время сканирования найдет архив, защищенный паролем, и в качестве стандартного действия будет установлено **Запрашивать пароль**, то вам будет предложено ввести пароль. Защищенные паролем архивы нельзя сканировать, не предоставив пароль. Доступными являются следующие варианты:

- **Я хочу ввести пароль для этого объекта.** Если вы хотите чтобы BitDefender проверил архив, выберите эту опцию и введите пароль. Если вы не знаете пароля, выберите любую другую опцию.
- **Я не хочу вводить пароль (пропустить объект).** Выберите эту опцию, чтобы пропустить этот архив.
- **Я не хочу вводить пароль (пропустить все подобные объекты).** Выберите эту опцию если не хотите чтобы вас беспокоили по поводу

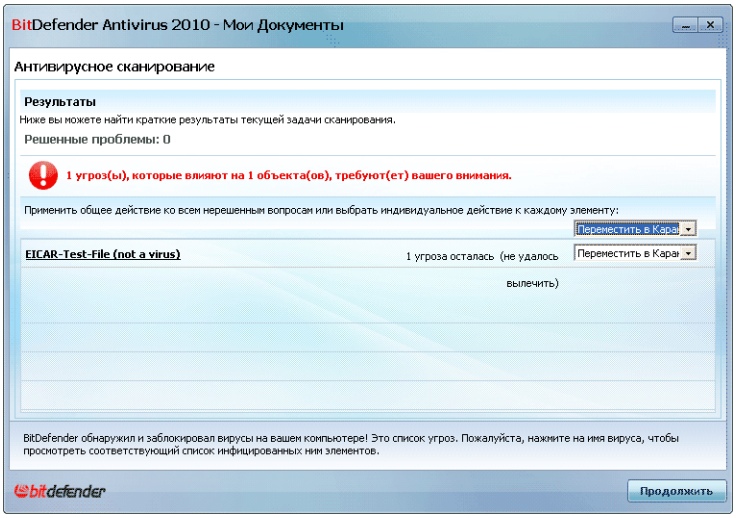
защищенных паролем архивов. BitDefender не будет иметь возможности сканировать их, но запись останется в журнале сканирования.

Для продолжения нажмите **OK**.

Останавливая или приостанавливая сканирование. Вы можете остановить процесс проверки в любое время, нажав **Стоп& Да**. При этом вы попадете на самый последний шаг мастера. Чтобы временно приостановить процесс проверки, нажмите **Пауза**. Чтобы продолжить проверку, нажмите **Возобновить**.

11.1.2. Шаг 2/3 - Выбор Действия

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



Действия

Вы можете просмотреть количество проблем, угрожающих безопасности Вашей системы.

Зараженные объекты разделены на группы в зависимости от типа 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.

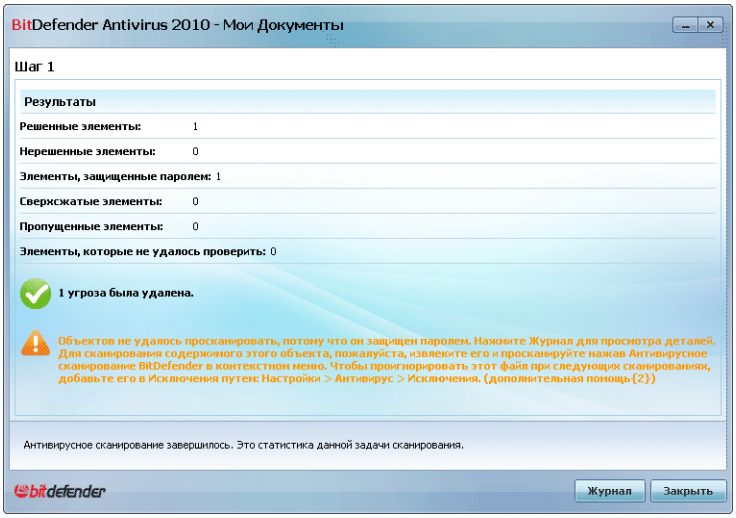
Одна или несколько из следующих опций может появиться в меню:

Действие	Описание
Ничего не делать	Над обнаруженными файлами не будет производиться никаких действий. После завершения сканирования вы можете открыть отчет о проверке, чтобы просмотреть сведения об этих файлах.
Вылечить	Удаляет вредоносный код из инфицированных файлов.
Удалить	Удаление обнаруженных файлов.
Переместить в карантин	Зараженные файлы перемещаются в Карантин. Добавленные в карантин файлы нельзя выполнять или открывать; таким образом, риск заражения сводится к нулю.
Переименовать файлы	Изменяет имена скрытых файлов, добавляя в конце имени `.bd.ren`. В результате у вас будет возможность искать подобные файлы на вашем компьютере. Обратите внимание, что эти скрытые файлы - не те файлы, которые вы сознательно скрываете от Windows. Это файлы, спрятнные особыми программами - руткитами. Сами по себе руткиты не вредны. Но они часто используются для того, чтобы сделать вирусы невидимыми для обычных антивирусных программ.

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

11.1.3. Шаг 3/3 - Просмотр результатов

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



Резюме

Здесь Вы можете просмотреть краткий обзор. Если вас интересует подробная информация о процессе сканирования, нажмите **Показать журнал**.

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.

BitDefender обнаружил 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.

11.2. Мастер Пользовательского Сканирования

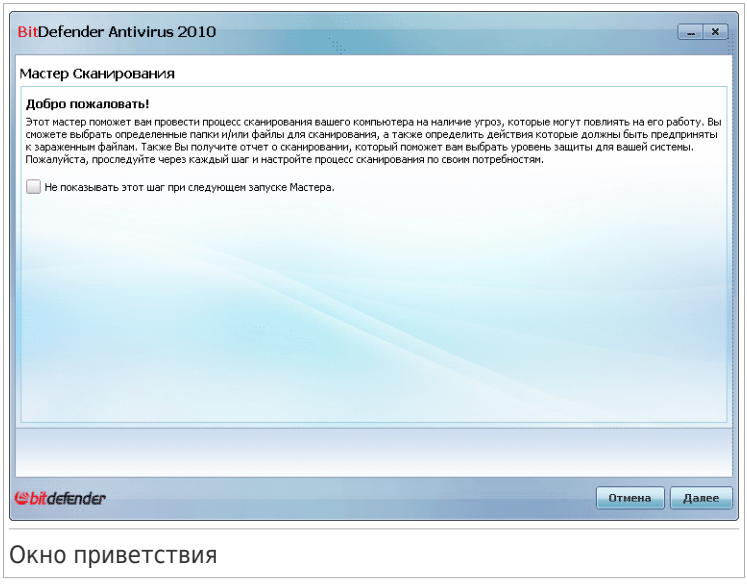
Мастер Пользовательского Сканирования позволяет вам создать и запустить пользовательскую задачу по сканированию и по желанию сохранить ее в качестве Быстрой Задачи при использовании в BitDefender среднем режиме.

Чтобы запустить пользовательскую задачу по сканированию с использованием Мастера Пользовательского Сканирования, следуйте инструкции:

1. В промежуточном режиме, перейдите к вкладке **Антивирус**.
2. В области Быстрых Задач, нажмите **Пользовательское Сканирование**.
3. Чтобы завершить процесс проверки выполните последовательность из шести шагов.

11.2.1. Шаг 1/6 - Экран приветствия

Это окно приветствия.



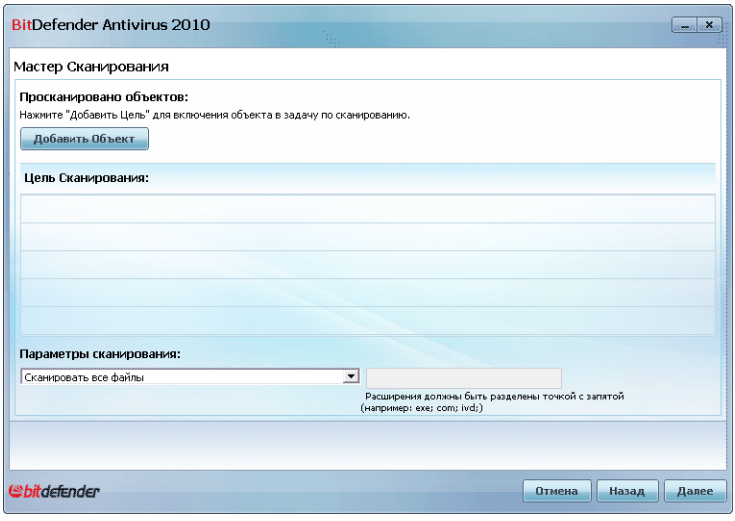
Окно приветствия

Если хотите пропустить это окно при запуске мастера в будущем, выберите **Не показывать это шаг при следующем запуске мастера**.

Щелкните **Далее**.

11.2.2. Шаг 2/6 - Выберите Цель

Здесь вы можете указать файлы или папки для сканирования, а также опции сканирования.



Выбор цели

Нажмите **Добавить Объект**,выберите файл или папку, которую вы хотите добавить, и нажмите **OK**. Путь к выбранной директории появится в колонке **Сканировать Объект**. Если вы передумали насчет пути, нажмите кнопку **Удалить**, которая находится рядом. Нажмите кнопку **Удалить Все**, для удаления всех местоположений добавленных в список.

Посте выбора местоположения, выберите **Опции Сканирования**. Доступны следующие:

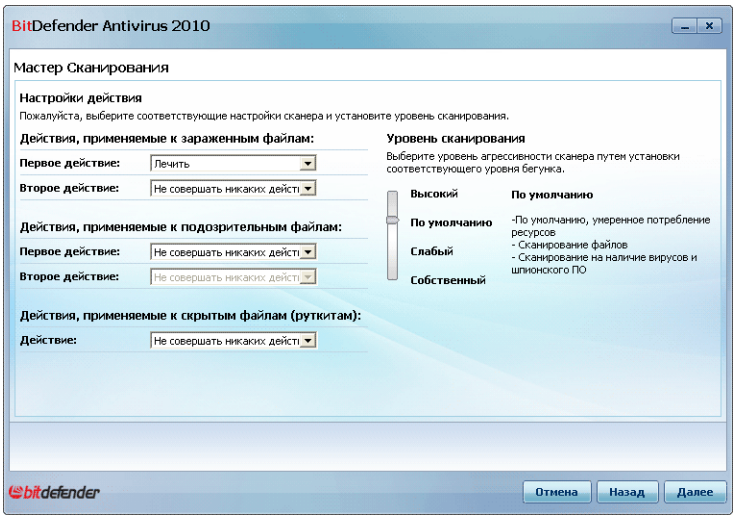
Настройка	Описание
Проверить все файлы	Выберите эту опцию для сканирования всех файлов в выбранных папках.
Сканировать файлы только с расширением приложения	Проверяются только файлы программ, то есть файлы с расширением: `.exe`; `.bat`; `.com`; `.dll`; `.ocx`; `.scr`; `.bin`; `.dat`; `.386`; `.vxd`; `.sys`; `.wdm`; `.cla`; `.class`; `.ovl`; `.ole`; `.exe`; `.hlp`; `.doc`; `.dot`;

Настройка	Описание
	.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 только файлы с расширениями, заданными пользователем	Проверяются только файлы с заданным расширением. Задаваемые расширения разделяются знаком ";".

Щелкните **Далее**.

11.2.3. Шаг 3/6 - Выберите Действия

Здесь вы можете задать параметры сканирования и уровень проверки.



Выберите Действия

- Выбрерите действия, которые будут применены по отношению к зараженным и подозрительным файлам. Доступными являются следующие варианты:

Действие	Описание
Ничего не делать	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 скрытым объектам (руткитам). Доступными являются следующие варианты:

Действие	Описание
Ничего не делать	Не выполняются никакие действия со скрытыми файлами. Названия этих файлов появятся в файле отчета.
Переименовать	Изменяет имена скрытых файлов, добавляя в конце имени `.bd.ren`. В результате у вас будет возможность искать подобные файлы на вашем компьютере.

- Настройка агрессивности сканирования. Есть 3 уровня на выбор. Передвиньте бегунок по шкале, чтобы установить соответствующий уровень защиты:

Уровень сканирования	Описание
Разрешающий	Сканируются только файлы приложений и только на вирусы. Уровень потребления ресурсов является низким.
По умолчанию	Уровень потребления ресурсов средний. Все файлы сканируются на вирусы и программы-шпионы.
Агрессивный	Все файлы (включая архивы) сканируются на наличие вирусов и шпионского ПО. Скрытые файлы и процессы включены в проверку, уровень потребления ресурсов выше.

Опытные пользователи, возможно, захотят воспользоваться предложенными настройками сканирования BitDefender. Сканер может быть установлен только для поиска вредоносных программ. Это может значительно сократить время сканирования и улучшить чувствительность компьютера во время сканирования.

Перетащите бегунок на **Пользовательский** и нажмите **Пользовательский Уровень**. Появится новое окно. Укажите тип вредоносных программ, сканируемых BitDefender, выбрав соответствующую опцию:

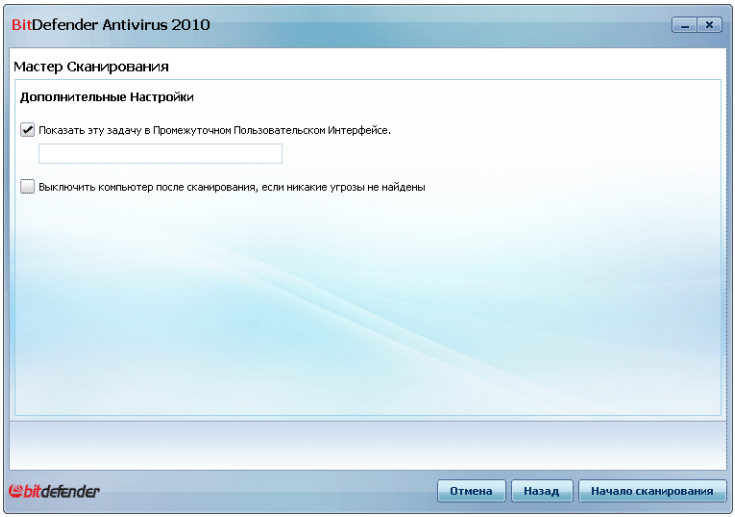
Настройка	Описание
Проверка на вирусы	Сканирование на известные вирусы. BitDefender также обнаруживает неполные или поврежденные тела вирусов, удаляя любую потенциально опасную угрозу безопасности Вашей системы.
Проверка на вредоносное рекламное ПО	Проверка на вредоносное рекламное ПО. Эти файлы будут считаться зараженными. Программное обеспечение, которое включает 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.
Сканировать на наличие приложения	Сканирование допустимых приложений, которые могут быть использованы как инструмент злоумышленника с целью скрытия вредоносного ПО или с другим злым умыслом.
Проверка 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.
Сканировать на наличие на клавиатурных шпионов	Сканирует на наличие вредоносного приложения, записывающего нажатия клавиш.

Нажмите **OK** и закройте окно.

Щелкните **Далее**.

11.2.4. Step 4/6 - Дополнительные настройки

Доступны дополнительные настройки сканирования:



Дополнительные Настройки

- Чтобы сохранить пользовательские задачи, создннные для использования в будущем, выберите **Показать эту задачу в Промежуточном Интерфейсе Пользователя** и введите имя этой задачи в соответствующем поле редактирования.

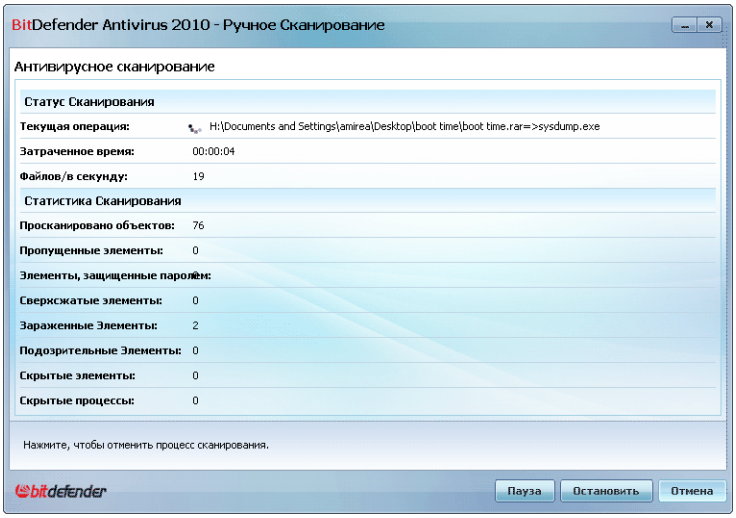
  Задача будет добавлена в список Быстрых задач уже доступных во вкладке безопасности и так же появится в **Режиме опытного пользователя > Антивирусе > Сканировании вирусов**.

- Для выключения компьютера по завершению сканирования, выберите **Выключить компьютер по завершению сканирования, если угрозы не обнаружены**

Нажмите **Начать Сканирование**.

11.2.5. Шаг 5/6 - Сканирование

BitDefender начнет проверку выбранных объектов:



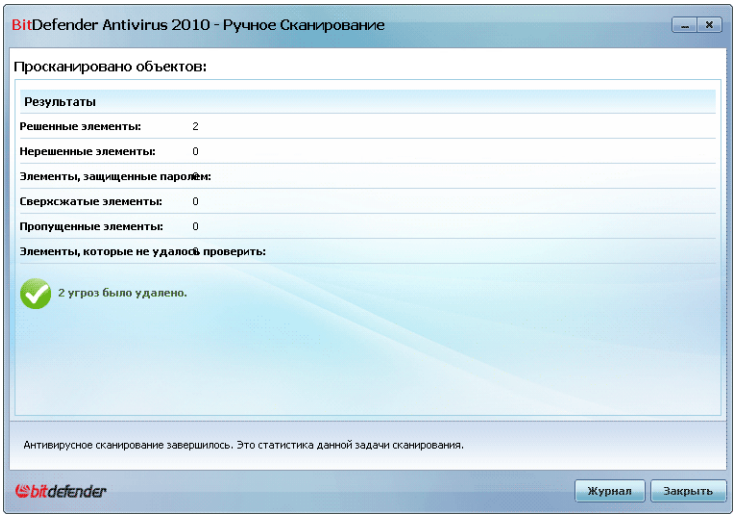
Сканирование

Замечание

В зависимости от сложности задач проверки, процесс сканирования может занять некоторое время. Можете нажать иконку хода сканирования в панели задач, чтобы открыть окно сканирования и увидеть процесс.

11.2.6. Шаг 6/6 - Просмотр результатов

По завершению BitDefender процесса сканирования, результаты сканирования будут отображаться в новом окне:



Резюме

Вы можете проверить результаты сканирования. Если вас интересует подробная информация о процессе сканирования, нажмите **Показать журнал**.

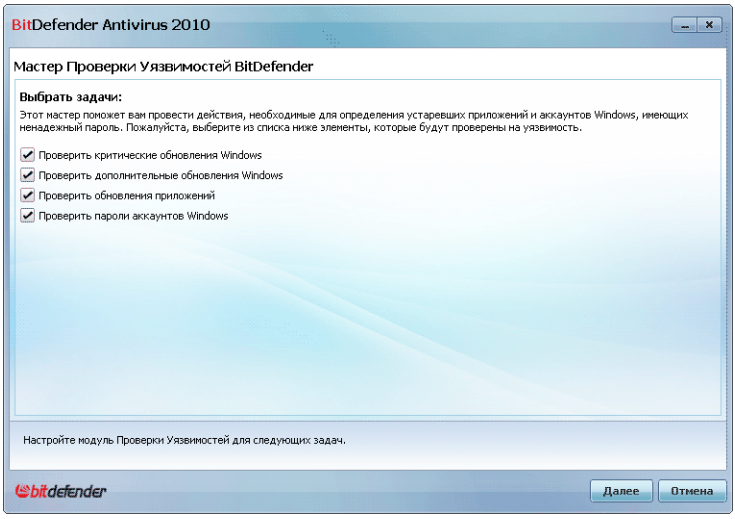
Важно
Если потребуется, перезагрузите Вашу систему для завершения процесса очистки.

Нажмите **Закрыть**, чтобы закрыть окно.

11.3. Мастер Проверки на Наличие Уязвимостей

этот мастер проверяет систему на наличие уязвимостей и помогает устранить их.

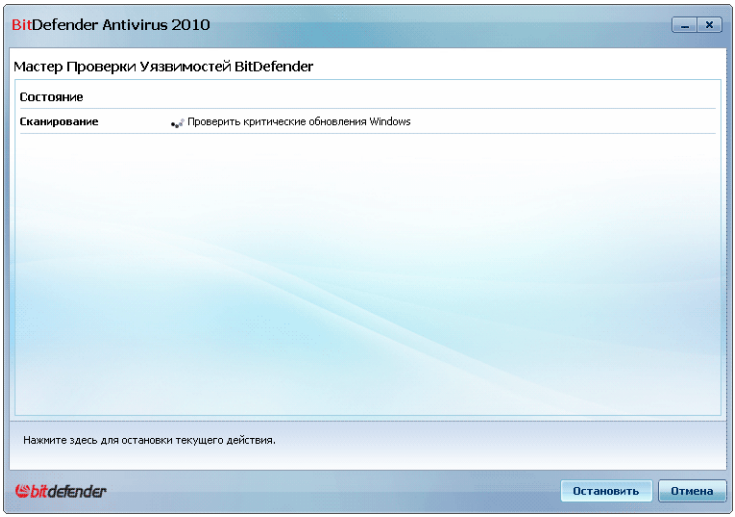
11.3.1. Шаг 1/6 - Выберите уязвимости для проверки



Уязвимости

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

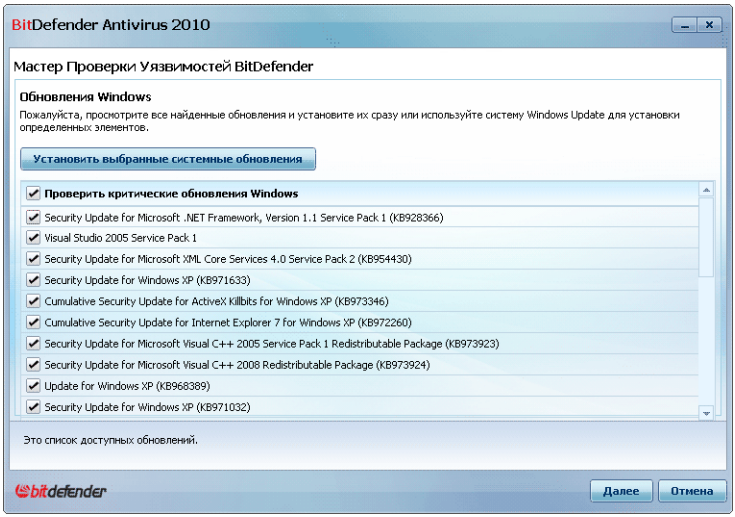
11.3.2. Шаг 2/6 - Проверка уязвимостей



Проверка уязвимостей

Подождите, пока BitDefender завершит проверку уязвимостей.

11.3.3. Шаг 3/6 - Обновление Windows

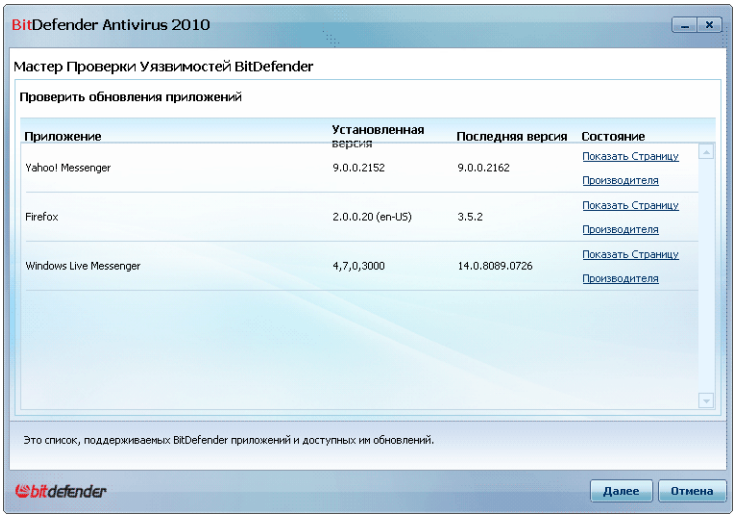


Обновления Windows

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

Щелкните **Далее**.

11.3.4. Шаг 4/6 - Обновление приложений

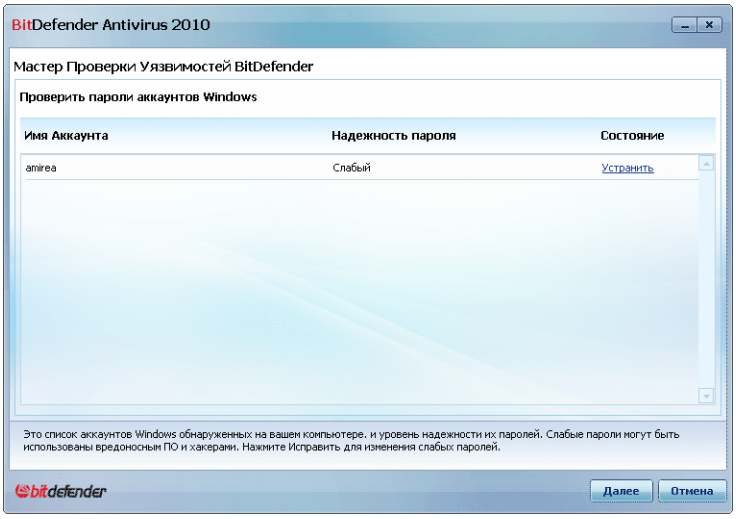


Приложения

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 **Далее**.

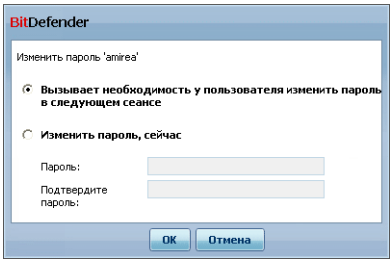
11.3.5. Шаг 5/6 - Смена слабых паролей



Пользовательские пароли

Вы можете просмотреть список учетных записей пользователей Windows, установленных на вашем компьютере, и уровень защиты, обеспечиваемый их паролями. Пароль может быть **сложным** (его трудно подобрать) или **простым** (не устойчив к взлому).

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



Изменить пароль

Выберите метод устранения проблемы:

- **Заставить пользователя изменить пароль при следующем всоде в систему.** BitDefender выведет запрос на смену пароля в при следующем входе в Windows.
- **Изменить пароль.** Необходимо ввести пароль в поля ввода. Удостоверьтесь, что пользователь знает о смене пароля.

Замечание

Чтобы получить сильный пароль, используйте комбинации символов в верхнем и нижнем регистре, числа и специальные символы (такие как, например, #, $ или @). Вы можете поискать в интернете способы создания сложных паролей.

Нажмите **OK**, чтобы сменить пароль.

Щелкните **Далее**.

11.3.6. Шаг 6/6 - Просмотр результатов

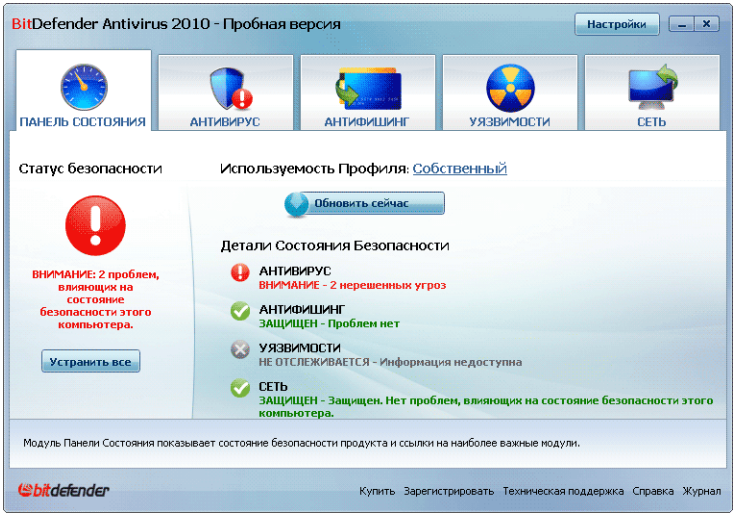
Результаты

Нажмите **Закрыть**.

Средний Уровень

12. Панель управления

Вкладка Панель Инструментов содержит информацию о состоянии безопасности компьютера и позволяет вам устранить нерешенные проблемы.



Панель управления

Панель Управления состоит из следующих разделов:

- **Общее состояние** - Сообщает о наличии угроз безопасности компьютера и помогает решить их. При наличии текущих проблем вы увидите **красный круг с восклицательным знаком** и кнопку **Устранить Все Угрозы** button. Нажмите Устранить Все Угрозы, чтобы запустить мастер.
- **Детали ССостояния Безопасности** - Показывает состояние каждого основного модуля, используя описание и иконки:

  Зеленый круг с галочкой: Угроз безопасности нет. Ваш компьютер и данные защищены.

  Серый кружок с восклицательным знаком: Активность компонентов модуля, не контролируется. Таким образом, отсутствует информация относительно их статуса безопасности. С этим модулем могут быть связаны некоторые вопросы.

  Красный кружок с восклицательным знаком: Существуют проблемы, угрожающие безопсности вашей системы. Критические вопросы требуют

вашего немедленного внимания. Не критические вопросы также должны быть решены в кратчайшие сроки.

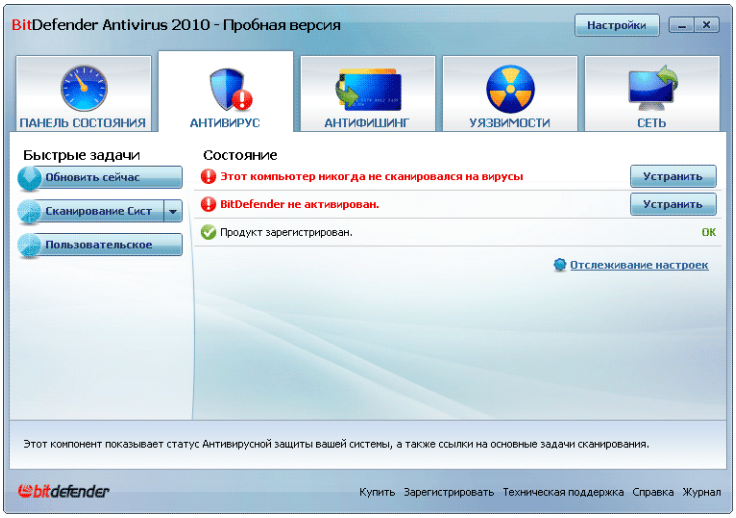
Нажмите на название модуля, чтобы увидеть более подробную информацию о его состоянии , и чтобы настроить отлеживание статуса его компонентов.

- **Используемость Профиля** - показывает используемый в данный момент пользовательский профиль и предлагает соответствующую ссылку на данный профиль:
  - Когда выбран **Обычный** профиль, кнопка **Сканировать Сейчас** позволяет выполнить Сканирование Системы с использованием Мастера Сканирования на Антивирусы. За исключением архивов, вся система будет просканирована. По умолчанию, систма проверяется на все типы вредоносного ПО,кроме руткитов.
  - При выборе профиля**Геймер**, кнопка **Включить /Выключить Режи Игры** позволяет вам включить/выключаитьРежим Игры. Режим Игры изменяет параметры настроек системы защиты для того, чтобы снизить к минимуму воздействие на компьютер во время игры.
  - Когда выбран профиль **Пользовательский** , кнопка **Обновить Сейчас** запускает немедленное обновление. Откроется новое окно, где Вы можете увидеть результаты проверки.

  Если вы хотите переключиться на другой профиль или редактировать текущий, нажмите на профиль и следуйте Мастеру настроек.

13. 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 моуль состоит из двух разделов:

- **Область Состояния** - отображает текущее состояние всех контролируемых компонентов безопасности и позволяет вам выбрать какие компоненты следует контролировать.
- **Быстрые Задачи** - здесь вы можете найти ссылки на наиболее важные задачи безопасности: обновление, сканирование системы, сканирование документов, глубокое сканирование, пользовательское сканирование, сканирование на наличие уязвимостей.

13.1. Область Состояния

Область состояния - область, где вы можете увидеть полный список компонентов модуля безопасности и их текущий статус. Путем мониторинга каждого модуля защиты, BitDefender проинформарует вас не только тогда, когда вы изменяете параметры, способные повлиять на безопасность вашего компьютера, но и когда вы забудете сделать важные задачи.

Текущее состояние компонента определяется описанием и одним из следующих значков:

Зеленый круг с галочкой: Угроз нет.

Красный кружок с восклицательным знаком: Существуют угрозы.

Описания выделены красным цветом. Просто нажмите на соответствующую кнопку **Устранить**, чтобы устранить проблему. Если проблему не удается решить сразу же, то выполните все действия мастера, чтобы исправить данную проблему.

13.1.1. Настройка Статуса Отслеживания

Для выбора компонентов для проверки BitDefender нажмите **Настройка Отслеживания Состояния** , поставьте галочку **Включить сигналы** рядом с соответствующими функциями, которые требуется отследить.

Важно

Чтобы убедиться, что система полностью защищена, включите отслеживание всех компонентов и устраните все обнаруженные угрозы.

BitDefender может отследить статус следующих компонентов безопасности:

- **Антивирус** - BitDefender контролирует состояние двух компонентов Антивирусного модуля: защита в реальном времени и сканирование по запросу. Наиболее распространенные отчеты по проблемам этого компонента, приведенные в следующей таблице.

Проблема	Описание
Защита в режиме реального времени выключена	Документы не проверяются при запуске вами или приложением, работающим в вашей системе.
Этот ПК никогда не сканировался на наличие вирусов	Сканирование системы по требованию для проверки файлов, хранящихся на Вашем компьютере, никогда не производилось.
Постедняя проверка системы была отменена до ее завершения	Полная проверка системы была запущена, но не была закончена.
Состояние Антивируса критическое	Защита системы в реальном времени отключена, требуется проверка системы.

- **Обновить** - BitDefender проверяет статус обновления вирусных сигнатур. Наиболее распространенные отчеты по проблемам этого компонента, приведенные в следующей таблице.

Проблема	Описание
Автоматическое обновление выключено	Вирусные сигнатуры BitDefender не обновляются регулярно.
Обновление не производилось x дней	Вирусные сигнатуры BitDefender устарели.

13.2. Быстрые задачи

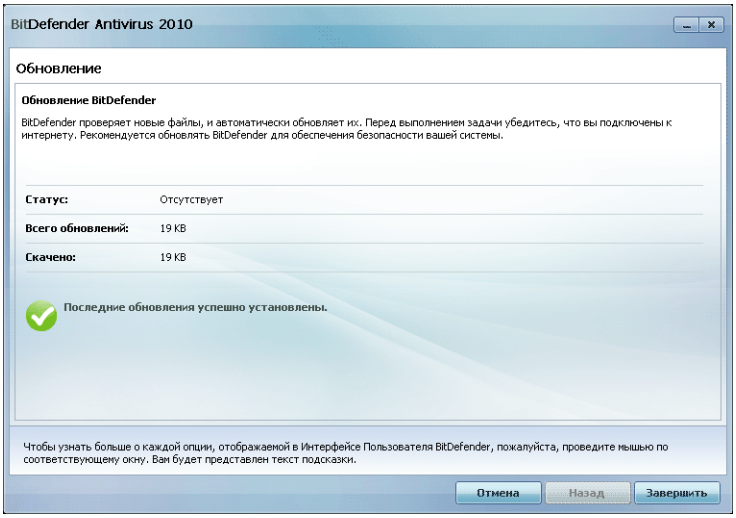
Здесь вы можете найти ссылки на наиважнейшие задачи безопасности:

- **Обновить сейчас** - запускает немедленное обновление.
- **Сканирование Системы** - запускает стандартное сканирование вашей системы (архивы исключены). Для дополнительных задач сканирования по требованию, нажмите стрелку на этой кнопке и выберите другую задачу сканирования: Сканирование Моих Документов или Глубокое Сканирование Системы.
- **Пользовательское сканирование** - запускает мастера, который поможет вам создать и запустить пользовательскую задачу.

13.2.1. Обновление BitDefender

Каждый день появляются и обнаруживаются все новые вредоносные программы. Вот почему так важно постоянно обновлять вирусные сигнатурные Bitdefender в соответствии с 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 запросу.

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.

13.2.2. Сканирование с помощью BitDefender

Чтобы проверить компьютер на наличие вредоносных программ, выполните определенную задачу по сканированию, нажав на соответствующую кнопку

или выбрав ее из выпадающего меню. Данная таблица содержит список задач сканирования с их описанием:

Задача	Описание
Сканирование Системы	Проверка всей системы кроме архивов. В настройках по умолчанию проводится проверка на все типы вирусного ПО, кроме руткитов.
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.
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.
Пользовательское Сканирование	Используйте эту задачу, чтобы выбрать конкретные файлы и папки, которые будут сканироваться.

Замечание

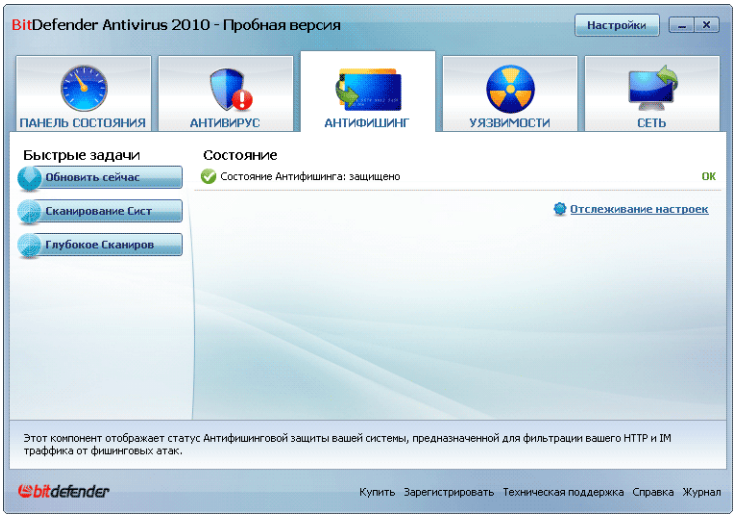
Поскольку задания **Глубокая проверка системы** и **Проверка системы** проводят анализ всей системы, их выполнение может занять определенный промежуток времени. Поэтому, рекомендуем выполнять эти задачи с небольшим приоритетом, либо когда система не используется.

При запуске проверки системы, глубокого сканирования системы или сканирования папки "Мои документы", появится мастер Антивирусного Сканирования. Чтобы завершить процесс проверки выполните последовательность из трех шагов. Для получения дополнительной информации перейдите к *«Мастер антивирусного сканирования»* (p. 56).

При выполнении выборочной проверки, мастер Пользовательского Сканирования проведет вас через процесс сканирования. Следуйте инструкции из шести этапов для проверки отдельных файлов или папок. Для получения дополнительной информации перейдите к *«Мастер Пользовательского Сканирования»* (p. 61).

14. 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:

- **Область Состояния** - DOотображает текущее состояние модуля антифишинга и позволяет вам включить/отключить отслеживание активности данного модуля.
- **Быстрые Задачи** - Здесь вы найдете ссылки на наиболее важные задачи безопасности: сканирование системы, глубокое сканирование, обновление.

14.1. Область Состояния

Текущее состояние компонента определяется описанием и одним из следующих значков:

Зеленый круг с галочкой: Угроз нет.
Красный кружок с восклицательным знаком: Существуют угрозы.

Описания выделены красным цветом. Просто нажмите на соответствующую кнопку **Устранить**, чтобы устранить проблему.

Наиболее общая проблема для этого модуля это **Антифишинг Отключен**. Это значит, что антифишинг отключен для следующих приложений: Internet Explorer, Mozilla Firefox, Yahoo! Messenger или Windows Live Messenger.

14.2. Быстрые задачи

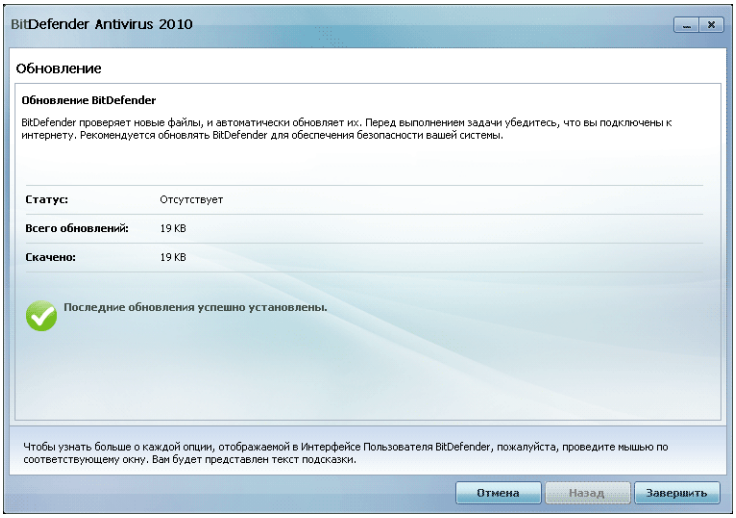
Здесь вы можете найти ссылки на наиважнейшие задачи безопасности:

- **Обновить сейчас** - запускает немедленное обновление.
- **Сканирование Системы** - запускает полное сканирование компьютера (исключая архивы).
- **Глубокое Сканирование Системы** - запускает полное сканирование вашего компьютера (включая архивы).

14.2.1. Обновление BitDefender

Каждый день появляются и обнаруживаются все новые вредоносные программы. Вот почему так важно постоянно обновлять вирусные сигнатурные Bitdefender в соответствии с 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 запросу.

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.

14.2.2. Сканирование с помощью BitDefender

Чтобы проверить компьютер на наличие вредоносных программ, выполните определенную задачу по сканированию, нажав на соответствующую кнопку

или выбрав ее из выпадающего меню. Данная таблица содержит список задач сканирования с их описанием:

Задача	Описание
Сканирование Системы	Проверка всей системы кроме архивов. В настройках по умолчанию проводится проверка на все типы вирусного ПО, кроме руткитов.
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.

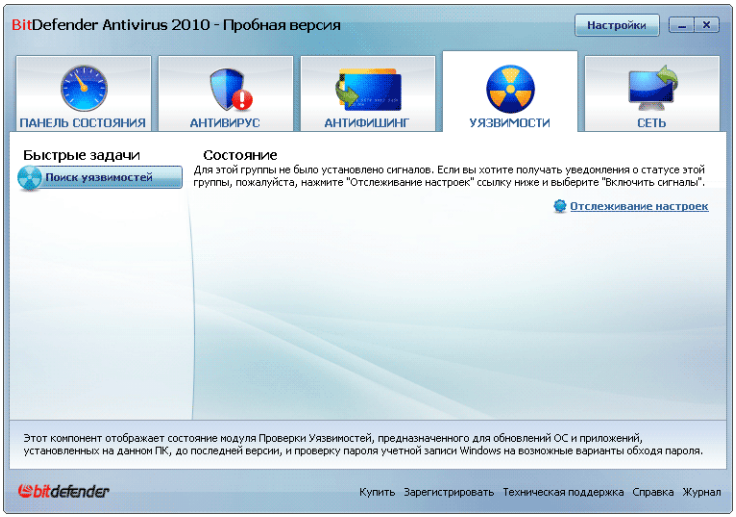
Замечание

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

При запуске Сканирования Системы или Глубокого Сканирования Системы появится Мастер Антивирусного Сканирования. Чтобы завершить процесс проверки выполните последовательность из трех шагов. Для получения дополнительной информации перейдите к *«Мастер антивирусного сканирования»* (p. 56).

15. 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:

- **Область состояния** -Отображает состояние модуля Проверки на наличие Уязвимостей и позволяет вам включить/отключить отслеживание активности данного модуля.
- **Быстрые Задачи** - здесь вы можете найти ссылки на мастера проверки на уязвимости.

15.1. Область Состояния

Текущее состояние компонента определяется описанием и одним из следующих значков:

Зеленый круг с галочкой: Угроз нет.
Красный кружок с восклицательным знаком: Существуют угрозы.

Описания выделены красным цветом. Просто нажмите кнопку **Устранить** или **Установить** соответствующую решению указанной проблемы.

Наиболее распространенные отчеты по проблемам этого компонента, приведенные в следующей таблице.

Состояние	Описание
Проверка на Уязвимости отключена	BitDefender не проводит проверку на возможные уязвимости в отношении отсутствующих обновлений Windows, обновлений приложений, слабых паролей.
Были обнаружены множественные уязвимости	BitDefender обнаружил отсутствие обновлений Windows/приложений и слабые пароли.
Критичные обновления Microsoft	Критические обновления Microsoft обнаружены, но не установлены.
Другие обновления Microsoft	Не критические обновления Microsoft доступны, но не установлены.
Автоматические обновления Windows отключены	Обновления безопасности Windows устанавливаются автоматически по мере доступности.
Приложение (устарело)	Новая версия Приложения доступна, но не установлена.
Пользователь (Слабый пароль)	Пароль пользователя легко взламывается людьми, имеющими специальное программное обеспечение.

15.2. Быстрые задачи

Доступно только одно задание:

- **Сканирование уязвимостей** - запускает мастер, который проверит вашу систему на наличие уязвимостей и поможет их устранить.

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.

Для проверки компьютера на уязвимости, нашмите **Проверка на уязвимости** и далее следуйте «*Мастер Проверки на Наличие Уязвимостей*» (p. 68).

16. Сеть

Модуль Домашняя Сеть позволяет управлять обновлениями BitDefender, установленными на ваших домашних компьютерах, с одного компьютера. Чтобы открыть Сетевой модуль, нажмите вкладку **Сеть**.

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. Подключите каждый компьютер, которым вы хотите управлять, к сети (установите пароль).
3. Вернитесь к своему компьютеру и добавьте те компьютеры, которыми вы хотите управлять.

16.1. Быстрые задачи

В самом начале доступна только одна кнопка.

- **Включить Сеть** - Установка сетевого пароля, таким образом создавая и присоединяясь к сети.

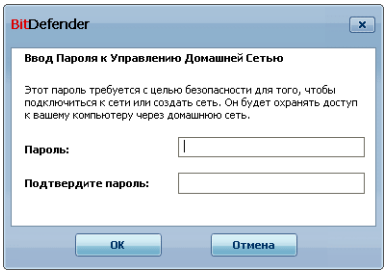
После входа в сеть появятся еще несколько кнопок.

- **Выход из сети** - позволяет выйти из сети.
- **Добавить компьютер** - 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.

16.1.1. Подключение к сети BitDefender

Чтобы подключиться к домашней сети BitDefender, выполните следующую процедуру:

1. Нажмите **Управление Сетью**. Появится окно настройки пароля для управления домашней сетью.



Настройка пароля

2. Введите пароль в каждом из полей ввода.
3. Нажмите **OK**.

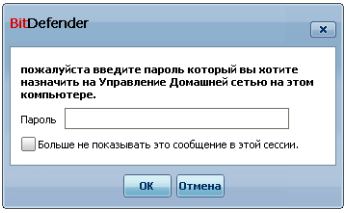
На карте сети будет отображаться имя компьютера.

16.1.2. Добавление компьютеров в сеть BitDefender.

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

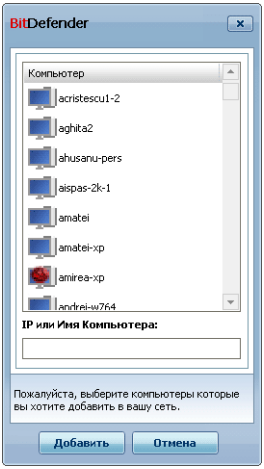
Чтобы добавить компьютер в домашнюю сеть BitDefender, выполните следующую процедуру:

1. Нажмите **Добавить Компьютер**. Появится окно ввода пароля для управления домашней 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. Значок имеют следующее значение:

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

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

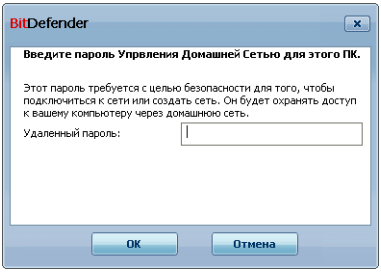
Указывает на автономный компьютер, на котором установлен BitDefender.

3. Выполните одно из следующих действий:

- 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.



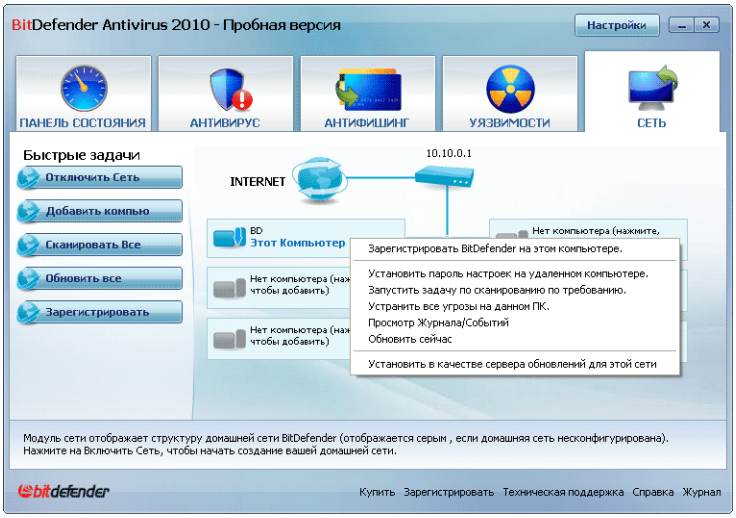
Авторизация

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

Замечание
Вы можете добавить до пяти компьютеров на карту сети.

16.1.3. 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 административных задач, которые можно запустить на удаленном компьютере.

- **Удалить ПК из домашней сети**

  Позволяет удалить ПК из сети.

- **Зарегистрировать BitDefender на этом компьютере**

  Позволяет зарегистрировать BitDefender на этом компьютере, с помощью лицензионного ключа.

- **Установить пароль настроек на удаленном ПК**

  Позволяет создать пароль для ограничения доступа к настройкам BitDefender на этом компьютере.

- **Запустить задачу сканирования по запросу**

  Позволяет запустить сканирование по требованию, на удаленном компьютере. Вы можете выполнить любую из следующих задач сканирования: Сканирование Моих Документов, Системное Сканирование или Глубокое Системное Сканирование.

- **Устранить все проблемы на этом ПК**

  Позволяет исправить проблемы, влияющие на безопасность этого компьютера следуя мастеру Устранить все угрозы

- **Простотр Журнала/Событий**

  Позволяет получить доступ к **Истории&Событий** модуля продукта BitDefender, установленного на этом компьютере.

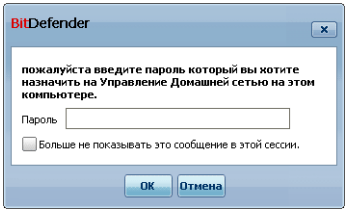
- **Обновить сейчас**

  Инициирует процесс обновления для продукта BitDefender, установленном на этом компьютере.

- **Назначить сервером обновлений этой сети**

  Позволяет установить этот компьютер, как сервер обновлений для всех продуктов BitDefender, установленных на компьютерах в сети. Использование этой опции позволит снизить интернет-трафик, потому что только один компьютер в сети будет подключаться к интернету для загрузки обновлений.

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



Введите пароль

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

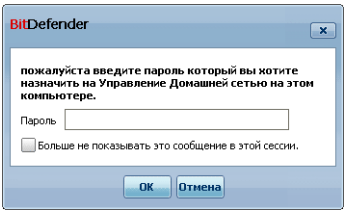
Замечание

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.

16.1.4. Сканирование всех компьютеров

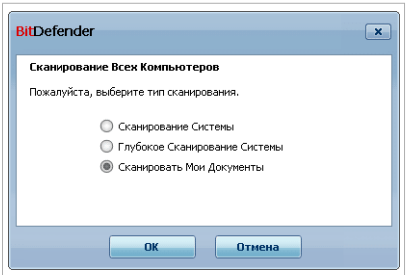
Для сканирования всех управляемых компьютеров выполните следующую процедуру:

1. Нажмите **Сканировать Все**. Появится окно ввода пароля для управления домашней сетью.



Введите пароль

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



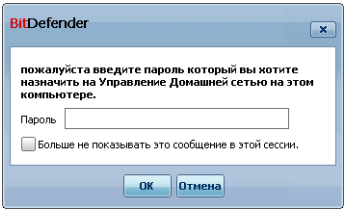
Выберите тип сканирования

3. Нажмите **OK**.

16.1.5. Обновление всех компьютеров

Для обновления всех управляемых компьютеров выполните следующую процедуру:

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



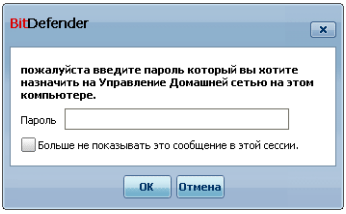
Введите пароль

2. Нажмите **OK**.

16.1.6. Регистрация всех компьютеров

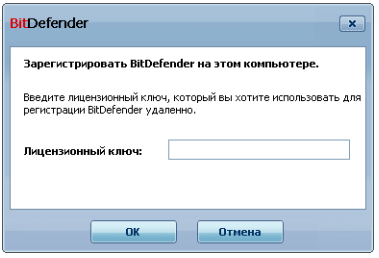
Для регистрации всех управляемых компьютеров выполните следующую процедуру:

1. Нажмите **Зарегистрировать Все**. Появится окно ввода пароля для управления домашней сетью.



Введите пароль

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



Регистрация

3. Нажмите **OK**.

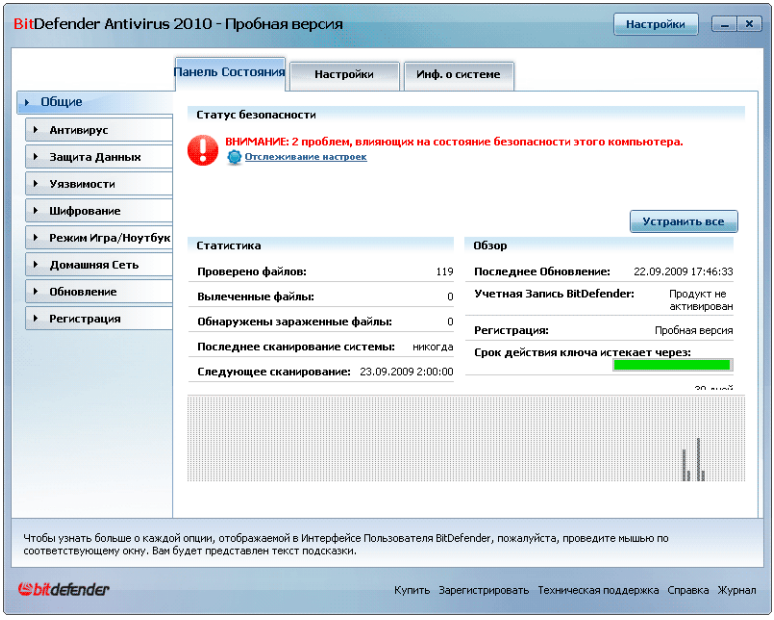
Режим Опытного Пользователя

17. Общие

Модуль Общие предоставляет сведения о системе и активности BitDefender. Здесь вы также можете изменить общие характеристики BitDefender.

17.1. Панель управления

Чтобы проверить наличие угроз, а также статистику деятельности компьютера и статус вашей регистрации, перейдите в закладку **Общие>Панель Инструментов** в Режиме Опытного Пользователя.



Панель управления

Панель управления состоит из нескольких разделов:

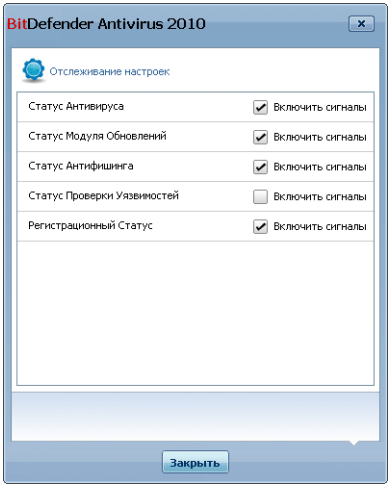
- **Общее Состояние** - информирует Вас о любых проблемах, затрагивающих безопасность вашего компьютера.
- **Статистика** - Важные сведения об активности BitDefender.
- **Обзор** - Отображение состояния обновления, состояния учетной записи и сведений о лицензии.

- **Активнось Файлов** - указывает на изменение числа проверенных объектов при помощи Антивируса BitDefender. Высота панели указывает на интенсивность траффика в течение этого промежутка времени.

17.1.1. Общее Состояние

Здесь вы можете увидеть количество проблем, влияющих на безопасность компьютера. Чтобы удалить все угрозы, нажмите**Устранить все угрозы**. Это приведет к запуску мастераУстранить все угрозы.

Чтобы настроить, какие модули будут отслеживаться BitDefender Antivirus 2010, нажмите **Настройка Отслеживания Состояния**. Появится новое окно:



Настройка Отслеживания Состояния

Если вы хотите что бы BitDefender контролировал компонент, выберите флажок **Включить сигналы** соответствующий этому компоненту. BitDefender может отследить статус следующих компонентов безопасности:

- **Антивирус** - BitDefender контролирует состояние 2х компонентов Антивирусного модуля: защита в реальном времени и сканирование по запросу. Наиболее распространенные отчеты по проблемам этого компонента, приведенные в следующей таблице.

Проблема	Описание
Защита в режиме реального времени выключена	Документы не проверяются при запуске вами или приложением, работающим в вашей системе.
Вы никогда не проводили сканирование на наличие вирусоносов	Сканирование системы по требованию для проверки файлов, хранящихся на Вашем компьютере, никогда не производилось.
Постедняя проверка системы была отменена до ее завершения	Полная проверка системы была запущена, но не была закончена.
Состояние Антивируса критическое	Защита системы в реальном времени отключена, требуется проверка системы.

- **Обновить** - BitDefender проверяет статус обновления вирусных сигнатур. Наиболее распространенные отчеты по проблемам этого компонента, приведенные в следующей таблице.

Проблема	Описание
Автоматическое обновление выключено	Вирусные сигнатуры BitDefender не обновляются регулярно.
Обновление не производилось x дней	Вирусные сигнатуры BitDefender устарели.

- **Антифишинг** - BitDefender отслеживает статус функций Антифишинга. Если он не включен для всех поддерживаемых приложений, будет выведено сообщение **Антифишинг выключен**.
- **Проверка на уязвимости** - BitDefender отслеживает функции Проверки на уязвимости. Проверка на уязвимости сообщает вам, если вам требуется установить какие-либо обновления Windows, обновления приложений или если вам необходимо усилить пароль.

  Наиболее распространенные отчеты по проблемам этого компонента, приведенные в следующей таблице.

Состояние	Описание
Проверка на Уязвимости отключена	BitDefender не проводит проверку на возможные уязвимости в отношении отсутствующих

Состояние	Описание
	обновлений Windows, обновлений приложений, слабых паролей.
Были обнаружены множественные уязвимости	BitDefender обнаружил отсутствие обновлений Windows/приложений и слабые пароли.
Критичные обновления Microsoft	Критические обновления Microsoft обнаружены, но не установлены.
Другие обновления Microsoft	Не критические обновления Microsoft доступны, но не установлены.
Автоматические обновления Windows отключены	Обновления безопасности Windows устанавливаются автоматически по мере доступности.
Приложение (устарело)	Новая версия Приложения доступна, но не установлена.
Пользователь (Слабый пароль)	Пароль пользователя легко взламывается людьми, имеющими специальное программное обеспечение.

Важно
Чтобы убедиться, что система полностью защищена, включите отслеживание всех компонентов и устраните все обнаруженные угрозы.

17.1.2. Статистика

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

Элемент	Описание
Проверенные файлы	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.
Обнаружены зараженные файлы	Показывает количество инфицированных файлов, которые были обнаружены на вашей системе во время последнего сканирования.

Элемент	Описание
Последнее Сканирование Системы	Показывает когда вы последний раз проводили сканирование. Если последнее сканирование производилось более недели назад, проверьте ваш компьютер как можно скореее. ТЧтобы просканировать весь компьютер перейдите на вкладку **Антивирус**, Сканирование и запустите полное или глубокое сканирование.
Следующее сканирование	Показывает когда произойдет следующее сканирование.

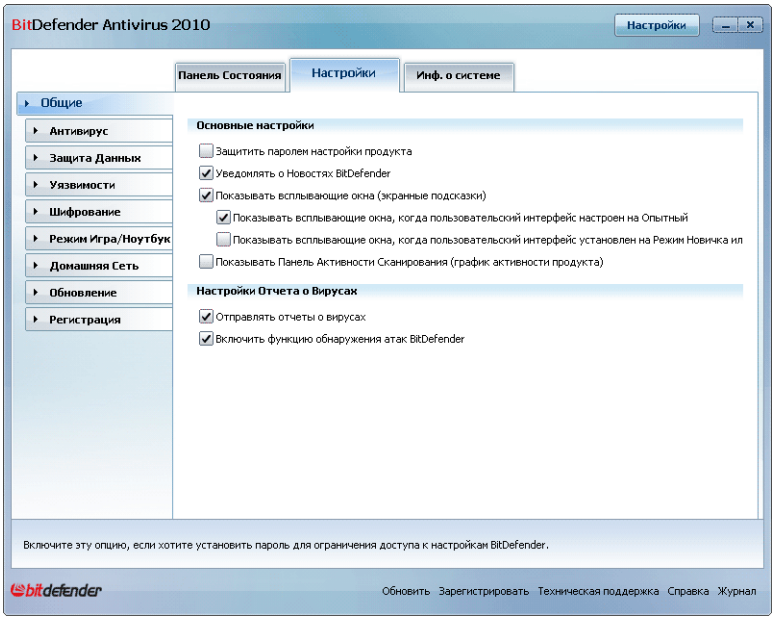
17.1.3. Обзор

Тут вы можете проверить статус обновлений, состояние вашей учетной записи, регистрационную и лицензионную информацию.

Элемент	Описание
Последнее обновление	Показывает когда вы последний раз обновляли BitDefender. Регулярно проводите обновления чтобы ваша система была полностью защищена.
Учетная Запись BitDefender	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 BitDefender или другими персонализированными услугами. Для активации продукта вам надо создать учетную запись. Для получения более подробной информации о аккаунте BitDefender, зайдите на *«Регистрация и Мой Аккаунт»* (p. 51).
Регистрация	Отображает тип и состояние вашего лицензионного ключа. Чтобы поддерживать систему в безопасности, настойчиво рекомендуется обновлять BitDefender, если срок действия ключа вышел.
Срок действия истекает через	Число дней до истечения срока действия лицензионного ключа. Если ваш лицензионный ключ истекает в течение нескольких дней, зарегистрируйте новый ключ. Чтобы купить лицензионный ключ, нажмите ссылку **Купить/Продлить**, расположенную в нижней части окна.

17.2. Настройки

Для настройки общих параметров BitDefender и управления его настройками перейдите в раздел **Общие>Настройки** в окне Режима Опытного Пользователя.



Общие настройки

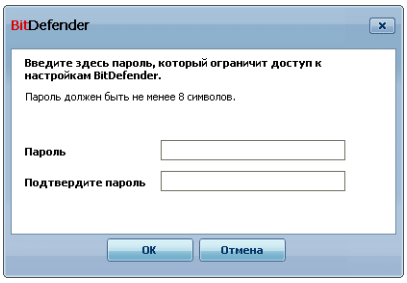
Здесь Вы можете настроить операции, выполняемые программой Bitdefender. По умолчанию, Bitdefender загружается при запуске операционной системы Windows и затем выполняется в свернутом виде.

17.2.1. Общие настройки

- **Включить защиту настроек программы паролем** - 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**, повторите в поле **Повторите пароль** и нажмите **OK**.

Если у Вас установленн пароль, то он будет запрашиваться 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 в интерфейсе в режиме Новичка/Промежуточном или Опытного Пользователя.
- **Включить панель активности сканирования (экранный график активности программы)** - показывает Активность Сканирования всегда при входе в Windows. Снимите галочку в этом поле, если больше не хотите, чтобы Панель активности сканирования отображалась.

Панель Активности Сканирования

Замечание

Эта настройка может быть изменена только для текущего пользователя Windows. Панель активности сканирования доступна только в режиме Опытного Пользователя.

17.2.2. Настройки отчета о вирусах

- **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.

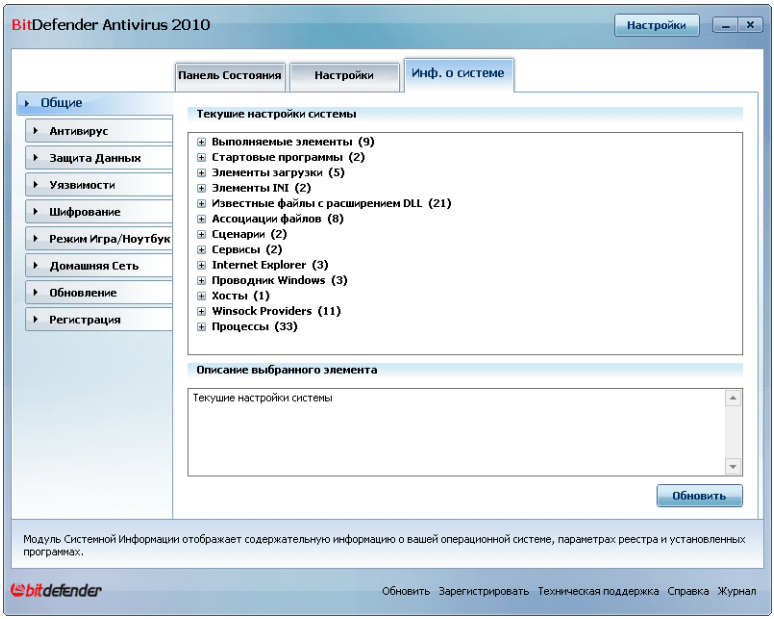
- **Включить функцию BitDefender обнаружения атак** - отправляет в лаборатории BitDefender Labs отчет о потенциальных атаках вирусов.

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

17.3. Информация о системе

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 **Общие>Информация о системе** в режиме Опытного Пользователя.



Информация о системе

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

Три кнопки доступны:

- **Восстановить** - смена текущих связей файлов к значениям 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**.

18. 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

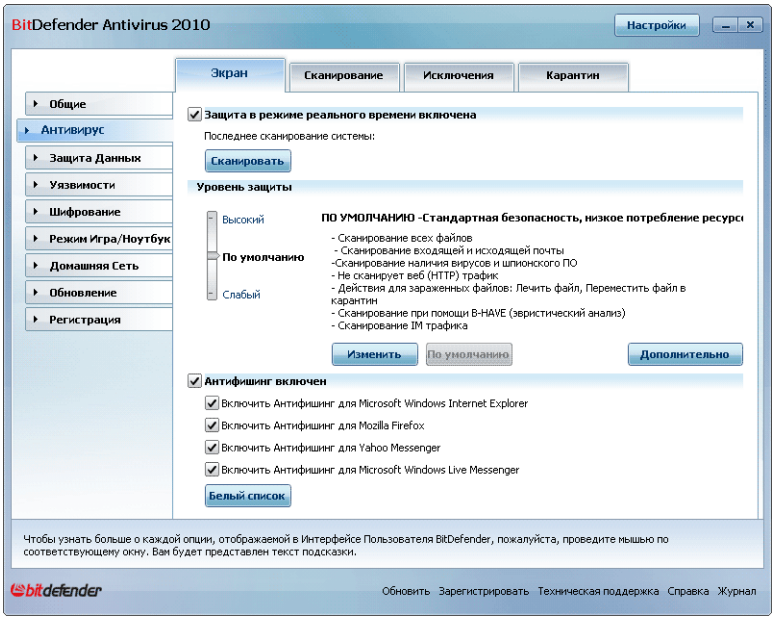
  Постоянная защита также называется сканированием на лету - файлы сканируются по мере доступа к ним.

- 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 запланированые действия, которые можно регулярно запускать по расписанию.

18.1. 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 режиме Опытного Пользователя.



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 в Ваш компьютер, включите **Постоянную защиту**.

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

18.1.1. Настройка уровня защиты

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

Существует 3 уровня защиты:

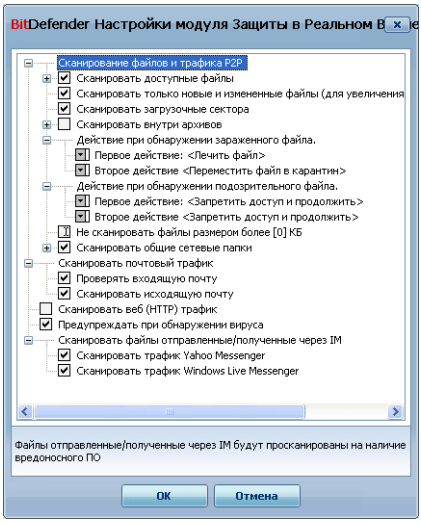
Уровень защиты	Описание
Разрешающий	Выполняет основные процессы безопасности. Потребляет малое количество ресурсов. Сканируются только программы и входящие почтовые сообщенийя. Кроме классического сигнатурного сканирования спользуется эвристический анализ. Меры, принятые к зараженным файлам: лечение файла/перемещение файла в карантин.
По умолчанию	Предлагает стандартный уровень безопасности. Потребляет малое количество ресурсов. Все файлы, входящие и исходящие электронные сообщения проверяются на вирусы и программы-шпионы. Кроме классического сигнатурного сканирования, также используется эвристический анализ. К зараженным файлам могут применяться следующие действия: вылечить файл/переместить файл в карантин.
Агрессивный	Предлагает высокий уровень безопасности. Потребляет среднее количество ресурсов. Все файлы, входящие и исходящие электронные сообщения, а также веб траффик проверяются на вирусы и программы-шпионы. Кроме классического сигнатурного сканирования, также используется эвристический анализ. К зараженным файлам могут применяться следующие действия: вылечить файл/переместить файл в карантин.

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

18.1.2. 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 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.
	Проверить только приложения	Проверяются только файлы программ, то есть файлы с расширением: `.exe`; `.bat`; `.com`; `.dll`; `.ocx`; `.scr`; `.bin`; `.dat`; `.386`; `.vxd`; `.sys`; `.wdm`; `.cla`; `.class`; `.ovl`;

Настройка		Описание
		.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 угроз	Проверка на наличие угроз. Обнаруженные файлы будут считаться зараженными. Программное обеспечение, которое включает компоненты рекламного ПО, может прекратить работу, если выбрана эта настройка. Выберите **Пропустить номеронабиратели и приложения из сканирования** и/или **Пропустить клавиатурных шпионов из сканирования** если хотите исключить эти типы файлов из сканирования.
Проверить только новые и измененные файлы		Проверяет файлы которые не были проверены раньше или изменились с момента последнего сканирования. Выбирая эту опцию вы можете ощутимо повысить производительность системы, почти не проигрывая в безопасности.
Проверить загрузочные секторы		Проверка загрузочных секторов системы.
Проверять внутри архивов		Проверяются также архивы, к которым есть доступ. Включение данной опции замедлит работу компьютера. Вы можете установить максимальный размер архива для сканирования (в килобайтах, введите 0, если вы хотите, чтобы все архивы для сканирования), а максимальная глубина архива для сканирования.

Настройка		Описание
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.
	Вылечить	Удаляет вредоносный код из инфицированных файлов.
	Удалить файл	Зараженный файл удаляется немедленно, без предупреждения.
	Переместить файл в карантин	Зараженные файлы перемещаются в Карантин. Добавленные в карантин файлы нельзя выполнять или открывать; таким образом, риск заражения сводится к нулю.
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. Добавленные в карантин файлы нельзя выполнять или открывать; таким образом, риск заражения сводится к нулю.
Не сканировать файлы размером более [x] Кб		Введите максимальный размер файла для проверки. Если введен 0 Kb, будут проверены все фалы, независимо от их размера.
Проверка общих сетевых ресурсов	**Проверить все файлы**	Будут проверены все открываемые файлы, независимо от их формата.
	Проверить только приложения	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;

Настройка		Описание
		.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 ";".

- **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 веб (HTTP) траффик** - scans the http traffic.
- **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.

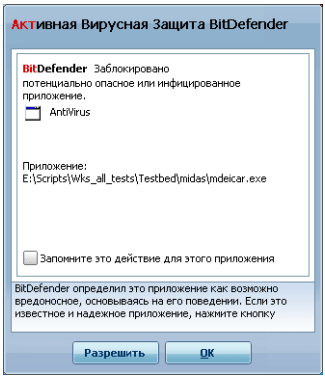
  В случае обнаружения подозрительного файла Вы можете запустить из окна предупреждений программу Мастер, которая поможет Вам посылать этот файл в лабораторию Bitdefender для дальнейшего анализа. При этом Вы можете указать свой адрес электронной почты, чтобы получить информацию относительно этого предупрежедния.
- **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.

18.1.3. Изменение настроек модуля Активный Вирусный Контроль

Активный Вирусный Контроль BitDefender 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.

AVC может быть настроен на предупреждение и предложит вам решение проблемы всякий раз, когда приложение будет пытаться выполнить возможные вредоносные действия.



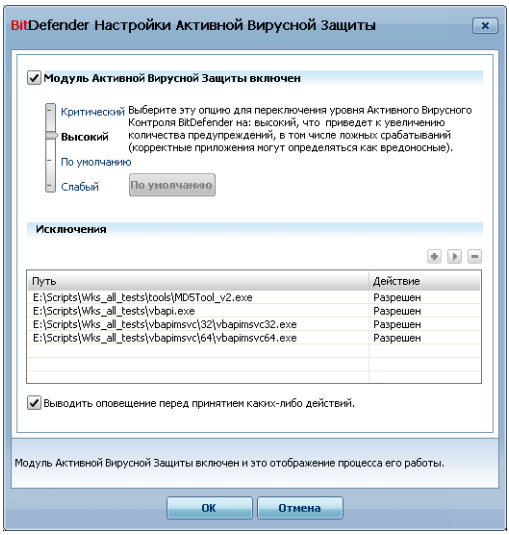
Предупреждение BitDefender AVC

Если вы знаете, что обнаруженному приложению можно доверять, нажмите **Разрешить**.

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

Выберите **Запомнить это действие для этого приложения** прежде чем принять действие, и BitDefender будет применять эти действия для обнаруженных приложений в будущем. Созданное, таким образом, правило будет отражено в таблице**Исключения**.

Чтобы настроить Активный Вирусный Контроль, нажмите **Настройки BD AVC**.



Настройки AVC BitDefender

Поставьте соответствующую галочку для активации Активного Вирусного Контроля.

Важно

Рендуется держать Активный Вирусный Контроль включенным, чтобы обеспечить защиту против неизвестных вирусов.

Если вы хотите , чтобы Активный Вирусный Контроль предупреждал вас о действиях приложений, пытающихся совержить вредоносное действие, и предложил решение проблемы , выберите **Спросить меня перед применением действия**.

Настройка уровня защиты

Уровень Активного Вирусного Контроля автоматически меняется при установке нового уровня защиты в режиме реального времени. 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 AVC изменится соответственно. При установке защиты в режиме реального времени на уровень **Разрешающий**, BitDefender AVC автоматически отключается, и вы не можете его настраивать.

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

Уровень защиты	Описание
Критический	Строгий контроль за всеми приложениями на предмет возможного вредоносного действия.
По умолчанию	Высокие уровни обнаружения, возможны ложные срабатывания.
Средний	Уровень контроля приложения средний, возможно небольшое количество ложных срабатываний.
Разрешающий	Низкие уровни обнаружения, нет ложных срабатываний.

Управление списком надежных/ненадежных приложений

Вы можете добавлять приложения, которым доверяете, в список доверенных приложений. Эти приложения не будут проверяться BitDefender AVC и доступ будет разрешен автоматически. Аналогичным образом, приложения, доступ к которым вы хотите закрыт, могут быть добавлены в список ненадежных приложений, и BitDefender AVC будет автоматически блокировать их.

Приложения, для которых были созданы правила, отражаются в таблице под заголовком **Исключения**. Путь к приложению и действие, установленное для него (доступ Разрешен или Заблокирован), указан для каждого правила.

Для управления списком используйте кнопки, находящиеся над таблицей:

- **Добавить** - добавляет новое приложение к списку.
- **Удалить** - удаляет приложение из списка.
- **Редактировать** - редактировать правило приложения.

18.1.4. Отключение постоянной защиты

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

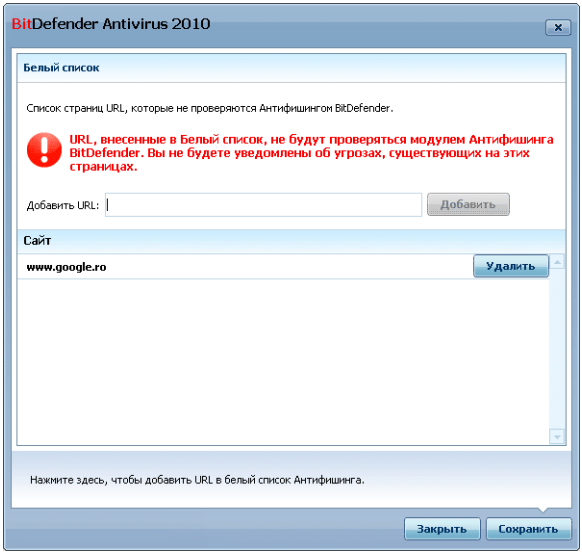
18.1.5. Настройка антифишинговой защиты

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. Больше информации здесь «*Интегрирование в веб браузеры*» (p. 210).

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

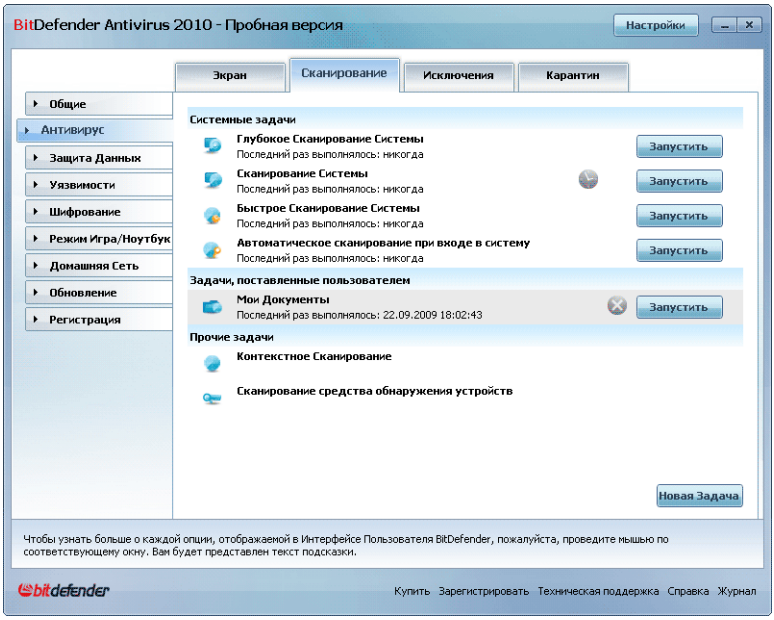
Нажмите **OK**, чтобы сохранить изменения и закрыть окно.

18.2. 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.

В режиме Опытного Пользователя 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.

18.2.1. 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. 123).

Существует три категории задач сканирования:

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

Задачи по умолчанию	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.
Сканирование Системы	Проверка всей системы кроме архивов. В настройках по умолчанию проводится проверка на все типы вирусного ПО, кроме руткитов.
Быстрая проверка системы	Сканирует папки Windows и Program Files. В конфигурации по умолчанию проверка производится на все виды вредоносных программ, кроме руткитов. Не производится проверка памяти, реестра и записей cookies.
Сканирование при входе	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 **при запуске системы**. Вы можете указать, сколько времени (в минутах) задание должно выполняться после запуска.

Замечание

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

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

  предусмотрена задача Мои документы. 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:

- **По графику** - указывает на то, что выполнение данной задачи запланировано позднее. Нажмите эту кнопку, чтобы перейти к разделу **Свойства** , Планировщик, где можно найти график задачи и изменить его.
- **Удалить** - удаляет выбранное задание.

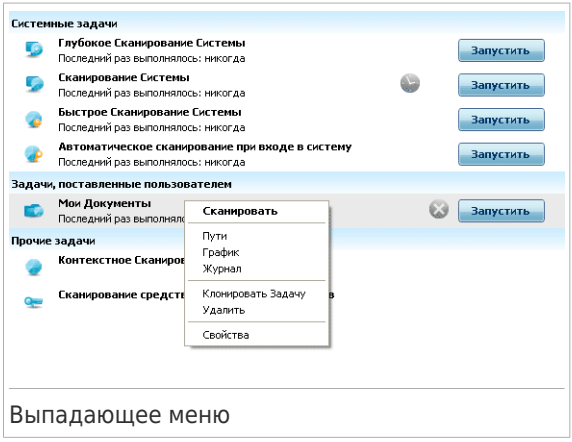
  Замечание
  Недоступно для системных задач. Вы не можете удалить системные задачи.

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

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

18.2.2. 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.
- **View LogsПросмотреть журнал** - открывает окно **Properties**, Журнал, где вы можете просмотреть отчеты, созданные после выполнения выбранного задания.
- **Повторить** - повторяет выбранную задачу. Данная функция полезна при создании новых задач, поскольку позволяет изменить настройки дубликата.
- **Удалить** - удаление выбранной задачи.

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

- **Свойства** - открывает окно **Свойства**, вкладку Обзоргде можно изменить настройки выбранной задачи.

Замечание
В связи с особенными свойствами категории/**Прочие задачи** , только функции **Простомтреть журнал** и **свойства** доступны.

18.2.3. Создание задач сканирования

Создать задачу сканирования, использую один из следующих способов:

- Повторить существующую задачу, переименовать и внести необходимые изменения вСвойства.
- Нажмите **Новое задание**, чтобы создать новое задание и настроить его.

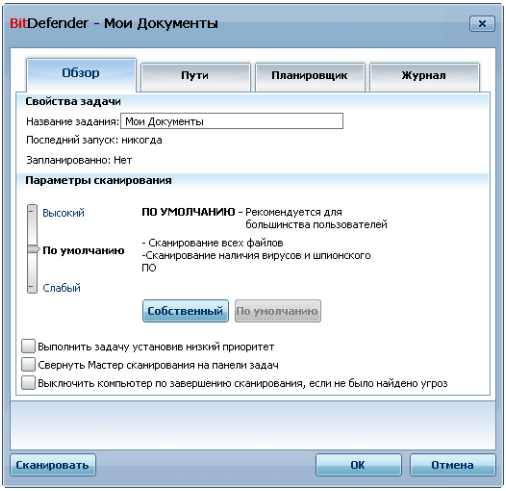
18.2.4. Настройка задач проверки

Каждая задача имеет собтсвенное окно **Свойства**, где можно настроить опции проверки, установить объект проверки, запланировать задачу или просмотреть отчеты. Чтобы открыть это окно, нажмите **Свойства** слева от задачи (или нажмите правой кнопкой мыши на задачу и нажмите**Свойства**).

Замечание
Чтобы получить больше информации, просмотрите журналы и таблицу **Журналы**, обратитесь к «*Просмотр журнала проверок*» (p. 143).

Изменение настроек сканирования

Чтобы изменить опции сканирования для определенной задачи, нажмите правой кнопкой мыши на задачу и выберите**Свойства**. 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
Разрешающий	Подразумевает среднюю эффективность выявления. Потребляет небольшое количество ресурсов. Только программы сканируются на наличие вирусов. Кроме классического сигнатурного сканирования используется также эвристический анализ.

Уровень защиты	Описание
По умолчанию	Подразумевает высокую эффективность выявления. Потребляет среднее количество ресурсов. Все файлы проверяются на наличие вирусов и программ-шпионов. Кроме классической сигнатурной проверки, 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 сигнатурной проверки, также используется эвристический анализ.

Доступен также ряд общих настроект для процесса проверки:

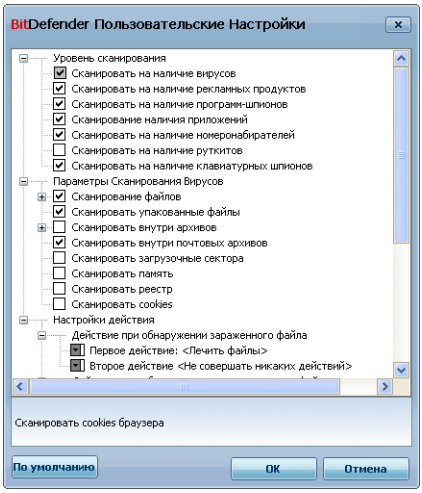
- **Выполнить задачу с низким приоритетом.** Уменьшается приоритет процесса проверки. Таким способом Вы ускоряете работу других программ, но увеличиваете время, необходимое для завершения процесса проверки.
- **Свернуть мастер сканирования.** Окно проверки свертывается панель задач. Чтобы открыть его,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

Нажмите **OK** 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 **Пользовательский**, чтобы установить Ваши настройки проверки. Откроется новое окно.



Настройки проверки

Опции сканирования организованы как расширяемое меню, очень похожее на то, которое используется 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 компоненты этого ПО, может прекратить работу, если выбрана эта настройка.

Настройка	Описание
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 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.
	Проверить файлы с расширением	Проверяются только файлы с заданным расширением. Задаваемые расширения разделяются знаком ";".
Проверить запакованные файлы		Проверяются запакованные файлы.

Настройка	Описание
Проверять внутри архивов	Сканирует внутри архивов `.zip`, `.rar`, `.ace`, `.iso` и других. Выберите **Сканировать установочные элементы и chm архивы**, если хотите проверить эти типы файлов. Сканирование заархивированных файлов увеличивает время проверки и требует большего объема системных ресурсов. Вы можете установить максимальный размер сканируемых архивов в килобайтах (KB), указав их размер в графе**Свести размер сканируемых архивов к**.
Сканировать внутри e-mail архивов	Проверяются файлы внутри почтовых архивов.
Проверить загрузочные секторы	Проверка загрузочных секторов системы.
Проверка памяти	Проверка памяти на вирусы и прочие вредоносные программы.
Проверка реестра	проверка реестра.
Проверка Cookies	Проверка файлов Cookies.

- **Настройки действий.** Укажите меры, которые должны быть приняты по каждой категории обнаруженных файлов с помощью ссылок в этой категории.

Замечание

Чтобы задать новое действие, нажмите на текущее **Первое действие** и выберите нужный вариант из меню. Укажите **/Второе действие** применяемое в случае невыполнения первого действия.

- Выбрерите действие, которое будет применено по отношению к зараженным файлам. Доступными являются следующие варианты:

Действие	Описание
Ничего не делать	Не выполняются никакие действия с зараженными файлами. Названия этих файлов появятся в файле отчета.

Действие	Описание
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
Ничего не делать	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
Ничего не делать	Не выполняются никакие действия со скрытыми файлами. Названия этих файлов появятся в файле отчета.
Переименовать файлы	Изменяет имена скрытых файлов, добавляя в конце имени `.bd.ren`. В результате у вас

Действие	Описание
	будет возможность искать подобные файлы на вашем компьютере.
Переместить файлы в карантин	Скрытые файлы перемещаются в Карантин. Добавленные в карантин файлы нельзя выполнять или открывать; таким образом, риск заражения сводится к нулю.

Замечание

Обратите внимание, что эти скрытые файлы - не те файлы, которые вы сознательно скрываете от Windows. Это файлы, спрятнные особыми программами - руткитами. Сами по себе руткиты не вредны. Но они часто используются для того, чтобы сделать вирусы невидимыми для обычных антивирусных программ.

- **Настройки реакции на защищенные паролем файлы.** Файлы, зашифрованные средствами Windows могут быть важны для вас. Поэтомы вы можете настроить реакцию на зараженные и подозрительные файлы, зашифрованные средствами Windows. Еще одна категория файлов, которая требует особых действий - защищенные паролем архивы. Защищенные паролем архивы нельзя сканировать, не предоставив пароль. Используйте эти опции чтобы настроить реакцию на защищенные паролем архивы и зашфированные Winodws файлы.
  - **Действие при обнаружении зашифрованного зараженного файла.** Выбрать действие, применимое к инфицированным файлами, зашифрованными средствами Windows. Доступными являются следующие варианты:

Действие	Описание
Не совершать никаких действий	Фиксировать только инфицированные файлы, зашифрованные Windows. 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.
Удалить файлы	Немедленно удалять инфицированные файлы с диска без предупреждения.

Действие	Описание
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.

- **Действие при обнаружении подозрительного файла.** Определите что делать с инфицированными файлами, зашифрованными средствами Windows Доступными являются следующие варианты:

Действие	Описание
Не совершать никаких действий	Фиксировать только подозрительные файлы, зашифрованные Windows. 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.

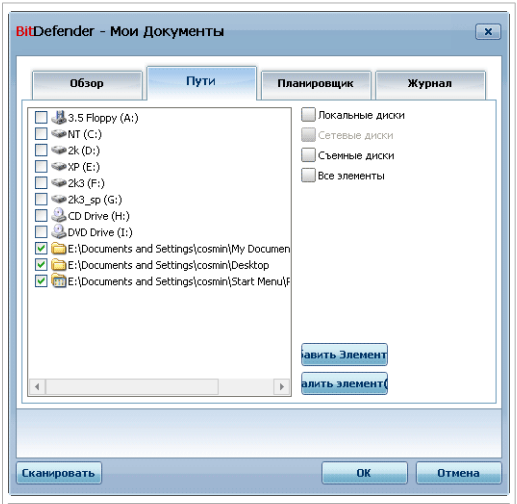
- **Действие при обнаружении файла защищенного паролем найдено.** Выберите действие, которое будет применено к защищенными паролем файлам. Доступными являются следующие варианты:

Действие	Описание
Только запись	Вести только учет защищенных паролем файлов в отчете о проверке. После завершения сканирования вы можете открыть отчет о проверке, чтобы просмотреть сведения об этих файлах.
Запрос пароля	Запрашивать у пользователя пароль для сканирования обнаруженного файла, защищенного паролем.

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

Установка объекта сканирования

Для определения объекта сканирования в задачу конкретного пользователя нажмите правой кнопкой мыши и выберите **Пути**. Или же, если вы уже находитесь в окне свойств задания выберите закладку**Пути**. Появится следующее окно:



Сканировать Объект

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 Папку(и)** - открывает окно обзора, где можно выбрать файл(ы)/папку (папки), которые необходимо проверить.

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

- **Убрать Элемент(ы)** - удаляет ранее выбранные файлы или папки из списка объектов для проверки.

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

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

- **Локальные диски** - проверка локальных 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.

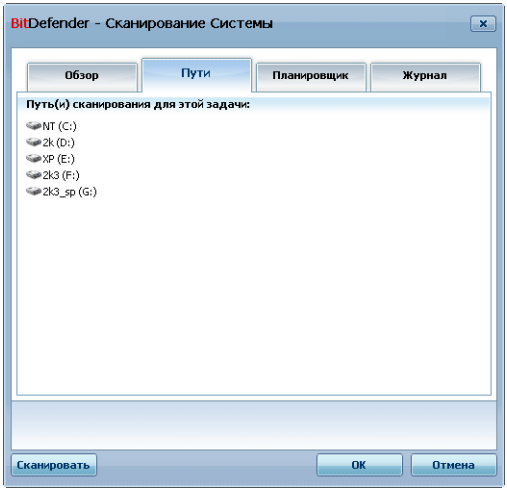
Замечание
Если Вы хотите проверить на наличие вирусов весь компьютер, поставьте значок в поле **Все объекты**.

Нажмите **OK** 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**. При запуске **Сканирование системы**, появится, например, следующее окно:



Цель сканирования задачи "Полное сканирование системы"

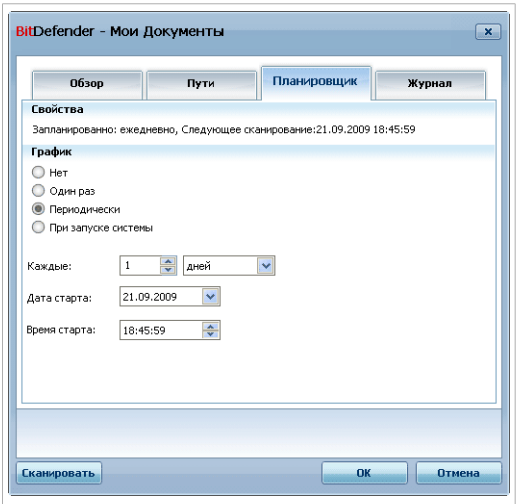
Сканирование системы и **Глубокое сканирование системы** просканируют все локальные диски в то время, как **Быстрое сканирование системы** просканирует только папки`Windows` и `Program Files`.

Нажмите **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 увидеть график конкретных задач или изменить его, щелкните правой кнопкой мыши и выберите задачу **Расписание**. Если вы уже находитесь в Свойствах задачи, выберите закладку**Планировщик** . Появится следующее окно:



Планировщик

Вы можете просмотреть запланированные задачи, если такие есть.

При планировании задачи нужно выбрать одну 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 заданных даты и времени.

  Если хотите, чтобы сканирование повторялось через определенные промежутки времени, выберите **Периодически** и в поле **Каждые** введите число минут/часов/дней/недель/месяцев, соотвествующих необходимому интервалу. Также необходимо указать дату и время первого запуска в полях **Дата/Время запуска**.

- **При запуске системы** - запуск сканирования спустя заданное количество минут после того, как пользователь вошел в систему.

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

18.2.5. Сканирование папок и файлов

Перед тем, как запустить процесс проверки, Вы должны убедиться, что вирусные сигнатуры BitDefender обновлены. 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 проведено последнее обновление перейдите сюда: **Обновление>Обновление** в Расширенном интерфейсе.

Замечание

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

Подсказки сканирования

Вот еще несколько подсказок, которые могут быть весьма полезными:

- В зависимости от объема вашего жесткого диска полное сканирование системы может занять какое-то время (до часа или даже более). Таким образом, вам стоит запускать подобные сканирования когда вы не пользуетесь компьютером на протяжении длительного времени. (например ночью).

  Вы можете запланировать сканирование на удобное вам время. Убедитесь, что вы оставляете компьютер включенным. При использовании Windows Vista убедитесь что ваш компьютер не находится в спящем режиме во время, на которое запланировано сканирование.

- Если вы часто загружаете файлы из интернета в отдельную папку, рекомендуется создать новое задание сканирования и включить папку в

задачу по сканированию. Запланируйте ежедневный или более частый запуск задания.

- Существует тип вредоносного ПО, который сам записывает себя в автозагрузку. Чтобы защитить ваш компьютер от подобных вирусов запланируйте задачу**Сканирование при загрузке**,выполняемое при загрузке системы. Помните, что сканирование при загрузке может влиять на производительность системы некоторое время после загрузки.

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 **Сканировать BitDefender**.
- 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.

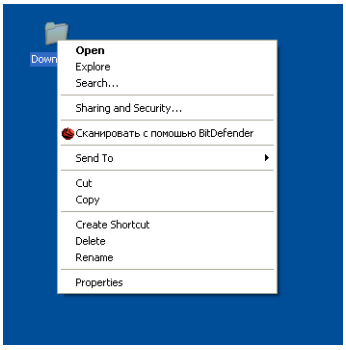
Чтобы запустить задачу сканирования, используйте один из следующих методов:

- дважды щелкните на нужной задаче в списке.
- нажмите кнопку **Проверить сейчас** сответствующую задаче.
- выберите задачу и нажмите **Запустить задачу**.

Появится Мастер сканирования и проведет вас по процессу сканирования .

Проверка через контекстное меню

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



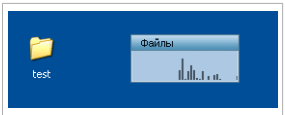
Контекстное сканирование

Щелкните правой кнопкой мышки на файле или папке, которые необходимо проверить, и выберите **Скнировать с BitDefender**. Появится Мастер сканирования и проведет вас по процессу сканирования .

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 Активности Сканирования**, как показано ниже.



Перетащить Файл

Переместите файл

Появится Мастер сканирования и проведет вас по процессу сканирования .

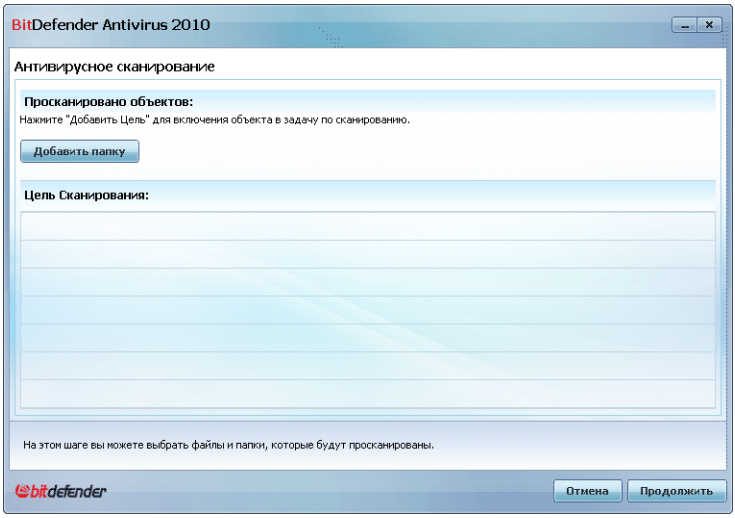
Ручное сканирование

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 2010 → Сканирование с BitDefender**. Появится следующее окно:



Ручное сканирование

Нажмите **Добавить Папку**, выберите местоположение которое вы хотите просканировать и нажмите **OK**. Если вы хотите просканировать многочисленные папки, повторите это действие для каждого дополнительного местоположения.

Пути к выбранным местоположениям появятся в колонке **Цель Сканирования**. Если вы передумали насчет пути, нажмите кнопку **Удалить**, которая находится рядом. Нажмите кнопку **Удалить все пути**, для удаления всех местоположений добавленных в список.

Когда вы закончите выбирать месторасположения, нажмите **Продолжить**. Появится Мастер сканирования и проведет вас по процессу сканирования .

Мастер антивирусного сканирования

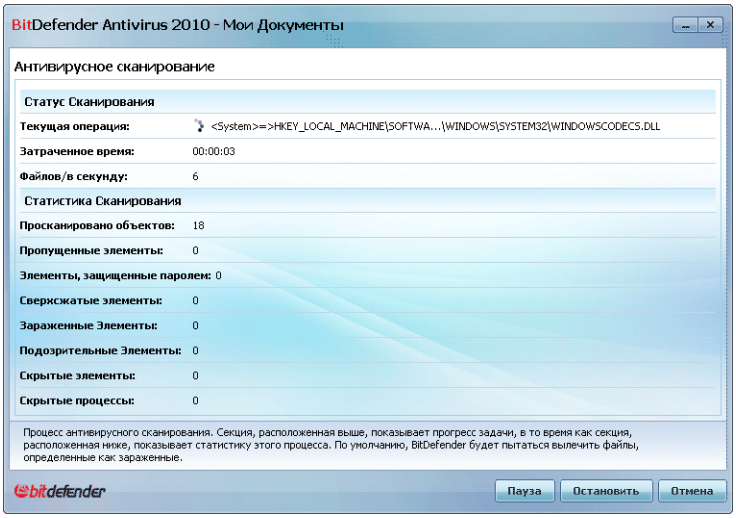
При запуске сканирования по требованию откроется мастер сканирования. Чтобы завершить процесс проверки выполните последовательность из трех шагов.

Замечание

Если мастер сканирования не появился, возможно сканирование настроено проходить в тихом фоновом режиме. Найдите иконку состояния сканирования на панели задач. Вы можете кликнуть в эту иконку, чтобы открыть окно сканирования и наблюдать прогресс проверки.

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.).

Дождитесь окончания сканирования BitDefender

Замечание

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

Архивы, защищенные паролем. Если BitDefender во время сканирования найдет архив, защищенный паролем, и в качестве стандартного действия будет установлено **Запрашивать пароль**, то вам будет предложено ввести пароль. Защищенные паролем архивы нельзя сканировать, не предоставив пароль. Доступными являются следующие варианты:

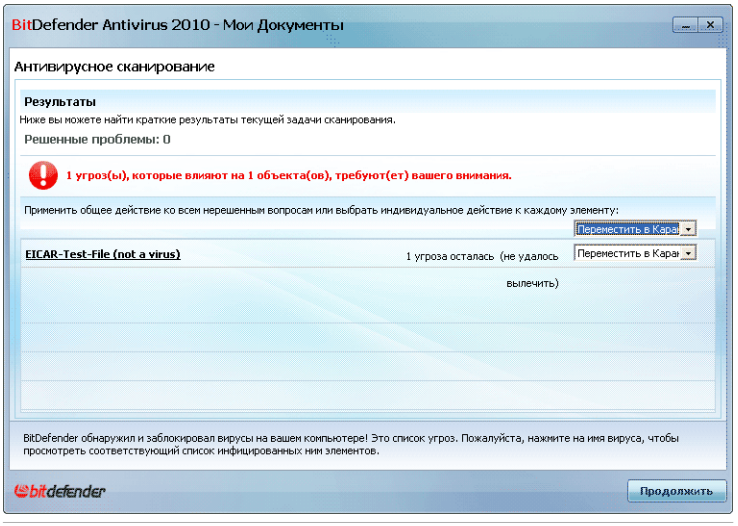
- **Пароль.** Если вы хотите чтобы BitDefender проверил архив, выберите эту опцию и введите пароль. Если вы не знаете пароля, выберите любую другую опцию.
- **Не спрашивать пароль и пропустить эти объекты без сканирования.** Выберите эту опцию, чтобы пропустить этот архив.
- **Пропустить все защищенные паролем элементы без их сканирования.** Выберите эту опцию если не хотите чтобы вас беспокоили по поводу защищенных паролем архивов. BitDefender не будет иметь возможности сканировать их, но запись останется в журнале сканирования.

Для продолжения нажмите **OK**.

Останавливая или приостанавливая сканирование. Вы можете остановить процесс проверки в любое время, нажав **Стоп& Да**. При этом вы попадете на самый последний шаг мастера. Чтобы временно приостановить процесс проверки, нажмите **Пауза**. Чтобы продолжить проверку, нажмите **Возобновить**.

Шаг 2/3 - Выбор Действия

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



Действия

Вы можете просмотреть количество проблем, угрожающих безопасности Вашей системы.

Зараженные объекты разделены на группы в зависимости от типа 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.

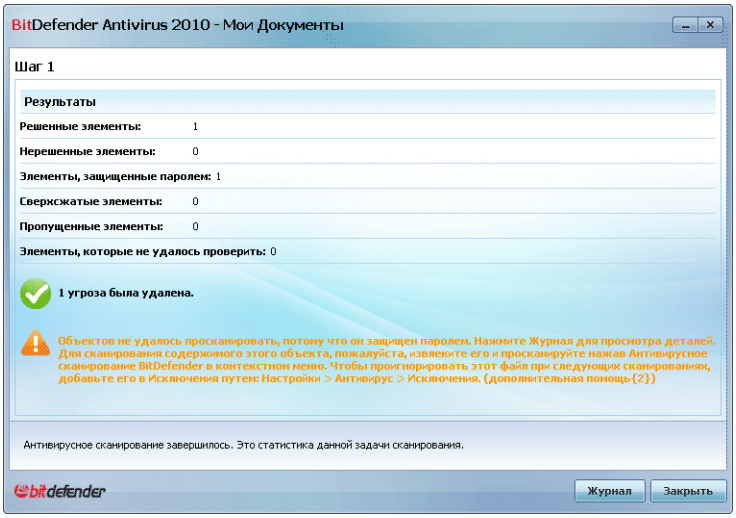
Одна или несколько из следующих опций может появиться в меню:

Действие	Описание
Ничего не делать	Над обнаруженными файлами не будет производиться никаких действий. После завершения сканирования вы можете открыть отчет о проверке, чтобы просмотреть сведения об этих файлах.
Вылечить	Удаляет вредоносный код из инфицированных файлов.
Удалить	Удаление обнаруженных файлов.
Переместить в карантин	Зараженные файлы перемещаются в Карантин. Добавленные в карантин файлы нельзя выполнять или открывать; таким образом, риск заражения сводится к нулю.
Переименовать файлы	Изменяет имена скрытых файлов, добавляя в конце имени `.bd.ren`. В результате у вас будет возможность искать подобные файлы на вашем компьютере. Обратите внимание, что эти скрытые файлы - не те файлы, которые вы сознательно скрываете от Windows. Это файлы, спрятнные особыми программами - руткитами. Сами по себе руткиты не вредны. Но они часто используются для того, чтобы сделать вирусы невидимыми для обычных антивирусных программ.

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. Если вас интересует подробная информация о процессе сканирования, нажмите **Показать журнал**.

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.

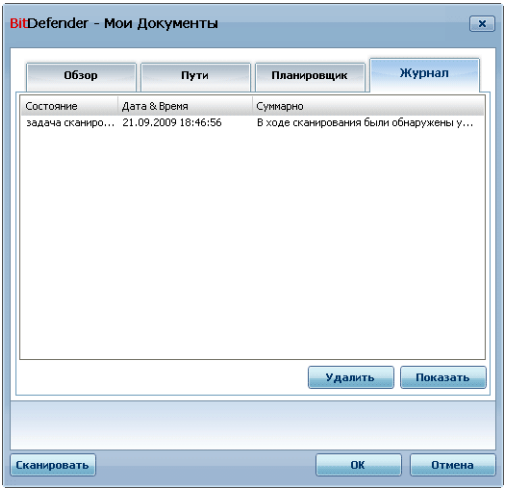
BitDefender обнаружил подозрительные файлы

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.

18.2.6. Просмотр журнала проверок

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



Журналы проверки

Здесь Вы можете увидеть файлы отчетов, которые создавались каждый раз, когда выполнялась задача. По каждому файлу вы получите информацию относительно состояния записанного процесса сканирования, даты и времени процесса, а также отчет результатов сканирования.

Доступны две кнопки:

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

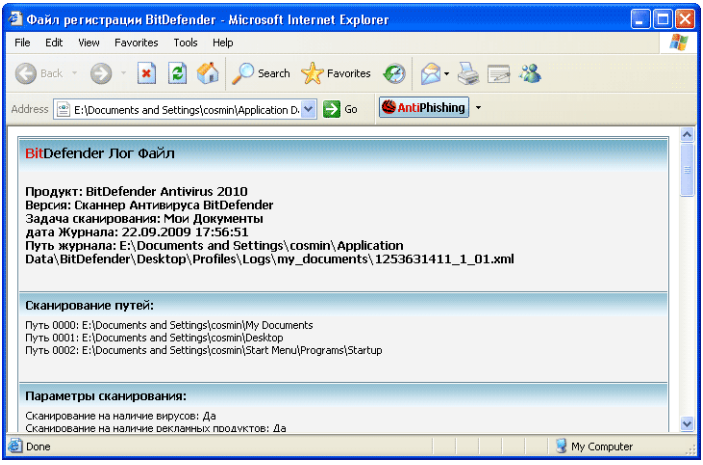
Замечание

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

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

Пример журанала проверок

Следующий рисунок представляет собой пример журнала сканирования:



Пример журанала проверок

Журнал сканирования содержит подробную информацию о записаном процессе сканирования, такую, как опции сканирования, цели сканирования, обнаруженных угрозах и мерах, принятых по отношению к этим угрозам.

18.3. Объекты, исключеные из сканирования

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 из проверки при входе в систему и/или проверки по требованию. Данная функция предназначена для уменьшения времени проверки и исключения вмешательства в вашу работу.

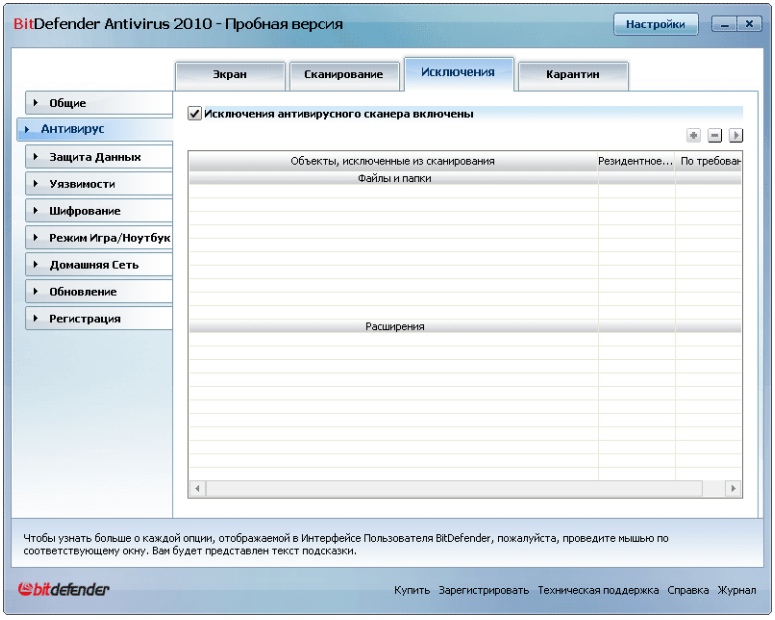
Два типа объектов могуть быть исключены из сканирования:

- **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, независимо от того, используются ли они Вами, либо приложением.

В режиме Опытного Пользователя перейдите к разделу **Антивирус>Исключения** 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. Контекстное сканирование - тип сканирования по требованию: щелкаете правой кнопкой на нужный файл или папку и выбираете **Сканировать с BitDefender**.

Чтобы удалить запись из таблицы, выберите и нажмите на кнопку **Удалить**.

Чтобы редактировать запись в таблице, 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**.

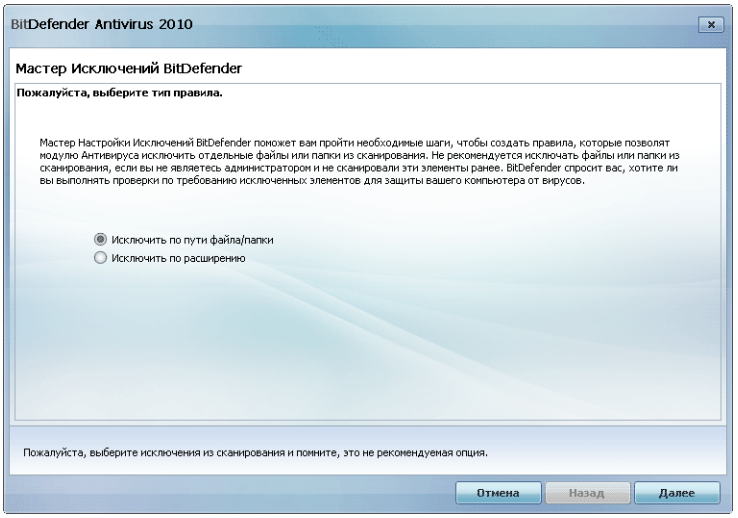
Замечание
Вы также можете нажать правой кнопкой мыши на объекте и воспользоваться пунктами меню для его редактирования или удаления.

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

18.3.1. 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 настроек.

Шаг 1/4 - Выберите тип объекта

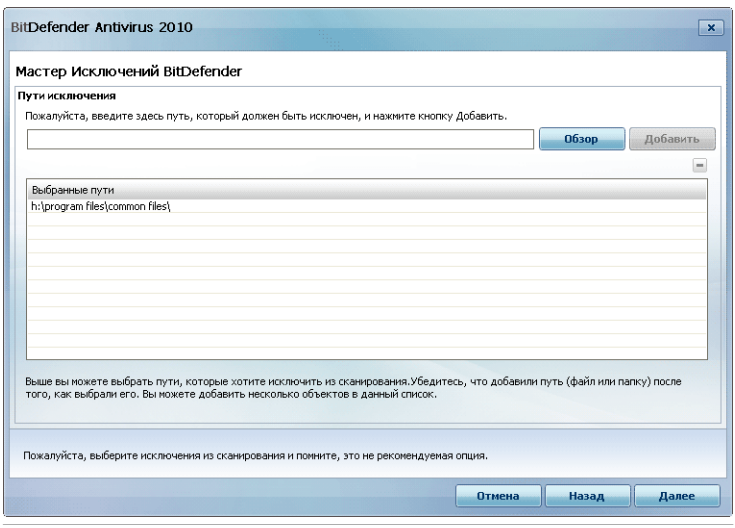


Тип объекта

Выберите опцию для исключения пути из сканирования.

Щелкните **Далее**.

Шаг 2/4 - Укажите пути исключения



Пути исключения

Чтобы определить пути, которые будут исключены из сканирования, используйте один 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

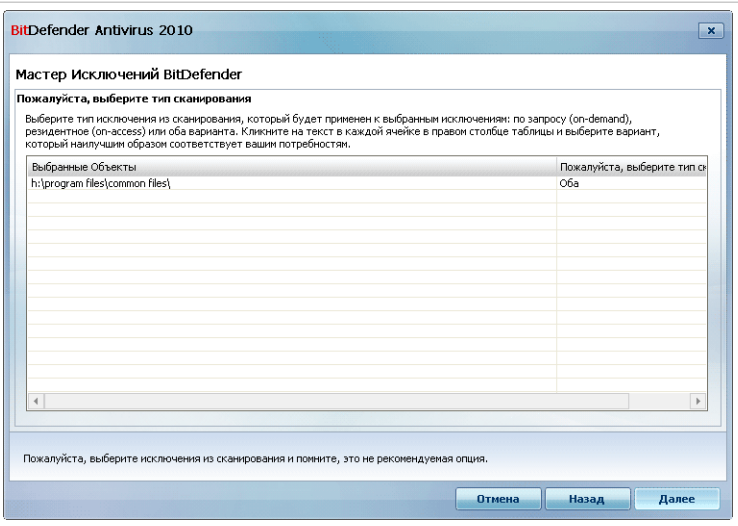
Если указанный путь не существует, появится сообщение об ошибке. Нажмите **ОК** и проверьте правильность пути.

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

Чтобы удалить запись из таблицы, выберите и нажмите на кнопку **Удалить**.

Щелкните **Далее**.

Шаг 3/4 - Выберите тип проверки



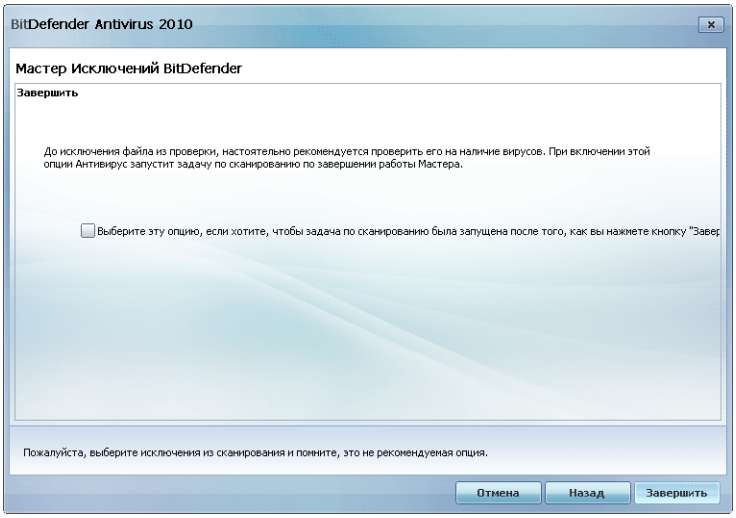
Тип сканирования

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 **Далее**.

Шаг 4/4 - Сканирование исключенных файлов



Сканирование исключенных файлов

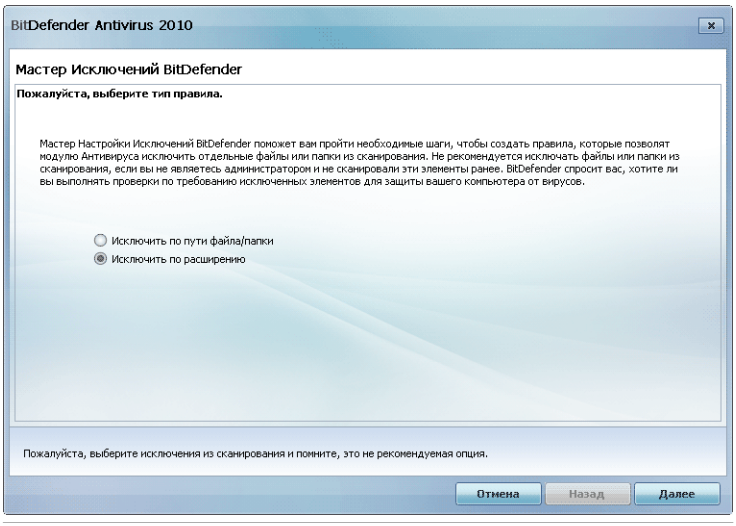
Настоятельно рекомендуется проверять файлы в указанных папках, чтобы убедиться, что они не заражены. Поставьте флажок для сканирования этих файлов перед исключением их из списка проверки.

Нажмите **Завершить**.

18.3.2. 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 настроек.

Шаг 1/4 - Выберите тип объекта

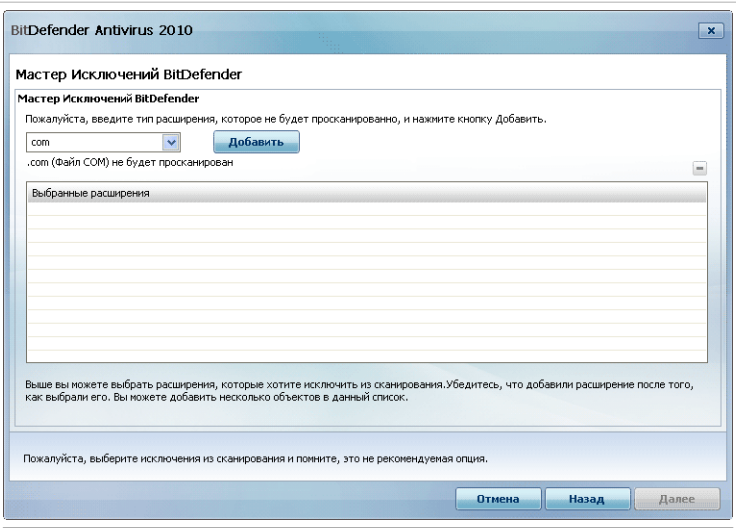


Тип объекта

Выберите опцию исключения расширений из сканирования.

Щелкните **Далее**.

Шаг 2/4 - Задайте расширения, которые необходимо исключить



Исключенные расширения

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.

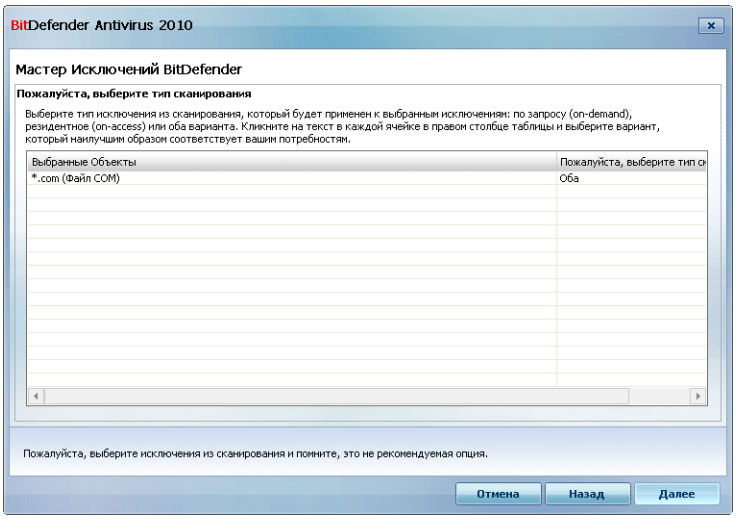
- Укажите расширение, которое должно быть исключенно из сканирования, в редактирующей области и нажмите **Добавить**.

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

Чтобы удалить запись из таблицы, выберите и нажмите на кнопку **Удалить**.

Щелкните **Далее**.

Шаг 3/4 - Выберите тип проверки



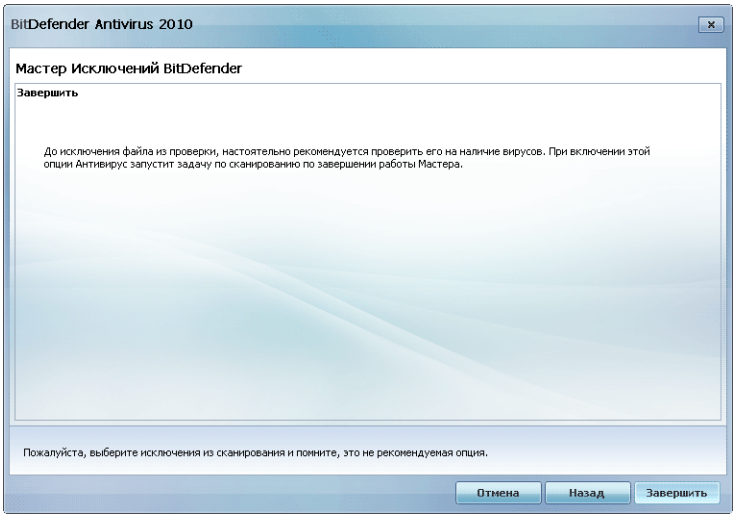
Тип сканирования

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

По умолчанию, выбранные расширения исключаются как из проверки при входе в систему, так и из проверки по запросу. Чтобы изменить эту настройку, нажмите на правой колонке и выберите необходимый пункт из списка.

Щелкните **Далее**.

Шаг 4/4 - Выберите тип проверки



Тип сканирования

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

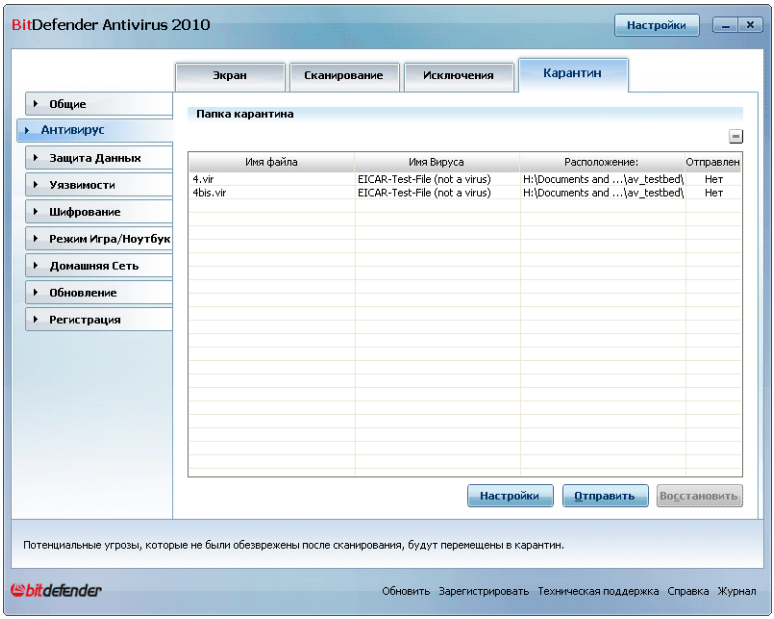
Нажмите **Завершить**.

18.4. Карантин

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.

Вдобавок, BitDefender проверяет файлы в карантине после каждого обновления сигнатур. Очищенные файлы автоматически возвращаются на свое место.

В режиме Опытного Пользователя перейдите к разделу **Антивирус>Карантин**, 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.

18.4.1. Управление файлами в карантине

Вы можете отослать любые файлы из карантина в лабораторию BitDefender, нажав **Отправить**. По умолчанию, BitDefender автоматически высылает файлы из карантина на проверку каждые 60 минут.

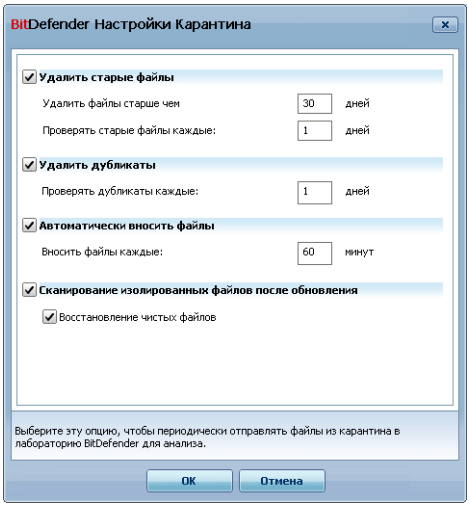
Чтобы удалить выбранный файл из карантина, нажмите кнопку **Удалить**. Если хотите восстановить выбранный файл в его первоначальное местоположение, нажмите **Восстановить**.

Контекстное меню. Имеется контекстное меню, которое легко позволяет управлять файлами в карантине. Доступны те же функции, аналогичные

описанным ранее. Вы также можете выбрать **Обновить**, чтобы обновить содержимое раздела Карантин.

18.4.2. Изменение настроек Карантина

Чтобы изменить настройки Карантина, нажмите **Настройки**. Появится новое окно.



Настройки Карантина

Используя настройки Карантина, можно задать задачу BitDefender для автоматического выполнения следующего действия:

Удаление старых файлов. Чтобы автоматически удалить старые файлы в карантине, включите соответствующую опцию. Вы должны указать количество дней, по истечении которых файлы из карантина будут удалены и период, в который BitDefender будет 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 до следующей проверки дубликатов.

Замечание

По умолчанию, BitDefender ежедневно проверяет файлы в карантине на наличие дубликатов.

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

Замечание

По умолчанию, BitDefender автоматически высылает файлы из карантина на проверку каждые 60 минут.

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

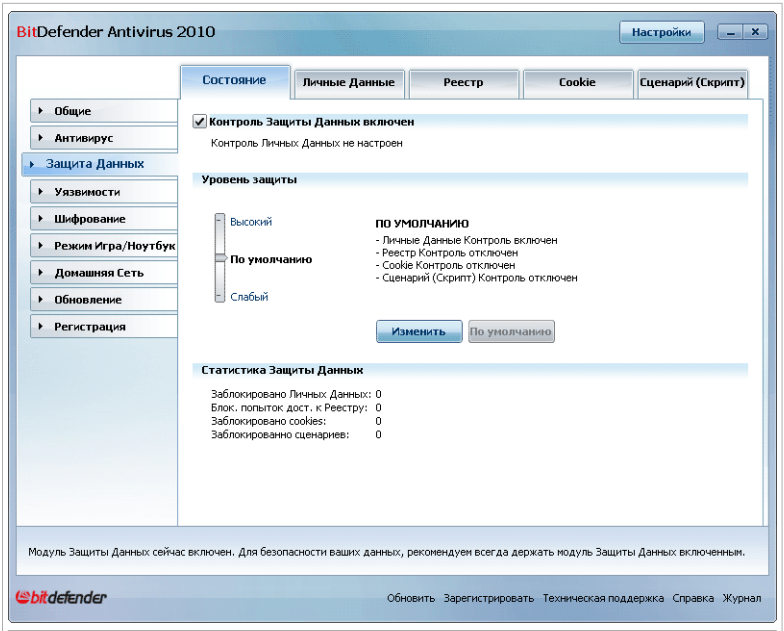
Нажмите **OK**, чтобы сохранить изменения и закройте окно.

19. Контроль Конфиденциальных Данных

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, пытающиеся нарушить конфиденциальность Вашей информации и выслать Вашу личную информацию, например, номер кредитной карты, с Вашего компьютера хакеру.

19.1. Статус Контроля Конфиденциальных Данных

Чтобы настроить и следить за работой модуля Контроля личных данных, в Режиме Опытного Пользователя перейдите в раздел **Контроль Личных Данных>Состояние**.



Статус Контроля Конфиденциальных Данных

Здесь вы можете проверить, включен ли модуль Контроля Конфиденциальных Данных. Если вы хотите сменить состояние модуля Контроля Конфиденциальных Данных, уберите или установите соответствующий флажок.

Важно

Чтобы защитить Ваш компьютер от кражи данных и обеспечить защиту конфиденциальной информации **Контроль конфиденциальных данных** должен быть включен.

Контроль конфиденциальных данных защищает ваш компьютер, используя важные элементы управления защитой:

- Контроль Конфиденциальных Данных - защита конфиденциальных данных путем фильтрации всего исходящего веб трафика (HTTP), электронной почты (SMTP) и мгновенных сообщений согласно правил, указанных в разделе Конфиденциальные данные.
- Контроль Реестра - 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 Конфиденциальных Данных**.

19.1.1. Настройка 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	Все элементы защиты отключены.
По умолчанию	Включен только **Контроль Конфиденциальных Данных**.
Агрессивный	**Контроль Конфиденциальных Данных**, **Контроль Реестра**, **Контроль Cookie** и **Контроль Сценариев** включены.

Вы можете настроить уровень защиты, нажав **Пользовательский уровень**. В появившемся окне, выберите элементы защиты, которые Вы хотите включить и нажмите **OK**.

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

19.2. Контроль Конфиденциальных Данных

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 получения личной информации.

Независимо от того, адрес ли это Вашей электронной почты или номер Вашей кредитной карты, вы можете пострадать при утечке этой информации: Вас могут засыпать спамовыми сообщениями или Ваш счет может быть опустошен.

Контроль конфиденциальных данных защищает вас от кражи данных при подключении к сети. Основываясь на созданных вами правилах, Контроль Конфиденциальных Данных сканирует веб-траффик, электронную почту и траффик мгновенных сообщений на совпадение с определенным набором 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. Если ваша учетная запись Windows является учетной записью администратора, правила которые вы создаете, могут быть сконфигурированы для применения в момент, когда другие пользователи компьютера входят в свои учетные записи пользователей Windows.

Зачем нужен Контроль Конфиденциальных Данных?

- Функция защиты данных очень эффективна при блокировании клавиатурных шпионов. 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.

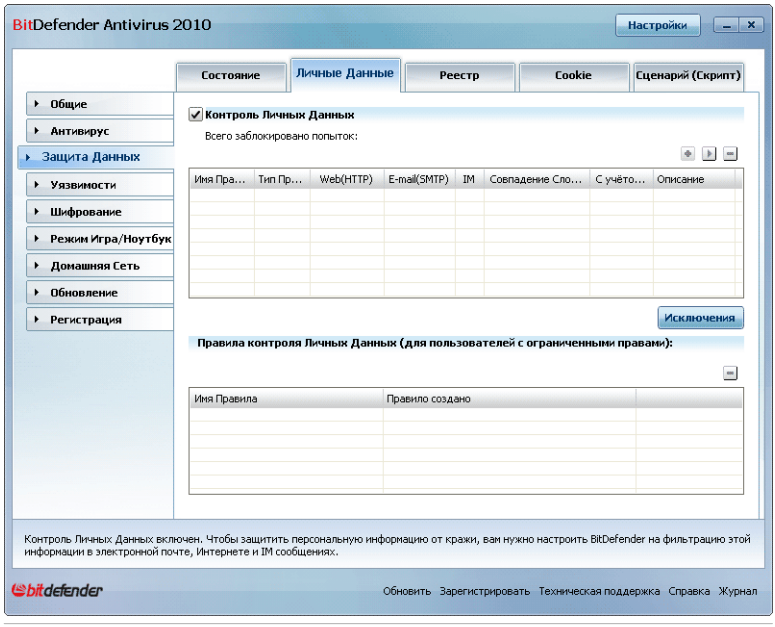
  Даже если такому приложению удастся избежать обнаружение антивирусом, оно не сможет отправлять украденные данные по электронной почте, по сети или в мгновенных сообщениях, если вы создали соответствующие правила защиты.

- 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 информацию о вашем банковском счете. 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 Контроля Конфиденциальных Данных перейдите **Конфиденциальные Данные>Конфиденциальность** в режиме Опытного Пользователя.



Контроль Конфиденциальных Данных

Если вы хотите использовать Контроль Конфиденциальных Данных, необходимо выполнить следующие шаги:

1. Установите флажок **Включить Контроль Конфиденциальных Данных**.

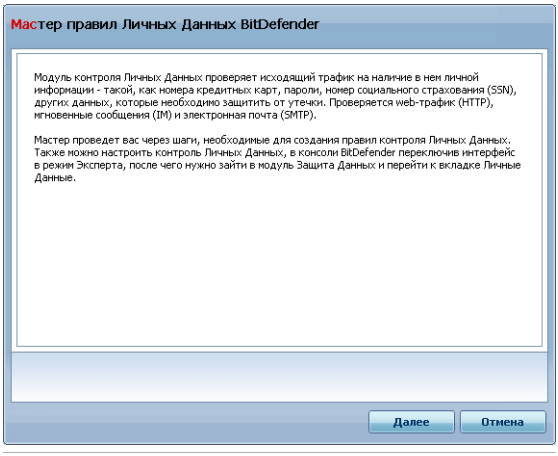
2. Создайте правила для защиты ваших данных. Для получения более подробной информаци перейдите по ссылке *«Создание правил конфиденциальности»* (p. 161).
3. При необходимости, определите особые исключения для созданных вами правил. Более подробные сведения вы найдете по ссылке *«Определение исключений»* (p. 164).
4. Если вы являетесь администратором, вы можете исключить себя из правил конфиденциальности, созданных другими администраторами.

   Более подробные сведения вы найдете по ссылке *«Правила, установленные другими администраторами»* (p. 166).

19.2.1. Создание правил конфиденциальности

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

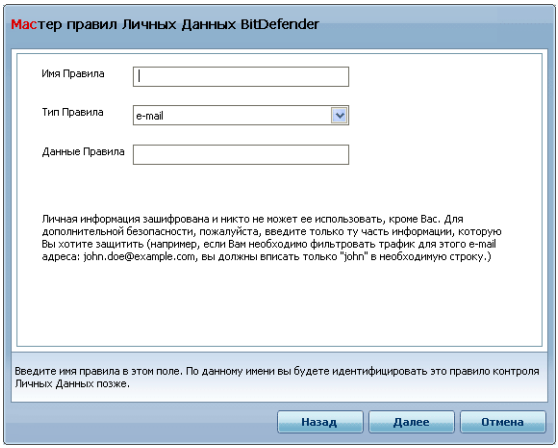
Шаг 1/4 - Окно приветствия



Окно приветствия

Щелкните **Далее**.

Шаг 2/4 - Задать тип правила и данные



Установка типа 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 полностью или частично здесь.

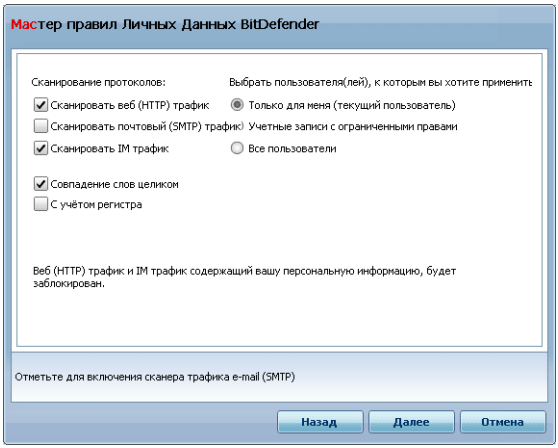
Замечание

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 **Далее**.

Шаг 3/4 - Выбор типа трафиика и пользователей



Выберите тип траффика и пользователей

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

- **Проверять веб (HTTP) траффик** - поверяет HTTP (веб) трафик и блокирует исходящие данные, содержащие данные правила.
- **Проверка e-mail (SMTP раффика)** - поверяет SMTP (почтовый) трафик и блокирует исходящие электронные сообщения, содержащие данные правила.
- **Проверка IM (Instant Messaging) траффика** - поверяет трафик мгновенных сообщений и блокирует исходящие сообщения в чатах, содержащие данные правила.

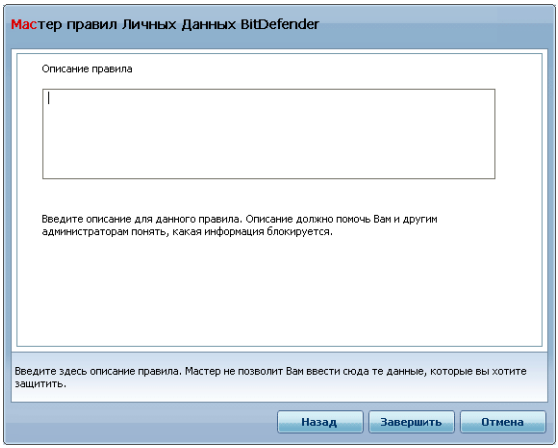
Вы можете применять правило только в случае, если совпадение произойдет по всем словам, или же если совпадение произойдет по нахождению искомой строки.

Укажите пользователей, к которым применимы данные правила.

- **Только для меня (текущий пользователь)** - правило будет применено только к вашей учетной записи.
- **Учетные записи пользователей с ограниченными правами** - правило будет применено к вам и учетным записям пользователей с ограниченными правами.
- **Все пользователи** - правило будет применено ко всем учетным записям.

Щелкните **Далее**.

Шаг 4/4 - Введите описание правила



Опишите правило

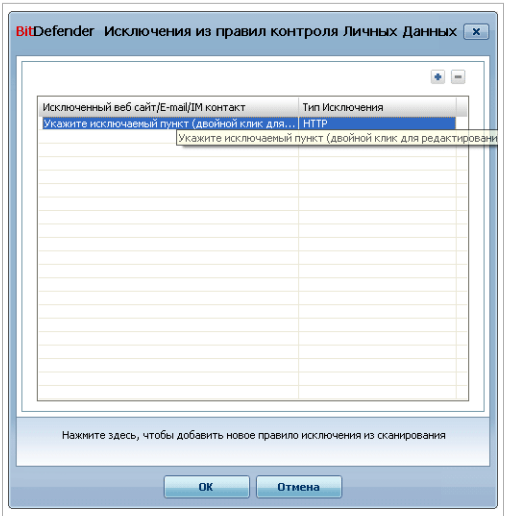
Введите краткое описание правила в поле редактирования. Так как заблокированные данные (символьные строки) не отображаются в виде простого текста при доступе к правилу, описание должно помочь вам легко идентифицировать их.

Нажмите **Завершить**. Правило будет отображаться в таблице.

19.2.2. Определение исключений

Бывают случаи, когда вам необходимо 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.

Чтобы открыть окно управления мсключениями, нажмите **Исключения**.



Исключения

Чтобы добавить исключение, следуйте инструкции:

1. Нажмите **Добавить** чтобы добавить новый элемент в таблицу.
2. Дважды нажмите **Укажите исключаемый пункт**и укажите веб-сайт, адрес электронной почты или IM контакт, который вы хотите добавить в качестве исключения.
3. Дважды нажмите**Тип Траффика** и выберите в меню соответствующий тип ранее указанного адреса.
   - Если вы указали веб адрес, выберите **HTTP**.
   - Если вы указали e-mail адрес, выберите **E-mail (SMTP)**.
   - Если вы указали IM контакт, выберите **IM**.

Чтобы удалить запись из таблицы, выберите и нажмите на кнопку **Удалить**.

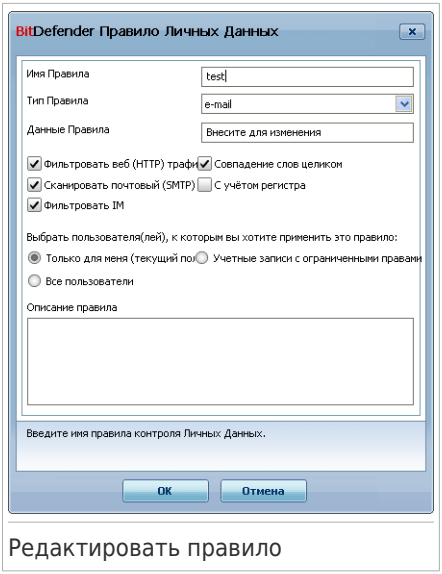
Нажмите **OK** чтобы сохранить сделанные изменения.

19.2.3. Управление правилами

В этом окне Вы видите список правил, приведенный в таблице.

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

Чтобы редактировать правило, необходимо его выбрать 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.

19.2.4. Правила, установленные другими администраторами

Если вы не являетесь единственным пользователем с правами администратора в системе, другие администраторы могут создавать собственные правила конфиденциальности. В случае, если вы не хотите, чтобы правила, созданные другими пользователями, применялись к вам при входе в систему, BitDefender дает возможность исключить себя из любого правила, созданного не вами.

Вы можете видеть все правила, созданные другими администраторами, в таблице **Правила Контроля Конфиденциальных Данных**. В таблице указаны все правила, их имена и пользователи, создавшие их.

Чтобы удалить себя из правила, выберите правило в таблице и нажмите **Удалить**.

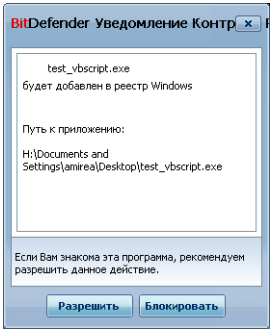
19.3. Контроль Реестра

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

В разделе **Реестр** 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.

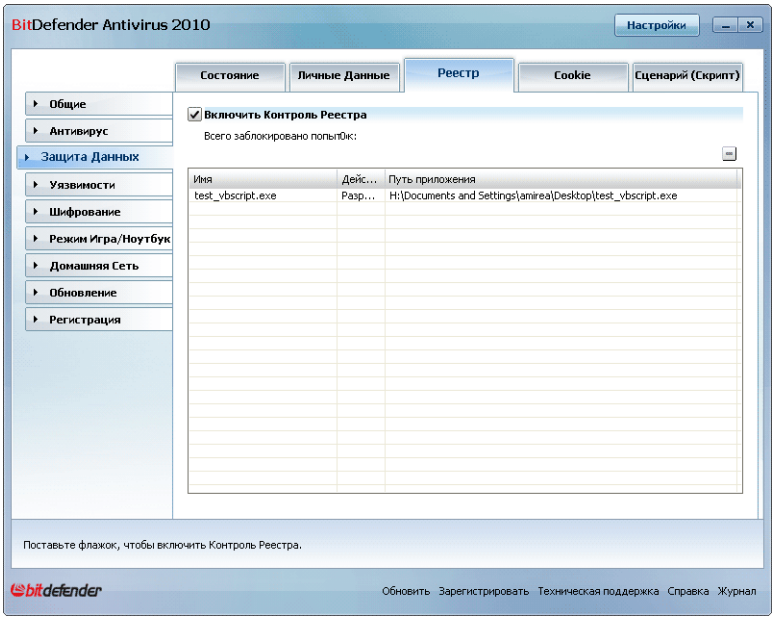
Если вы не узнаете, что это за программа и если одна выглядит подозрительно, нажмите **Блокировать**, чтобы не позволить ей вносить изменения в системный реестр. Иначе нажмите кнопку **Разрешить**, чтобы позволить ей вносить изменения.

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 Контроля Реестра перейдите **Контроль Личных Данных>Реестр** в режиме Опытного Пользователя.



Контроль Реестра

В этом окне Вы видите список правил, приведенный в таблице.

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

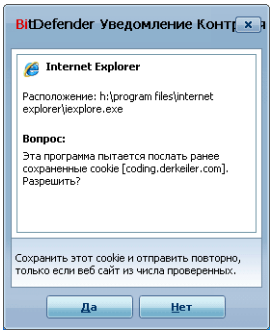
19.4. Контроль Cookie

Cookies встречаются в Интернете очень часто. Это небольшие файлы, хранящиеся на Вашем компьютере. Сайты в сети создают такие файлы, чтобы отслеживать некоторую 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**.Будучи включенной, **Контроль cookie** спрашивает у вас разрешение всякий раз, когда новый сайт пытается создать файл cookie:



Cookie Предупреждение

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

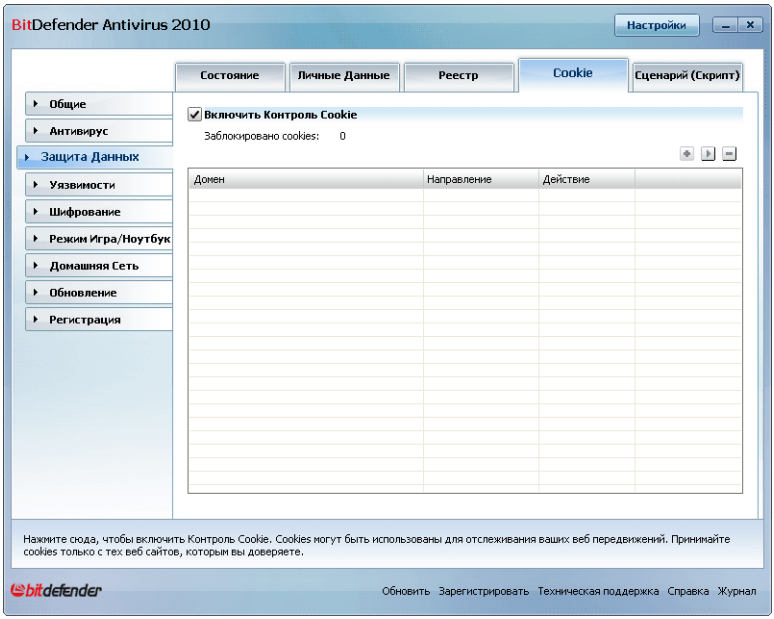
Нажмите **Да** или **Нет** и правило будет создано, применено и внесено в список в таблице.

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 Контроля Cookie перейдите **Контроль Конфиденциальных Данных>Cookie** в режиме Продвинутого Пользователя.



Контроль Cookie

В этом окне Вы видите список правил, приведенный в таблице.

Чтобы удалить правило, выберите его и нажмите кнопку **Удалить**. Чтобы редактировать параметры правил, выберите правило и нажмите кнопку **Редактировать** или дважды кликните по правилу. Сделайте желаемые изменения в окне настроек.

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

19.4.1. Окно настроек

При редактировании или добавления правила вручную, появится окно настроек.

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	cookies в этом домене будут выполняться.
Запретить	cookies в этом домене не будут выполняться.

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

Тип	Описание
Исходящие	Правило применяется только для cookies, которые отсылаются обратно к подключенному сайту.
Входящие	Правило применяется только для cookies, которые поступают от подключенного сайта.
Оба	Правило применяется и ко входящему, и к исходящему трафику.

Замечание

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

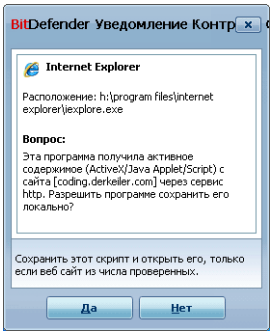
Нажмите **Завершить**.

19.5. Контроль Сценариев

Сценарии и другие приложения, такие как 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 сети. 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:

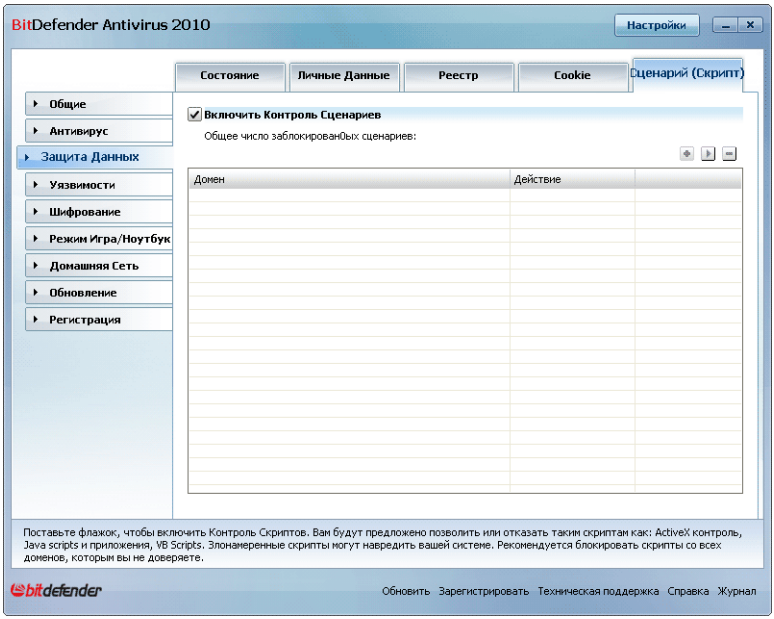


Предупреждение о сценариях

В этом окне Вы видите название ресурса.

Нажмите **Да** или **Нет** и правило будет создано, применено и внесено в список в таблице.

Для настройки Контроля Сценариев перейдите **Контроль Конфиденциальных Данных>Сценарии** в режиме Продвинутого Пользователя.



Контроль Сценариев

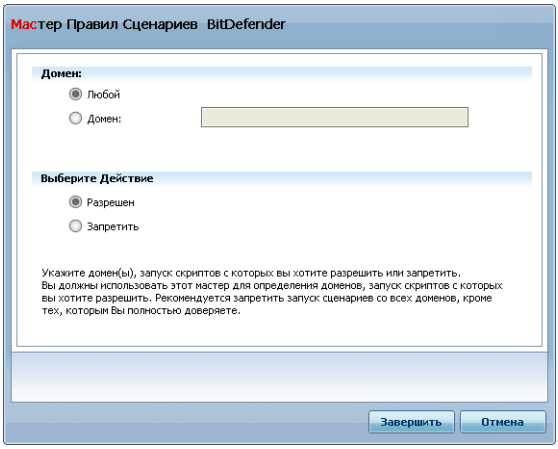
В этом окне Вы видите список правил, приведенный в таблице.

Чтобы удалить правило, выберите его и нажмите кнопку **Удалить**. Чтобы редактировать параметры правил, выберите правило и нажмите кнопку **Редактировать** или дважды кликните по правилу. Сделайте желаемые изменения в окне настроек.

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

19.5.1. Окно настроек

При редактировании или добавления правила вручную, появится окно настроек.



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.

Нажмите **Завершить**.

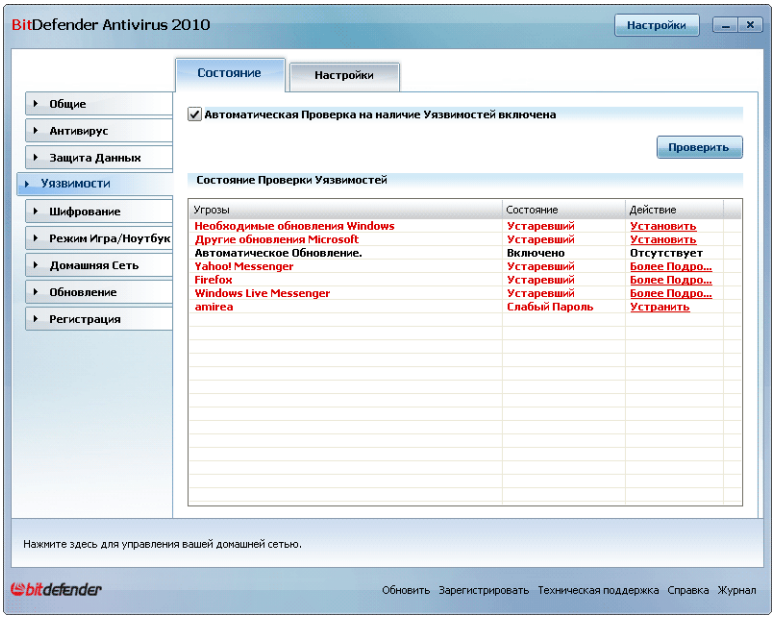
20. Уязвимости

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.

20.1. Состояние

Для настройки автоматической проверки на наличие уязвимостей или запуска проверки перейдите к разделу **Уязвимости>Состояние** в режиме Опытного Пользователя.



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.

20.1.1. Устранение уязвимостей

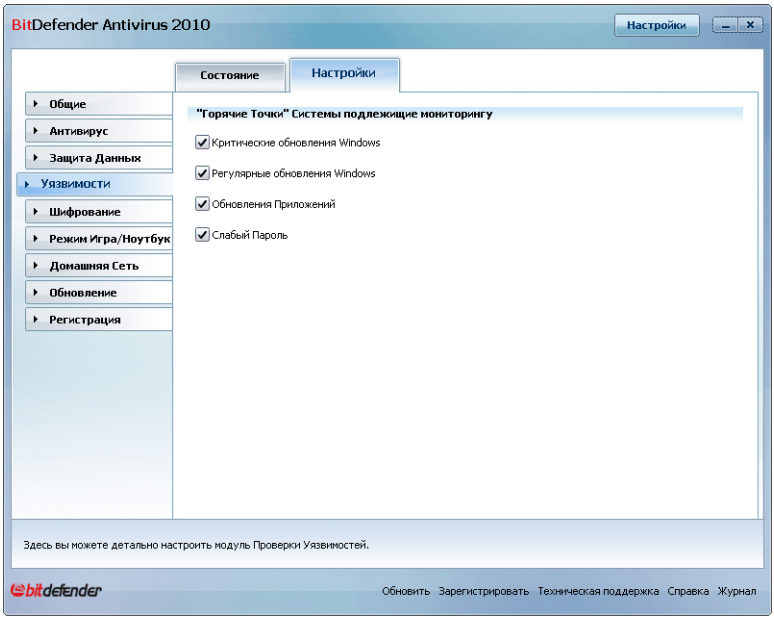
В зависимости от проблемы, для того, чтобы устранить конкретную уязвимость предпримите следующие действия:

- Если доступны обновления Windows, нажмите **Установить** в колонке **Действие** для установки.
- Если версия приложения устарела, воспользуйтесь ссылкой **Домашняя страница** для загрузки и установки последней версии данного приложения.
- Если учетная запись Windows снабжена слабым паролем, нажмите **Исправить** что бы сменить пароль при следующем входе в систему или смените его сами. Чтобы получить сильный пароль, используйте комбинации символов в верхнем и нижнем регистре, числа и специальные символы (такие как, например, #, $ или @).

Вы можете нажать кнопку **Проверить сейчас** и следовать указаниям мастера для пошагового устранения уязвимостей. Для получения дополнительной информации перейдите к *«Мастер Проверки на Наличие Уязвимостей»* (p. 68).

20.2. Настройки

Для настройки параметров автоматической проверки на наличие уязвимостей перейдите к разделу **Уязвимости>Настройки** в режиме Опытного Пользователя.



Автоматическое сканирование на наличие уязвимостей

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

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

Замечание

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

21. Шифрование приложений мгновенного обмена сообщениями IM

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.

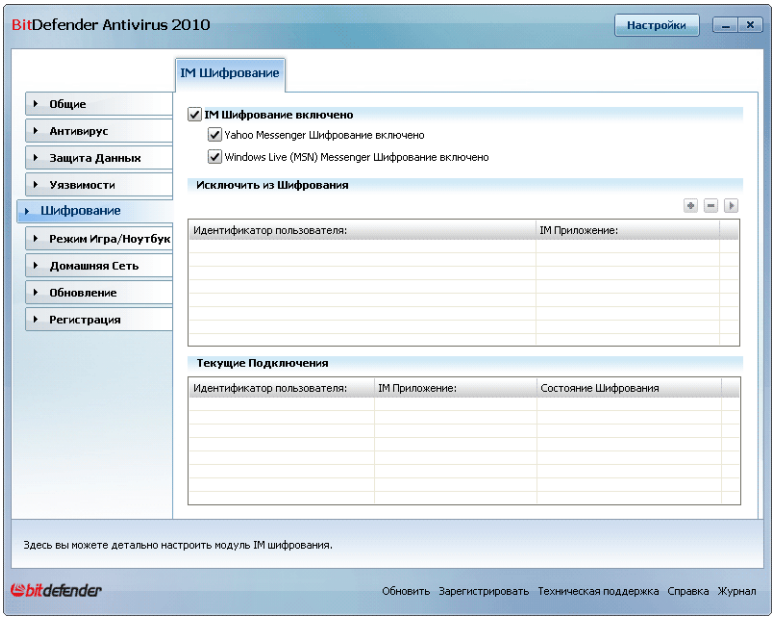
Важно

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 режиме Опытного Пользователя.

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 IM-программы»* (p. 213).



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.

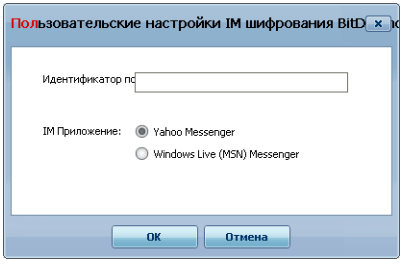
Отобразятся две таблицы:

- **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:
  - Вы отключили функцию шифрования для данного контакта.
  - У вашего контакта не установлена версия BitDefender, которая поддерживает шифрование мгновенных сообщений.

21.1. 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 ID вашего контакта.
3. Выберите интернет-пейджер, связанный с данным контактом.
4. Нажмите **OK**.

22. Режи Игры/Режим Ноутбука

Режи Игры/Режим Ноутбука позволяет настраивать специальные режимы работы BitDefender:

- Режим Игры временно изменяет параметры продукта с целью минимизации потребления ресурсов при игре.
- Режим Ноутбука предотвращает выполнение запланированных заданий при работе ноутбука от батареи с целью экономии заряда батареи.

22.1. Режим Игры

Режим Игры изменяет параметры настроек системы защиты для того, чтобы снизить к минимуму воздействие на компьютер во время игры. При включении Режима Игры, применяются следующие настройки:

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

Замечание

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

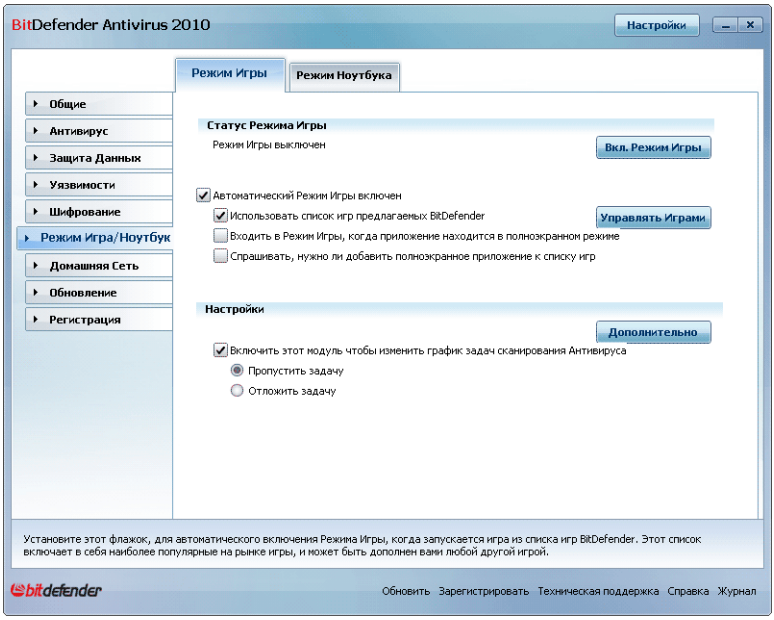
- Запланированные задания проверки отключены по умолчанию

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

Находясь в Режиме Игры, вы будете видеть букву G поверх значка BitDefender.

Для настройки игрового режима перейдите в раздел **Игра/Режим ноутбука>Игровой режим** в режиме Опытного Пользователя.



Режим Игры

Вверху раздела отображается состояние Режима Игры. Нажмите **Включить Режим Игры** или **Выключить Режим Игры** для изменения текущего статуса.

22.1.1. Настройка автоматического перехода в Режим Игры

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

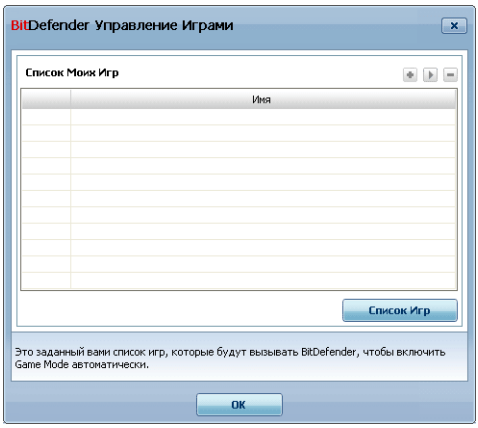
- **Использовать список игр предлагаемых BitDefender** - для автоматического входа в Режим Игры при запуске игры из списка известных игр BitDefender. Для просмотра этого списка нажмите **Управление Играми**, затем **Список Игр**.
- **Вход в режим игры при полноэкранном режиме** - для автоматического перехода в режим игры 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. Добавив новое приложение в список игр, при следующем его запуске BitDefender автоматически перейдет в режим игры.

Замечание

Если вы не хотите, чтобы BitDefender автоматически переходил в режим игры, снимите флажок **Автоматический режим игры**.

22.1.2. Управление списком игр

BitDefender автоматически переходит в Режим Игры при запуске приложения из списка игр. Для просмотра и управления списком игр нажмите **Управление 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 списка нажмите **Список /Игр**.
- 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 Режим Игры для обычных приложений, которые переходят в полноэкранный режим, таких как, например, веб-браузеры и проигрыватели видео.

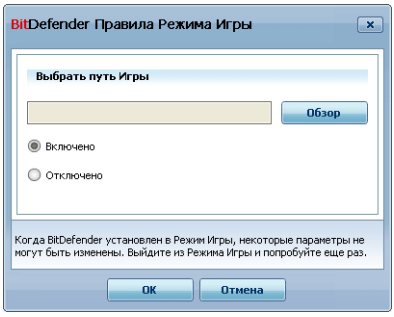
Для управления списком игр вы можете воспользоваться кнопками, находящимся вверху таблицы:

- **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.

22.1.3. Настройка Параметров Режима Игры

Для настройки режима работы при запланированных заданиях воспользуйтесь следующими параметрами:

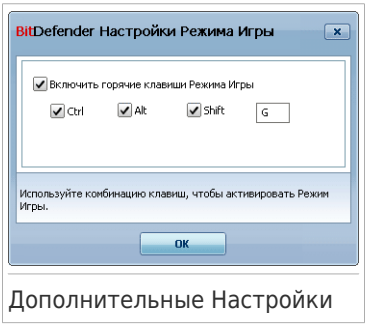
- **Включить этот модуль для изменения запланированных задач антивирусного сканирования** - для предотвращения запуска запланированных задач в Режиме Игры. Вы можете выбрать один из следующих параметров:

Настройка	Описание
Пропустить задачу	Никогда не запускать запланированное задание.
Отложить задачу	Выполнять запланированное задание сразу после выхода из режима игры.

22.1.4. 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 **Дополнительные Настройки**. Появится новое окно.



Дополнительные Настройки

2. Используя парамер **Использовать Горячие Клавиши**, задайте желаемую горячую клавишу :
   - 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 **Использовать горячую клавишу** вы отключите использование данной горячей клавиши.

3. Нажмите **OK** чтобы сохранить сделанные изменения.

22.2. Режим Ноутбука

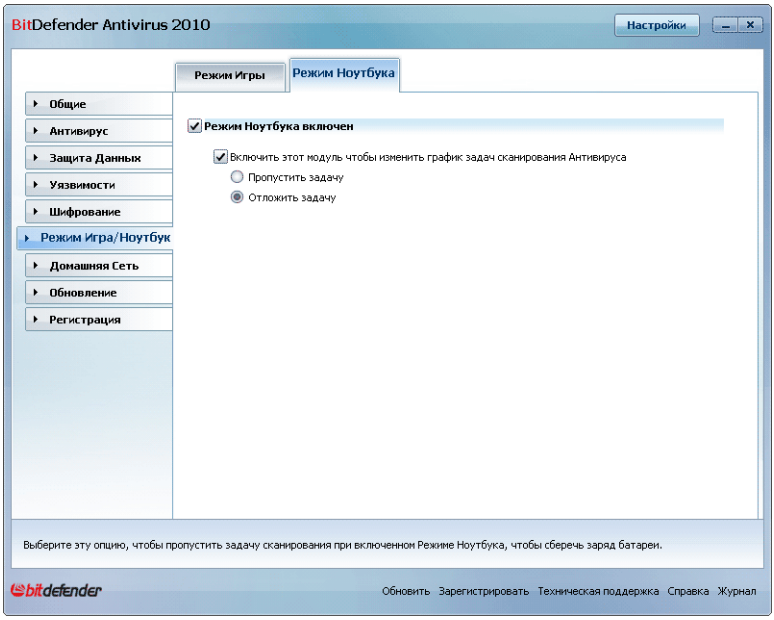
Режим ноутбука специально предназначен для пользователей портативных компьютеров. Его цель - минимизировать влияние работы BitDefender на энергопотребление, когда эти устройства работают от батареи.

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>Режим Ноутбука** в режиме Опытного Пользователя.



Режим Ноутбука

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

22.2.1. Настройка Параметров Режима Ноутбука

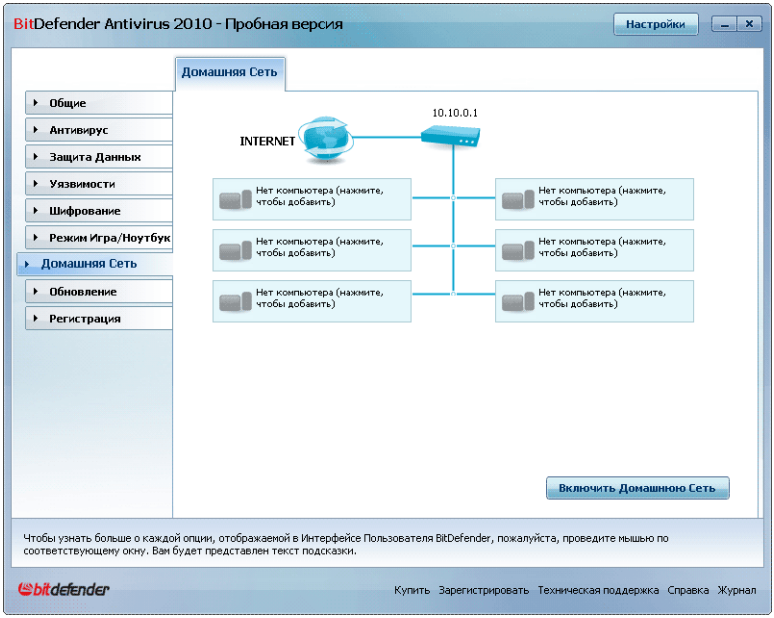
Для настройки режима работы при запланированных заданиях воспользуйтесь следующими параметрами:

- **Включить этот модуль для изменения запланированных задач антивирусного сканирования** - для предотвращения запуска запланированных задач в Режиме Ноутбука. Вы можете выбрать один из следующих параметров:

Настройка	Описание
Пропустить задачу	Никогда не запускать запланированное задание.
Отложить задачу	Выполнять запланированное задание сразу после выхода из Режима ноутбука.

23. Домашняя Сеть

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



Карта сети

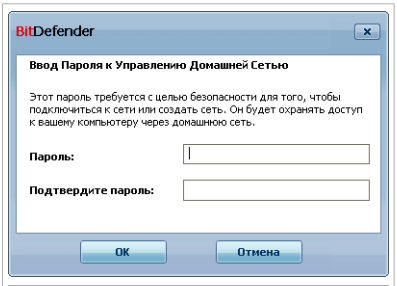
Для управления продуктами BitDefender, установленными на ваших домашних компьютерах, необходимо выполнить следующую процедуру:

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

23.1. Подключение к сети BitDefender

Чтобы подключиться к домашней сети BitDefender, выполните следующую процедуру:

1. Нажмите **Управление Сетью**. Появится окно настройки пароля для управления домашней сетью.



Настройка пароля

2. Введите пароль в каждом из полей ввода.
3. Нажмите **OK**.

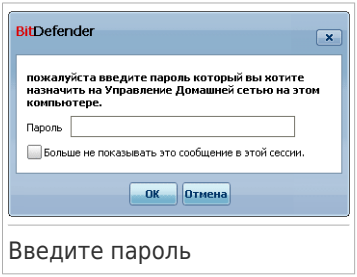
На карте сети будет отображаться имя компьютера.

23.2. Добавление компьютеров в сеть BitDefender.

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

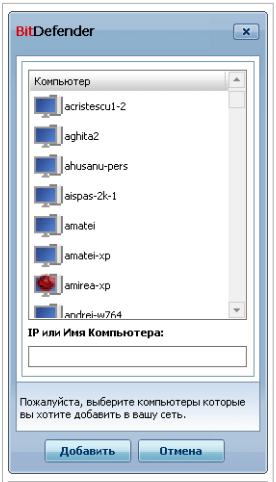
Чтобы добавить компьютер в домашнюю сеть BitDefender, выполните следующую процедуру:

1. Нажмите **Добавить Компьютер**. Появится окно ввода пароля для управления домашней сетью.



Введите пароль

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



Добавить компьютер

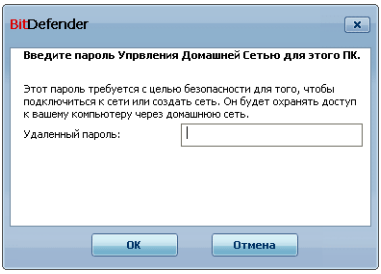
Вы увидите список компьютеров, находящихся в сети. Значок имеют следующее значение:

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. Выполните одно из следующих действий:
   - 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.



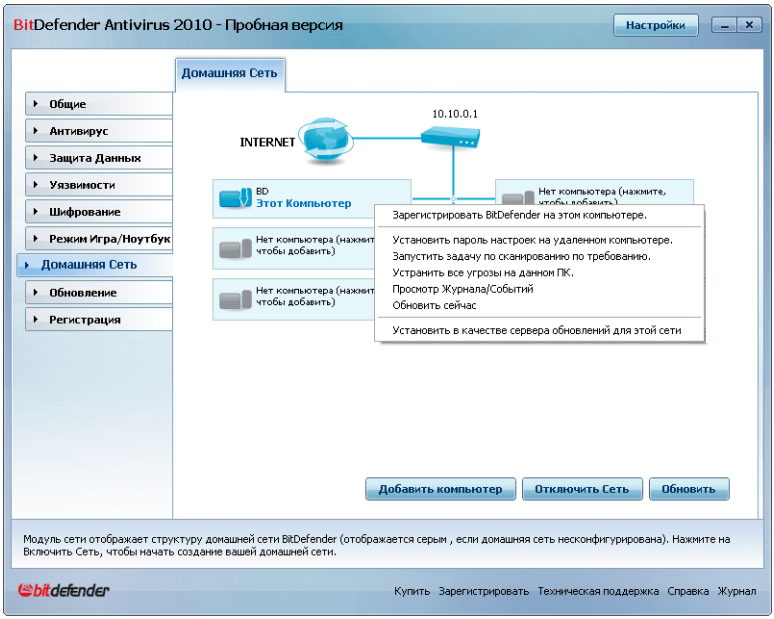
Авторизация

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

Замечание
Вы можете добавить до пяти компьютеров на карту сети.

23.3. 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 мыши на имени компьютера на карте сети, вы увидите список административных задач, которые можно запустить на удаленном компьютере.

- **Удалить ПК из домашней сети**

  Позволяет удалить ПК из сети.

- **Зарегистрировать BitDefender на этом компьютере**

  Позволяет зарегистрировать BitDefender на этом компьютере, с помощью лицензионного ключа.

- **Установить пароль настроек на удаленном ПК**

  Позволяет создать пароль для ограничения доступа к настройкам BitDefender на этом компьютере.

- **Запустить задачу сканирования по запросу**

  Позволяет запустить сканирование по требованию, на удаленном компьютере. Вы можете выполнить любую из следующих задач

сканирования: Сканирование Моих Документов, Системное Сканирование или Глубокое Системное Сканирование.

- **Устранить все проблемы на этом ПК**

  Позволяет исправить проблемы, влияющие на безопасность этого компьютера следуя мастеру Устранить все угрозы

- **Простотр Журнала/Событий**

  Позволяет получить доступ к **Истории&Событий** модуля продукта BitDefender, установленного на этом компьютере.

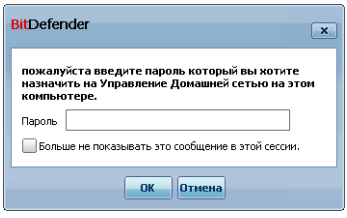
- **Обновить сейчас**

  Инициирует процесс обновления для продукта BitDefender, установленном на этом компьютере.

- **Назначить сервером обновлений этой сети**

  Позволяет установить этот компьютер, как сервер обновлений для всех продуктов BitDefender, установленных на компьютерах в сети. Использование этой опции позволит снизить интернет-трафик, потому что только один компьютер в сети будет подключаться к интернету для загрузки обновлений.

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.

24. Обновление

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

Если Вы подключаетесь к Интернет через широкополосное соединения или DSL, BitDefender берет на себя решение вопросов безопасности: по умолчанию проверяет наличие обновлений сразу же при подключении, и затем каждый **час**.

Если будет обнаружено обновление, вам будет предложено подтвердить его установку, или же обновление начнется автоматически, в зависимости от настроек автоматического обновления.

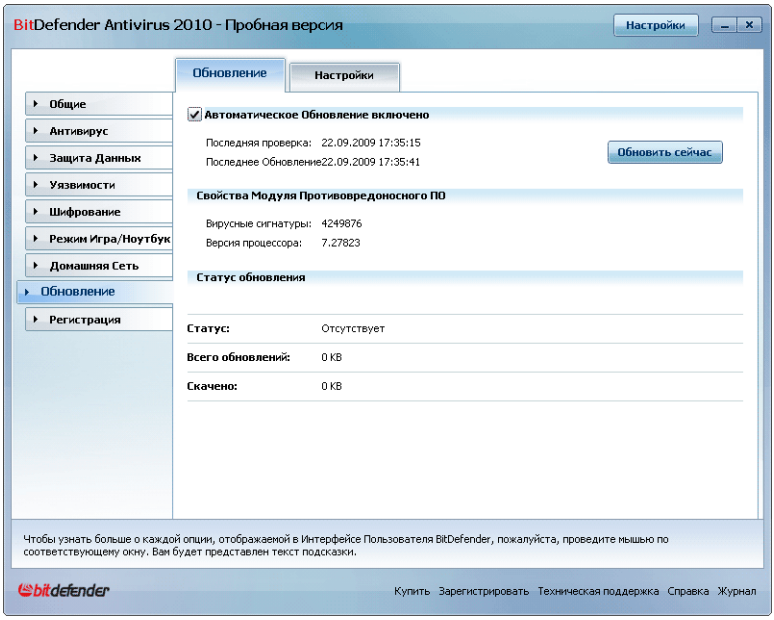
Процесс обновления происходит "на лету", т.е. файлы заменяются по мере обновления. Таким образом, процесс обновления не влияет на работоспособность продукта, и, в то же время, исключается возможность возникновения уязвимости Вашего компьютера.

Обновления происходят следующим путем:

- **Обновления модуля антивируса** - при появлении новых угроз, необходимо обновить файл вирусных сигнатур для обеспечения беспрерывной защиты от них. Этот тип обновления также известен как **Обновление Описаний Вирусов**.
- **Обновление защиты от программ-шпионов** - сигнатуры новых программ-шпионов будут добавлены в базу данных. Этот тип обновления также известен как **Обновление модуля Антишпион**.
- **Обновления программного продукта** - при выпуске новой версии программы в новую версию добавляются новые функции и методы проверки, что только улучшает работу программы. Этот тип обновления также известен как **Обновление программы**.

24.1. Автоматическое обновление

Для просмотра сведений, связанных с обновлением, и выполнения автоматических обновлений перейдите в раздел **Обновление>Обновление** в режиме Опытного Пользователя.



Автоматическое обновление

Здесь Вы можете просмотреть, когда была последняя проверка на наличие доступных 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 количестве сигнатур.

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.

24.1.1. Запрос обновления

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

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
Может потребоваться перезагрузка компьютера для завершения обновления. Мы рекомендуем сделать это как можно раньше.

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

24.1.2. Отключение автоматического обновления

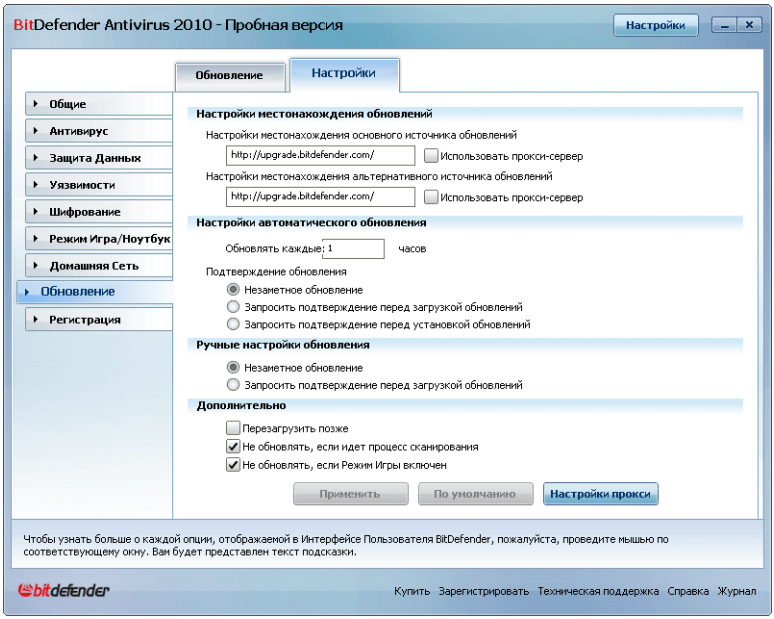
Если Вы выберите эту опцию, то появится окно с предупреждением: Вы должны подтвердить свое намерение, выбрав промежуток времени, на который Вы хотите отключить автоматическое обновление. Вы можете отключить на 5, 15 или 30 минут, на час, навсегда или до следующей перезагрузки системы.

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.

24.2. Настройки обновления

Обновление может быть выполнено через локальную сеть, через Интернет напрямую или через прокси-сервер. По умолчанию BitDefender проверяет наличие обновлений ежечасно через Интернет и устанавливает доступные обновления без уведомления.

Чтобы установить настройки обновлений и настроить прокси, перейдите в раздел **Обновления>Настройки** в Режиме Опытного Пользователя.



Настройки обновления

Настройки обновления сгруппированы в 4 категории: (**Настройки местоположения обновления**, **Настройки автоматического обновления**, **Настройки ручного обновления** и **Дополнительные настройки**). Каждая из категорий будет описано отдельно.

24.2.1. 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 местоположение обновления введите URL адрес локального зеркала в поле **URL**, соответствующем месту, которое Вы хотите изменить.

Замечание

Рекомендуем установить локальное зеркало в качестве основного местоположения обновления и оставить альтернативное местоположеине без изменений, в качестве запасного на случай, если локальное зеркало станет недоступным.

Если компания использует прокси сервер для выхода в Интернет, поставьте отметку в поле **использовать прокси**, а затем нажмите **Настройки прокси** для изменения настроек прокси. За более подробной информацией перейдите *«Управление прокси»* (p. 199)

24.2.2. Настройки автоматического обновления

Чтобы настроить процесс обновлений, автоматически выполняемый BitDefender,используйте опции в категории **Настройки автомотического обновления**.

Вы можете указать количество часов между думя последовательными проверками на наличие обновлений в поле **Обновлять каждый...**. По умолчанию интервал составляет 1 час.

Чтобы указать, как необходимо проводить процесс автоматического обновления, выберите одну из следующих опций:

- **Тихое Обновление** - 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.

24.2.3. Настройка обновления вручную

Чтобы указать, как необходимо проводить процесс ручного обновления (обновления по запросу пользователя), выберите одну из следующих опций в категории **Настройки ручного обновления**:

- **Тихое обновление** - 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.

24.2.4. Изменение дополнительных настроек

Чтобы процесс обновления BitDefender не мешал Вашей работе на компьютере, настройте опции в категории **Дополнительные настройки**:

- **Перезагрузить позже** - 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 будет проводить обновление во время сканирования, процесс сканирования будет прерван.

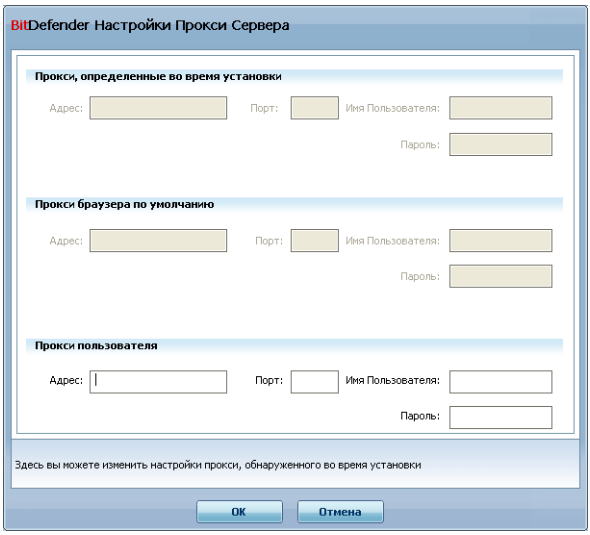
- **Не выполнять обновление, когда включен режим игры** - BitDefender не будет проводить обновление, пока включен режим игры. Таким образом, Вы можете минимизировать влияние продукта на работу системы в течение игр.

24.2.5. 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, установившего 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.

Для управления настройками прокси нажмите **Настройки прокси**.Откроется новое окно.



Управление прокси

Есть три параметра настройки для прокси:

- **Прокси определенные во время установки ПО** - 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.
- **Прокси браузер по умолчанию** - прокси-сервера для текущего пользователя, извлеченный из браузера по умолчанию. Если прокси-сервер требует ввода имени пользователя и пароля, вы должны указать 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.

- **Спользовательсике 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, используемый BitDefender для подсоединения к прокси серверу.

- **Пользователь** - введите имя пользователя, опознаваемого прокси-сервером.
- **Пароль** - введите пароль пользователя, указанного ранее.

При попытке соединения к Интернету, будет поочередно пробоваться каждый набор настроек прокси, пока BitDefender не удастся установить соединение.

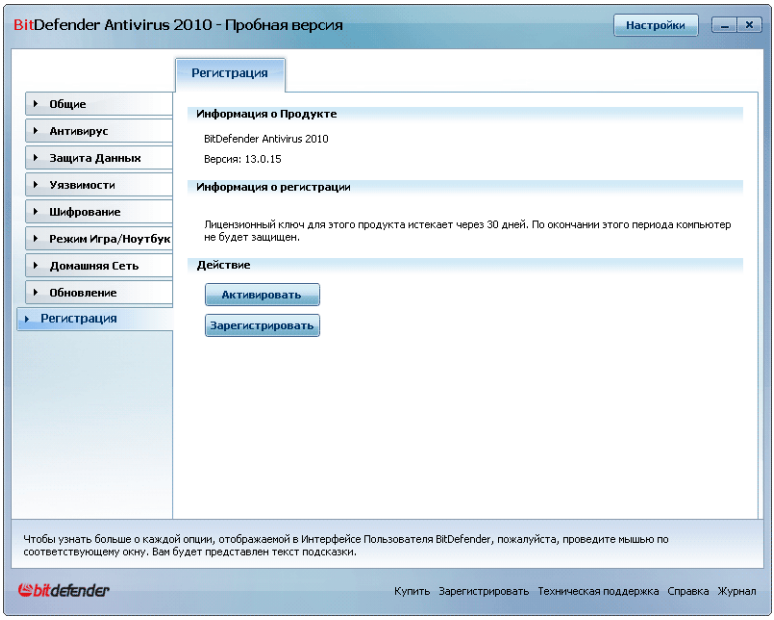
Прежде всего, для соединения к Интернет будет использованы Ваши собственные настройки прокси. Если это не поможет, следующими будут использованы настройки сервера, обнаруженные при установке продукта. В конце концов, если ни один из вариантов не сработает, будут использованы настройки прокси сервера, который использует браузер по умолчанию для соединения с Интернет.

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

Нажмите**Применить** чтобы сохранить изменения или нажмите **По умолчанию** чтобы загрузить настройки по умолчанию.

25. Регистрация

Чтобы найти полные сведения по вашему продукту BitDefender и состояние регистрации, перейдите в раздел **Регистрация** в режиме Опытного Пользователя.



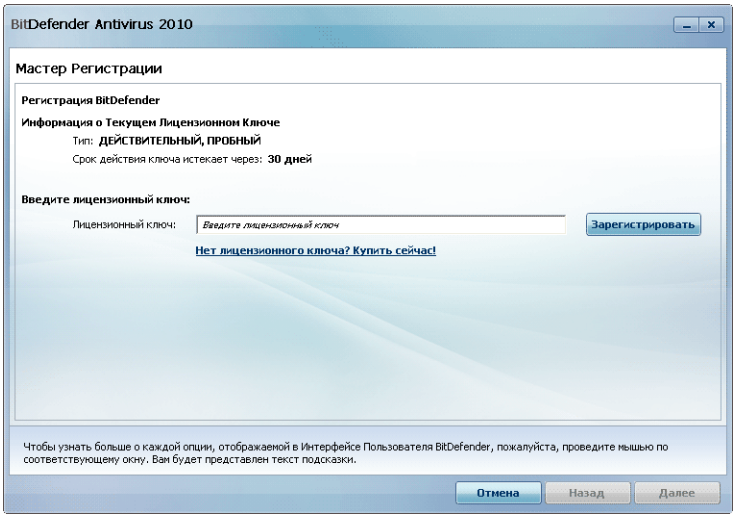
Регистрация

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.

25.1. Регистрация BitDefender Antivirus 2010

Нажмите **Зарегистрировать Сейчас** 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 2010:

1. 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.

2. Нажмите **зарегистрировать Сейчас**.
3. Нажмите **Завершить**.

25.2. Создание учетной записи BitDefender

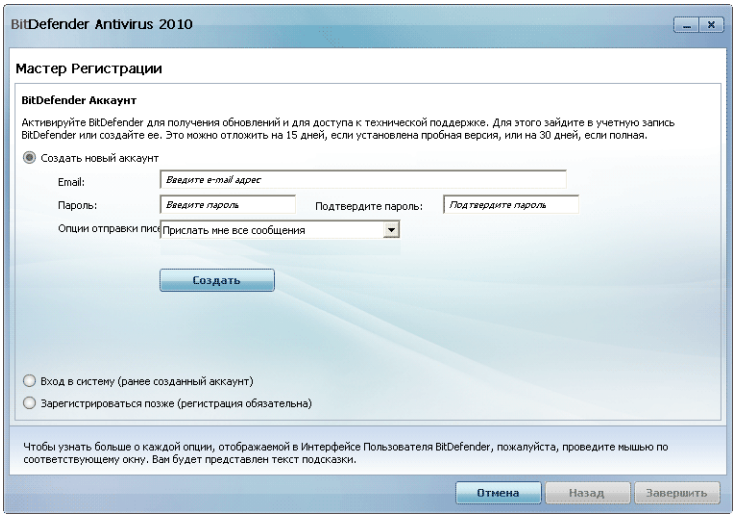
Создание учетной записи BitDefender является обязательной частью процесса регистрации. Учетная запись BitDefender даст вам доступ к обновлениям, специальным предложениям и поощрениям. Если вы потеряете лицензионный

ключ BitDefender, вы сможете зайти в свою учетную запись по ссылке http://myaccount.bitdefender.com, чтобы восстановить его.

Важно

Вам необходимо создать аккаунт в течении 15 дней со дня установки BitDefender (если вы его зарегистрировали, срок пробного периода становится равным 30 дней). В противном случае, BitDefender не будет обновляться.

Если вы еще не создали учетную запись BitDefender, нажмите **Активировать Продукт**, чтобы открыть окно регистрации учетной записи.



Создание учетной записи

Если Вы не хотите создавать учетную запись BitDefender прямо сейчас, выберите **Зарегистрировать позже** и нажмите **Завершить**. В ином случае, действуйте исходя из вашей ситуации:

- «У меня нет учетной записи BitDefender» (p. 204)
- «У меня уже есть учетная запись BitDefender» (p. 205)

У меня нет учетной записи BitDefender

Для успешного создания аккаунта BitDefender, следуйте этим шагам:

1. Выберите **Создать новый аккаунт**.4564 messages remaining

2. Напечатайте необходимую информацию в соответствующих полях. Предоставленные Вами данные конфиденциальны.
   - **Адрес электронной почты** - введите адрес своей электронной почты.
   - **Пароль** - введите пароль Вашей учетной записи BitDefender. Пароль должен содержать не менее 6 и не более 16 символов.
   - **Повторите пароль** - снова введите набранный ранее пароль.

   Замечание
   После активации учетной записи, вы можете использовать имеющийся адрес электронной почты и пароль, чтобы войти в свой аккаунт на http://myaccount.bitdefender.com.

3. Дополнительно, BitDefender может информировать вас о специальных предожениях и поощрениях по электронной почте, указанной в вашей учетной записи. Выберите одну из доступных опций из меню:
   - **Отправлять мне все сообщения**
   - **Отправлять мне только сообщения, связанные с продуктом**
   - **Не отправлять мне сообщения**
4. Нажмите **Создать**.
5. Нажмите **Завершить** для завершения работы мастера.
6. **Активируйте ваш аккаунт.** Чтобы использовать аккаунт вы должны его активировать. Проверьте почту и следуйте инструкциям в письме, отправленном вам сервисом регистрации BitDefender.

У меня уже есть учетная запись BitDefender

BitDefender автоматически определит, если вы решистрировали учетную запись BitDefender ранее на этом компьютере. В этом случае, введите пароль от вашего аккаунта и нажмите **Вход в Систему**. Нажмите **Завершить** для завершения работы мастера.

Если у вас уже есть активный аккаунт, но BitDefender не может его обнаружить, следуйте этим шагам что бы привязать продукт к этому аккаунту:

1. Выберите **Вход в систему (ранее созданный аккаунт)**.
2. Напечатайте e-mail адрес и пароль вашего аккаунта в соответствующих полях.

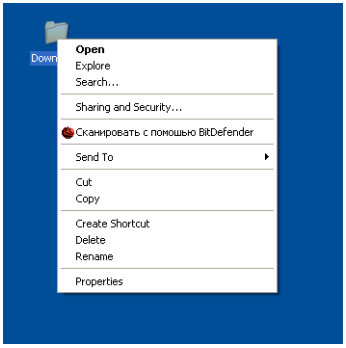
   Замечание
   Если Вы забыли пароль, нажмите **Забыли пароль?** и следуйте инструкциям.

3. Дополнительно, BitDefender может информировать вас о специальных предожениях и поощрениях по электронной почте, указанной в вашей учетной записи. Выберите одну из доступных опций из меню:
   - **Отправлять мне все сообщения**
   - **Отправлять мне только сообщения, связанные с продуктом**
   - **Не отправлять мне сообщения**
4. Нажмите **Вход в Систему**.
5. Нажмите **Завершить** для завершения работы мастера.

Интеграция в Windows и стороннее ПО

26. Интеграция в контекстное меню Windows

Контекстное меню Windows появляется когда вы щелкаете правой кнопкой на папке или файле в вашем компьютере.



Контексное меню Windows

BitDefender интегрируется в контекстное меню Windows чтобы обеспечить возможность быстрого сканирования файлов и папок. Вы можете быстро найти BitDefender в контекстном меню, увидев значок BitDefender.

26.1. Сканировать с помощью BitDefender

Вы можете легко сканировать файлы, папки или даже целые диски через контекстное меню Windows. Щелкните правой кнопкой мыши по нужному объекту и выберите в меню **Сканировать с BitDefender**. Появится Мастер сканирования и проведет вас по процессу сканирования .

Параметры сканирования. Опции сканирования предварительно настроены для достижения наилучших результатов обнаружения. При обнаружении инФицированных файлов, BitDefender попробует их излечить (удалить вредоносные коды). Если это не получится, то Мастер сканирования даст вам возможность определить что с ними делать.

Чтобы изменить настройки сканирования, выполните следующие шаги:

1. Откройте BitDefender и установите пользовательский интерфейс в Режим опытного пользователя.
2. Нажмите **Антивирус** в левом меню.
3. Нажмите на вкладку **Сканирование Вирусов**.
4. Правой кнопкой мыши нажмите **Контекстное сканирование** и выберите **Открыть**. Появится новое окно.

5. Нажмите **Пользовательский** и настройте параметры сканирования по своему усмотрению. Для того чтобы узнать на что влияет настройка, подержите курсор мыши над ней. Внизу окна появится подсказка.
6. Нажмите **OK** чтобы сохранить сделанные изменения.
7. Нажмите **OK** чтобы прменить новые настройки сканирования.

Важно
Не стоит менять настройки или метод сканирования без веской на то причины.

27. Интегрирование в веб браузеры

BitDefender защищает Вас от попыток фишинга, когда Вы работаете Интернете. Сканирует просматриваемые веб сайты и сообщает, если существует угрозы фишинга. Можно создать Белый Список веб-сайтов, которых не надо сканировать с BitDefender.

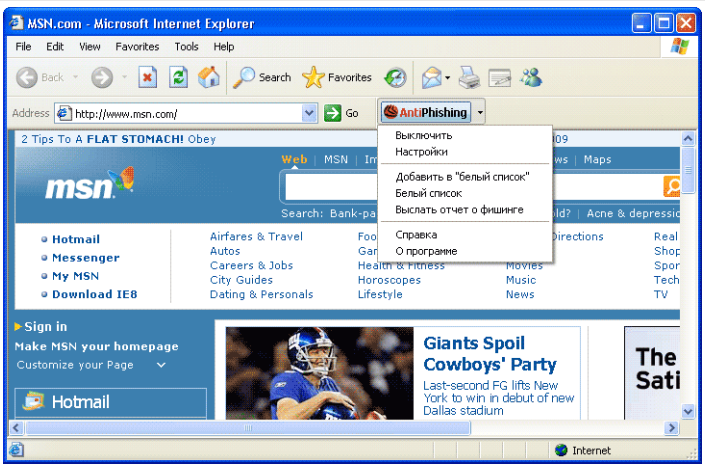
BitDefender интегрируется непосредственно через интуитивную панель инструментов в следующие веб-браузеры:

- Internet Explorer
- Mozilla Firefox

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

Панель инструментов антифишинга, представленная иконкой BitDefender, располагается в верхней части браузера. Нажмите, чтобы открыть меню панели инструментов.

Замечание
Если Вы не видите панель инструментов, откройте меню **Просмотр**, перейдите к **Панель инструментов** и выберите **Панель инструментов BitDefender**.



Панель инструментов антифишинга

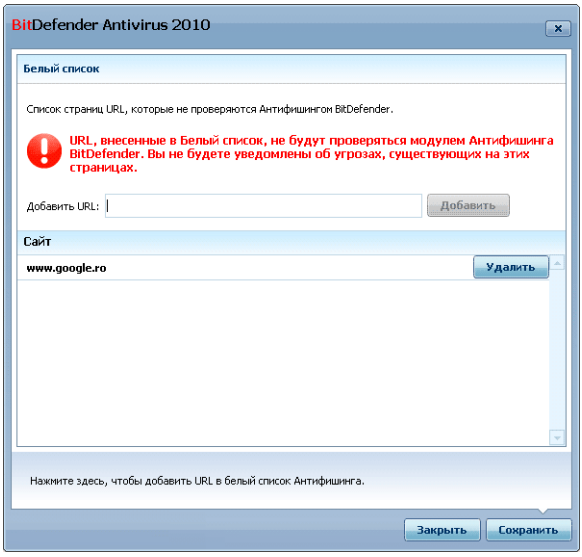
Следующие команды доступны в меню панели инструментов:

- **Включить / Выключить** - включает / выключает антифишинг-защиту BitDefender в текущем браузере.
- **Настройки** - открывает окно, где Вы можете определить настройки панели инструментов антифишинга. Доступными являются следующие варианты:
  - **Защита от фишинга в режиме реального времени** - обнаруживает и сообщает об обнаружении фишинг-сайта (созданного для кражи ичной информации). Эта настройка контролирует защиту от фишинга BitDefender только в текущем браузере.
  - **Запрос перед добавлением в белый список** - спрашивает Вас перед добавлением веб сайта в Белый список.
- **Добавить в Белый список** - добовляет текущий веб сайт 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.

- **Белый Список** - открывает Белый список.



Белый спиок антифишинга

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 Белй Список 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**.

- **Отправить отчет о фишинге** - информирует специалистов BitDefender о подозрении на то, что данный сайт используется для фишинга. Сообщая о фишинг-сайтах вы помогаете другим не допустить кражу личной информации.
- **Справка** - 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.

28. Интеграция в IM-программы

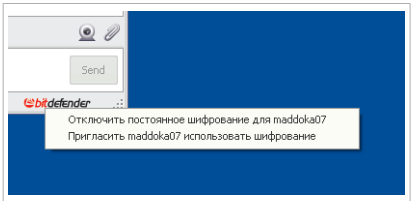
BitDefender предоставляет возможности защиты конфиденциальных документов и обмена сообщениями между интернет-пейджерами Yahoo Messenger и MSN Messenger.

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. Панель инструментов расположена в праом нижнем углу окна чата. Поищите значок BitDefender чтобы найти ее.



Панель инструментов BitDefender

Замечание
Панель показывает, что общение защифровано, отображая ключик рядом с логотипом BitDefender.

Щелчок на панели инструментов BitDefender вызывает следующие параметры:

- **Навсегда отменить шифрование для контакта.**
- **Предложить собеседнику использовать шифрование.** Чтобы зашифровать ваше общение, ваш собеседник должен установить BitDefender и использовать совместимую IM программу.

Как?

29. Как сканировать Файлы и папки

Сканировать с помощью BitDefender легко. Есть 4 способа заставить BitDefender сканировать файли и папки на вирусы:

- Через контекстное меню Windows
- Используя задачи сканирования
- Используя ручное сканирование BitDefender
- Используя Панель Активности Сканирования

После начала сканирования, появится Мастер Сканирования на Антивирусы и проведет вас через весь процесс. Для получения дополнительной информации перейдите к «*Мастер антивирусного сканирования*» (p. 56).

29.1. Использование контекстного меню Windows

Это самый простой и рекомендуемый способ проверить файл или папку на вашем компьютере. Щелкните правой кнопкой мыши по нужному объекту и выберите в меню **Сканировать с BitDefender**. Следуйте подсказкам мастера Сканирования на Антивирусы.

Типичные ситуации, в которых вы можете пользоваться этим методом сканирования:

- Вы подозреваете, что файл или папка заражена.
- когда вы загружаете из интернета файлы, которые, как вам кажется, могут быть опасны.
- Проверить сетевые папки перед копированием на ваш компьютер.

29.2. Использование Задач канирования

Если вы хотите проверять ваш компьютер или отдельные папки регулярно, вам стоит воспользоваться задачами сканирования. Задачи сканирования информируют BitDefender, какие объекты сканировать и какие действия применять. Более того, вы можете запланировать их запуск на регулярной основе или в определенное время.

Чтобы проверить ваш компьютер с использованием задач сканирования, откройте интерфейс BitDefender и запустите нужную задачу. В зависимости от режима просмотра пользовательского интерфейса, задачи сканирования запускаются разними способами.

Запуск заданий сканирования в Режиме Новичка

В Режиме Новичка можно запустить только стандартную проверку всего компьютера, нажав **Сканировать Сейчас**. Следуйте подсказкам мастера Сканирования на Антивирусы.

Запуск заданий сканирования в Режиме Пользователя

В Режиме Пользователя вы можете запустить несколько предварительно настроенных задач проверки. Вы также можете настроить и запустить пользовательские задачи по сканированию для проверки конкретных файлов на Вашем компьютере с помощью пользовательских параметров сканирования. Выполните следующие действия, чтобы запустить задачу проверки в Режиме Пользователя:

1. Щелкните на вкладке **Антивирус**.
2. В левой области Быстрых Задач нажмите **Сканирование Системы** для запуска стандартной задачи по сканированию всего компьютера. Для запуска иной задачи нажмите стрелку на кнопке и выберите желаеую задачу. Для настройки и запуска пользовательского сканирования, нажмите **Пользовательское Сканирование**. Вам доступны следующие задания:

Задача Сканирования	Описание
Сканирование Системы	Проверка всей системы кроме архивов. В настройках по умолчанию проводится проверка на все типы вирусного ПО, кроме руткитов.
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.
Сканировать Мои документы	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.
Пользовательское Сканирование	Эта опция помогает настроить и запустить сканирование пользовательских задач, позволяющие вам уточнить, какие файлы сканировать и общие параметры сканирования. Вы можете сохранять пользовательские задачи

Задача Сканирования	Описание
	проверки, чтобы в дальнейшем иметь к ним доступ в режиме Новичка или Опытного Пользователя.

3. Следуйте подсказкам мастера Сканирования на Антивирусы. Для запуска пользовательских зада необходимо запустить мастера Пользовательского Сканирования.

Запуск заданий сканирования в Режиме Опытного Пользователя

В режиме Опытного Пользователя вы можете запустить все предварительно настроенные задачи проверки, а также изменять их параметры сканирования. Более того, вы можете создавать пользовательские задачи проверки, если вы хотите сканировать определенные области вашего компьютера. Выполните следующие действия, чтобы запустить задачу проверки в Режиме Опытного Пользователя:

1. Нажмите **Антивирус** в левом меню.
2. Нажмите на вкладку **Сканирование Вирусов**. Здесь вы модете найти набор задач по умолчанию и создать свои собственные. По умолчанию вам доступны следующие задачи сканирования:

Задачи по умолчанию	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.
Сканирование Системы	Проверка всей системы кроме архивов. В настройках по умолчанию проводится проверка на все типы вирусного ПО, кроме руткитов.
Быстрая проверка системы	Сканирует папки Windows и Program Files. В конфигурации по умолчанию проверка производится на все виды вредоносных программ, кроме руткитов. Не производится проверка памяти, реестра и записей cookies.
Мои документы	Используйте данное задание для проверки основных папок пользователя: Мои документы, Рабочий стол and Автозагрузка. Это позволит

Задачи по умолчанию	Описание
	обеспечить безопасность Ваших документов, безопасность рабочего пространства и запуск незараженных программ при загрузке.

3. Нажмите дважды на необходимую задачу.
4. Следуйте подсказкам мастера Сканирования на Антивирусы.

29.3. Ручная проверка BitDefender

Ручное сканирование BitDefender дает вам возможность сканировать конкретную папку или диск не создавая задания сканирования. Эта функция разработана для использования в Безопасном режиме Windows Если ваша система заражена устойчивым вирусом попробуйте удалить его, запустив Безопасный режим Windows и просканировав все жесткие диски используя ручное сканирование BitDefender.

Чтобы запустить ручную проверку BitDefender следуйте инструкции:

1. В меню Пуск, перейдите к **Пуск → Программы → BitDefender 2010 → BitDefender Ручное сканирование**. Появится новое окно.
2. Нажмите **Добавить Папку** что бы выбрать цель сканирования. Появится новое окно.
3. Выберите объект проверки:
   - Чобы проверить Рабочий, стол выберите **Рабочий стол**.
   - Чтобы просканировать весь жесткий диск, выберите его в папке Мой Компьютер.
   - Чтобы проверить конкретную папку, найдите ее и выберите.
4. Нажмите **OK**.
5. Нажмите **Продолжить** что бы начать сканирование.
6. Следуйте подсказкам мастера Сканирования на Антивирусы.

Что такое Безопасный режим?
Безопасный режим - специальный способ запуска Windows, используемый главным образом для устранения проблем, влияющих на нормальную работу Windows. Это проблемы от конфликтующих драйверов до вирусов, мешаюших работе Windows в обычном режиме. В Безопасном режиме Windows загружает только самые необходимые компоненты и драйверы, способные работать в Безопасном Режиме. По этой причине большинство программ, в том числе и вирусов, не могут работать в этом режиме и легко могут быть удалены.
Чтобы запустить систему в Безопасном режиме, перезапустите ваш компьютер и нажмите F8 до появления меню доплнительных опций загрузки Windows.

Вам необходимо выбрать **Безопасный Режим с Поддержкой Сети** , чтобы иметь доступ к интернету.

Замечание

Чтобы получить более подробную информацию о безопасном режиме обратитесь к справочной системе Windows (**Справка и поддержка** в меню Пуск). Также вы можете найти полезную информацию поискав в интернет.

29.4. Использование Панели Активности Сканирования

Панель Активности Сканирования

В окне **График активности** графически показано, как проходит проверка Вашей системы на наличие вирусов. Это маленькое окошко по умолчанию доступно только в Режиме опытного пользователя.

Вы можете использовать панель активности сканирования чтобы быстро сканирования файлов и папкок. Перетащите файл или папку, которую надо проверить на панель активности сканирования. Следуйте подсказкам мастера Сканирования на Антивирусы.

Замечание

Для получения дополнительной информации перейдите к *«Панель Активности Сканирования»* (p. 32).

30. Как запланировать сканирование компьютера

Периодическое сканирование - лучший способ защитить его от вредоносного ПО. BitDefender позволяет запланировать задачи сканирования, поэтому вы можете автоматически проверять ваш компьютер.

Чтобы запланировать сканирование вашего компьютера проделайте эти действия:

1. Откройте BitDefender и установите пользовательский интерфейс в Режим опытного пользователя.
2. Нажмите **Антивирус** в левом меню.
3. Нажмите на вкладку **Сканирование Вирусов**. Здесь вы модете найти набор задач по умолчанию и создать свои собственные.
   - Системные задачи доступны для запуска в любой учетной записи Windows.
   - Пользовательские задачи доступны только тем пользователям, которые их создали.

   По умолчанию вы можете запланировать следующие задачи сканирования:

Задачи по умолчанию	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.
Сканирование Системы	Проверка всей системы кроме архивов. В настройках по умолчанию проводится проверка на все типы вирусного ПО, кроме руткитов.
Быстрая проверка системы	Сканирует папки `Windows` и `Program Files`. В конфигурации по умолчанию проверка производится на все виды вредоносных программ, кроме руткитов. Не производится проверка памяти, реестра и записей cookies.
Автоматическое Сканирование при Входе	Проверка элементов, запускающихся при входе пользователя в систему. Чтобы использовать эту задачу, надо запланировать ее запуск на загрузку системы. По умолчанию проверка элементов автозапуска отключена.

Задачи по умолчанию	Описание
Мои документы	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.

Если ни одна из этих задач не подходит, вы можете создать новую и запланировать ее запуск на нужное вам время.

4. Щелкните правой кнопкой мыши по нужной задаче и выберите **Запланировать**. Появится новое окно.
5. Запланируйте запуск задачи по усмотрению:
   - Чтобы запустить задачу только один раз, выберите **Единоразово** и определите дату и время запуска.
   - Чтобы запустить задачу после запуска системы, выберите **При запуске системы**. Вы можете указать, сколько времени (в минутах) задание должно выполняться после запуска.
   - Чтобы запускать задачу периодически, выберите **Периодически** и определите частоту, дату и время запуска.

Замечание

Например, для того чтобы проверять ваш компьютер каждую субботу в два часа ночи, настройте планирование следующим образом:

a. Выберите **Периодически**.
b. В поле **Каждые** введите 1 и затем выберите **недель** в меню. Таким образом, задание будет запускаться раз в неделю.
c. Установите датой запуска первую субботу.
d. Установите временем начала 2:00:00 ночи.

6. Нажмите **OK**, чтобы сохранить изменения. Задача запустится автоматически в заданный день и время. Если ваш компьютер выключен в запланированное время задача запустится когда вы включите компьютер.

Устранение неполадок и получение справки

31. Устранение неполадок

Эта глава описывает некоторые проблемы, которые могут возникнуть при использовании BitDefender и представляет вам возможные пути решения этих проблем. Большинство из этих проблем можно решить с помощью соответствующей конфигурации настроек продукта.

Если вы не можете найти тут вашу проблему, или если представленные пути не решают ее, Вы можете связаться с представителями BitDefender технической поддержки, представленных в разделе «*Техническая поддержка*» (p. 228).

31.1. Проблемы Установки

Этот раздел поможет Вам устранить наиболее распространенные проблемы с установкой BitDefender. Эти проблемы могут быть сгруппированы в следующие категории:

- Ошибки подтверждения установки: мастер увстановки не может быть запущен из-за особенностей вашей системы.
- Сбой Установки : мастер установки был запущен, но его работы не была удачно завершена.

31.1.1. Ошибки подтверждения установки

После запуска мастера установки, проверяется ряд условий для подтверждения возможности установки. В следующей таблице представлены наиболее распространенные ошибки проверки установки и решения для их преодоления.

Ошибка	Описание&Решение
У вас не достаточно прав для установки программы.	Для того, чтобы запустить мастера настройки и установки BitDefender, вам необходимы права администратора. Сделайте следующее: ● Войдите в систему под учетной записью администратора Windows и запустите мастер установки снова. ● Щелкните правой кнопкой на хранилище в таблице и выберите **Запустить от имени**. Введите имя пользователя и пароль учетной записи администратора Windows.
Программа установки обнаружила предыдущую версию BitDefender,	BitDefender был ранее установлена на вашей системе, но не был полностью удален, в связи с чем блокируется новая установка BitDefender.

Ошибка	Описание&Решение
которая была не правильно удалена.	ЧтДля решения этой проблемы и установки BitDefender, выполните следующие действия: 1. Перейдите к www.bitdefender.com/uninstall и загрузите инструмент удаления на ваш компьютер. 2. Запустить инструмент удаления, используя права администратора. 3. Перезагрузите компьютер. 4. Запустите мастер установки снова, чтобы установить BitDefender.
Продукт BitDefender не совместим с Вашей операционной системой.	Вы пытаетесь установить BitDefender на неподдерживаемую операционную систему. Пожалуйста, проверьте *«Системные требования»* (p. 2), чтобы уточнить, какие операционные системы поддерживает BitDefender. Если ваша операционная система Windows XP with Service Pack 1 или без Service Pack, вы можете установить Service Pack 2 или выше, затем запустить мастер установки снова.
Установочный файл предназначен для различных типов процессоров.	Если вы получаете эту ошибку, значит вы пытаетесь запустить неверную версию установочного файла. Существует две версии установочного файла BitDefender: один для 32-битных процессоров, другой для 64-битных процессоров. Чтобы убедиться в корректности версии для вашей системы, скачайте инсталляционный файл непосредственно из www.bitdefender.com.

31.1.2. Сбой Установки

Возможны несколько вариантов сбоя установки:

- В процессе установки появляется экран ошибки. Вам может быть предложено отменить установку или появится кнопка для запуска инструмента удаления, который очистит систему.

  Замечание
  Сразу после начала установки, вы можете получить уведомление о том, что не хватает свободного пространства на диске для установки BitDefender. В

таком случае, освободите необходимое количество дискового пространства там, где вы хотите установить BitDefender, а затем продолжите или возобновите установку.

- Установка зависает и, возможно, ваша система не отвечает. Поможет только перезапуск системы.
- Установка завершена, но вы не можете воспользоваться некоторыми или всеми функциями BitDefender.

Для устранения неполадок и установки BitDefender, выполните следующие действия:

1. **Очистить систему после неудачной установки.** Если происходит сбой установки, некоторые регистрационные ключи и файлы BitDefender могут остаться в вашей системе. Такие оставшиеся файлы могут помешать новой установки BitDefender. Они также могут повлиять на производительность и стабильность системы. Именно поэтому вы должны удалить их, прежде чем пытаться установить продукт снова.

   Если на экране ошибки присутствует кнопка для запуска демонтирования программы, воспользуйтесь ею и очистите систему. В ином случае следуйте следующее:

   a. Перейдите к www.bitdefender.com/uninstall и загрузите инструмент удаления на ваш компьютер.

   b. Запустить инструмент удаления, используя права администратора.

   c. Перезагрузите компьютер.

2. **Проверьте возможные причины, помешавшие установке.** Прежде чем приступить к переустановке продукта, проверьте и устраните возможные условия, которые возможно привели к сбою установки:

   a. Проверьте, не установлены ли другие средства безопасности, так как они могут нарушить нормальное функционирование BitDefender. Если они установлены, мы рекомендуем Вам удалить все другие решения безопасности, а затем переустановить BitDefender.

   b. Вам также следует проверить, не заражена ли система. Сделайте следующее:

      - Воспользуйтесь диском-реаниматором BitDefender для проверки компьютера и устраните все возможные угрозы. Для получения дополнительной информации перейдите к «Диск-реаниматор BitDefender» (p. 232).
      - Откройте окно Internet Explorer, перейдите www.bitdefender.com и запустите онлайн сканирование(нажмите **онлайн сканирование**).

3. Попробуйте установить BitDefender еще раз. Рекомендуется скачивать и запускать последнюю версию установочного файла с www.bitdefender.com.
4. Если снова происходит сбой установки, обратитесь за поддержкой BitDefender *«Техническая поддержка»* (p. 228).

31.2. BitDefender не отвечает

Эта глава поможет Вам устранить ошибки *BitDefender не отвечает*. Вы можете столкнуться с этой ошибкой следующим образом:

- Иконка BitDefender на панели задач отображается серым цветом, и всплывающее окно информирует Вас о том, что BitDefender не отвечает.
- Окно BitDefender показывает, что BitDefender не отвечает.

Ошибка может быть вызвана одной из следующих причин:

- устанавливается важное обновление.
- временным ошибкам связи BitDefender.
- некоторые из сервисов BitDefender остановлены.
- другие средства безопасности работают одновременно с BitDefender.
- вирусы в системе мешают нормальному функционированию BitDefender.

Для устранения этой ошибки, попробуйте выполнить следующие действия:

1. Несколько минут подождите возможных изменений. Ошибка может быть временной.
2. Перезагрузите компьютер и дождитесь загрузки BitDefender. Откройте BitDefender и проверьте, не устранена ли ошибка. Перезагрузка компьютера обычно решает поблему.
3. Проверьте, не установлены ли другие средства безопасности, так как они могут нарушить нормальное функционирование BitDefender. Если они установлены, мы рекомендуем Вам удалить все другие решения безопасности, а затем переустановить BitDefender.
4. Если ошибка повторяется, возможно проблема более серьезна (например, система заражена вирусом, мешающим работать BitDefender). За технической поддержкой, пожалуйсиа, обращайтесь по ссылке *«Техническая поддержка»* (p. 228).

31.3. Сбой Удаления BitDefender

Эта статья поможет вам в решении ошибок, которые могут возникнуть в процессе удаления BitDefender. Есть 2 возможные ситуации:

- В процессе удаления появляется экран ошибки. Этот экран выводит кнопку запуска инструмента удаления, который очистит вашу систему.
- Удаление зависает и, возможно, ваша система застынет. Нажмите **Отмена**, для прекращения удаления. Если не поможет, перезагрузите систему.

Если удаление прерывается, некоторые ключи реестра и файлы BitDefender могут остаться в вашей системе. Такие остатки могут помешать новой установке BitDefender. Также, они могут повлиять на производительность и стабильность системы. Чтобы полностью удалить BitDefender из вашей системы, вы должны запустить Инструмент Удаления.

Если удаление прервано экраном ошибки, нажмите кнопку нажмите кнопку для запуска инструмента удаления, что бы очистить вашу систему. В ином случае следуйте следующее:

1. Перейдите к www.bitdefender.com/uninstall и загрузите инструмент удаления на ваш компьютер.
2. Запустить инструмент удаления, используя права администратора. Инструмент удаления удалит все файлы и регистрационные ключи, которые не были удалены во время процесса автоматического удаления.
3. Перезагрузите компьютер.

Если эта информация не помогла, вы можете обратиться в поддержку BitDefender, как указано в секции «*Техническая поддержка*» (p. 228).

32. Техническая поддержка

BitDefender предоставляет своим клиентам быструю и грамотную техподдержку. База Знаний BitDefender содержит статьи, которые включают в себя вырианты решения большинства ваших проблем и вопросов, связанных с BitDefender. Если вы не можете найти решение в Базе Знаний, свяжитесь с техподдержкой BitDefender. Наши представители ответят на ваши вопросы и окажут необходимую помощь.

32.1. 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 доступна круглосуточно по адресу http://kb.bitdefender.com.

32.2. Обращение за помощью

Чтобы запросить помощь, вам надо воспользоваться Системой самообслуживания BitDefender. Просто следуйте инструкции:

1. Перейдите http://www.bitdefender.com/help. Тут вы можете найти Базу Знаний BitDefender. База Знаний включает в себя статьи, содержащие решения проблем, связанных с BitDefender.
2. Поищите в Базе Зананий статьи, которые могут помочь вам решить вашу проблему.

3. Пожалуйста прочтите подходящую статью и попробуйте предлагаемое решение.
4. Если это не решит вашей пробелмы, используйте ссылку и статье, чтобы связаться с техподдержкой.
5. Войдите в Вашу учетную запись BitDefender
6. Свяжитесь с техподдержкой BitDefender по эелектронной почте, чату или телефону.

32.3. 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.

32.3.1. Адреса веб-сайтов

Отдел продаж: sales@bitdefender.com
Техподдержка: www.bitdefender.com/help
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
Местные дистрибуторы: http://www.bitdefender.com/site/Partnership/list/
База Знаний BitDefender: http://kb.bitdefender.com

32.3.2. Местный дистрибьютор

Местные дистрибьюторы BitDefender готовы предоставить вам любую требуемую информацию.

Телефон: +7(495)232-52-15
Факс: +7(495)232-52-15
Электронная почта: sales@bdef.ru
Купить: http://www.bitdefender.com/links/ru/buy/antivirus.html
Техническая поддержка: http://www.bitdefender.com/links/ru/support/antivirus.html
Сайт:http://www.bitdefender.com/links/ru/homepage.html

32.3.3. Офисы BitDefender

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.

США

BitDefender, LLC
6301 NW 5th Way, Suite 3500
Fort Lauderdale, Florida 33309
Телефон (офис и продажи): 1-954-776-6262
Продажи: sales@bitdefender.com
Техническая поддержка: http://www.bitdefender.com/help
Сайт: http://www.bitdefender.com

Германия

BitDefender GmbH
Airport Office Center
Robert-Bosch-Straße 2
59439 Holzwickede
Deutschland
Офис: +49 2301 91 84 222
Продажи: vertrieb@bitdefender.de
Техническая поддержка: http://kb.bitdefender.de
Сайт: http://www.bitdefender.de

Великобритания и Ирландия

Business Centre 10 Queen Street
Newcastle, Staffordshire
ST5 1ED
Электронная почта: info@bitdefender.co.uk
Телефон: +44 (0) 8451-305096
Продажи: sales@bitdefender.co.uk
Техническая поддержка: http://www.bitdefender.com/help
Сайт: http://www.bitdefender.co.uk

Испания

BitDefender España SLU
C/ Balmes, 191, 2º, 1ª, 08006
Barcelona
Факс: +34 932179128
Телефон: +34 902190765

Продажи: comercial@bitdefender.es
Техническая поддержка: www.bitdefender.es/ayuda
Сайт: http://www.bitdefender.es

Россия и страны СНГ (кроме Украины)

BITDEFENDER SRL
West Gate Park, Building H2, 24 Preciziei Street
Bucharest
Факс: +40 21 2641799
Телефон отдела продаж: +40 21 2063470
e-mail отдела продаж: sales@bitdefender.ro
Техническая поддержка: http://www.bitdefender.ro/suport
Сайт: http://www.bitdefender.ro

Диск-реаниматор BitDefender

33. Обзор

BitDefender Antivirus 2010 поставляется вместе с загрузочным компакт-диском (Реаниматор BitDefender), который может проверить и вылечить все существующие жесткие диски до загрузки операционной системы.

Рекомендуем использовать компакт-диск BitDefender Реаниматор в случае, если операционная система не работает должным образом из-за заражения вирусом. Это обычно случается, когда не используется антивирусная программа.

Обновление базы данных вирусных сигнатур осуществляется автоматически без вмешательства пользователя каждый раз, когда Вы запускаете компакт-диск BitDefender Реаниматор.

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 диск-реаниматор BitDefender тут: http://download.bitdefender.com/rescue_cd/

33.1. Системные требования

Перед загрузкой диска-рениматора BitDefender, 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

Диск-реаниматор BitDefender 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 установки диска-реаниматора BitDefender 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.

33.2. Прилагаемое программное обеспечение

В Диск-Реаниматор BitDefender входят следующие пакеты программ.

Xedit
Это текстовый редактор.

Vim
Это мощный текстовый редактор, поддерживающий выделение 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.

За более подробной информацией перейдите по ссылке домашняя страница RoxFiler.

MidnightCommander
GNU Midnight Commander (mc) - файловый менеджер.

Более подробная информация по ссылке 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 по ссылке домашняя страница Partimage.

GtkRecover

GtkRecover - GTK версия консольной программы восстановления. Она помогает восстановить Ваши файлы.

Более подробная информация по ссылке домашняя страница GtkRecover.

ChkRootKit

ChkRootKit - инструмент, который помогает Вам просматривать ваш компьютер на наличие руткитов.

Более подробная информация по ссылке домашняя страница ChkRootKit.

Nessus Network Scanner

Nessus - сканер безопасности для Linux, Solaris, FreeBSD и Mac OS X.

Более подробная информация по ссылке домашняя страница Nessus.

Iptraf

Iptraf – консольная утилита для сбора сетевой статистики.

Более подробная информация по ссылке домашняя страница Iptraf.

Iftop

Iftop - утилита позволяющая мониторить трафик в реальном времени.

Более подробная информация по ссылкедомашняя страница Iftop.

MTR

MTR - диагностический инструмент сети.

Более подробная информация по ссылке домашняя страница MTR.

PPPStatus

PPPStatus отображает статистическую информацию о входящих и исходящих потоках трафика по TCP/IP.

Более подробная информация по ссылке домашняя страница PPPStatus.

Wavemon

Wavemon - программа мониторинга для беспроводных сетевых устройств.

Более подробная информация по ссылке домашняя страница Wavemon.

USBView

USBView показывает информацию об устройствах, связанных с USB.

Более подробная информация по ссылке 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 известных веб браузеров.

Более подробная информация домашняя страница Mozilla Firefox.

Elinks

Elinks - текстовый веб браузер.

Более подробная информация домашняя страница Elinks.

34. Как пользоваться Диском-Реаниматором 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.

34.1. Запуск Диска-реаниматора BitDefender

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 Диска-Реаниатора BitDefender.

Экран загрузки

При загрузке обновление базы данных вирусных сигнатур осуществляется автоматически без вмешательства пользователя. На это может потребоваться время.

После окончания загрузки на экране появится новый интерфейс - рабочий стол. Теперь Можно начинать работу с Диском-Реаниатором BitDefender.

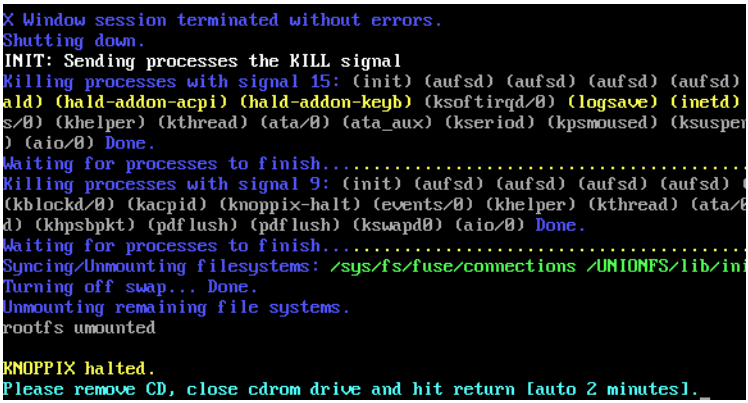
Рабочий Стол

34.2. Остановка Диска-Реаниатора BitDefender

Вы можете выполнить безопасное отключение компьютера, для чего следует выбрать команду **Выход** в контекстном меню Диска-Реаниатора BitDefender (открывающееся после щелчка правой кнопкой мыши), либо использовать команду **Остановка** в терминале.

Выберите команду "ВЫХОД"

Когда Диск-Реаниатор BitDefender 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

34.3. 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, угрожающих безопасности 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 проверить только определенную директорию, вы можете воспользоваться одной из следующих возможностей:

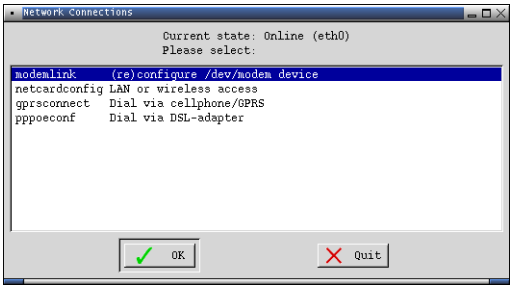
- Воспользуйтесь **Сканнер командной строки BitDefender**.
  1. Дважды нажмите иконку ЗАПУСК СКАНИРОВАНИЯ на рабочем столе для запуска **Сканнера коммандной строки BitDefender**.
  2. Нажмите **Сканнер**, и откроется новое окно.
  3. Выберите директорию, которую хотели бы проверить и нажмите **Открыть** для запуска сканирования с помощью того же мастера, который появился при первой загрузке.
- Используйте контекстное меню - просмотрите ваши папки, щелкните правой кнопкой мыши по файлу или каталогу и выберите **Отправить**. Затем откройте **Сканнер BitDefender**.
- Или вместо этого вы можете запустить командную сроку с терминала. **Антивирусный Сканнер BitDefender** начнет проверку выбранного Вами файла или папки с заданным по умолчанию местоположением.

```
# bdscan /path/to/scan/
```

34.4. 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 подходит 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. 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, посоветуйтесь с системным или сетевым администратором.

Важно
Имейте в виду, что вы всего лишь активируете модем, выбрав описанные выше параметры. Для настройки сетевого подключения выполните следующие шаги.

1. Щелкните правой кнопкой мыши по рабочей области. Появится контекстное меню диска-реаниматора BitDefender.
2. Выберите опцию **Терминал (как root)**.
3. Попробуйте ввести следующие команды:

```
# pppconfig
```

4. Следуйте указаниям на экране. Если вы не уверены, посоветуйтесь с системным или сетевым администратором.

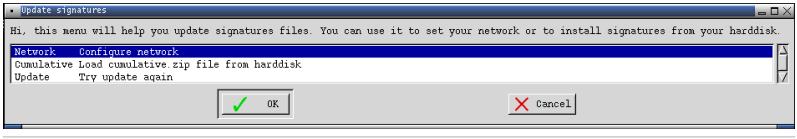
34.5. Как обновлять BitDefender?

Во время загрузки обновления вирусных сигнатур осуществляется автоматически. Однако, если вы пропустили этот шаг или просто хотите провести обновление после загрузки, существуют два способа обновления BitDefender.

- Воспользуйтесь **Сканнер командной строки BitDefender**.

1. Нажмите дважды иконку ЗАПУСК СКАНИРОВАНИЯ на Рабочем Столе дя запуска **Сканнера комендной строки BitDefender**.
2. Нажмите **Обновить**.

- Используйте быструю клавижу **Обновить Сигнатуры** на Рабочем Столе.
  1. Дважды щелкните на ярлыке Обновить сигнатуры на рабочем столе. Появится следующее окно.



Обновление сигнатур

  2. Выполните одно из следующих действий:
     - 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. Нажмите **OK**.

34.5.1. Как обновить BitDefender через прокси?

Если присутствует прокси-сервер между вашим компьютером и Интернет, то необходимо произвести некоторые настройки, чтобы обновить вирусные сигнатуры.

Для обновления BitDefender через прокси, используйте одну из опций:

- Воспользуйтесь **Сканнер командной строки BitDefender**.
  1. Дважды нажмите иконку ЗАПУСК СКАНИРОВАНИЯ на рабочем столе для запуска **Сканнера коммандной строки BitDefender**.
  2. Нажмите **Настройки**, и откроется новое окно.
  3. В разделе **Настройки Обновлений**, выберите**включить HTTP Proxy** Укажите хост прокси(как: `host[:port]`), пользователя прокси (как: `[domain\]username`) и пароль. Выберите **Обойти прокси-сервер, когда он не доступен** для связи напрямую, когда прокси-сервер не доступен.
  4. Нажмите **Сохранить**
  5. Нажмте **Обновить**

- Использовать Терминал (как root).
  1. Щелкните правой кнопкой мыши по рабочей области. Появится контекстное меню диска-реаниматора BitDefender.
  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. Раскоментируйте 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 текущий файл, подтвердите сохранение, затем нажмите **F10**, чтобы закрыть это.
7. Тип команды: **bdscan update**.

34.6. 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 возможно понадобится ввести `sda1`.

2. Ждите, пока диск-реаниматор BitDefender не загрузится. Появится следующее окно.

Экран Рабочего Стола

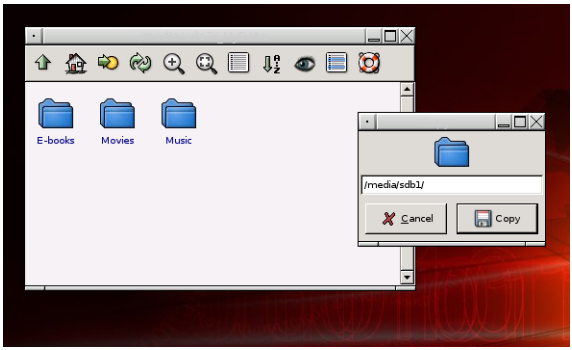
3. Дважды нажмите на раздел, где расположены данные, которые Вы хотите сохранить (например `[sda3]`).

   Замечание
   При работе с диском-реаниматором BitDefender вы столкнетесь 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, МоиДанные который содержит поддиректории Видео, Музыка и e-Книги.
5. Нажмите правой кнопкой мыши на выбранные 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 возможно понадобится ввести `sda1`.

34.7. Как пользоваться консольным режимом работы?

Если разрешение экрана не достаточно высоко для запуска графического пльзовательского интерфейса, вы можете запустить диск-реаниматор BitDefender в консольном режиме. Простой текстовый режим позволяет выполнить полную проверку компьютера.

Для запуска компакт-диска в консольном режиме, настройте BIOS вашего компьютера для загрузки с компакт-диска, поместите компакт-диск в дисковод и перезагрузите компьютер. Дождитесь загрузки заставки появляться и выберите**Запустить knoppix в консольном режиме**.

После перезагрузки следуйте инструкции для выполнения полного сканирования компьютера.

BitDefender обнаруживает сегментации на вашем жестком диске и автоматически обновляет базу данных вредоносных сигнатур перед запуском сканирования. Если обнаружатся инфицированные файлы, BitDefender вылечит их. По окончании процесса сканирования отобрадается журнал сканирования.

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

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.

Рекламное ПО

Рекламное ПО часто устанавливаттся «в качестве нагрузки» к основным приложениям, которые предоставляются бесплатно, при условии что пользователь соглашается установить программу-Рекламное ПО. Поскольку Рекламное ПО-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.

Архив

Диск или директория, содержащие запасные файлы.

Файл, содержащий один или несколько файлов в сжатом формате.

Лазейки 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.

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.

Дисковод 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.

Ложное срабатывание

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 называемое «ложное срабатывание».

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.

Почтовый 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.

Маршрут между двумя объектами, например, канал связи между двумя компьютерами.

Фишинг

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

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

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.

Действиями программ-шпионов являются не только нарушением этики и конфиденциальности, но и кража 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.

Область пиктограмм 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.

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. Будучи вирусом одного из наиболее опасных типов, Трояны 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, разработана для замены 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.

Червь

Программа, которая распространяется по сети, копируя и отправляя себя дальше. Она не может присоединяться к другим программам.