bitdefender
ANTIVIRUS v10

10th anniversary

Руководство пользователя

Антивирус

Антишпион

bitdefender
secure your every bit

BitDefender Antivirus v10

Руководство пользователя

BitDefender

Опубликовано 2007.05.09
Version 10.2

Правовые положения


bitdefender
secure your every bit

Содержание

Лицензии и гарантии

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.

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

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

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

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

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

ПРИКЛАДНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ. Вы можете установить и использовать BitDefender на необходимом количестве компьютеров в рамках ограничения общего количества 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. Дозволенное количество первичных пользователей - это количество пользователей лицензии.

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

ОБНОВЛЕНИЯ. В случае, когда BitDefender является обновлением, вы можете обновлять свой программный продукт только тогда, когда Ваша лицензия, предоставленная компанией SOFTWIN, действительна. Обновление BitDefender заменяет и/или дополняет исходный программный продукт, лицензия на который у Вас уже есть. Вы можете использовать обновленный продукт только согласно условиям данного Лицензионного соглашения. Если BitDefender является обновлением какой-либо программы из лицензионного пакета, лицензированного как один продукт, программный продукт BitDefender может использоваться только как часть пакета и не может быть использован в количестве, большем чем общее количество лицензированных пользователей. Условия данной лицензии заменяют и превалируют над всеми предыдущими соглашениями, которые были заключены между Вами и SOFTWIN 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 минипрограммы, входящие в программный продукт BitDefender), сопутствующие печатные материалы и любые копии программного продукта BitDefender являются собственностью компании SOFTWIN. BitDefender защищен законом об авторском праве и международными соглашениями. Поэтому Вы должны обращаться с ним, как и с любым другим лицензионным продуктом. Вы не имеете права копировать сопутствующие печатные материалы. На всех копиях должна стоять пометка об авторских правах, независимо от того, на каком носителе или в какой форме существует продукт BitDefender. Вы не имеете права выдавать сублицензии, сдавать в аренду или продавать BitDefender. Вы не имеете права восстанавливать алгоритм работы, вносить изменения, раскодировать, создавать свои продукты на основе BitDefender, изменять, переводить или предпринимать какие-либо попытки дешифровать исходный код программного продукта BitDefender.

ОГРАНИЧЕННАЯ ГАРАНТИЯ. Компания SOFTWIN дает четырнадцатидневную гарантию со дня покупки, что все носители, на которых распространяется программный продукт BitDefender, не имеют дефектов. При нарушении гарантии компания SOFTWIN может на свое усмотрение заменить поврежденный

экземпляр или вернуть уплаченные деньги. Компания SOFTWIN не гарантирует, что программный продукт BitDefender будет работать без ошибок или сбоев, или что ошибки будут исправлены. Компания SOFTWIN не гарантирует, что программный продукт BitDefender будет отвечать всем Вашим требованиям.

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

ОТКАЗ ОТ ОТВЕТСТВЕННОСТИ ЗА ПОВРЕЖДЕНИЯ. Любое лицо, использующее, тестирующее или оценивающее программный продукт BitDefender несет все риски, касающиеся качества его работы. Компания SOFTWIN не несет никакой ответственности за любой ущерб, включая и не ограничиваясь, прямой и непрямой ущерб, возникший в результате неправильного использования, работы или доставки BitDefender, даже если компания SOFTWIN предупреждала о такой возможности. В НЕКОТОРЫХ СТРАНАХ НЕ РАЗРЕШЕНО ОГРАНИЧИВАТЬ ИЛИ ОТКАЗЫВАТЬСЯ ОТ ОТВЕТСТВЕННОСТИ ЗА СЛУЧАЙНЫЕ ИЛИ КОСВЕННЫЕ УБЫТКИ, ПОЭТОМУ ЭТИ ОГРАНИЧЕНИЯ МОГУТ ВАС НЕ КАСАТЬСЯ. В ЛЮБОМ СЛУЧАЕ ОТВЕТСТВЕННОСТЬ КОМПАНИИ SOFTWIN НЕ ДОЛЖНА ПРЕВЫШАТЬ СУММЫ, УПЛАЧЕННОЙ ЗА ПРОГРАММНЫЙ ПРОДУКТ BITDEFENDER. Перечисленные отказы и ограничения действуют независимо от того, принимаете ли Вы, оцениваете или тестируете BitDefender.

ВАЖНОЕ ЗАМЕЧАНИЕ ДЛЯ ПОЛЬЗОВАТЕЛЕЙ. ДАННОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ НЕ ОТКАЗОУСТОЙЧИВО И НЕ ПРЕДНАЗНАЧЕНО ДЛЯ РАБОТЫ В ОПАСНЫХ УСЛОВИЯХ, ТРЕБУЮЩИХ БЕСПЕРЕБОЙНОЙ РАБОТЫ. ДАННОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ НЕ ПРЕДНАЗНАЧЕНО ДЛЯ ИСПОЛЬЗОВАНИЯ В СИСТЕМАХ НАВИГАЦИИ САМОЛЕТОВ, В ЯДЕРНЫХ ЦЕНТРАХ ИЛИ СИСТЕМАХ СВЯЗИ, В СИСТЕМАХ ВООРУЖЕНИЙ, 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.

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

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

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

Название BitDefender и логотип BitDefender являются торговыми марками компании SOFTWIN. 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 SOFTWIN или любых его дилеров при расторжении лицензии. Условия, касающиеся конфиденциальности и использования, остаются в силе и после расторжения.

SOFTWIN 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 SOFTWIN имеет высшую юридическую силу.

Обратная связь: SOFTWIN, at 5, Fabrica de Glucoza street, 72322-Sector 2, Bucharest, Romania, or at Tel No: 40-21-2330780 or Fax:40-21-2330763, элетронная почта: <office@bitdefender.com>.

Предисловие

Данное руководство пользователя предназначено для всех пользователей, которые выбрали **BitDefender Antivirus v10** для обеспечения защиты персональных компьютеров. Информация, представленная в этой книге, доступна не только для опытных компьютерных пользователей, но и для любого пользователя, знакомого с операционной системой Windows.

В этой книге Вы найдете описание программного продукта **BitDefender Antivirus v10**, а также найдете сведения о нашей компании и группе разработчиков этого продукта, пройдете вместе с нами через процесс установки и получите инструкции, как конфигурировать эту программу. Вы узнаете, как использовать, обновлять, тестировать и настраивать продукт **BitDefender Antivirus v10**. Вы узнаете,как добиться наилучших результатов при работе с BitDefender.

Надеемся, что чтение будет увлекательным и полезным для Вас.

1. Соглашения, используемые в данной книге

1.1. Типографские обозначения

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

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

Виды шрифтов и стилей	Описание
`filename`	Названия файлов и папок приводятся с использованием шрифтов с `фиксированной шириной символов`.
option	Все опции программы напечатаны, используя **полужирный** шрифт.
`sample code listing`	Программные коды приводятся с помощью шрифтов с `фиксированной ширины` символов.

1.2. Замечания

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

Замечание

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

Важно

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

Внимание

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

2. Структура книги

Данная книга состоит из 7 разделов, описывающих основные темы: О программе BitDefender, Установка программы, Описание и особенности, Консоль управления, Практические приемы, Реаниматор BitDefender и Получение справки. Кроме того, приводится глоссарий, в котором разъясняются некоторые технические термины.

О программе BitDefender. Краткое введение в программу BitDefender.

Установка программы. Пошаговые инструкции по установке продукта BitDefender на рабочей станции. Это – подробное руководство по установке **BitDefender Antivirus v10**. После проверки выполнения необходимых условий для успешной установки программы, Вы проходите все этапы инсталляционного процесса. В конце дается описание процедуры удаления продукта для случая, если Вам необходимо деинсталлировать BitDefender.

Описание и особенности. Здесь представлено краткое описание функций и программных модулей **BitDefender Antivirus v10**

Консоль управления. Описание основных процедур администрирования и обслуживания BitDefender. Данный раздел поясняет как использовать все опции **BitDefender Antivirus v10**, как регистрировать программу, как проверить ваш компьютер на вирусы, как производить обновления. Вас научат конфигурировать и использовать модули BitDefender.

Практические приемы. Выполнение данных инструкций позволит максимально успешно воспользоваться возможностями BitDefender.

Реаниматор BitDefender. Описание компакт-диска Реаниматор BitDefender. Этот материал поможет Вам изучить и использовать возможности, которые дает использование данного загрузочного компакт-диска.

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

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

3. Ваши комментарии

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

Пожалуйста, направляйте свои замечания по электронной почте по адресу <documentation@bitdef.ru>.

Важно

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

О программе BitDefender

1. Что такое BitDefender?

BitDefender - ведущий мировой разработчик решений в области безопасности, удовлетворяющий всем современным требованиям компьютерной индустрии. Компания предлагает один из самых быстрых и эффективных пакетов прогаммного обеспечения в сфере безопасности, устанавливая новые стандарты для предотвращения угроз, их своевременного выявления и устранения. BitDefender предоставляет свои продукты и услуги 41 миллиону пользователей более чем в 180 странах. BitDefender имеет представительства в **Соединеннных Штатах**, **Великобритании**, **Германии**, **Испании**, **Румынии**.

- Включает в себя антивирус, брандмауэр, антишпион, антиспам и контроль доступа;
- Серия продуктов BitDefender подразумевает установку для комплексных компьютерных структур (рабочих станций, файловых серверов, почтовых серверов, и шлюзов) для платформ Windows, Linux и FreeBSD;
- Всемирная сеть дистрибуции, продукты, доступные на 18 языках;
- Простой в использовании, с мастером установки, который быстро проводит инсталляцию, задавая всего несколько вопросов;
- Продукты, сертифицированные на международном уровне: Virus Bulletin, ICSA Labs, Checkmark, IST Prize и др.;
- Непрерывная забота о пользователях - поддержка пользователей осуществляется круглосуточно;
- Молниеносная реакция на появление новых видов компьютерных угроз;
- Высочайший уровень обнаружения;
- Ежечасные обновления вирусных баз - автоматические или по расписанию, для защиты от самых новых вирусов.

1.1. Почему именно BitDefender?

Проверенное решение. Быстрая реакция на новые угрозы. Высокая скорость реагирования продукта BitDefender на новые вирусные угрозы была продемонстрирована в условиях эпидемии компьютерных вирусов, таких как CodeRed, Nimda, Sircam, а также кода Badtrans.B и быстро распространяющихся зловредных кодов. Лаборатория BitDefender первой разработала решения по лечению данных вирусов и кодов и открыла бесплатный доступ к этим решениям

в сети Интернет для всех заинтересованных пользователей. В настоящее время, когда наблюдается интенсивное распространение различных модификаций вируса Klez, оперативность обновления антивирусной защиты стала еще более значимой для любой компьютерной системы.

Инновационное решение. Лауреат Европейской Комиссии и Ассоциации европейских академий Eurocase. BitDefender был удостоен награды IST-Prize за инновационное решение Европейской Комиссии и Ассоциации 18европейских академий. Эта награда присуждается ежегодно в течение последних 8 лет инновационным продуктам, которые считаются лучшими европейскими инновациями в сфере информационных технологий.

Всесторонняя защита. Защищена каждая точка вашей сети, обеспечена полная защита системы. Программные решения BitDefender для обеспечения защиты корпоративных сетей и систем в полной мере удовлетворяют требования защиты современной бизнес-среды, обеспечивая эффективное управление по защите от комплексных угроз, которым подвергаются сети - от маленьких локальных сетей до больших мультисерверных и мультиплатформенных.

Максимальный уровень защиты для Вашей системы. Надежный барьер для любых возможных угроз вашей компьютерной системы. Поскольку методы вирусного обнаружения, основанные на анализе кода, не всегда обеспечивают хорошие результаты, разработчики BitDefender предложили защиту, основанную на анализе поведения программ и позволяющую обезвреживать даже неизвестные новейшие зловредные коды.

Корпоративные пользователи стремятся избежать **финансовых потерь** в результате следующих угроз, для борьбы с которыми и создаются программы компьютерной защиты:

- Атаки вирусов-червей
- Потеря информации из-за заражения электронной почты
- Выход из строя почтовых программ
- Очистка и восстановление систем
- Потеря производительности конечных пользователей, в связи с недоступностью используемой ими системы
- Взлом системы и получение несанкционированного доступа, повлекшие за собой ущерб

Кроме того, за счет использования набора программ BitDefender, Вы сможете добиться одновременно нескольких **преимуществ и финансовой выгоды**:

- Повысите пропускную способность и доступность своей сети за счет предотвращения распространения атак зловредных кодов (например, вирусов Nimda, вирусов-троянов, и зловредных кодов DDoS).
- Защитите удаленных пользователей от атак.
- Уменьшите административные затраты и быстро улучшите использование ресурсов за счет возможностей продукта BitDefender для администрирования сетей на предприятиях.
- Предотвратите распространение зловредных кодов и вирусов по электронной почте за счет использования процессора межсетевого обмена программы BitDefender для защиты электронной почты. Вы получите возможность на временной или постоянной основе блокировать подключения к сети различных приложений: несанкционированных, уязвимых для хакерских атак или слишком затратных.

Более детальную информацию о BitDefender можно получить, посетив: http://www.bitdef.ru.

Установка программы

2. Установка BitDefender Antivirus v10.

Глава **Установка BitDefender Antivirus v10** данного руководства пользователя содержит следующие темы:

- Системные требования
- Пошаговая установка
- Мастер установки
- Обновление
- Удаление, восстановление или изменение BitDefender

2.1. Системные требования

Для надежного функционирования продукта перед установкой убедитесь, что на Вашем компьютере запущена одна из следующих операционных систем и выполняются следующие системные требования:

Microsoft Windows 98 SE / NT-SP6 / Me / 2000 / XP 32-bit

- Процессор Pentium II 350 MHz или выше
- Минимум 128Мб оперативной памяти (рекомендуется 256Мб)
- Минимум 60Мб свободного дискового пространства на жестком диске
- Internet Explorer 5.5 или выше

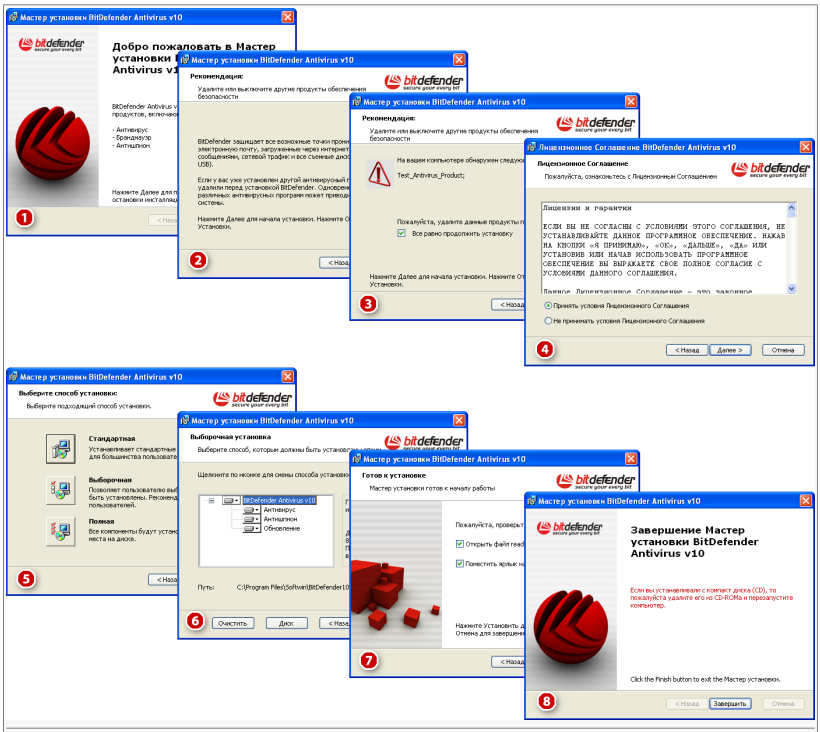
Microsoft Windows Vista 32-bit

- Процессор 800 MHz или выше
- Минимум 512Мб оперативной памяти (рекомендуется 1Гб)
- Минимум 60Мб свободного дискового пространства на жестком диске

Пробную версию**BitDefender Antivirus v10** можно загрузить с сайтаhttp://www.bitdef.ru, посвященного безопасности данных.

2.2. Пошаговая установка

Найдите файл setup и дважды щелкните по нему. Запустится мастер установки, который проведет процесс настройки.



Пошаговая установка

1. Нажмите **Далее** чтобы продолжить, или **Отменить** если Вы хотите прервать установку.
2. Нажмите **Далее** чтобы продолжить, или **Назад** если Вы хотите вернуться к первому шагу.
3. BitDefender Antivirus v10 предупредит Вас, если на вашем компьютере установлены другие антивирусные продукты.

Внимание

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

Нажмите **Назад** чтобы вернуться к предыдущему шагу или на кнопке **Далее** чтобы продолжить.

Замечание

Если BitDefender Antivirus v10 не обнаружил в вашей системе других антивирусных продуктов, данный шаг будет пропущен.

4. Пожалуйста, прочитайте Лицензионное соглашение, нажмите **Я принимаю условия Лицензионного соглашения** и затем нажмите **Далее**. Если Вы не согласны с условиями, нажмите **Отменить**. Установка будет прервана, и Вы выйдете из программы установки.
5. Можно выбрать тип установки: обычную, выборочную и полную.

   Обычная
   Программа будет установлена с самыми общими установками. Этот вариант рекомендуется для большинства пользователей.

   Выборочная
   Вы можете выбрать компоненты для установки. Рекомендуется только для опытных пользователей.

   Полная
   Полная установка продукта. Будут установлены все модули BitDefender.

   Выбрав вариант **Обычная** или **Полная**, вы пропустите шаг 6.
6. При **Выборочной** установке появится новое окно со списком всех компонентов BitDefender, из которых Вы сможете выбрать необходимые для установки.

   Нажав на название модуля, справа вы увидете краткое описание (включая и минимальный необходимый размер дискового пространства). Нажатие на значок модуля откроет окно, где можно выбрать, устанавливать ли данный модуль или нет.

   Вы можете выбрать папку, в которую желаете установить продукт. По умолчанию это `C:\Program Files\Softwin\BitDefender 10`.

   Если вы хотите выбрать другую папку, нажмите **Обзор**, а затем в открывшемся окне выберите папку, куда хотите установить BitDefender Antivirus v10. Нажмите **Далее**.
7. Существуют две опции, выбранные по умолчанию:
   - **Открыть файл readme** - открывает ознакомительный файл в конце установки.
   - **Создать ярлык на рабочем столе** - создает ярлык BitDefender Antivirus v10 на вашем рабочем столе в конце установки.

- **Выключить Защиту Windows** - выключает Защиту Windows;доступно только для Windows Vista.

Нажмите **Установить** чтобы начать установку программы.

Важно

В процессе установки будет запущен мастер установки. Мастер поможет вам зарегистрировать ваш **BitDefender Antivirus v10**, создать учетную запись BitDefender и настроить BitDefender для выполнения важных задач безопасности. Завершите процесс установки при помощи мастера, чтобы перейти к следующему шагу.

8. Нажмите **Завершить**, чтобы завершить установку. Если вы установили продукт в папку по умолчанию, будет создана новая папка `Softwin` в `Program Files`, в которой будет находиться подкаталог `BitDefender 10`.

Замечание

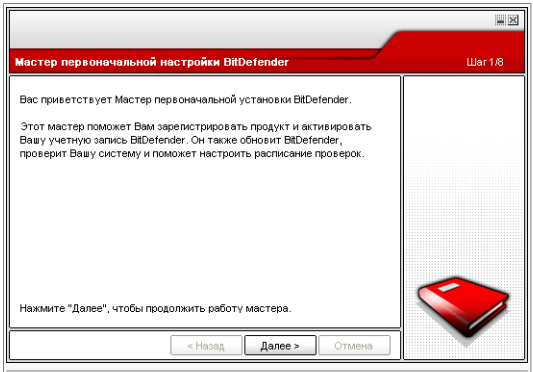
Может появиться сообщение с просьбой перезапустить вашу систему для того, чтобы мастер установки мог завершить инсталляционный процесс.

2.3. Мастер начальной настройки

В процессе установки будет запущен мастер установки. Мастер поможет вам зарегистрировать ваш **BitDefender Antivirus v10**, создать учетную запись BitDefender и настроить BitDefender для выполнения важных задач безопасности.

Завершение всех шагов мастера необязательно; однако, мы рекомендуем Вам завершить все шаги, чтобы сэкономить время и убедиться, что Ваша система находится в безопасности еще до установки BitDefender Antivirus v10.

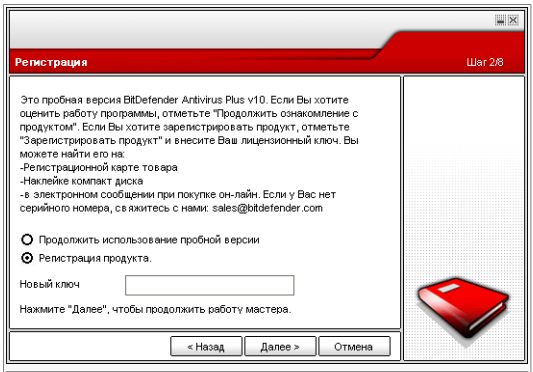
2.3.1. Шаг 1/8 - Мастер настройки BitDefender.



Окно приветствия

Нажмите **Далее**.

2.3.2. Шаг 2/8 - Регистрация BitDefender Antivirus v10



Регистрация

Выберите **Зарегистрировать продукт**, чтобы зарегистрировать **BitDefender Antivirus v10**. Введите лицензионный ключ в поле **Новый ключ**.

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

Нажмите **Далее**.

2.3.3. Шаг 3/8 - Создать учетную запись BitDefender

Создание учетной записи

У меня нет учетной записи BitDefender

Чтобы воспользоваться технической поддержкой BitDefender и прочими бесплатными услугами, Вам необходимо создать учетную запись.

Введите действующий адрес электронной почты в поле **E-mail**. Придумайте пароль и введите его в поле **Пароль**. Подтвердите пароль, вводя его еще раз в поле **Подтверждение пароля**. Используйте адрес электронной почты и пароль, чтобы войти в Вашу учетную запись по адресу http://myaccount.bitdef.ru.

Замечание

Пароль должен состоять минимум из четырех символов.

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

Важно

Активируйте свою учетную запись прежде чем переходить к следующему шагу.

Если Вы не хотите создавать учетную запись BitDefender, выберите **Пропустить этот шаг**. Вы также пропустите и следующий шаг мастера.

Нажмите **Далее**, чтобы продолжить, или **Отменить**, чтобы прервать работу мастера.

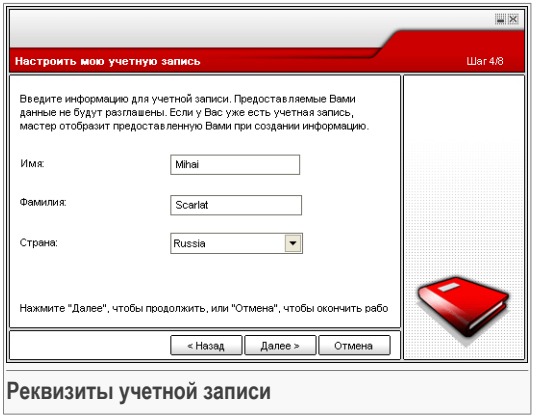
У меня уже есть учетная запись BitDefender .

Если у Вас уже имеется активная учетная запись, предоставьте адрес электронной почты и пароль вашей учетной записи. Если Вы введете неверный пароль, Вам будет предложено попробовать еще раз при нажатии **Далее**. Нажмите **ОК**, чтобы ввести пароль еще раз, или **Отмена**, чтобы прервать работу мастера.

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

Нажмите **Далее**, чтобы продолжить, или **Отменить**, чтобы прервать работу мастера.

2.3.4. Шаг 4/8 - Введите реквизиты учетной записи.



Реквизиты учетной записи

Замечание

Если Вы выбрали **Пропустить этот шаг** на третьем шаге, Вы не попадете в меню данного шага.

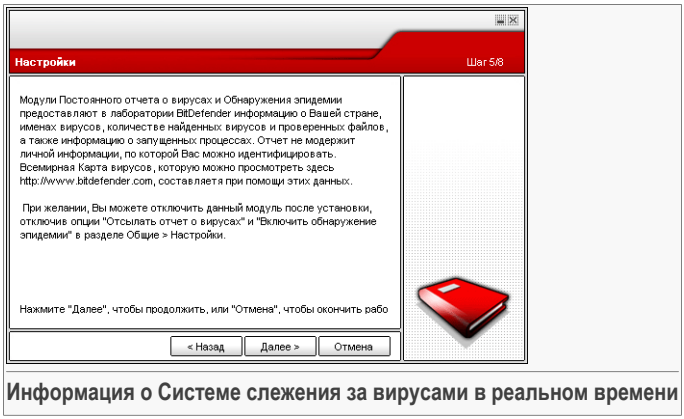
Введите имя и фамилию, выберите страну проживания.

Если у Вас уже есть учетная запись, мастер отобразит информацию, предоставленную Вами ранее, если таковая имеется. По желанию, здесь можно скорректировать данную информацию.

Важно
Предоставленные Вами данные конфиденциальны.

Нажмите **Далее**, чтобы продолжить, или **Отменить**, чтобы прервать работу мастера.

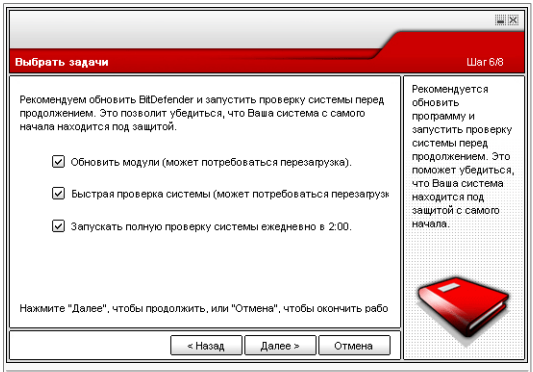
2.3.5. Шаг 5/8 - Информация о системе слежения за вирусами в реальном времени



Информация о Системе слежения за вирусами в реальном времени

Нажмите **Далее**, чтобы продолжить, или **Отменить**, чтобы прервать работу мастера.

2.3.6. Шаг 6/8 - Выбор задач для запуска



Выбор задачи

Настройте BitDefender Antivirus v10 на выполнение важных задач для обеспечения безопасности Вашей системы.

Доступны следующие варианты:

- **Обновить модули BitDefender Antivirus v10 (может потребоваться перезагрузка)** - на следующем шаге будет произведено обновление модулей BitDefender Antivirus v10, чтобы обеспечить защиту Вашего компьютера от новых вирусов и угроз.
- **Запустить быструю проверку системы** - на следующем шаге будет проведена быстрая проверка системы, чтобы BitDefender Antivirus v10 мог убедиться, что файлы в папках `Windows` и `Program Files` не заражены.
- **Запускать полное сканирование системы ежедневно в 2:00 утра** - запускает полное сканирование системы ежедневно в 2:00 утра.

Важно

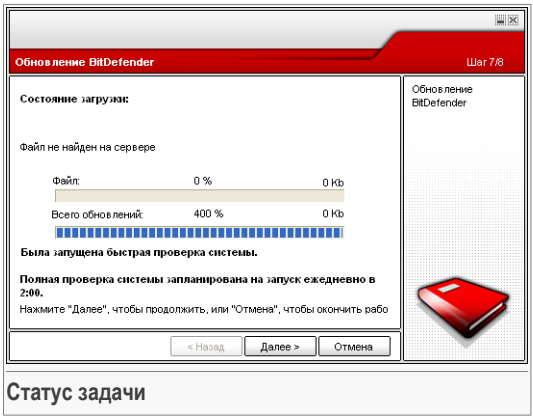
Рекомендуем Вам включить данные опции перед тем, как перейти к следующему шагу, чтобы обеспечить полную безопасность Вашей системы.

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

Вы можете внести любые изменения, возвращаясь к предыдущим шагам (нажав **Назад**). После этого момента процесс установки необратим: то есть вы не сможете возвратиться к предыдущим шагам.

Нажмите **Далее**, чтобы продолжить, или **Отменить**, чтобы прервать работу мастера.

2.3.7. Шаг 7/8 - Ожидание завершения задач

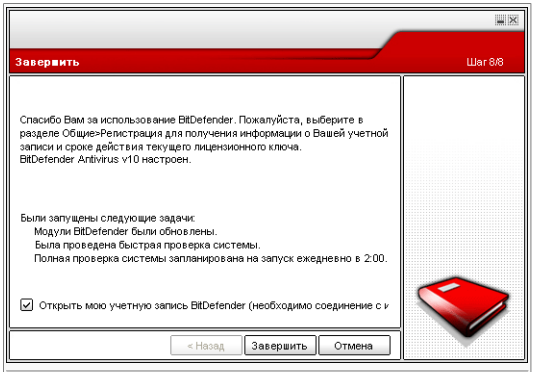


Статус задачи

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

Нажмите **Далее**, чтобы продолжить, или **Отменить**, чтобы прервать работу мастера.

2.3.8. Шаг 8/8 – Итоговый отчет



Завершение

Это последний шаг мастера установки.

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

Нажмите **Завершить**, чтобы завершить работу мастера и продолжить установку программы.

2.4. Обновление

Процедура обновления программного продукта может быть выполнена одним из следующих способов:

- **Установить, не удаляя предыдущую версию - для версий for v8 или выше, за исключением Internet Security**

  Дважды щелкните на файле установки и следуйте указаниям мастера установки, описанным в разделе «*Пошаговая установка*» (p. 9).

  Важно

  Во время установки программы появится сообщение об ошибке `службы Filespy`. Нажмите **OK** и продолжайте установку.

- **Удалить предыдущую версию и установить новую - для всех версий BitDefender**

Прежде всего, удалите предыдущую версию, затем перегрузите компьютер и установите новую, следуя указаниям раздела «*Пошаговая установка*» (p. 9).

Важно

Если вы обновляете продукт с версии BitDefender v8 или выше, рекомендуем сохранить BitDefender настройки. После завершения процесса обновления, Вы сможете их снова загрузить.

2.5. Удаление, восстановление или изменение BitDefender.

Если Вы хотите удалить, восстановить или изменить **BitDefender Antivirus v10**, выполните следующие действия, начиная с меню Пуск Windows: **Пуск** → **Программы** → **BitDefender 10** → **Изменить, восстановить или удалить**.

Подтвердите свой выбор, нажав **Далее**. В появившемся окне можно выбрать следующее:

- **Изменить** - выбор новых компонентов, которые необходимо установить, или уже установленных, которые необходимо удалить.

  Замечание

  Чтобы узнать как закончился процесс установки посмотрите шаг шестой в «*Пошаговая установка*» (p. 9) этом разделе.

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

  Важно

  Перед тем, как восстанавливать продукт, рекомендуем Вам сохранить Настройки BitDefender. После окончания процеса восстановления вы сможете их снова загрузить.

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

  Если Вы хотите удалить BitDefender, то Вы больше не будете защищены против вирусов, программ-шпионов и хакеров. Если Вы хотите, чтобы Брандмауэр Windows и Защита Windows были включены после деинсталляции BitDefender, выберите соответствующие флажки в следующем шаге мастера.

  Мы были бы благодарны, если бы Вы перед удалением BitDefender сообщили нам причину. Выберите соответствующий флажок **Обратная связь** и заполните online-форму, чтобы выслать нам Ваши предложения.

Чтобы продолжить установку, выберите одно из трех перечисленных действий. Рекомендуем **Удалить** программу для полной переустановки. После удаления программы удалите папку `Softwin` из каталога `Program Files`.

Описание и особенности

3. BitDefender Antivirus v10

Программное решение для антивирусной защиты и защиты от сетевых атак для Вашего персонального компьютера!

BitDefender Antivirus v10 мощный инструмент для антивирусной защиты и защиты от сетевых атак с функциями, наиболее подходящими для нужд безопасности Вашего компьютера. Легкие в использовании автоматические обновления делают **BitDefender Antivirus** продуктом, который можно "установить и забыть".

3.1. Антивирус

Целью модуля антивирус является обнаружение и удаление всех известных вирусов. Он использует надежные алгоритмы защиты, сертифицированные компаниями ICSA Labs, Virus Bulletin, Checkmark, Checkvir и TÜV.

Проактивное обнаружение. B-HAVE (Поведенческий Эвристический Анализатор в виртуальной среде) - это эмуляция виртуального компьютера в компьютере, в котором запускаются элементы программного обеспечения с целью выявления потенциальных вредных кодов. Эта уникальная технология BitDefender обеспечивает новый уровень защиты, который гарантирует безопасность операционной системы от неизвестных вирусов, обнаруживая компоненты зловредных кодов, образы которых еще не занесены в базы данных.

Постоянная антивирусная защита. Модули проверки BitDefender проверяют и лечат зараженные файлы, сводя к минимуму риск потери данных. Зараженные документы могут быть восстановлены, а не удалены.

Обнаружение и удаление руткитов. BitDefender ищет руткиты (скрытые программы, которые могут управлять компьютером пользователя), и удаляет их при обнаружении.

Сканирование интернет-трафика. Весь интернет-трафик в реальном времени проходит через специальный фильтр перед тем, как попасть к вашему браузеру, что обеспечивает безопасное и приятное использование интернета.

Защита приложений P2P и мессенджеров. Проверка на наличие вирусов, распространяемых с помощью мессенджеров и программ обмена файлами.

Полная защита электронной почты. BitDefender работает на уровне протоколов POP3/SMTP, фильтруя входящие и исходящие электронные сообщения,

независимо от типа используемого почтового клиента (Outlook™, Outlook Express™, The Bat!™, Netscape® и т.д.) без дополнительной настройки.

3.2. Антишпион

BitDefender отслеживает и предотвращает потенциальную угрозу сетевых атак в реальном времени до того, как они могут нанести ущерб Вашей системе. За счет использования обширной базы данных образов программ-шпионов, последние не смогут проникнуть в ваш компьютер.

Защита от программ-шпионов в реальном времени. Bitdefender контролирует множество потенциальных "горячих точек" в вашей системе, где могут действовать программы-шпионы, а также проверяет любые изменения в вашей системе и программном обеспечении. Известные угрозы со стороны программ-шпионов также блокируются в реальном времени.

Сканирование и удаление программ-шпионов. Bitdefender может проверить вашу систему или ее часть на наличие угроз со стороны известных программ-шпионов. При сканировании используется постоянно обновляемая база данных образов программ-шпионов.

Обеспечение конфиденциальности. Модуль обеспечения конфиденциальности отслеживает трафик HTTP (веб) и SMTP (электронная почта) Вашего компьютера на наличие личной информации - например, номер кредитной карты, номер социального страхования и прочее (например, части паролей).

Anti-Dialer. Настраиваемая программа anti-dialer блокирует работу программ набора телефонного номера, спасая Вас от получения огромных счетов за телефон.

Контроль за cookies. Фильтры защиты от сетевых атак отслеживают входящие и исходящие файлы cookie, сохраняя конфиденциальность указанной Вами личной информации, в то время, когда вы находитесь в сети Интернет.

Контроль активного контента. Заблаговременно блокируется выполнение таких потенциально опасных программ, как: ActiveX, Java Applets или коды Java Scripts.

3.3. Другие особенности

Установка и использование. Мастер настройки запускается сразу после установки, помогая пользователям выбрать наиболее подходящие настройки обновления, реализуя запланированные задачи сканирования и обеспечивая быструю регистрацию и активацию продукта.

Удобство в использовании. BitDefender спроектировал свои модули, делая основной акцент на простоте использования и избежании беспорядочных действий. В результате, большинство модулей BitDefender v10 требуют незначительного вмешательства пользователей за счет использования автоматизации и обучения системы.

Ежечасные обновления. Ваша копия BitDefender будет обновляться 24 раза в сутки через Интернет, напрямую или через прокси сервер. При необходимости, продукт способен самостоятельно восстанавливаться, загружая поврежденные или недостающие файлы с серверов BitDefender.

Круглосуточная поддержка. Реализована онлайн благодаря квалифицированным представителям службы поддержки и возможности доступа к базе данных с ответами на Часто Возникающие Вопросы.

Реаниматор Bitdefender. BitDefender Antivirus v10 поставляется на загрузочном диске. Данный компакт диск можно использовать для анализа/восстановления/обезвреживания вирусов зараженной системы, которая не запускается.

4. Модули BitDefender

BitDefender Antivirus v10 состоит из следующих модулей: **Общий**, **Антивирус**, **Защита от сетевых атак** и **Обновления**.

4.1. Общий модуль

Изначальная конфигурация поставляемого программного продукта BitDefender обеспечивает максимальную безопасность.

При помощи Общего модуля Вы можете настроить уровень безопасности и выполнять важные задачи по обеспечению безопасности. Также, здесь можно зарегистрировать продукт и настроить общее поведение BitDefender.

4.2. Модуль Антивирус

BitDefender защищает Вас от вирусов, сетевых атак и прочих вредоносных программ, проникающих в Вашу систему, сканируя файлы, электронные сообщения, закачиваемые файлы, и всю прочую информацию, поступающую в Вашу систему.

Настройки защиты BitDefender разделены на две категории:

- Входное сканирование - предотвращает доступ в систему новых вирусов, сетевых атак и прочих вердоносных программ. Эта система также называется Постоянная защита - файлы сканируется по мере того, как пользователь использует их. К примеру, BitDefender сканирует текстовый файл на наличие известных угроз при его открытии, а также электронные сообщение, когда Вы их получаете. Таким образом, BitDefender сразу же проверяет все файлы, с которыми Вы работаете, перед тем, как вы их откроете.
- "Проверка по требованию - обнаруживает вирусы, программы-шпионы и прочие вредоносные программы, которые уже находятся на вашем компьютере. Это классический пример проверки по желанию пользователя – Вы выбираете диск, папку, или файл для проверки BitDefender, а BitDefender проверяет их по Вашему требованию.

4.3. Модуль защиты от сетевых атак

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

4.4. Модуль обновлений

Каждый день появляются и обнаруживаются все новые вредоносные программы. Вот почему так важно постоянно обновлять Bitdefender образами новых вредоносных программ. По умолчанию, Bitdefender автоматически проверяет обновления каждый час.

Существуют следующие варианты обновления:

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

Кроме того, с точки зрения действий пользователя можно выделить:

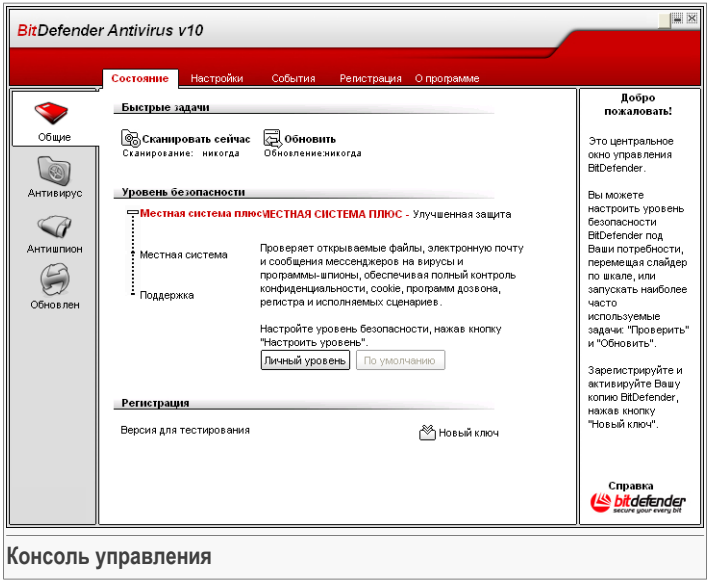
- автоматическое обновление - BitDefender автоматически связывается с сервером обновлений, чтобы проверить наличие обновления. Если обновление уже выпущено, Bitdefender обновляется автоматически. Автоматическое обновление может также быть выполнено, в любое время по нажатию **Обновить сейчас** в модуле Обновления.
- Обновление вручную - вы должны загрузить и установить последние образы вредоносных программ вручную.

Консоль управления

5. Краткий обзор

BitDefender Antivirus v10 был разработан с централизованной консолью управлния, которая позволяет настраивать опции защиты для модулей BitDefender. Другими словами, все, что Вам нужно сделать, чтобы получить доступ к модулям, - это открыть консоль управления: **Антивирус**, **Защита от сетевых атак** и **Обновление**.

Чтобы войти в консоль управления, воспользуйтесь меню Пуск Windows и следующим путем: **Пуск** → **Программы** → **BitDefender 10** → **BitDefender Antivirus v10**, или более быстрый вариант - двойной щелчок на **значок BitDefender** в системном трее.



Консоль управления

В левой части консоли управления расположены ссылки на рабочие модули:

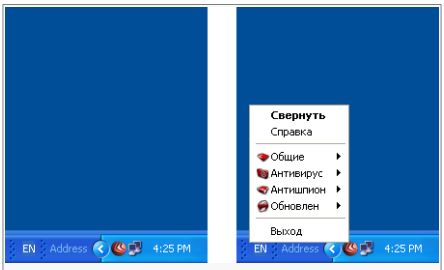
- Общие - в данном разделе можно установить общий уровень безопасности и выполнить основные задачи обеспечения безопасности. Здесь также можно зарегистрировать продукт и просмотреть общую информацию о настройках, самом продукте, а также найти контактную информацию.

- Антивирус - в данном разделе вы можете настроить модуль **Антивирус**.
- Антишпион - в этом разделе Вы можете конфигурировать модуль **Антишпион**.
- Обновление - открывает доступ в окно **Настройки обновления**.

В правой части консоли управления можно найти информацию о разделе, в которым вы находитесь в данный момент. Ссылка **Помощь** в правом нижнем углу открывает файл **Помощи**.

5.1. Системный трей

Если свернуть окно консоли управления, в системном трее появится значок:



Значок BitDefender в системном трее.

Двойной щелчок по данному значку откроет консоль управления. Нажатие правой кнопкой откроет контекстное меню. Оно позволяет быстро управлять BitDefender:

- **Показать / Закрыть** - открывает консоль управления или сворачивает ее в системный трей.
- **Помощь** - открывает файл помощи.
- **BitDefender Общие** - управление модулем Общие.
  - **Новый ключ** - запуск мастера регистрации, который поможет Вам пройти процесс регистрации.
  - **Редактировать** - запуск мастера, который поможет Вам создать учетную запись BitDefender.
- **Антивирус** - управление модулем антивирус.
  - **Постоянная защита включена / отключена** - показывает статус постоянной защиты (включена/отключена). Используйте этот пункт, что бы включить или отключить постоянную защиту.
  - **Сканирование** - открывает подменю, где можно выбрать и запустить одну из задач проверки, доступных в разделе Сканирование
- **Антишпион** - администрирование модуляЗащита от сетевых атак.
  - **Поведенческая защита от атак включена / отключена** - показывает статус поведенческой защиты от сетевых атак (включена/отключена). Используйте этот пункт, что бы включить или отключить защиту от атак.
  - **Дополнительные настройки** - позволяет настроить дополнительные параметры управления защитой от сетевых атак.
- **Обновления** - управление модулем Обновления.

- **Обновить сейчас** - запускает немедленное обновление.
- **Автоматическое обновление включено / отключено** - показывает статус автоматического обновления (включено / отключено). Воспользуйтесь этим пунктом для включения или отключения автоматических обновлений.

- **Выход** -закрывает программу. Выбирая этот вариант, занчок исчезнет из области уведомлений, и открыть консоль управления можно будет только через меню Пуск Windows.

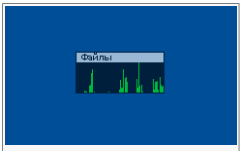
Замечание

Значок будет затенен, если отключены один или несколько модулей BitDefender. Это позволит Вам знать, что некоторые модули BitDefender отключены, без необходимости открывать консоль управления.
Значек начнет мигать, когда появится доступное обновление.

5.2. Строка состояния сканирования

В окне **Строка состояния активности** графическое отображение процесса проверки Вашей системы.

Зеленые полоски (**Файловая зона**) показывают, количество файлов, проверяемых в секунду, по шкале от 0 до 50.



Строка состояния

Замечание

Строка состояния сканирования будет перечеркнута красным крестом в соответствующей области (**Файловая зона**), когда Антивирусный монитор отключен. Таким образом, даже не открывая консоли управления, Вы будете знать, защищена ли ваша система.

Чтобы убрать это окно с экрана, просто щелкните правой кнопкой мышки на нем и выберите пункт меню **Скрыть**.

Замечание

Чтобы полностью спрятать данное окно, отключите опцию **Включить Строку состояния сканирования (график состояния продукта)** (в модуле **Общие**, раздел Настройки).

6. Общий модуль

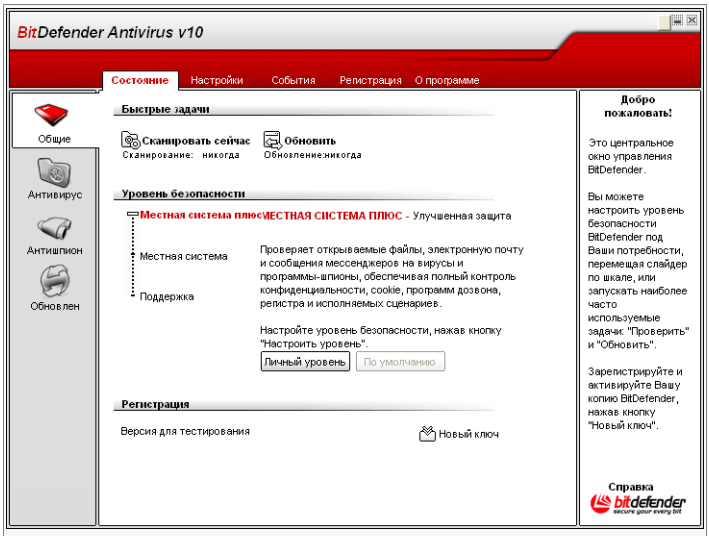
Глава **Общие** этого руководства пользователя содержит следующие разделы:

- Центр управления
- Настройки консоли управления
- События
- Регистрация программы
- О программе

Замечание

Для получения более подробной информации относительно модуля **Общие** выделите галочкой описание «*Общий модуль*» (p. 29).

6.1. Центр Управления



Центр Управления

В данном разделе можно настроить общий уровень безопасности и выполнить важные задачи BitDefender. Здесь также можно зарегистрировать продукт и посмотреть срок его действия.

6.1.1. Быстрые задачи

BitDefender позволяет организовать быстрый доступ к основным задачам обеспечения безопасности. При помощи этих задач можно поддерживать актуальность баз Вашего BitDefender, сканировать систему или блокировать нежелательный трафик.

Чтобы проверить всю систему, нажмите **Запустить сканирование**. Появится ссылка окно сканирования, и будет запущена полная проверка системы.

Важно

Настоятельно рекомендуем запускать полную проверку хотя бы раз в неделю. Чтобы подробнее узнать о задачах проверки и процессе сканирования, ознакомьтесь с разделом Проверка по требованию руководства пользователя.

Перед проверкой Вашей системы, рекомендуем обновить BitDefender, чтобы он мог распознать самые новые угрозы. Чтобы обновить BitDefender нажмите **Обновить сейчас**. Подождите несколько секунд, пока завершиться процесс обновления или, что более предпочтительно, проверьте статус обновлений в разделе Обновления

Замечание

Чтобы подробнее узнать о процессе обновления, ознакомьтесь с разделом Автоматическое обновление данного руководства пользователя.

6.1.2. Уровни безопасности

Вы можете выбрать именно такой уровень безопасности, который больше подходит Вашим потребностям в обеспечении безопасности. Передвиньте бегунок вдоль шкалы и установите соотвествующий уровень безопасности.

Существует 3 уровня безопасности:

Уровень безопасности	Описание
Обслуживание	Защита полностью отключена. Включена только функция **Автоматическое обновление**. Происходит только обновление BitDefender. Хотя этот уровень и не предполагает обеспечения безопасности, он может быть полезен для системных администраторов.
Персональная система	Включена только антивирусная защита. Данный уровень особо рекомендуется для компьютеров, которые не соединены в локальную сеть и не имеют доступа в Интернет. Требует очень мало ресурсов. На наличие вирусов проверяются все открываемые файлы.
Персональная система Плюс	Подразумевает антивирусную защиту и защиту от сетевых атак. Особо рекомендуется для компьютеров, которые не соединены в локальную сеть и не имеют доступа в Интернет. Требует очень мало ресурсов. На наличие вирусов и программ-шпионов проверяются все открываемые файлы.

BitDefender Antivirus v10 екомендуется для компьютеров, которые не соединены в локальную сеть и не имеют доступа в Интернет.

Вы можете настроить уровень безопасности нажав **Настроить уровень**. В появившемся окне выберите опции защиты BitDefender, которые вы хотите включить, и нажмите **OK**.

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

6.1.3. Статус регистрации

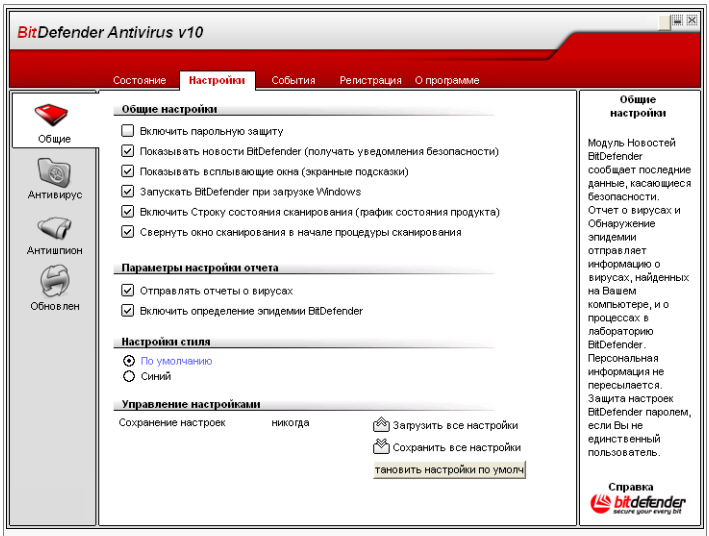
Здесь можно просмотреть информацию о статусе Вашей лицензии BitDefender. Здесь также можно зарегистрировать продукт или узнать дату окончания лицензии.

Чтобы ввести новый ключ, нажмите **Новый ключ**. Пройдите все шаги мастера регистрации, чтобы успешно зарегистрировать BitDefender.

Замечание

Чтобы узнать подробнее о процессе регистрации, ознакомьтесь с разделом Регистрация продукта данного руководства пользователя.

6.2. Настройки консоли управления



Настройки консоли управления

Здесь Вы можете настроить общее поведение Bitdefender. По умолчанию, Bitdefender загружается при запуске операционной системы Windows и затем выполняется в свернутом виде в панели задач.

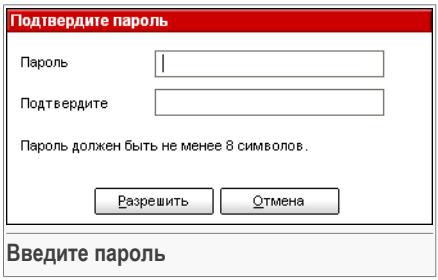
6.2.1. Общие настройки

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

  Замечание

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

  Если Вы выбираете эту опцию, появится следующее окно:



Введите пароль

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

С этого момента всякий раз, когда Вы захотите изменить настройки программы BitDefender, Вы должны будете ввести пароль.

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.
- **Запуск BitDefender при загрузке Windows** - BitDefender автоматически запускается при загрузке системы.

Замечание

Мы рекомендуем выбрать эту функцию.

- **Включить строку состояния сканирования (графическое отображение состояния программы)** - включает/отключает Строку состояния сканирования.
- **Сворачивать консоль при запуске** - сворачивает консоль управления BitDefender после того, как она была запущена при загрузке системы. Отображаться только значок BitDefender в системном трее.

6.2.2. 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 эпидемий** - отправляет в лаборатории BitDefender Labs отчет о потенциальных вирусных эпидемиях.

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

6.2.3. Настройки фона

Позволяет выбрать цвет консоли управления. Фоном называется изображение, которое будет находиться на заднем плане. Чтобы выбрать разный фон, нажмите на соотвествующий цвет.

6.2.4. Управление настройками

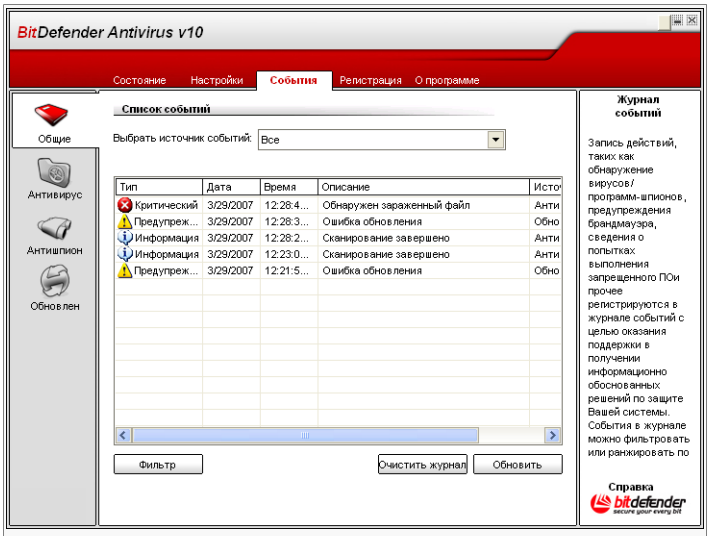
Используйте кнопки **Сохранить все настройки** / **Загрузить все настройки**, чтобы сохранить/загрузить все настройки, сделанные Вами в BitDefender в соотвествующем месте. Таким способом Вы можете использовать те же самые настройки после переустановки или восстановления Вашего BitDefender.

Важно

Только пользователи с правами администратора могут сохранять и загружать настройки.

Что бы загрузить настройки по умолчанию, нажмите **Настройки по умолчанию**.

6.3. События



События

В этом разделе отображены все события, зафиксированные программой Bitdefender.

Есть 3 типа событий: **Информация**, **Предупреждение** и **Критическое событие**.

Примеры событий:

- **Информация** - о том, когда была проверена электронная почта;
- **Предупреждение** - об обнаружении подозрительного файл;
- **Критическое событие** - обнаружение зараженного файла.

Для каждого события предлагается следующая информация: дата и время, когда произошло событие, небольшое описание и источник (**Антивирус**, **Брандмауэр**, **Защита от сетевых атак** or **Обновления**). Двойной щелчок на событии покажет его свойства.

Вы можете фильтровать эти события двумя способами (по типу или источнику):

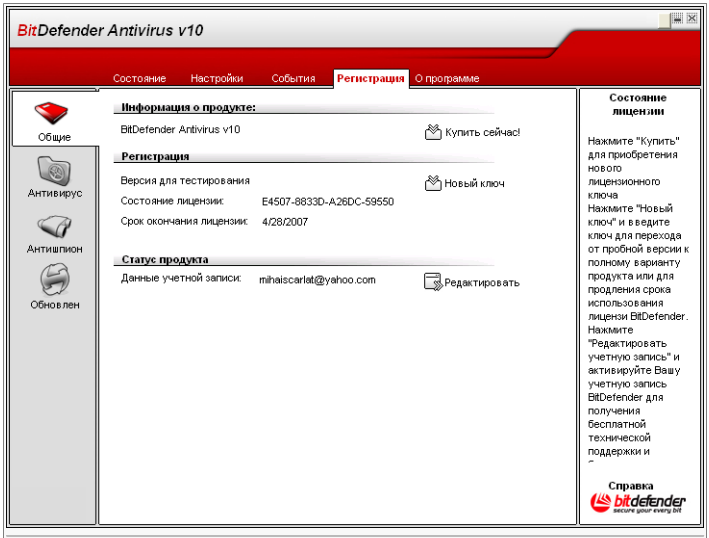
- Нажмите **Фильтр**, чтобы выбрать какие типы событий следует отображать.

- Выберите источник события в раскрывающемся меню.

Если консоль управления открыта на разделе **События** а в то же самое время происходит какое-либо событие, Вы должны нажать **Обновить** для того, чтобы увидеть информацию об этом событии.

Чтобы удалить все события из списка, нажмите **Очистить журнал** и **Да** для подтверждения выбора.

6.4. Регистрация продукта



Регистрация продукта

Данный раздел содержит информацию о продукте BitDefender (статус регистрации, ID продукта, дата истечения лицензии), а также об учетной записи BitDefender. Здесь можно зарегистрировать продукт и настроить учетную запись BitDefender.

Нажмите кнопку **Купить**, чтобы получить новый лицензионный ключ в онлайн магазине BitDefender.

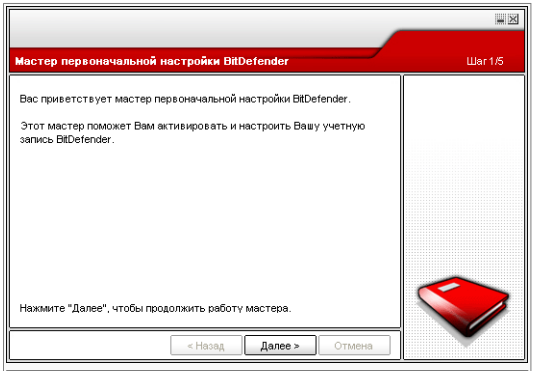
Нажав **Новый ключ**, Вы можете зарегистрировать продукт, изменить ключ регистрации или настройки учетной записи. Чтобы настроить учетную запись

BitDefender, нажмите **Редактировать**. В обоих случаях запустится мастер регистрации.

6.4.1. Мастер регистрации

Мастер регистрации имеет 5 шагов.

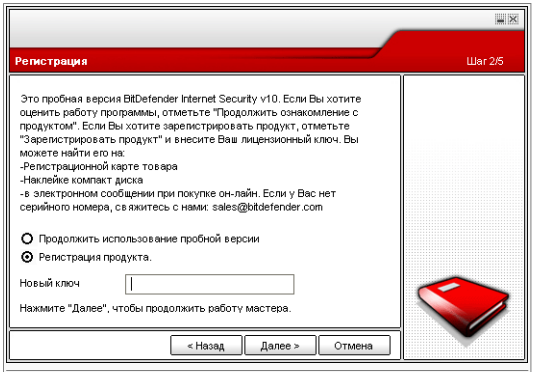
Шаг 1/5 - Добро пожаловать в Мастер регистрации BitDefender.



Окно приветствия

Нажмите **Далее**.

Шаг 2/5 - Регистрация BitDefender



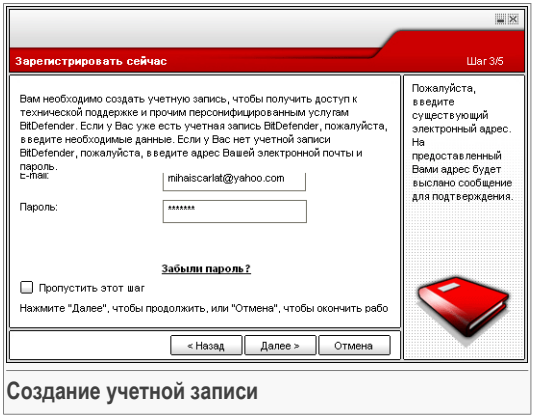
Регистрация

Выберите **Зарегистрировать продукт**, чтобы зарегистрировать **BitDefender Antivirus v10**. Введите лицензионный ключ в поле **Новый ключ**.

Чтобы продолжить пользоваться пробной версией, выберите **Продолжить оценку продукта**.

Нажмите **Далее**.

Шаг 3/5 - Создание учетной записи BitDefender



Создание учетной записи

У меня нет учетной записи BitDefender

Чтобы воспользоваться технической поддержкой BitDefender и прочими бесплатными услугами, Вам необходимо создать учетную запись.

Введите действующий адрес электронной почты в поле **E-mail**. Придумайте пароль и введите его в поле **Пароль**. Подтвердите пароль, вводя его еще раз в поле **Подтверждение пароля**. Используйте адрес электронной почты и пароль, чтобы войти в Вашу учетную запись по адресу http://myaccount.bitdef.ru.

Замечание

Пароль должен состоять минимум из четырех символов.

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

Важно

Активируйте свою учетную запись прежде чем переходить к следующему шагу.

Если Вы не хотите создавать учетную запись BitDefender, выберите **Пропустить этот шаг**. Вы также пропустите и следующий шаг мастера.

Для продолжения нажмите **Далее**.

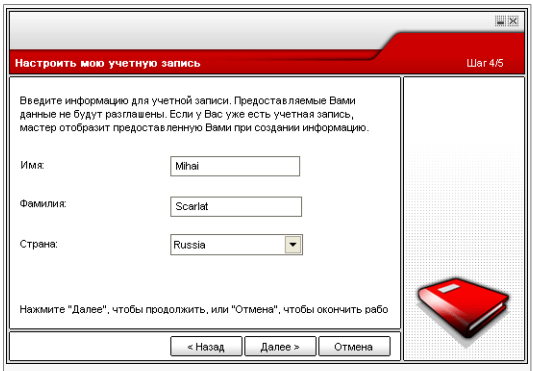
У меня уже есть учетная запись BitDefender .

Если у Вас уже имеется активная учетная запись, предоставьте адрес электронной почты и пароль вашей учетной записи. Если Вы введете неверный пароль, Вам будет предложено попробовать еще раз при нажатии **Далее**. Нажмите **ОК**, чтобы ввести пароль еще раз, или **Отмена**, чтобы прервать работу мастера.

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

Для продолжения нажмите **Далее**.

Шаг 4/5 - Введите информацию об учетной записи



Реквизиты учетной записи

Замечание

Если Вы выбрали **Пропустить этот шаг** на третьем шаге, Вы не будете проходить через этот шаг.

Введите Ваши имя и фамилию, а также страну проживания.

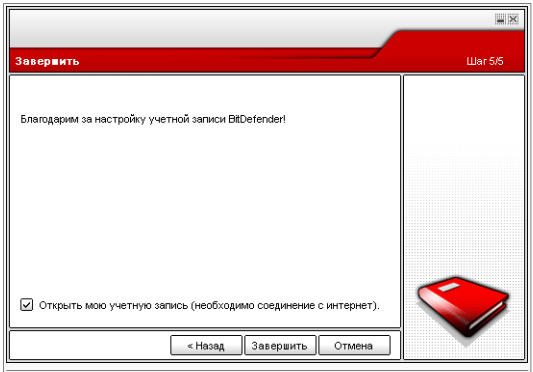
Если у Вас уже есть учетная запись, мастер отобразит информацию, предоставленную Вами ранее, если таковая имеется. Здесь также можно изменить эту информацию по желанию.

Важно

Предоставленные Вами данные конфиденциальны.

Нажмите **Далее**.

Шаг 5/5 – Итоговый отчет



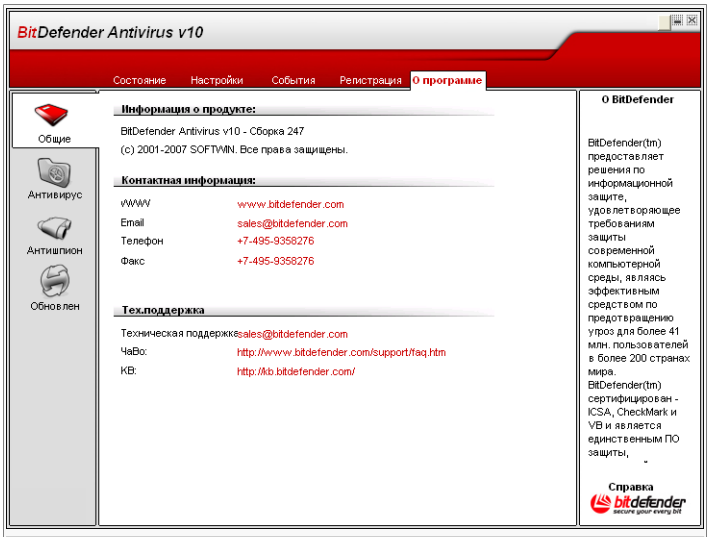
Завершение

Последний шаг мастера натсройки. Вы можете внести необходимые изменения, вернувшись на предыдущие шаги, (нажав **Назад**).

Если Вы не хотите вносить никаких изменений, нажмите **Завершить** чтобы завершить работу мастера.

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

6.5. О программе



Общая информация

В данном разделе можно найти контактную информацию и информацию о программе.

BitDefender™ - ведущий мировой поставщик продуктов и услуг в сфере обеспечения безопасности, которые удовлетворяют требования защиты современной компьютерной-среды. Компания предлагает самые быстрые и эффективные решения, устанавливая новые стандарты в сфере безопасности, своевременного обнаружения и ликвидации угроз. BitDefender предоставляет свои продукты и услуги более чем 41 миллиону пользователей в более чем 180 странах.

Торговая марка BitDefender™ сертифицирована всеми главными независимыми экспертами - **ICSA Labs**, **CheckMark** и **Virus Bulletin**, и является единственным программным продуктом, обеспечивающим безопасность, получившим награду **IST Prize**.

Более детальную информацию о BitDefender можно получить, посетив: http://www.bitdef.ru.

7. Модуль Антивирус

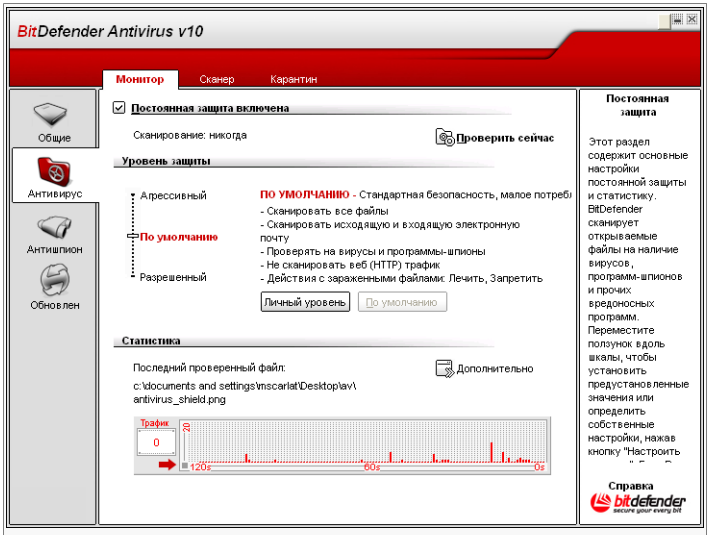
Глава **Антивирус** данного руководства для пользователя содержит следующие темы:

- Входное сканирование
- Сканирование по запросу
- Карантин

Замечание

Для получения более подробной информации о модуле **Антивирус** ознакомьтесь с «*Модуль Антивирус*» (p. 29).

7.1. Входное сканирование



Постоянная защита

В данном разделе можно настроить **постоянную защиту**, а также можно просмотреть информацию о действиях защиты. **Постоянная защита** защищает

Ваш компьютер, сканируя электронные сообщения, загружаемые файлы и все открываемые файлы.

Важно

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

В нижней части данного раздела отображается статистика **постоянной защиты** о количестве проверенных файлов и электронных сообщений. Нажмите **Подробная статистика**, чтобы промотреть более детальную информацию о статистических данных.

7.1.1. Уровень защиты

Вы можете выбрать уровень защиты, наиболее удовлетворяющие Ваши потребности в безопасности. Передвиньте бегунок по шкале в соотвествующий уровень защиты.

Существует 3 уровня защиты:

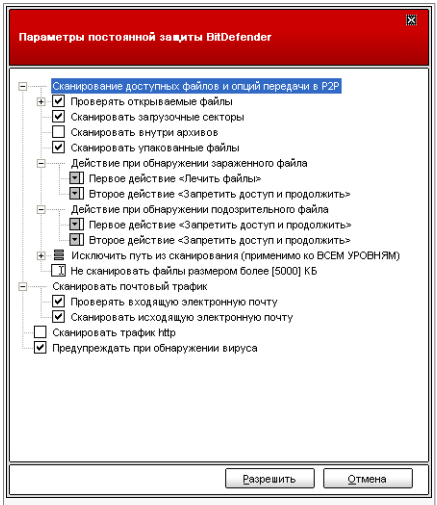
Уровень защиты	Описание
Разрешающий	Охватывает основные нужды в безопасности. Потребляет малое количество ресурсов. Программы и входящие электронные сообщения проверяются только на наличие вирусов. Кроме классического сканирования при помощи базы образов, также используется эвристический анализ. К зараженным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

Уровень защиты	Описание
	программы-шпионы. Кроме классического сканирования при помощи базы образов, также используется эвристический анализ. К зараженным файлам могут применяться следующие действия: вылечить файл/запретить доступ.

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

Опытные пользователи могут воспользоваться дополнительными настройками, предлагаемыми программным продуктом 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:



Натсройка "щита"

Меню настроек проверки очень похоже на подобные меню операционной системы Windows.

Щелчок мышки на значке "+" разворачивает список, а на значке "-" – закрывает его.

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 служб мгновенной доставки сообщений (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 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 заданным расширением	Проверяются только файлы с заданным расширением. Задаваемые расширения разделяются знаком ";".
	Исключить файлы с расширениями:[]	Файлы с заданным расширением НЕ проверяются. Задаваемые расширения разделяются знаком ";".
	Проверка на наличие других угроз	Проверка наличия других угроз. Эти файлы будут считаться зараженными. Программное обеспечение, которое включает компоненты adware, может прекратить работу, если выбрана эта настройка. Поставьте значок в поле **Пропускать программы дозвона и приложения при сканировании**, если Вы хотите пропускать подобные файлы при сканировании.
Проверка дисковода при обращении		Поверка дисковода дискет при первом обращении.
Проверять внутри архивов		Проверяются также архивы. Включение данной опции замедлит работу компьютера.
Проверить запакованные файлы		Проверяются все запакованные файлы.
Первоначальное действие		Из выпадающего списка, Вы можете выбрать одно из следующих действий,

Настройка		Описание
		которое будет выполнено при обнаружении зараженноого или подозрительного файла.
	Запретить доступ и продолжать	При обнаружении зараженного файла доступ к нему будет запрещен.
	Вылечить файл	Выполняется лечение зараженного файла.
	Удалить файл	Зараженный файл удаляется немедленно, без предупреждения.
	Переместить в карантин	Зараженные файлы перемещаются в карантинную папку.
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 в карантин	Зараженные файлы перемещаются в карантинную папку.
Не проверять файлы, чей размер превышает [x] Kb		Введите максимальный размер файла для проверки. Если введен 0 Kb, будут проверены все фалы, независимо от их размера.
Исключить файлы в заданном пути (применимо ко ВСЕМ УРОВНЯМ)		Нажмите "+", соответствующий данной опции, чтобы определить каталог, который будет исключен из списка предназначенных для сканирования. Вследствие этого, данная опция откроется в новую: появится `Новый пункт`. Поставьте галочку, уведомляющую о новом пункте, и в окне обзора выберите каталог, каторый будет исключен из списка сканирования. Выбранные здесь объекты не будут проверяться, независимо от выбранного

Настройка	Описание
	уровня защиты (кроме **Настроенного уровня**).

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

  Доступны следующие варианты:

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

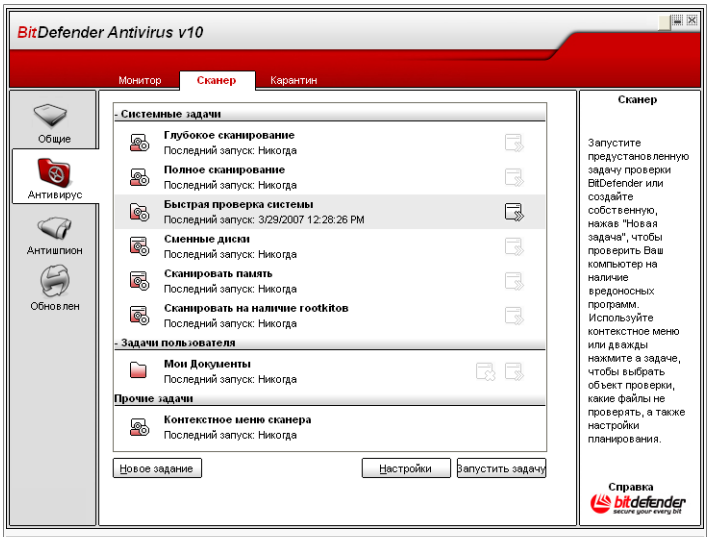
- **Сканировать траффик http** - сканировать трафик http.
- **Предупреждать об обнаружении вируса** - при обнаружении вируса в файле или электронном сообщении появляется окно с предупреждением.

  Предупреждение об обнаружении зараженного вирусом файла содержит название вируса, путь к зараженному файлу, действие 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 мастера, который поможет Вам выслать этот файл в лабораторию Bitdefender для дальнейшего анализа. При этом Вы можете указать свой адрес электронной почты, чтобы получить информацию относительно этого предупрежедния.

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

7.2. Сканирование по требованию



Задачи сканирования

В этом разделе Вы можете конфигурировать проверку Вашего компьютера Bitdefender.

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. Вот поэтому полезно проверить Ваш компьютер на наличие вирусов после установки программы, а также в дальнейшем регулярно проверять компьютер.

7.2.1. Задачи сканирования

Сканирование по требованию, основывается на задачах сканирования. Пользователь может проверить компьютер, используя стандартные задачи или собственные задачи (задачи, определенные пользователем).

Существует три категории задач сканирования:

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

Стандартные задачи	Описание
Глубокая проверка системы	Проверка всей системы, включая архивы, на наличие вирусов и программ-шпионов.
Полная проверка системы	Проверка всей системы, кроме архивов, на наличие вирусов и программ-шпионов.
Быстрая проверка системы	Проверка всех программ на наличие вирусов и программ-шпионов.
Проверка съемных дисков	Проверка съемных дисков на наличие вирусов и программ-шпионов.
Проверка памяти	Проверка памяти на наличие известных программ-шпионов.
Проверка на руткиты	Проверка памяти на скрытые вредоносные программы.

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

  Имеется задача, названная `Мои документы`. Этой задачей можно пользоваться для проверки Ваших документов в папке`Мои документы`.

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

Справа от каждой задачи доступны три кнопки:

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

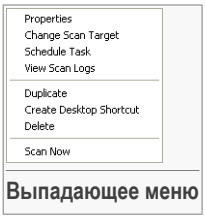
Замечание

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

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

7.2.2. Выпадающее меню

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



Выпадающее меню

В выпадающем меню имеются следующие команды:

- **Проверить** - запуск выбранной задачи, немедленное начало процесса проверки.
- **Сменить объект сканирования** - открывает окно **Свойства**, вкладку **Путь проверки**, где можно изменить объект проверки для выбранной задачи.
- **Запланировать задание** - открывает окно **Свойства**, вкладку **Планировщик**, где можно запланировать выполнение выбранной задачи.
- **Просмотр журнала проверок** - открывает окно **Свойства**, вкладку **Журнал проверок**, где можно просмотреть сгенерированный отчет после выполнения выбранной задачи.
- **Создать копию** - создать копию выбранной задачи.

Замечание

Данная функция полезна при создании новых задач, поскольку можно изменить настройки дубликата.

- **Создать ярлык на рабочем столе** - создание ярлыка для выбранной задачи на рабочем столе.
- **Удалить** - удаление выбранной задачи.

Замечание

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

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

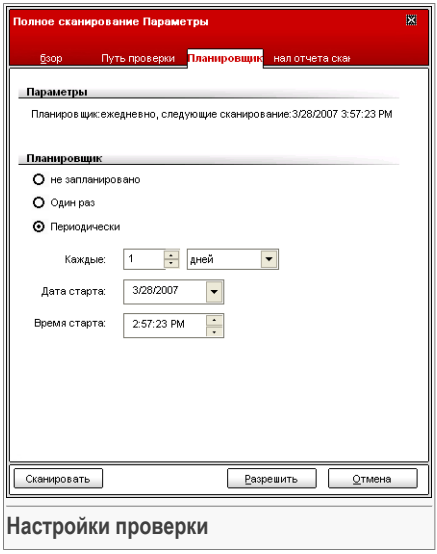
Важно

Из-за их особенных свойств для категории**Прочие задачи** доступны только опции **Свойства** и**Просмотр журналов проверки**.

7.2.3. Свойства задач проверки

Каждая задача имеет собтсвенное окно **Свойства**, где можно настроить опции проверки, установить объект проверки, запланировать задачу или просмотреть отчеты. Выберите в окне задачу и нажмите **Свойства** (или правым кликом по задаче и выбрать **Свойства**).

Настройки проверки



Настройки проверки

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

Уровень проверки

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

Существует 3 уровня проверки:

Уровень защиты	Описание
Низкий	Подразумевает среднюю эффективность выявления. Потребляет небольшое количество ресурсов.

Уровень защиты	Описание
	Программы проверяются только на наличие вирусов. Кроме классической проверки при помощи базы образов, также используется эвристический анализ. К зараженным файлам применяются следующие действия: вылечить файл/поместить в карантин.
Средний	Подразумевает высокую эффективность выявления. Потребляет среднее количество ресурсов. Все файлы проверяются на наличие вирусов и программ-шпионов. Кроме классической проверки при помощи базы образов, также используется эвристический анализ. К зараженным файлам применяются следующие действия: вылечить файл/поместить в карантин.
Высокий	Подразумевает очень высокую эффективность выявления. Потребляет значительное количество ресурсов. Все файлы и архивы проверяются на наличие вирусов и программ-шпионов. Кроме классической проверки при помощи базы образов, также используется эвристический анализ. К зараженным файлам применяются следующие действия: вылечить файл/поместить в карантин.

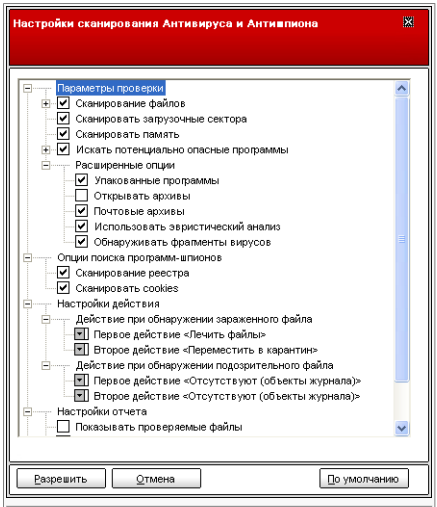
Важно

Проверка на руткиты имеет несколько уровней сканирования. Однако, это различные варианты:

- **Низкий** - Сканируются только процессы. С найденными объектами ничего не будет сделано.
- **Средний** - Сканируются файлы и процессы с целью поиска скрытых объектов. С найденными объектами ничего не будет сделано.
- **Высокий** - Сканируются файлы и процессы с целью поиска скрытых объектов. Найденные объекты переименовываются.

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

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



Настройки проверки

Меню настроек проверки очень похоже на подобные меню операционной системы Windows.

Опции сканирования сгруппированы в пять категорий:

- **Опции проверки на вирусы**
- **Опции проверки на программы-шпионы**
- **Настройки действий**
- **Настройки отчета**
- **Другие настройки**

Щелчок мышки на значке "+" разворачивает список, а на значке "-" – закрывает его.

Важно

Для **Сканирования на наличие руткитов** доступны три категории заданий: **Настройки сканирования**, **Настройки отчета** и **Другие настройки**. В первом случае Вы можете выбрать что именно сканировать(файли,память или то и другое), а так же какие именно действия требуется совершить над найденными объектами (**Не совершать/Переименовать**). Последние две категории идентичны описанным ниже.

- Выберите тип объектов для проверки (архивы, электронные сообщения и т.д.)и другие настройки. Их можно просмотреть в разделах категории **Настройки проверки на вирусы**.

Настройка		Описание
Проверка файлов	**Проверить все файлы**	Проверяются все открываемые файлы, независимо от их формата.
	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 заданным расширением	Проверяются только файлы с заданным расширением. Задаваемые расширения разделяются знаком ";".
	Исключить файлы с расширениями, заданными пользователем	Файлы с заданным расширением НЕ проверяются. Задаваемые расширения разделяются знаком ";".
Проверить загрузочные секторы		Проверка загрузочных секторов системы.
Проверка памяти		Проверка памяти на вирусы и прочие вредоносные программы.
Обнаружение riskware		Проверка наличия других угроз помимо вирусов, типа программ - номеронабирателей и программ типа adware. Эти файлы будут считаться зараженными. Программное обеспечение, которое включает компоненты adware, может прекратить работу, если выбрана эта настройка. Выберите **Исключить приложения и программы дозвоны**, если вы хотите исключать подобные фалы из списка проверяемых.

Настройка		Описание
Расширенные опции проверки	**Открыть запакованные программы**	Проверяются запакованные файлы.
	Открыть архивы	Проверка внутри архивов.
	Открыть почтовые архивы	Проверка внутри почтовых архивов.
	Использовать эвристический метод обнаружения	Используется эвристический метод проверки файлов. Новые вирусы обнаруживаются на основе определенных образцов и алгоритмов, без образа вируса. Могут появиться ложные предупреждения. Обнаруженный файл рассматривается как подозрительный. В этом случае мы рекомендуем отправить этот файл в лабораторию BitDefender на анализ.
	Искать части вирусных тел	Поиск частей вирусных тел.

- Укажите объект сканирования на наличие программ-шпионов (регистр, файлы cookies). Это можно сделать, выбрав определенные опции в категории **Настройки проверки на наличие программ-шпионов**.

Настройка	Описание
Проверка записей системного реестра	Проверка записей системного реестра.
Проверка файлов Cookies	Проверка файлов Cookies.

- Укажите действие, которое следует предпринять по отношению к зараженным или подозрительным файлам. Откройте категорию **Настройки действий** чтобы ознакомиться со всеми возможными вариантами действия по отношению к этим файлам.

  Выберите действия, которые следует предпринять по отношению к зараженным или подозрительным файлам при их обнаружении. Вы можете определить различные действия для зараженных и подозреваемых файлов. Кроме того,

Вы можете выбрать вторую опцию возможных действий над зараженными или подозрительными файлами на случай, если выполнение первого действия окажется невозможным.

Действие	Описание
Никаких (только отчет)	Не выполняются никакие действия с зараженными файлами. Названия этих файлов появятся в файле отчета.
Запрос пользователя о действии	При обнаружении зараженного файла появляется окно с запросом: пользователю предлагается выбрать необходимое действие с этим файлом. В зависимости от важности данного файла можно выбрать следующие действия: вылечить, изолировать в карантинной зоне или удалить его.
Вылечить файлы	Выполняется лечение зараженного файла.
Удалить файлы	Зараженный файл удаляется немедленно, без предупреждения.
Переместить файлы в карантин	Зараженные файлы перемещаются в карантинную папку.
Переименовать файлы	Изменить расширение зараженных файлов на `.vir`. Переименованные файлы не открываются, а значит вирус не распространяется. В то же время, они сохраняются для последующего изучения и анализа.

Важно

Переименовать файлы - так же можно переименовать найденные скрытые файлы (руткиты). Новое расширение обнаруженных файлов будет `.bd.ren`. Переименованные файлы не открываются и не распространяются, а это значит, что потенциальная угроза удалена. В то же время, они сохраняются для последующего изучения и анализа.

- Определение опций для файлов отчета. Открыть категорию **Настройки отчета**, где Вы можете выбрать следующие варианты:

Настройка	Описание
Показывать все проверенные файлы	Перечисляются все проверенные файлы и их состояние (заражены или нет) в файле отчета.

Настройка	Описание
	Если эта функция включена, компьютер работает медленно.
Удалить записи старше [x] дней	Данное поле позволяет укзать срок сохранения отчетов в разделе Журнал проверок. Выберите данную настройку и введите период времени. По умолчанию период времени составляет 180 дней.

Замечание

Файлы отчетов можно просмотреть в разделе Журнал проверок в окне **Свойства**.

- Определение прочих опций. Откройте категорию **Другие настройки**, где Вы можете выбрать следующие варианты:

Настройка	Описание
Направить подозрительные файлы в лабораторию BitDefender	Вам будет предложено после завершения процесса проверки переслать все подозрительные файлы в лабораторию BitDefender.

Чтобы загрузить настройки по умолчанию, нажмите **По умолчанию**.

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

Другие настройки

Имеется ряд общих настроект для процесса проверки:

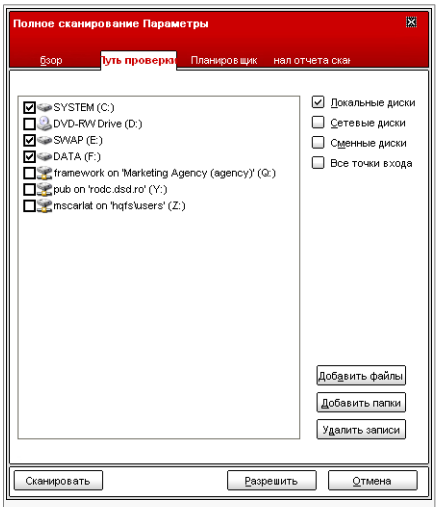
Настройка	Описание
Выполнить задачу с низким приоритетом	Уменьшается приоритет процесса проверки. Таким способом Вы ускоряете работу других программ, но увеличиваете время, необходимое для завершения процесса проверки.
Выключить компьютер после завершения проверки	Компьютер отключается после завершения процесса проверки.

Настройка	Описание
Направить подозрительные файлы в лабораторию BitDefender	Вам будет предложено после завершения процесса проверки переслать все подозрительные файлы в лабораторию BitDefender.
Свернуть окно проверки в системный трей при запуске	Окно проверки свертывается в системный трей. Чтобы открыть его, следует дважды щелкнуть на значке BitDefender.

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

Объект сканирования

Выберите задание, нажмите **Свойства** и нажмите **Путь проверки** чтобы перейти в этот раздел.



Объект сканирования

Здесь можно задать объект сканирования.

В этом разделе находятся следующие кнопки:

- **Добавить файлы** - открывает окно обзора, где можно выбрать файлы, которые необходимо проверить.
- **Добавить папки** - то же самое, только Вы можете выбрать папкуи, а не файлы.

Замечание

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

- **Убрать из списка** - удаляет файлы или папкки из списка объектов для проверки.

Замечание

Удалить можно только те файлы или папки, 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.

- **Жесткие диски** - проверка всех жестких дисков на локальном компьютере.
- **Сетевые диски** - проверка всех сетевых дисков.
- **Съемные диски** - проверка съемных дисков (CDROM, гибкий диск).
- **Все объекты** - проверка всех дисков: жестких, сетевых и съемных.

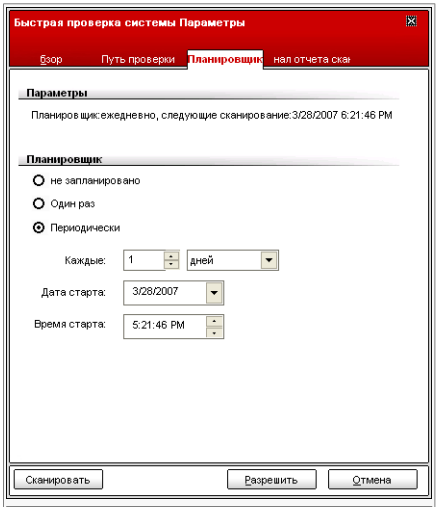
Замечание

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

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

Планировщик

Выберите задание, нажмите **Свойства** и затем нажмите **Планировщик**, чтобы перейти в этот раздел.



Планировщик

Здесь можно узнать, запланировано ли задание на выполнение, и изменить настройки планрования.

Важно

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

Чтобы запланировать задачу, вы должны выбрать один из следующих вариантов:

- **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.

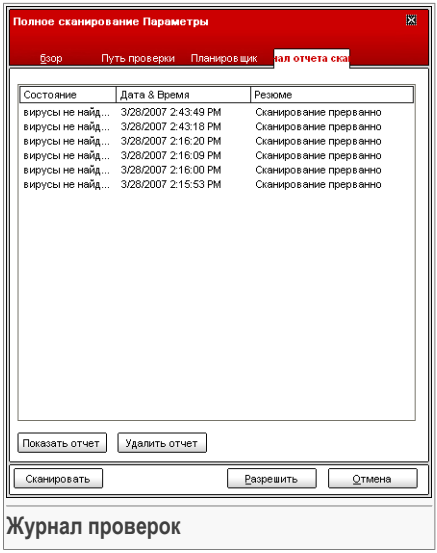
  Если Вы хотите повторять процесс проверки через определенные интервалы времени, выберите **Периодически** и в поле **Каждые** введите число минут/часов/дней/недель/месяцев/лет, соотвествующих необходимому

интервалу. Также необходимо указать дату и время первого запуска в полях **Дата/Время запуска**.

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

Журнал проверок

Выберите задание, нажмите **Свойства** и затем нажмите **Журнал проверок**, чтобы перейти в данный раздел.



Журнал проверок

Здесь можно просмотреть файлы отчетов, сгенерированные при каждой проверке. Каждый файл включает информацию о статусе (чистый/зараженный), дату и время проверки, а также итог (завершение проверки).

Доступны две кнопки:

- **Показать отчет** - просмотр выбранного файла отчета.
- **Удалить** - удаление выбранного файла отчета.

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

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

7.2.4. Типы проверки по требованию

BitDefender имеет три типа проверок по требованию:

- Немедленная проверка - запуск задачи проверки из списка системных / определенных пользователем задач;
- Контекстная проверка - щелкните правой клавишей мыши на файле или папке и выберите BitDefender Antivirus v10;
- Проверка с перетаскиванием - перетащите файл или папку на Панель состояния проверки;

Немедленная проверка

Для проверки Вашего компьютера или его части можно воспользоваться задачами проверки по умолчанию, либо можно создать собственные задачи проверки. Существует два метода создания задач проверки:

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

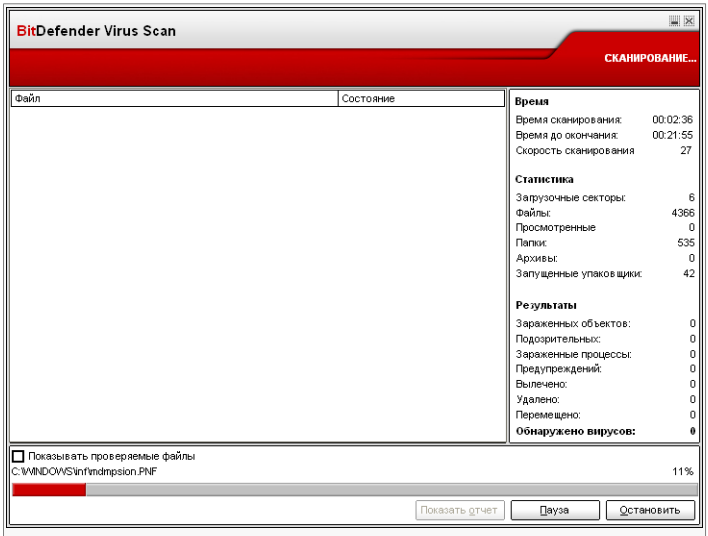
Чтобы BitDefender полностью проверил все Ваши файлы, необходимо закрыть все запущенные приложения, особенно почтовые программы (Outlook,Outlook Express или Eudora).

Прежде чем начать проверку компьютера, убедитесь, что в базе данных BitDefender есть образы всех новых вирусов, так как они появляются и обнаруживаются каждый день. Информация о последнем обновлении содержится в верхней части модуля Обновление.

Для запуска проверки, используйте один из способов:

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

Появится окно просмотра.



Окно проверки

Появится значок в системном трее, когда будет выполняться процесс проверки.

Пока идет проверка, BitDefender покажет прогресс и предупредит Вас, если будут найдены угрозы. Вы можете видеть статистику процесса проверки. В зависимости от цели сканирования, spyware и/или вирусов будет доступна соответствующая информация. Если оба доступны, нажмите соответственную таблицу, чтобы узнать больше о процессе проверки на spyware или вирус.

Поставив отметку в поле **Показывать последний проверенный файл** Вы будете получать информацию о последнем проверенном файле.

Замечание

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

Доступны три кнопки:

- **Стоп** -откроется новое окно, в котором Вы сможете завершить проверку системы. Нажмите **Да**&**Закрыть**, чтобы закрыть окно проверки.

Замечание

Если при проверки были обнаружены подозрительные файлы, то Вы можете их выслать в Лабоаторию BitDefender.

- **Пауза** - проверка на время остановится, чтобы возобновить ее нажмите **Возобновить**.
- **Показать отчет** - откроется отчет о проверке.

Замечание

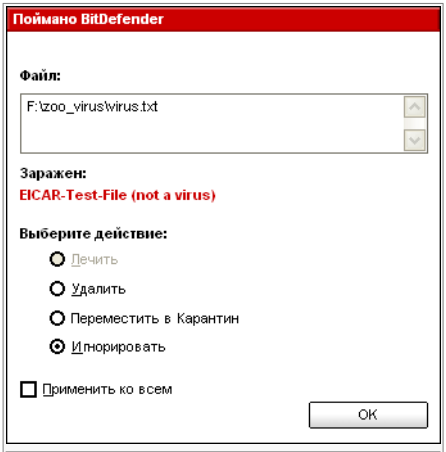
Если нажать правой кнопкой мыши на запушенном процессе, откроется выпадающее (контекстное) меню, которое позволяет управлять окном проверки. Опции (**Пауза / Продолжить**, **Остановить** и **Остановить&Закрыть**) подобны клавишам в окне проверки.

Если установлена опция **Спросить пользователя** в свойствах окна, тогда при обнаружении зараженного файла отобразится предупреждающее окно с просьбой выбрать действие над зараженным файлом.

В окне Вы увидите название файла и название вируса.

Вы можете выбрать одно из следующих действий над зараженным файлом:

- **Вылечить** - Вылечить зараженный файл;
- **Удалить** - Удалить зараженный файл;
- **Переместить в карантин** - Переместить зараженный в карантинную зону;
- **Пропустить** - Проигнорировать заражение. С зараженным файлом ничего не будет сделано.



Выбор Действия

Если Вы проверяете папку и хотите, чтобы выбранные настройки применялись ко всем файлам, выберите настройку **Применять ко всем**.

Замечание

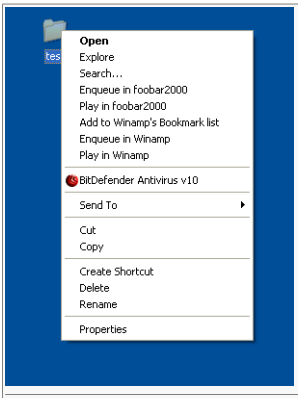
Если действие **Вылечить** не включено, значит данный файл не может быть вылечен. Лучше всего изолировать его в карантинной папке и отправить нам для анализа или удалить.

Нажмите **OK**.

Замечание

Отчеты автоматически сохраняются в разделе Журнал проверок в окне **Свойства** соответствующей задачи.

Проверка через контекстное меню



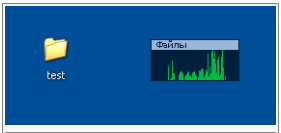
Проверка через контекстное меню

Щелкните правой кнопкой мышки на файле или папке, которые необходимо проверить, и выберите **BitDefender Antivirus v10**.

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

Проверка перетягиванием.

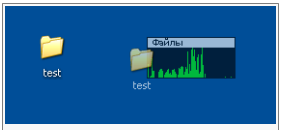
Перетяните файл или папку, которую вы хотите проверить, в **Область состояния проверки**, как показано ниже.



Перетаскивание файла

Если обнаружен зараженный файл, откроется окно предупреждения, запрашивая действие над зараженным файлом.

При обоих методах проверки (контекстная и проверка перетаскиванием) появится окно проверки



Перетаскивание файла

7.2.5. Сканирование на руткиты

BitDefender делает все,чтобы защитить Вас от угроз. Мы создали эффективный детектор руткитов. BitDefender теперь в состоянии обнаружить руткиты исследуя скрытые файлы, папки или процессы. Кроме того, это может защитить вашу систему, переименовывая другое зловредное ПО, которое использует руткиты.

Что бы проверить Ваш компьютер на наличие руткитов, нажмите **Сканирование на руткиты**. Появится окно сканирования.

Важно

Когда Вы проверяете на руткиты, настоятельно рекомендуется не совершать никаких действий над скрытыми файлами.

По окончанию сканирования, Вы сможете просмотреть результаты. Если скрытые файлы были обнаружены, проверьте их тщательно: присутствие скрытых файлов может указывать на возможное заражение.

Если вы уверены, что обнаруженные файлы являются зловредными программами, то мы рекомендуем выбрать действие **Переименовать файлы** и запустить **Сканирование на руткиты** заново. Таким образом, скрытые файлы будут блокированы.

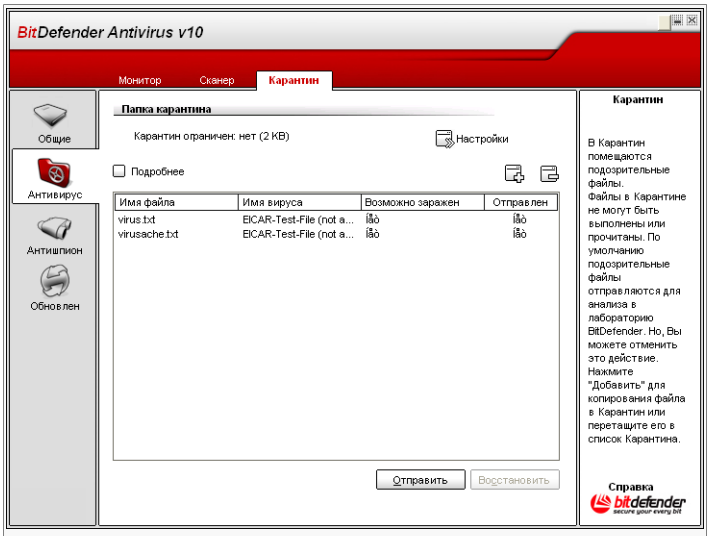
Внимание

НЕ ВСЕ СКРЫТЫЕ ФАЙЛЫ - ЗЛОВРЕДНЫЕ ПРОГРАММЫ! Перед переименованием скрытых файлов, удостоверьтесь, что они не принадлежат ни к известному приложению, ни к операционной системе. Переименование таких файлов может привести к проблемам в Вашей системе.

Важно

Если ваша система была взломана, есть только один безопасный путь полного отказа от вторжения: переустановка системы.

7.3. Карантин



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.

Изолированные файлы обрабатывает компонент, названный **Карантином**. В этом модуле уже есть функция автоматической отправки зараженных файлов в лаборатории BitDefender.

Как вы могли заметить, раздел **Карантин** содержит список уже изолированных файлов. Для каждого файла есть его имя, размер, дата помещения в карантин и дата отправки на рассмотрение. Если Вы хотите узнать больше информации о файлах в карантине, нажмите **Подробнее**.

Замечание

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

Нажмите **Добавить**, чтобы добавить в карантин файл, который, по Вашему мнению, может быть заражен. Откроется окно, в котором можно выбрать файл, указав его расположение на диске. Таким образом, он будет скопирован в карантин. Если вы хотите переместить файл в карантин, необходимо поставить галочку в опции **Удалить исходный файл**. Более быстрый метод добавить подозрительные файлы в карантин - это просто перетащить их в список карантина.

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

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

Важно

Перед отправкой файлов уточните некоторую информацию. Для этого нажмите **Настройки** и заполните необходимые поля раздела.

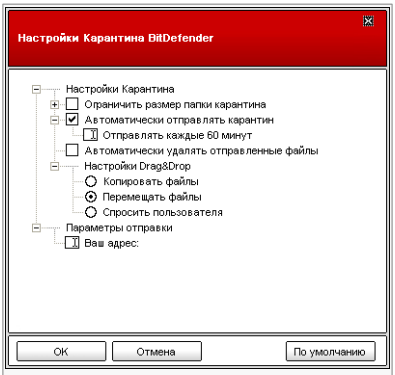
Нажмите **Настройки**, чтобы открыть подробные настройки зоны карантина. Появится новое окно.

Настройки карантина сгруппированы в две категории:

- **Настройки карантина**
- **Настройки электронной почты**

Замечание

Щелчок мышки на значке "+" разворачивает список, а на значке "-" – закрывает его.



Настройки карантина

Настройки карантина

- **Ограничение размера папки Карантин** - задает размер папки карантина. По умолчанию размер составляет 12000 kB. Если вы хотите изменить значение, то введите его в соответсвующем поле.

  Если Вы выбрали флажок **Автоматически удалять старые файлы**, то если карантин переполнен, и требуется добавить новые файлы, то старые файлы в карантине автоматически удаляются, освобождая пространство.

Замечание

По умолчанию, папка карантина не имеет ограничений по размеру.

- **Автоматически отсылать карантин** - автоматически отсылать файлы в карантине в лаборатории BitDefender для дальнейшего анализа. Можно установить период времени, между двумя последовательными сеансами связи в минутах в поле **Отсылать каждые x минут**.
- **Автоматически удалять отправленные файлы** - автоматически удаляет файлы после их отправки в лаборатории BitDefender на анализ.
- **Перетащить файл** - если Вы добавляете файлы в карантин, перетаскивая их, вы можете настроить действия: копировать, переместить или спросить у пользователя.

Настройки электронной почты

- **Ваш адрес** - введите свой адрес электронной почты, если Вы хотите получить ответ от наших экспертов об отправленных подозрительных файлах.

Чтобы сохранить изменения, нажмите **ОК**. Чтобы загрузить настройки по умолчанию, нажмите **По умолчанию**.

8. Модуль защиты от сетевых атак

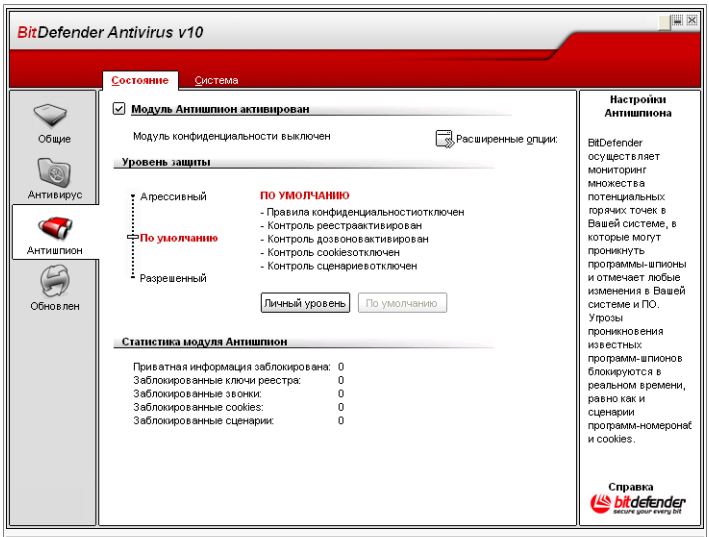
Глава **Антишпион** этого руководства для пользователя содержит следующие темы:

- Статус Антишпиона
- Дополнительные настройки - Контроль конфиденциальности
- Дополнительные настройки - Контроль регистра
- Дополнительные настройки - Контроль дозвона
- Дополнительные настройки - Контроль cookie
- Дополнительные настройки - Контроль скриптов
- Информация о системе

Замечание

Для получения более подробной информации о модуле **Антишпион** прочтите материал, описанный в разделе «*Модуль защиты от сетевых атак*» (p. 30).

8.1. Статус Антишпиона



Статус Антишпиона

В данном разделе можно настроить**Поведенческий антишпион**, а также просмотреть информацию о его работе.

Важно

Чтобы программы-шпионы не попали на Ваш компьютер, **Поведенческий антишпион** должен быть постоянно включен.

В нижней части данного раздела можно просмотреть **Статистику антишпиона**.

Модуль **Антишпион** защищает Ваш компьютер от сетевых атак и программ-шпионов посредствам 5 основных модулей контроля:

- Контроль конфиденциальности - защищает Ваши персональные конфиденциальные данные, проверяя весь исходящий HTTP и SMTP трафик согласно правилам, созданным Вами в разделе Конфиденциальность
- Контроль регистра - спрашивает разрешения всякий раз, когда какая-либо программа будет пытаться менять запись в реестре, для того чтобы загружаться при запуске системы.

- Контроль дозвона - запрашивает разрешение всякий раз, когда программы дозвона обращаются к модему компьютера.
- Контроль cookie - запрашивает разрешение всякий раз, когда новый вебсайт пытается записать cookie.
- Контроль сценариев - запрашивает разрешение всякий раз, когда вебсайт пытается инициировать выполнение сценария или другого активного контента.

Чтобы установить настройки для этих модулей контроля, нажмите Дополнительные настройки.

8.1.1. Уровень защиты

Вы можете выбрать уровень защиты, наиболее удовлетворяющие Ваши потребности в безопасности. Передвиньте бегунок по шкале в соотвествующий уровень защиты.

Существует 3 уровня защиты:

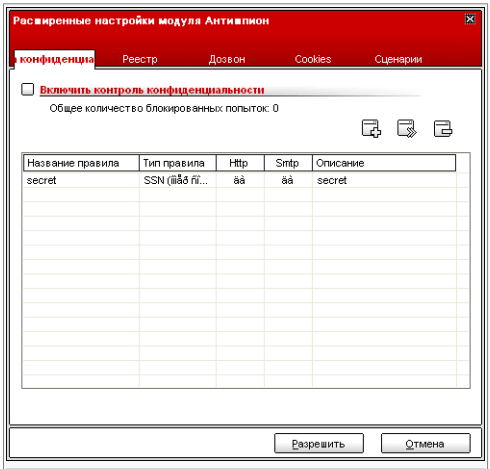
Уровень защиты	Описание
Разрешающий	Включен только **Контроль регистра**
Стандартный	Включены только **Контроль регистра** и **Контроль дозвона**.
Агрессивный	Включены только **Контроль регистра**, **Контроль дозвона** и **Контроль конфиденциальности**.

Вы можете настроить уровень защиты, нажав **Настроить уровень**. В отрывшемся окне выберите настройки Антишпиона, которые Вы хотите включить и нажмите **OK**.

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

8.2. Дополнительные настройки - Контроль конфиденциальности

Чтобы перейти в этот раздел, нажмите кнопку **Дополнительные настройки** в модуле **Antispyware**, раздел Статус section.



Контроль

Сохранение конфиденциальности информации является важной задачей, постоянно не дающей нам покоя. Кражи данных все чаще происходят с развитием интернет технологий, и Интеренет используется для все новых и новых методов обмана людей с целью получения конфиденциальной информации.

Будь то Ваш электронный адрес или номер кредитной карты, если подобная информация попадет не в те руки, то может причинить немалый урон: Ваш ящик будет переполнять спам или Ваш счет может быть опустошен.

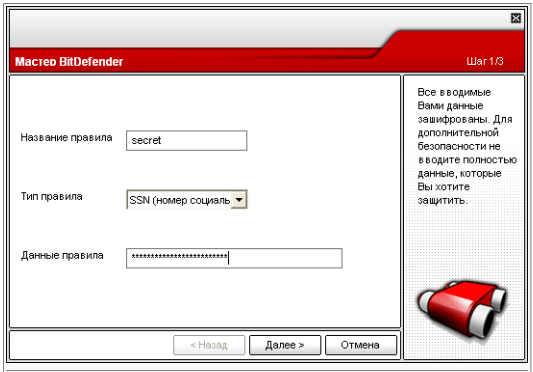
Контроль конфиденциальности позволяет безопасно хранить конфиденциальную информацию. Этот модуль проверяет HTTP или SMTP трафик в поисках указанных Вами строк. Если найдено совпадения, соотвествующая веб-страница или электронное сообщение блокируется.

Правила необходимо вводить вручную (нажмите кнопку **Добавить** и выберите параметры для правила). Появится мастер конфигурации.

8.2.1. Мастер конфигурации

Мастер конфигурации запускает процедуру из трех шагов.

Шаг 1/3 - Установить тип правила и данных



Установить тип правила и данных

Введите название правила в поле для редактирования.

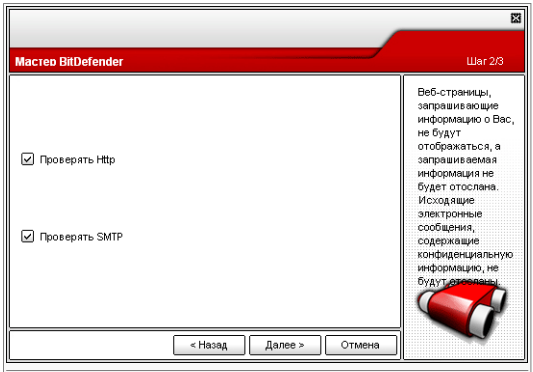
Вы должны установить следующие параметры:

- **Тип правила** - выберите тип правила (адрес, имя, кредитная карта, PIN-код и т.д.).
- **Данные правила** - введите данные правила.

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

Нажмите **Далее**.

Шаг 2/3 - Выбор трафика



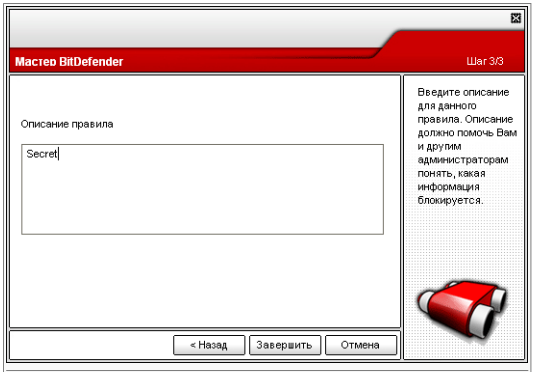
Выберите трафик

Выберите трафик, который будет проверяться BitDefender. Имеются следующие опции:

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

Нажмите **Далее**.

Шаг 3/3 - Описание правила



Опишите правило

Введите краткое описание правила в поле редактирования.

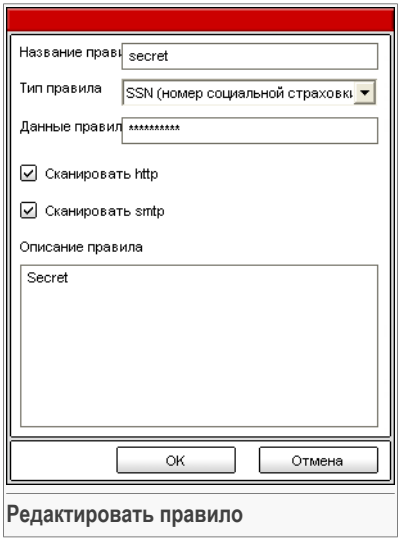
Нажмите **Завершить**.

8.2.2. Управление правилами

В этом окне Вы видите список правил в таблице.

Чтобы удалить правило, достаточно выбрать его и нажать кнопку **Удалить**. Чтобы временно отключить правило без его удаления, уберите галочку в соответствующем поле.

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



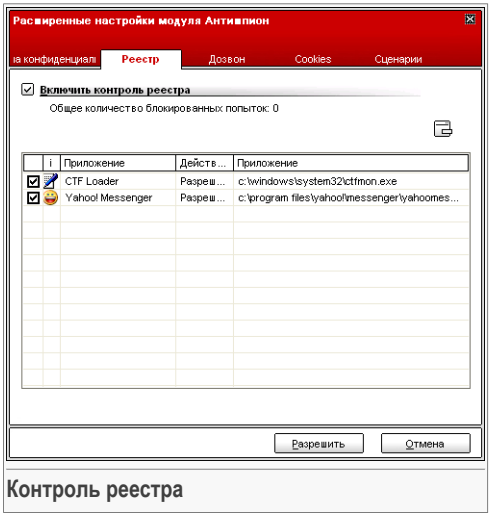
Редактировать правило

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

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

8.3. Дополнительные настройки - Управление реестром

Чтобы перейти в данный раздел, войдите в окно **Дополнительные настройки Антишпиона** (модуль **Антишпион**, раздел Статус , нажмите **Дополнительные настройки**) и нажмите вкладку **Регистр**.



Контроль реестра

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

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

Модуль **Контроль реестра** 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 системного реестра

Вы можете отклонить это изменение, нажав **Нет** или разрешить его, нажав **Да**.

Если Вы хотите, чтобы BitDefender запомнил Ваш ответ, поставьте отметку в поле **Запомнить ответ**.

Замечание

На основе Ваших ответов будет сформирован список правил.

Чтобы удалить запись реестра, просто выберите ее и нажмите кнопку **Удалить**. Чтобы временно отключить запись реестра не удаляя ее, уберите галочку в соотвествующем поле.

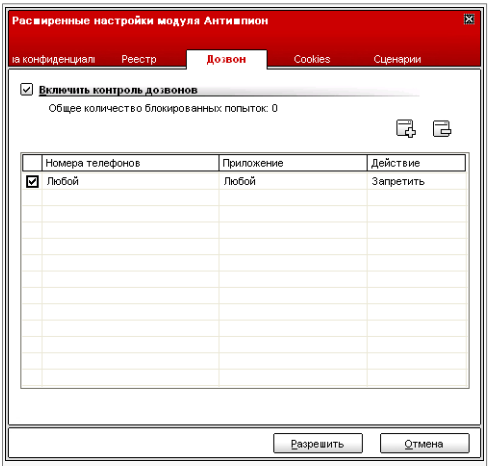
Замечание

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

Нажмите **OK**, чтобы закрыть окно.

8.4. Дополнительные настройки - Контроль дозвона

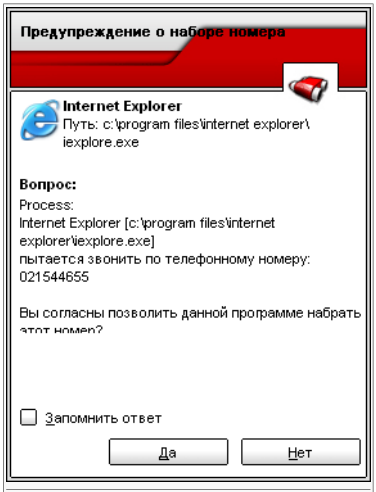
Чтобы попасть в этот раздел, откройте окно **Дополнительные настройки Антишпиона** (модуль **Антишпион**, расздел Статус, нажмите **Дополнительные настройки**) и нажмите вкладку**Дозвон** tab.



Контроль дозвона

Программы-номеронабиратели – это программа, которая с помощью модема набирает телефонные номера. Обычно такие программы используются для набора удаленных номеров и получения доступа к различным ресурсам, что в результате оказывается очень дорогим удовольствием.

Используя функцию **Контроль дозвона** Вы всегда сможете разрешать одни звонки и запрещать другие. Эта функция отслеживает все попытки получить доступ к модему компьютера и немедленно предупреждает об этом пользователя, советуя ему запретить или разрешить это действие:



Предупреждение о наборе

В этом окне Вы видите название программы и номер телефона.

Поставьте галочку в поле **Запомнить этот ответ** и нажмите **Да** или **Нет**. Будет создано новое правило, которое будет занесено в таблицу правил. Когда это же приложение будет набирать этот же номер, Вы уже не получите предупреждения.

Каждое запомненное правило можно найти и вызвать для редактирования в разделе **Дозвон**.

Важно

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

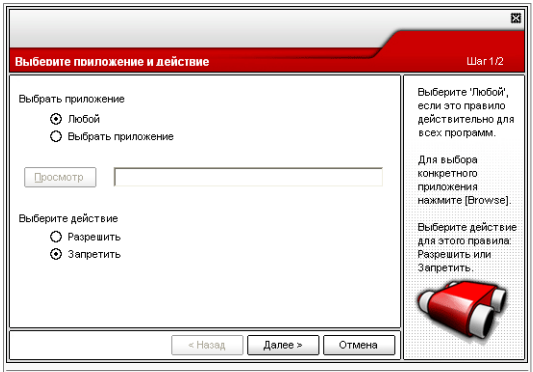
Чтобы удалить правило, достаточно выделить его и нажмите кнопку **Удалить**. Чтобы изменить параметр правила, дважды нажмите поле и внесите соответствующие изменения. Чтобы временно отключить правило без его удаления, уберите галочку в соответствующем поле.

Правила могут добавляться автоматически (через окна предупреждений) или вручную (по нажатию кнопки **Добавить** и выборе параметров для правила). Запустится мастер настройки.

8.4.1. Мастер конфигурации

Мастер настройки выполняет процедуру из 2 шагов.

Шаг 1/2 - Выбор приложения и действия



Выберите приложение и действие

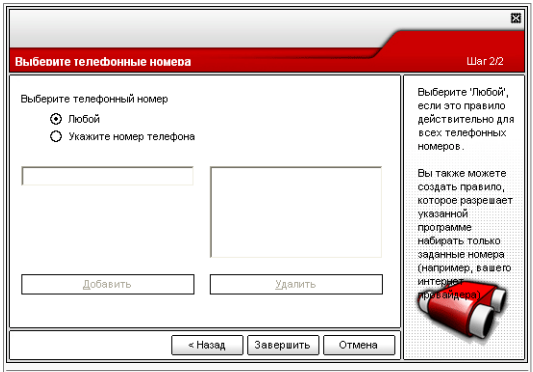
Вы можете установить следующие параметры:

- **Приложение** - выбор приложения, к которому применяется правило. Вы можете выбрать либо только одно приложение (нажмите **Выбрать приложение**, затем нажмите **Обзор** и выберите нужное приложение) или все приложения сразу (просто поставьте галочку в поле **Любое**).
- **Действие** - выбрать действие для правила.

Действие	Описание
Разрешить	Действие будет разрешено.
Запретить	Действие будет запрещено.

Нажмите **Далее**.

Шаг 2/2 - Выбор телефонных номеров



Выберите телефонные номера

Нажмите **Указать телефонные номера**, и введите телефонные номера, к которым будет применяться правило. Нажмите **Добавить**.

Замечание

В списке запрещенных телефонных номеров Вы можете использовать так называемый групповой символ. Например, запись 1900* означает, что запрещены все телефонные номера, начинающиеся на 1900.

Если Вы поставите галочку в поле **Любой** правило будет применяться ко всем телефонным номерам. Если Вы хотите удалить номер, просто выделите его и нажмите **Удалить**.

Замечание

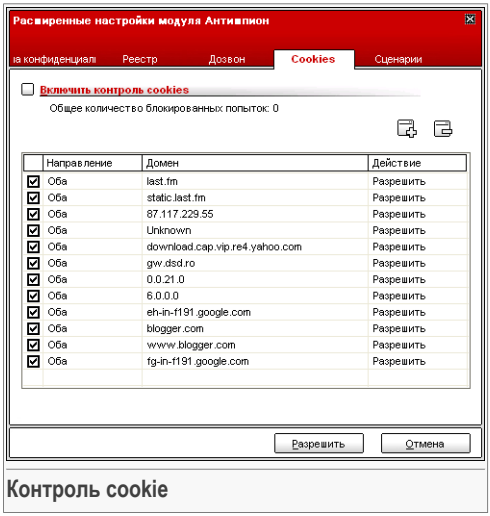
Вы также можете создать правило, разрешающее определенным программам набирать только определенные телефонные номера (например, только номер Вашего Интернет-провайдера или службы новостей по факсу).

Нажмите **Завершить**.

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

8.5. Дополнительные настройки - контроль cookie

Чтобы перейти в данный раздел, откройте окно **Дополнительные настройки Антишпиона** (модуль **Антишпион**, раздел Статус, нажмите **Дополнительные настройки**) и нажмите вкладку**Cookie**.



Контроль cookie

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

Файлы Cookies созданы, чтобы облегчить жизнь пользователя. 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**. Благодаря этой функции, у Вас спрашивается разрешение всякий раз, когда новый сайт пытается создать файл cookie:

Предупреждение о Cookie

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

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

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

Замечание

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

Каждое запомненное правило можно найти и вызвать для редактирования в разделе **Cookie**.

Важно

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

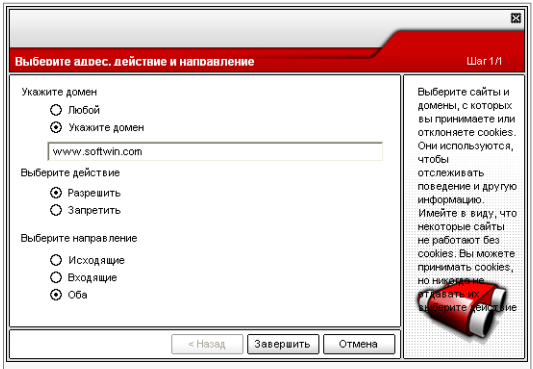
Чтобы удалить правило, достаточно выделить его и нажмите кнопку **Удалить**. Чтобы изменить параметр правила, дважды нажмите поле и внесите соответствующие изменения. Чтобы временно отключить правило без его удаления, уберите галочку в соответствующем поле.

Правила могут добавляться автоматически (через окна предупреждений) или вручную (по нажатию кнопки **Добавить** и выборе параметров для правила). Запустится мастер настройки.

8.5.1. Мастер конфигурации

Мастер конфигурации запускает процедуру из 1 шага.

Шаг 1/1 - Выбор адреса, действия и направления



Выберите адрес, действие и направление.

Вы можете установить следующие параметры:

- **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 файлов истории обращений cookies, которые отсылаются обратно к подключенному сайту.
Входящие	Правило применяется только для файлов истории обращений cookies, которые поступают от подключенного сайта.
Входящие и исходящие	Правило применяется и ко входящему, и к исходящему трафику.

Нажмите **Завершить**.

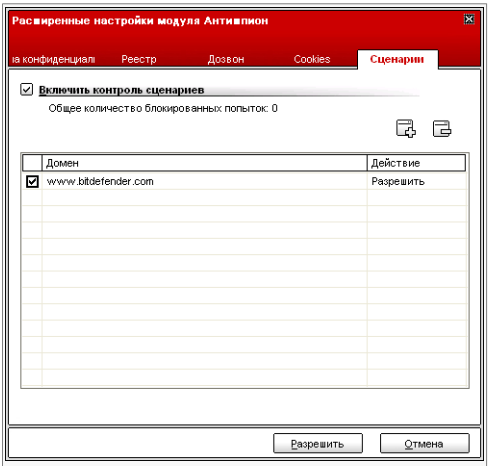
Замечание

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

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

8.6. Дополнительные настройки - Контроль сценариев

Чтобы перейти в этот раздел, откройте окно **Дополнительные свойства Антишпиона** (модуль **Антишпион**, раздел Статус, нажмите **Дополнительные настройки**) и нажмите вкладку **Сценарии**.

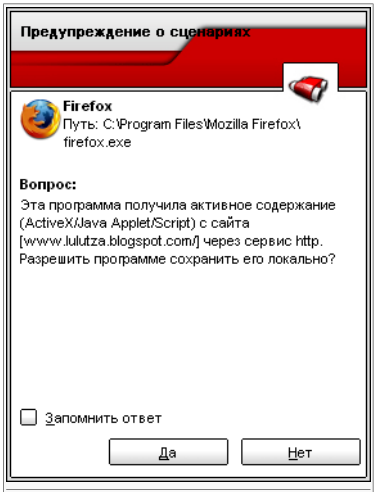


Контроль сценариев

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

В этом окне Вы видите название ресурса.

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

Каждое запомненное правило можно найти и вызвать для редактирования в разделе **Сценарии**.

Важно

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

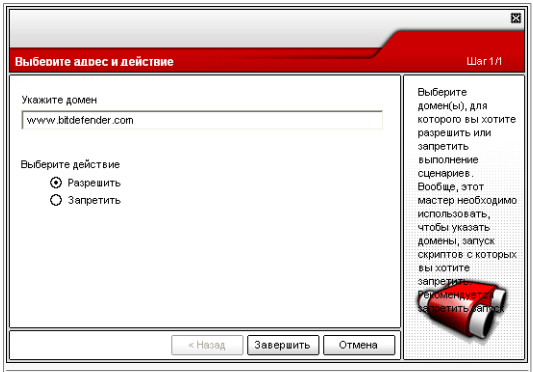
Чтобы удалить правило, достаточно выделить его и нажмите кнопку **Удалить**. Чтобы изменить параметр правила, дважды нажмите поле и внесите соответствующие изменения. Чтобы временно отключить правило без его удаления, уберите галочку в соответствующем поле.

Правила могут добавляться автоматически (через окна предупреждений) или вручную (по нажатию кнопки **Добавить** и выборе параметров для правила). Запустится мастер настройки.

8.6.1. Мастер конфигурации

Мастер конфигурации запускает процедуру из 1 шага.

Шаг 1/1 - Выбор адреса и действия



Выберите адрес и действие

Вы можете установить следующие параметры:

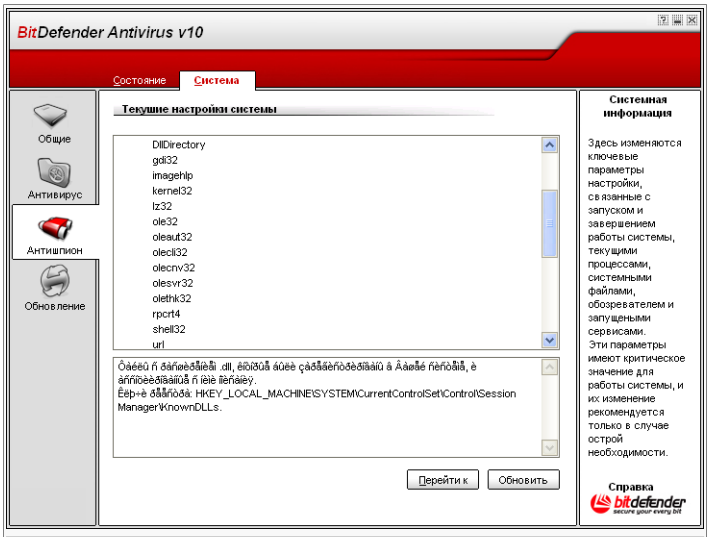
- **Адрес домена** - введите адрес домена, к которому будет применяться правило.
- **Действие** - выбрать действие для правила.

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

Нажмите **Завершить**.

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

8.7. Информация о системе



Информация о системе

Здесь Вы можете увидеть и изменить ключевые настройки блока информации о системе.

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

Доступны три кнопки:

- **Удалить** - удаление выбранного объекта.
- **Перейти** - открывается окно, в которое помещается выбранный объект (например, **Регистр**).
- **Обновить** - обновляется информация в разделе **Информация о системе**.

9. Модуль обновлений

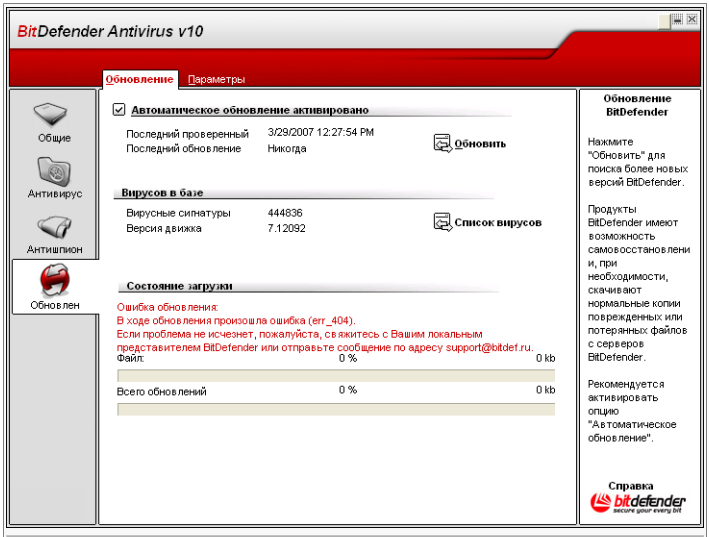
Раздел **Обновление** этого руководства пользователя содержит следующие темы:

- Автоматическое обновление
- Ручное обновление
- Настройки обновления

Замечание

Для получения более подробной информации о модуле **Обновления** прочтите материал, описанный в разделе «*Модуль обновлений*» (p. 30).

9.1. Автоматическое обновление



Автоматическое обновление

В этом разделе Вы можете просмотреть информацию, связанную с обновлениями.

Важно

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

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

Если программа обнаруживает новое обновление, то, в зависимости от настроек, установленных в разделе Опции автоматического обновления Вам будет предложенно подтвердить загрузку обновления или обновление будет производиться автоматически.

Автоматическое обновление может быть также произведено в любое время, по нажатию **Обновить**. Такое обновление также называется **Обновление пользователем**.

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

Важно

Вам может потребоваться перезагрузить компьютер, чтобы завершить обновление. Мы рекомендуем сделать это как можно раньше.

Замечание

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

Вы можете получить доступ к образам вредоносных программ вашего BitDefender, нажав **Показать список вирусов**. Будет создан HTML файл, содержаший все имеющиеся образы. Чтобы просмотреть список, нажмите **Показать список вирусов** еще раз.Вы можете организовать поиск в базе данных конкретного образа вредоносной программы или нажать **Список вирусов BitDefender**, чтобы просмотреть базу данных образов вирусов BitDefender онлайн.

9.2. Обновление вручную.

Этот метод позволяет установить последние обновления образов вирусов. Для установки обновления последней версии продукта Вам следует использовать Автоматическое обновление.

Важно

Используйте обновление вручную в случаях, когда отсутствует возможность выполнить автоматическое обновление или если ваш компьютер не подключен к сети Интернет.

Обновление вручную можно выполнить двумя способами:

- при помощи файла `weekly.exe`;
- при помощи `zip архивов`.

9.2.1. Обновление вручныую с использованием файла `weekly.exe`

Пакет обновления `weekly.exe` выходит каждую пятницу и включает в себя всю обновленную базу образов вирусов и обновления механизмов проверки, существующие на момент выхода обновления.

Чтобы выполнить обновление BitDefender с использованием файла `weekly.exe`, выполните следующие шаги:

1. Скачайте файл weekly.exe и сохраните его на свой жесткий диск.
2. Найдите на жестком диске полученный файл и дважды щелкните мышкой, чтобы запустить мастер обновления.
3. Нажмите **Далее**.
4. Поставьте галочку в поле **Я принимаю условия лицензионного соглашения** и нажмите **Далее**.
5. Нажмите **Установить**.
6. Нажмите **Завершить**.

9.2.2. Обновление вручную при помощи `zip архивов`

На сервере обновлений доступно два zip архива, которые содержат обновления модулей проверки и образов вирусов: `cumulative.zip` и `daily.zip`.

- `cumulative.zip` выходит каждый понедельник и включает в себя всю обновленную базу образов вирусов и обновления модулей проверки, существующие на момент выхода обновления.
- `daily.zip` выходит ежедневно и включает в себя все новые образы вирусов и обновления модулей проверки, появившиеся с момента выхода последнего пакета cumulative.zip до текущей даты.

BitDefender использует архитектуру сервисных служб. В связи с этим, процедура обновления вирусных образов варьируется в зависимости от используемой операционной системы:

- Windows NT-SP6, Windows 2000, Windows XP, Windows Vista.
- Windows 98, Windows Millennium.

Windows NT-SP6, Windows 2000, Windows XP, Windows Vista

Последовательность действий при обновлении:

1. **Скачать нужное обновление.** Если сегодня понедельник, загрузите cumulative.zip и сохраните его где-нибудь на Вашем жестком диске. В другой день загрузите daily.zip и сохраните на Вашем диске. Если Вы обновляете программу вручную впервые, то загрузите оба архива.
2. **Отключите антивирусную защиту BitDefender.**
   - **Выйдите из консоли управления BitDefender.** Нажмите значок BitDefender в системном трее правой кнопкой и выберите **Выход**.
   - **Откройте сервисы.** Нажмите **Начать**, а затем на **Панель управления**, дважды щелкните на **Инструменты администратора** и нажмите **Службы**.
   - **Остановите работу Антивирусного монитора BitDefender.** Выберите из списка службу **Антивирусного монитора BitDefender** и нажмите **Остановить**.
   - **Остановите работу Сканера BitDefender.** Выберите из списка службу **Сканер BitDefender** и нажмите **Остановить**.
3. **Извлеките содержимое архива.** Если у Вас есть оба архива обновления, начните с файла `cumulative.zip`. Извлеките содержимое этого архива в папку `C:\Program Files\Common Files\Softwin\BitDefender Scan Server\Plugins\` и подтвердите запись новых файлов поверх старых.
4. **Возобновите работу антивирусной защиты BitDefender.**
   - **Запустите Сканер BitDefender.** Выберите из списка службу **Сканер BitDefender** и нажмите **Начать**.
   - **Начните работу Антивирусного монитора BitDefender.** Выберите из списка службу **Антивирусного монитора BitDefender** и нажмите **Начать**.
   - **Откройте Консоль управления BitDefender.**

Замечание

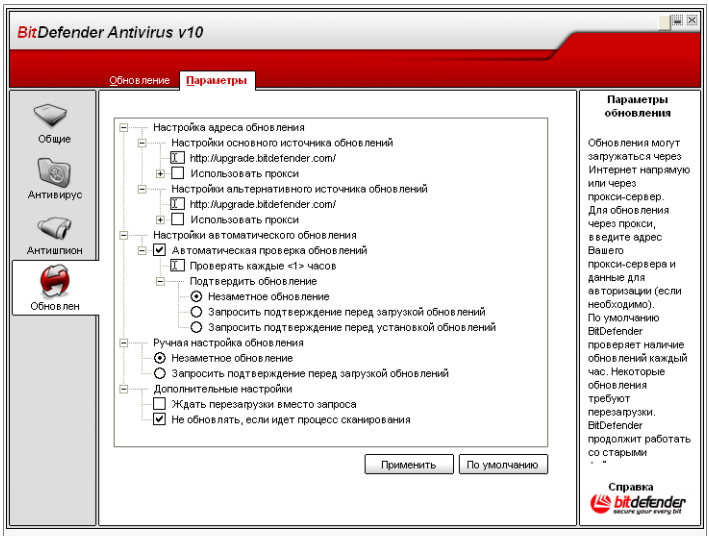
Если у Вас установлена Windows Vista, то Вам потребуется выполнить следующие действия.

Windows 98, Windows Millennium

Последовательность действий при обновлении:

1. **Скачать нужное обновление.** Если сегодня понедельник, загрузите cumulative.zip и сохраните его где-нибудь на Вашем жестком диске. В другой день загрузите daily.zip и сохраните на Вашем диске. Если Вы обновляете программу вручную впервые, то загрузите оба архива.
2. **Извлеките содержимое архива.** Если у Вас есть оба архива обновления, начните с файла `cumulative.zip`. Извлеките содержимое этого архива в папку `C:\Program Files\Common Files\Softwin\BitDefender Scan Server\Plugins\` и подтвердите запись новых файлов поверх старых.
3. **Перезагрузите компьютер.**

9.3. Настройки обновления



Настройки обновления

Обновление может быть выполнено через локальную сеть, через Интернет напрямую или через прокси-сервер.

В окне Настройки обновления Вы можете увидеть четыре типа настроек: (**Настройки местоположения обновления**, **Настройки автоматического обновления**, **Тип обновления вручную** и **Настройки интерфейса**). Разворачиваемое меню настроек похоже на все подобные меню операционной системы Windows.

Замечание

Щелчок мыши на значке "+" открывает категорию, а щелчок мыши на значке "-" закрывает ее.

9.3.1. Настройки местоположения обновления

Для более надежных и быстрых обновлений, Вы можете настроить 2 места обновления:**Основное местоположение обновлений** и **Альтернативное местоположение обновлений**. Для обоих необходимо выполнить следующие настройки:

- **Местоположение обновления** - Если Вы подключены к локальной сети, в которой уже хранится база данных образов вирусов BitDefender, Вы можете изменить местоположение обновления. По умолчанию это: http://upgrade.bitdef.ru.
- **Использование прокси-сервера** - Если в вашей компании используется прокси-сервер, поставьте галочку в поле этой настройки. Выберите следующие настройки:
  - **Настройки прокси-сервера** - введите IP или название прокси-сервера и порт, через который BitDefender подключается к нему.

    Важно

    Синтаксис: `name:port` или `ip:port`.

  - **Пользователь прокси-сервера** - введите имя пользователя, опознаваемого прокси-сервером.

    Важно

    Синтаксис: `domain\user`.

  - **Пароль прокси-сервера** - введите пароль пользователя, указанного ранее.

9.3.2. Опции автоматического обновления

- **Автоматическая проверка обновлений** - Эта функция позволяет BitDefender автоматически проверять наличие обновления на наших серверах.
- **Проверять каждые x часов** - установит, как часто BitDefender должен проверять наличие обновления. По умолчанию этот период составляет 1 час.
- **Обновление без предупреждения** - BitDefender автоматически скачивает и устанавливает обновления.
- **Запрос перед загрузкой** - каждый раз, когда появится новое обновление, BitDefender будет запрашивать ваше подтверждение перед каждой загрузкой.
- **Запрос перед установкой** - каждый раз, когда будет загружено новое обновление, BitDefender будет запрашивать ваше подтверждение перед его установкой.

Важно

Если Вы выберете опцию **Запрос перед загрузкой** или **Запрос перед установкой** а затем закроете консоль управления и сделаете выход из программы, то автоматическое обновление не будет выполняться.

9.3.3. Настройки обновления вручную

- **Обновление без предупреждения** - обновление вручную будет выполняться автоматически в фоновом режиме.
- **Запрос перед загрузкой** - каждый раз, когда Вы будете выполнять обновление вручную, BitDefender будет запрашивать ваше разрешение перед каждой загрузкой и установкой обновления.

Важно

Если Вы выберете опцию **Запрос перед загрузкой**, а затем закроете консоль управления и нажметевыход из программы, то обновление вручную не будет выполняться.

9.3.4. Дополнительные настройки

- **Ожидать перезагрузки без запроса** - Если для завершения установки обновления необходимо выполнить 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, процесс обновления BitDefender не будет мешать задачам проверки.

Замечание

Если BitDefender обновлен, во время сканирования, процесс сканирования будет прерван.

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

Практические приемы

10. Практические приемы

Раздел **Эффективные приемы** данного руководства пользователя содержит следующие темы:

- Как защитить Ваш компьютер от угроз вредоносных программ
- Как настроить задачу проверки

10.1. Как защитить Ваш компьютер от угроз вредоносных программ

Чтобы защитить Ваш компьютер от вирусов, сетевых атак и других вредоносных программ, Вам необходимо выполнить следующие шаги:

1. **Завершите работу мастера первоначальной настройки.** Во время процесса установки будет запущен мастер. Он поможет Вам зарегистрировать BitDefender и создать учетную запись BitDefender, чтобы Вы могли воспользоваться услугами технической поддержки. Он также поможет настроить BitDefender на выполнение важных задач обеспечения безопасности.

   Важно

   Если у Вас есть BitDefender Реаниматор CD, проверьте Вашу систему до установки BitDefender, чтобы убедиться, что в Вашей системе нет вредоносных программ.

2. **Обновите BitDefender.** Если Вы не завершили работу мастера первоначальной установки во время процесса установки, выполните обновление по запросу пользователя (модуль **Обновления**, раздел Обновления, и нажмите **Обновить**).

3. **Выполните полную проверку системы.** Перейдите в модуль **Антивирус**, раздел Монитор и нажмите **Проверить**.

   Замечание

   Вы так же можете запустить полную проверку системы в разделе Проверка. Выберите задачу **Полная проверка системы** и нажмите **Запустить задачу**.

4. **Предотвращение заражения.** В разделе **Монитор**, оставляйте включенной функцию постоянная защита, чтобы обеспечить защиту от вирусов, сетевых

атак и других вредоносных программ. Установите наиболее подходящий для Вас Уровень защиты. Вы можете настроить его, нажав **Настроить Уровень**.

Важно

Настройте Ваш BitDefender Antivirus v10 на проверку Вашей системы хотя бы раз в неделю при помощи планирования задачи **Полной проверки системы** в разделе Проверка

5. **Постоянно обновляйте BitDefender.** В модуле **Обновления**, разделе Обновления, включите **Автоматическое обновление**, чтобы быть защищенных от самых последних версий вредоносных программ.
6. **Запланируйте полную проверку системы.** Перейдите в раздел **Проверка** и запрограммируйте BitDefender проверять Вашу систему хотя бы раз в неделю при помощи планирования задания **Полная проверка системы**

10.2. Как настроить задачу проверки

Выполните следующие шаги, чтобы создать и настроить задачу проверки:

1. **Создайте новое задание.** Перейдите в раздел Проверка и нажмите **Новое задание**. Появится окно Свойства.

Замечание

Новое задание можно создать при помощи дублирования уже существующего задания. Для этого, нажмите правой кнопкой на задании и выберите **Дубликат** из выпадающего меню. Дважды нажмите на дубликате, чтобы открыть окно **Свойства**.

2. **Настройка уровня проверки.** Перейдите в раздел **Общая информация**, чтобы установить уровень проверки. При желании, можно настроить установки проверки, нажав **Настроить**.
3. **Установите объект проверки.** Перейдите в раздел **Путь проверки** то выберите объекты, которые должны быть проверены.
4. **Проверка по расписанию.** Если задача проверки сложная, возможно, Вы захотите запланировать его на позднее время, когда Ваш компьютер будет находиться в режиме ожидания. Это поможет BitDefender тщательно проверить Вашу систему. Перейдите в раздел **Планировщик**, чтобы запланировать задачу.

Реаниматор BitDefender

BitDefender Antivirus v10 поставляется вместе с загрузочным CD (Загрузочный CD BitDefender основывается на LinuxDefender), который может проверить и вылечить все существующие жесткие диски до загрузки операционной системы.

Вы должны использовать компакт-диск BitDefender Реаниматор в любое время, когда операционная система не работает должным образом из-за заражения вирусом. Это обычно случается, когда не используется антивирусная программа.

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

LinuxDefender представляет собой переработанное разработчиками BitDefender программное решение Knoppix, которое объединяет последнюю версию защитного решения BitDefender для Linux с оперативным компакт-диском GNU/Linux Knoppix, предоставляет мгновенную SMTP-защиту против вирусов и спама и делает возможным просматривать и обезвреживать существующие жесткие диски (включая файловые зоны Windows, записанные в системе NTFS), удаленные ресурсы Samba/Windows или точки входа NFS. Также имеется доступный через сеть интерфейс конфигурации для решений BitDefender.

11. Краткий обзор

Ключевые преимущества

- Мгновенная защита электронной почты (против вирусов и спама)
- Антивирусные решения для ваших жестких дисков
- Поддержка записи файловой системы NTFS (с использованием программы Captive project)
- Лечение зараженных файлов в файловых зонах, записаных в системе Windows XP

11.1. Что такое KNOPPIX?

Цитируется по http://knopper.net/knoppix:

« KNOPPIX is a bootable CD with a collection of GNU/Linux (http://www.linux.com/) software, automatic hardware detection, and support for many graphic cards, sound cards, SCSI and USB devices and other peripherals. KNOPPIX can be used as a Linux demo, educational CD, rescue system, or adapted and used as a platform for commercial software product demos. It is not necessary to install anything on a hard disk. »

11.2. Системные требования

Перед загрузкой LinuxDefender, 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

Минимальное допустимое значение - 64 МБ, рекомендуемое - 128 МБ для обеспечения лучших характеристик работы.

CD-ROM

LinuxDefender 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 LinuxDefender 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 защиты подключение к сети Интернет является ОБЯЗАТЕЛЬНЫМ.

Графическая разрешающая способность

Рекомендуется минимальная разрешающая способность 800x600 для удаленного администрирования на базе веб-сайта.

11.3. Включенное программное обеспечение

В компакт-диск BitDefender Реаниматор входят следующие пакеты программ.

- BitDefender SMTP прокси-сервер (Антивирус и Антиспам)
- Удаленный администратор BitDefender (интерфейс на основе веб-приложений)
- Программа BitDefender Linux (антивирусный сканер) + GTK Интерфейс
- Документация BitDefender (в форматах PDF и HTML)
- Дополнительные материалы BitDefender (иллюстративный материал, рекламные листки)
- Ядро Linux-Kernel 2.6
- Программа Captive project для записей в файловой системы NTFS
- Файловая система LUFS - Linux Userland
- Инструментальные средства для восстановления данных и исправления системы даже для других операционных систем
- Инструментальные средства для анализа сети и защиты для сетевых администраторов
- Решение для создания резервных копий Amanda backup
- thttpd
- Анализатор сетевого трафика IPTraf LAN IP монитор
- Контролер сетевой защиты Nessus
- Программное решение Parted, QTParted and partimage для работы с дисковыми секторами, обеспечивающее изменение размеров, сохранение и восстановление разбивки секторов дисков
- Программа Adobe Acrobat Reader
- Веб-браузер Mozilla Firefox

11.4. Антивирусный сканер BitDefender Linux

На компакт-диске LinuxDefender имеется SMTP прокси-сервер BitDefender, Антивирус и Антиспам для Linux, удаленный администратор BitDefender

(интерфейс на основе веб-приложений для настройки Bitdefender SMTP прокси-сервера) и BitDefender Linux Антивирусный сканер для проверки файлов по требованию.

11.4.1. BitDefender SMTP прокси-сервер

BitDefender для почтовых серверов Linux - SMTP прокси-сервер представляет собой безопасное решение для проверки контента, которое обеспечивает защиту от вирусов и спама на межсетевом уровне путем проверки всего почтового трафика на наличие известных и неизвестных хакерских программ и вредоносных кодов. Благодаря своей уникальной технологии, защищенной авторскими правами, BitDefender для почтовых серверов совместим с большинством существующих почтовых платформ и имеет сертификат "RedHat Ready".

Данное решение для защиты от вирусов и спама обеспечивает проверку, обезвреживание и фильтрование трафика электронной почты любого существующего почтового сервера независимо от платформы и операционной системы. BitDefender SMTP прокси-сервер запускается во время загрузки и проверяет весь входящий почтовый трафик. Чтобы конфигурировать BitDefender SMTP прокси-сервер, используйте удаленный администратор BitDefender и инструкции, приведенные ниже.

11.4.2. Удаленный администратор BitDefender

Вы можете обеспечивать настройку и управление сервисами BitDefender как дистанционно (после настройки сети), так и локально, для чего следует выполнить следующие этапы:

1. Запустите браузер Firefox и загрузите удаленный администратор BitDefender по адресу URL: https://localhost:8139 (или дважды щелкните мышкой на значке BitDefender Remote Admin на рабочем столе)
2. Войдите в систему, используя логин "bd" и пароль "bd"
3. Выберите "SMTP прокси-сервер" в левом меню
4. Выберите настройки для Real SMTP сервера и ожидающего порта
5. Добавьте домены электронной почты для пересылки данных
6. Добавьте сетевые домены для пересылки данных
7. Выберите "Антиспам" в левом меню для настройки действий против спама
8. Выберите "Антивирус" для настройки действий BitDefender против вирусов (что делать, когда вирус найден, где находится карантинная папка)
9. Дополнительно, можно настроить "Почтовые уведомления" и опции ведения журнала регистрации ("Журнал регистрации")

11.4.3. Антивирусный сканер BitDefender Linux

Антивирусный сканер, входящий в программу LinuxDefender, интегрируется непосредственно с раскрывающимся меню рабочего стола Windows. Эта версия имеет GTK + графический интерфейс.

Найдите в Проводнике ваш жесткий диск (или доступные удаленные ресурсы), щелкните правой кнопкой мышки на любом файле или папке и выберите опцию "Проверить с помощью BitDefender". Программа BitDefender Linux проверит выбранные объекты и выдаст отчет о результатах проверки. Более сложные варианты проверки можно найти в документации BitDefender Linux (в папке Документация BitDefender или в соотвествующем руководстве пользователя, а также в программе **/opt/BitDefender/lib/bdc**.

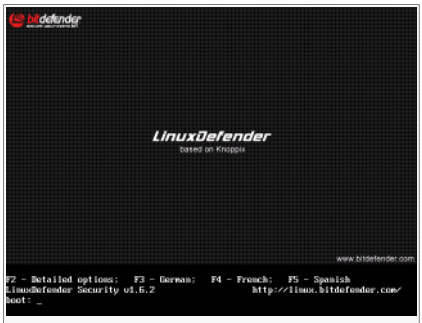
12. Работа с LinuxDefender

12.1. Запуск и остановка

12.1.1. Запуск программы LinuxDefender

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.

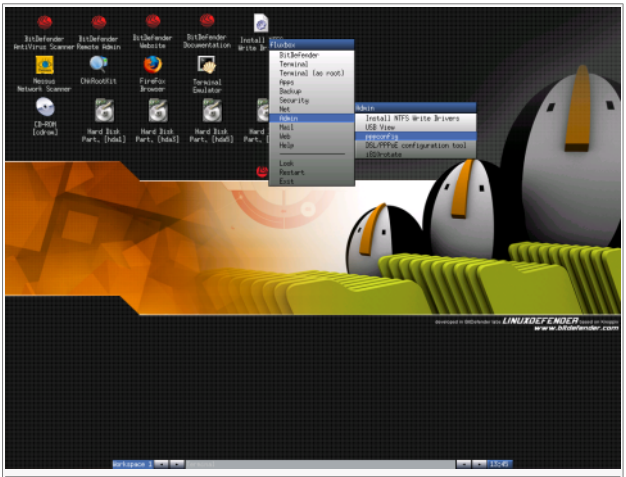
Подождите, пока на экране монитора появится информация и выполняйте соответствующие инструкции для запуска программы LinuxDefender.



Экран заставка загрузки

Путем нажатия на клавиатуре клавиши F2 выберите подробное описание опций. При нажатии F3 язык описания будет немецкий, при нажатии F4 –французский, при нажатии F5 – испанский. Быстрый запуск программы с опциями, заданными по умолчанию, можно осуществить простым нажатием клавиши ENTER.

После окончания загрузки на экране появится новый интерфейс - рабочий стол. Теперь Можно начинать работу с программой LinuxDefender.



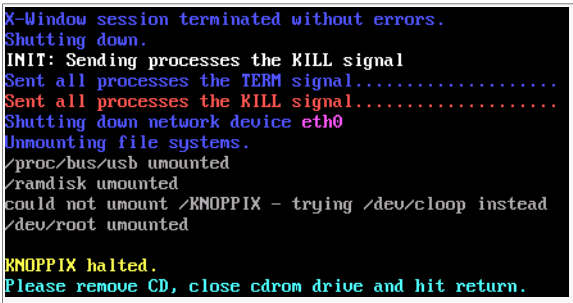
Рабочий стол

12.1.2. Завершение работы LinuxDefender

Для безопасного завершения программы LinuxDefender рекомендуется сначала отключить все жесткие диски, используя команду **umount** или щелкнув правой кнопкой мыши на иконку Разделы жесткого диска на рабочем столе и выбрав опцию **Unmount**. После этого можно выполнить безопасное отключение компьютера, для чего следует либо выбрать команду **Exit** в меню программы LinuxDefender (открывающееся после щелчка правой кнопкой мыши), либо использовать команду **halt** в терминале.

Выберите команду "EXIT"

После того, как LinuxDefender благополучно закроет все программы, на экране появится новое изображение, соответствующее показанному на следующем рисунке. Теперь можно извлечь компакт-диск, 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

12.2. Настройка Интернет соединения

Если Вы находитесь в сети DHCP, 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. Откройте меню LinuxDefender (щелкните правой кнопкой мыши) и выберите **Terminal**, чтобы открыть консоль.
2. Введите команду **netcardconfig** в открытом терминале для запуска программы сетевой настройки.
3. Если ваша сеть использует DHCP, выберите **yes** (если Вы не уверены, уточните это у своего сетевого администратора). В противном случае - см. ниже.
4. Теперь настройка сети должна произойти автоматически. Для того, чтобы узнать свой IP адрес, а также параметры настройки сетевой платы, воспользуйтесь командой **ifconfig**.
5. Если Вы используете статический IP-адрес (т.е., не используете протокол DHCP), то Вам следует выбрать **No** в ответ на вопрос о DHCP-протоколе.
6. Выполняйте появляющиеся на экране инструкции. Если Вы не уверены в своем ответе, посоветуйтесь с системным или сетевым администратором.

Если вы успешно выполнили все инструкции, можете проверить подключение к сети Интернет путем "прозванивания" сайта bitdef.ru, используя команду ping `bitdef.ru`.

```
$ ping -c 3 bitdefender.com
```

Если Вы используете модемную связь dial-up, выберите **pppconfig** в меню LinuxDefender/Admin. На экране появится инструкция по настройке PPP соединения с сетью Интернет.

12.3. Обновление BitDefender

Пакеты BitDefender для LinuxDefender используют системные диски ramdisk для обновляемых файлов. Это позволяет обновлять образы вирусов, механизмы антивирусной проверки и базы данных защиты от спама даже в том случае, когда ваша система запускается с носителя, предназначенного только для считывания, каким является компакт-диск LinuxDefender.

Удостоверьтесь в том, что подключение к сети Интернет функционирует. Сначала откройте опцию BitDefender Remote Admin и выберите **Live! Update** в левой части меню. Затем нажмите на кнопку **Update Now** чтобы проверить наличие новых обновлений.

В качестве альтернативного варианта, Вы можете ввести в терминал следующую команду.

```
# /opt/BitDefender/bin/bd update
```

Все процессы обновления регистрируются по умолчанию в файле журнала BitDefender. Вы можете просмотреть его с помощью следующей команды.

```
# tail -f /ramdisk/BitDefender/var/log/bd.log
```

Если Вы используете прокси-сервер для исходящих соединений, настройте параметры прокси-сервера в меню обновления **Live! Update** используя закладку **Configuration**.

12.4. Проверка на вирусы

12.4.1. Как получить доступ к своим данным, записанным в Windows?

Поддержка записи файловой системы NTFS

Поддержка записи файловой системы NTFS обеспечивается за счет использования программы Captive NTFS write project. Вам потребуются два файла драйвера вашей инсталляции Windows: `ntoskrnl.exe` и `ntfs.sys`. На сегодняшний день поставляются драйвера только для операционной системы Windows XP. Имейте в виду, что Вы можете использовать их также для доступа в разделы Windows 2000/NT/2003.

Установка NTFS драйверов

Чтобы получить доступ к разделам жесткого диска, записанным с помощью файловой системы NTFS Windows, и иметь возможность записать данные в этих разделах, Вы прежде всего должны установить драйверы файловой системы NTFS. В случаях, если ваша операционная система Windows использует файловую систему FAT вместо NTFS, или Вы нуждаетесь в доступе к вашим данным только для чтения, - Вы можете сразу присоединить диски и получить доступ к разделам жесткого диска Windows, так же как к любому диск системы Linux.

Чтобы обеспечить поддержку разделов файловой системы NTFS, Вы должны прежде всего установить драйверы файловой системы NTFS, которые можно найти на ваших жестких дисках, удаленных ресурсах, USB-носителях данных или в обновлениях Windows. Рекомендуется использовать драйверы, полученные из проверенных источников, поскольку локальные драйверы на хосте Windows могут быть оказаться зараженными вирусами или поврежденными.

Двойным щелчком на иконке, соответствующей закладке **Install NTFS Write Drivers** чтобы запустить инсталляционную программу **BitDefender Captive NTFS Installer**. Выберите первую опцию, если Вы хотите установить драйверы с локального жесткого диска.

Если драйверы находятся в другом месте, используйте опцию **Quick search** чтобы найти драйверы.

В качестве альтернативного варианта, Вы можете указать, где находятся ваши драйверы или загрузить драйверы из обновления Windows SP1.

Драйверы не устанавливаются на жестком диске, но временно используются программой LinuxDefender для обращения к разделам файловой системы NTFS Windows. Когда программа установит драйверы файловой системы NTFS, Вы сможете дважды щелкнуть мышкой на иконки файловой системы NTFS и просмотреть содержание этих разделов. В качестве мощного файл-менеджера, Вы можете использовать программу Midnight Commander, выбрав ее в меню LinuxDefender (или введя команду **mc** в консоли управления).

12.4.2. Как выполнить вирусную проверку?

Просмотрите ваши папки, щелкните правой кнопкой мышки на названии файла или каталога и выберите команду **Send to**. Затем выберите **BitDefender Scanner**.

Вместо этого, Вы можете запустить командную сроку с терминала. **BitDefender Antivirus Scanner** начнет проверку выбранного Вами файла или папки с заданным по умолчанию местоположением.

```
# /opt/BitDefender/bin/bdgtk2 /path/to/scan/
```

Затем нажмите **Сканирование**.

Если Вы хотите изменить настройки антивирусной защиты, выберите закладку **Configure Antivirus** в левой части панели программы.

12.5. Настройки фильтра почтовых сообщений

Вы можете использовать LinuxDefender, чтобы получить для каждого конкретного случая надежное решение проблемы фильтра почтовых сообщений, для реализации которого не требуется устанавливать какое-либо программное обеспечение или вносить изменения в настройки почтового сервера. Основная идея состоит в том, что система LinuxDefender встраивается в цепочку передачи данных перед вашим почтовым сервером, за счет чего BitDefender проверяет на спам и вирусы весь SMTP-трафик и лишь после этого передает информацию на реальный почтовый сервер.

12.5.1. Требования к системе

Ваш компьютер должен иметь процессор не ниже уровня Pentium 3, не менее 256 МБ оперативной памяти и диск CD/DVD для загрузки с него системы. Нужно обеспечить схему, по которой SMTP-трафик будет поступать в систему LinuxDefender вместо реального почтового сервера. Есть несколько способов обеспечить эту схему.

1. Измените IP-адрес вашего реального почтового сервера и присвойте старый IP-адрес вашей системе LinuxDefender
2. Измените ваши записи DNS таким образом, чтобы в записи MX для ваших доменов была указана система LinuxDefender
3. Настройте ваши программы почтовых клиентов так, чтобы они использовали новую систему LinuxDefender как SMTP-сервер
4. Измените ваши параметры настройки Брандмауэра так, чтобы направлять/переадресовывать все подключения SMTP на систему LinuxDefender вместо реального почтового сервера

В данном пособии не даются подробные объяснения, как реализовать вышеупомянутые схемы настройки. Для получения дополнительной информации Вы можете обратиться к следующим англоязычным источникам: Linux Networking guides и Netfilter documentation.

12.5.2. Мгновенный почтовый фильтр

Загрузите ваш LinuxDefender компакт-диск и ждите, пока загрузится и начнет фунционировать система X Windows.

Чтобы настроить конфигурацию BitDefender SMTP прокси-сервера, дважды щелкните на иконку **BitDefender Remote Admin** на рабочем столе. При этом откроется следующее окно. Для того, чтобы войти в систему как удаленный администратор, введите логин `bd` и пароль `bd`.

После успешного входа в систему, Вы сможете настроить конфигурацию BitDefender SMTP прокси-сервера.

Выберите **SMTP Proxy** чтобы настроить реальный почтовый сервер, который Вы хотите защитить от спама и вирусов.

Выберите закладку **Email domains** чтобы указать все почтовые домены, для которых Вы хотите обеспечить поступление электронной почты.

Нажмите кнопку **Add Email Domain** или **Add Bulk Domains** и выполняйте инструкции, появляющиеся на экране, чтобы установить домены для передачи электронной почты.

Выберите закладку **Net domains** чтобы указать все сети, через которые Вы хотите передавать электронную почту.

Нажмите кнопку **Add Net Domain** или **Add Bulk Net Domains** и выполняйте инструкции, появляющиеся на экране, чтобы установить сетевые домены для передачи электронной почты.

Выберите **Antivirus** в левой части меню, чтобы выбрать действие при обнаружении вируса и настроить другие антивирусные опции.

Теперь, весь SMTP трафик проверяется и фильтруется программой BitDefender. По умолчанию, все зараженные вирусом сообщения удаляются или перемещаются в карантин, а для всех спам-сообщений, обнаруженных BitDefender, делается пометка `[SPAM]` в разделе «Тема сообщения». Почтовый заголовок (`X-BitDefender-Spam: Yes/No`) добавляется ко всем электронным сообщениям, чтобы упростить ручную фильтрацию почты пользователем.

12.6. Контролер сетевой защиты Nessus

Помимо возможностей обезвреживания вредоносных кодов и программ, восстановления данных и фильтрации почтовых сообщений, которыми обладает программа LinuxDefender, она поставляется вместе с набором инструментальных средств для выполнения тщательной проверки безпасности хостов и сетевых элементов. Также возможным является системный анализ и нахождение проблем безопасности в сетях за счет использования инструментальных средств защиты, входящих в продукт LinuxDefender. Ниже приводится краткое описание запуска ускоренной проверки защиты ваших хостов или сетей.

12.6.1. Поиск руткитов

Прежде чем проверять защиту сетевых компьютерах, сначала убедитесь, что сам компьютер-хост LinuxDefender не заражен и работоспособен. Вы можете проверить на вирусы установленные жесткие диски, как это описано в пособии по проверке на вирусы **Scan for viruses** или Вы можете просканировать систему на наличие корневых руткитов Unix.

Прежде всего, подключите все разделы жесткого диска, дважды щелкнув мышкой на их иконках или используя команду **mount** в консоли. Затем двойным щелчком на иконке **ChkRootKit** проверьте содержимое компакт-диска или запустите командную строку **chkrootkit** в консоли управления, используя в ней `-r NEWROOT` параметр чтобы указать новый/(корневой) каталог хоста.

```
# chkrootkit  -r  /dev/hda3
```

Если система обнаружит корневой rootkit, то в файле chkrootkit он будет указан **ЖИРНЫМ ШРИФТОМ**, и с использованием заглавных букв.

12.6.2. Сетевой сканер Nessus

> Nessus самый популярный в мире сетевой сканер с открытым кодом, используемый более чем 75000 организаций по всему миру. Многие предприятия мирового масштаба достигают значительной экономии расходов при использовании Nessus для проверки критичных для ведения бизнеса устройств и приложений.
>
> *—www.nessus.org*

Программа Nessus может использоваться для удаленного сканирования сетевых компьютеров с точки зрения их уязвимости для различного рода вирусных угрозов. Она также предусматривает определенные меры для снижения риска безопасности и предотвращения случаев несанкционированного проникновения в систему.

Щелкните дважды на иконке **Nessus Security Scanner** на рабочем столе или запустите команду **startnessus** с компьютерного терминала. Подождите, пока не появится следующее окно. В зависимости от используемых компьютерных ресурсов, загрузка Nessus имеющей более чем 5000 плагинов с базами данных образов вирусов, может занимать до 10 минут. Для входа используйте логин `knoppix` и пароль `knoppix`.

Нажмите **Target selection** и введите IP-адрес компьютеров или имена хостов, степень уязвимости которых Вы хотели бы проверить. До начала сканирования удостоверьтесь в том, что вы используете опции программы, соответствующие именно вашему типу сети или системной конфигурации, за счет Вы сможете оптимизировать диапазон широкополосной передачи данных и получить более точный результат проверки. Чтобы начать проверку, нажмите **Start the scan**.

Когда процесс просмотра завершится, программа Nessus отобразит на экране полученные результаты и рекомендации. Вы можете сохранить это сообщение в нескольких форматах, включая HTML. Сохраненный отчет Вы сможете просмотреть с помощью любого используемого Вами браузера.

12.7. Поверка работоспособности RAM системы

Как правило, неожиданные нарушения устойчивости работы вашей системы (зависание системы или ее самопроизвольная перезагрузка) объясняется проблемой оперативной памяти компьютера. Проверить состояние модулей оперативной памяти вы можете, используя программу **memtest** следуя процедуре описанной ниже.

Включите компьютер и загрузитесь с компакт-диска LinuxDefender. В режиме загрузки наберите **memtest** и нажмите Enter.

Программа Memtest немедленно начнет работать, она осуществит ряд тестовых операций для проверки состояния памяти. Нажав c, можно устанавливать конкретные операции и другие опции программы Memtest.

Полный цикл операций Memtest может занимать до 8 часов, в зависимости от объема и скорости оперативной памяти вашей машины. Для окончательной проверки состояния оперативной памяти и исключения любых возможных ошибок рекомендуется провести все контрольные испытания Memtest. Прервать работу программы можно в любое время путем нажатия клавиши ESC.

При покупке нового аппаратного обеспечения (полностью всей системы или отдельных ее компонентов) рекомендуется использовать LinuxDefender и программы memtest для проверки совместимости компонентов и обнаружения возможных ошибок.

Получение справки

13. Тех. поддержка

13.1. Отдел поддержки

Являясь ценимым поставщиком, BitDefender стремится предоставлять своим клиентам беспрецедентный уровень быстрой и полной поддержки. Центр Поддержки (с которым можно связаться по следующему адресу) постоянно проинформирован о самых последних угрозах. Именно здесь вы можете получить быстрый ответ на все Ваши вопросы.

Стремление сохранить время и деньги клиентов, предоставляя им самые последние продукты по самым оптимальным ценам, всегда было высшим приоритетом BitDefender. Более того, мы считаем, что основами успешного бизнеса являются коммуникации и стремление довести до совершенства поддержку клиентов.

Вы можете в любое время обратиться за поддержкой по адресу <support@bitdef.ru>. Чтобы получить оперативный ответ пожалуйста, укажите в Вашем письме как можно больше подробностей о Вашем BitDefender, Вашей системе, опишите проблему, с которой Вы столкнулись как можно подробнее.

13.2. Поддержка в режиме «on-line»

13.2.1. База знаний BitDefender

«База знаний» BitDefender - это хранилище информации о продуктах BitDefender с открытым доступом для клиентов в режиме реального времени. В ней накапливаются, в виде отчетов, имеющих легкодоступный формат, результаты всей деятельности по оказанию технической поддержки и устранению ошибок в программе группами технической поддержки и разработчиками компании, а также имеются статьи более общего характера об обезвреживании вирусов, управлению внедрением решений BitDefender и подробными пояснениями различных проблем, равно как и множество других материалов.

База знаний BitDefender открыта для всех и снабжена поисковыми средствами, позволяющими легко найти ответ на интересующую Вас проблему. Этот ценный массив информации является еще одним источником технических знаний и экспертных решений для клиентов BitDefender. Все обоснованные информационные запросы и отзывы о найденных программных ошибках,

поступившие от клиентов BitDefender своевременно находят свое место в базе знаний BitDefender: в виде отчетов об устранении программных ошибок, обновлениях для максимального устранения недоделок и информационных материалов/статей, дополняющих файлы справки программного продукта.

База знаний BitDefender открыта круглосуточно по адресу http://kb.bitdef.ru.

13.3. Контактная информация

Эффективная связь является залогом успешного бизнеса. За последние 10 лет компании SOFTWIN 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.

13.3.1. Адреса веб-сайтов

Отдел продаж: <sales@bitdef.ru>
Тех. поддержка: <support@bitdef.ru>
Документация: <documentation@bitdef.ru>
Партнерские программы: <partners@bitdef.ru>
Маркетинг: <marketing@bitdef.ru>
Отдел по связям со СМИ: <pr@bitdef.ru>
Вакансии: <jobs@bitdef.ru>
Лаборатория – для вирусов: <virus_submission@bitdef.ru>
Лаборатория - для спама: <spam_submission@bitdef.ru>
Жалобы: <abuse@bitdef.ru>
Веб-сайт продукта: http://www.bitdef.ru
ftp архив продукта: ftp://ftp.bitdef.ru/pub
Локальные дистрибьюторы: http://www.bitdef.ru/partner_list
База знаний BitDefender: http://kb.bitdef.ru

13.3.2. Офисы филиалов

Офисный персонал компании, ответственный за продукт BitDefende, ответит на ваши запросы коммерческого и общего характера, относящейся к сфере их деятельности и географической привязке. Ниже приведены адреса и контактная информация этих офисов.

Германия

Softwin GmbH

Headquarter Western Europe
Karlsdorferstrasse 56
88069 Tettnang
Германия
Телефон: +34 932189615
Факс: +34 932179128
Электронный адрес<info@bitdef.ru>
Отдел продаж: <sales@bitdef.ru>
Веб сайт http://www.bitdef.ru
Тех. поддержка: <support@bitdef.ru>

Великобритания и Ирландия

One Victoria Square
Birmingham
B1 1BD
Телефон: +44 207 153 9959
Факс: +44 845 130 5069
Электронный адрес<info@bitdef.ru>
Отдел продаж: <sales@bitdef.ru>
Веб-сайт: http://www.bitdefender.co.uk
Тех. поддержка: <support@bitdef.ru>

Испания

Constelación Negocial, S.L
C/ Balmes 195, 2ª planta, 08006
Barcelona
Техническая поддержка: <soporte@bitdefender-es.com>
Отдел продаж: <comercial@bitdefender-es.com>
Телефон: +34 932189615
Факс: +34 932179128
Веб-сайт продукта: http://www.bitdefender-es.com

США

BitDefender, LLC
6301 NW 5th Way, Suite 3500
Fort Lauderdale, Florida 33309
Тех. поддержка: <support@bitdef.ru>
Обслуживание клиентов:954-776-6262
Веб сайт http://www.bitdef.ru

Румыния

SOFTWIN
5th Fabrica de Glucoza St.
PO BOX 52-93
Bucharest
Техническая поддержка: <suport@bitdefender.ro>
Отдел продаж: <sales@bitdefender.ro>
Телефон: +40 21 2330780
Факс: +40 21 2330763
Веб-сайт продукта: http://www.bitdefender.ro

Глоссарий

ActiveX

ActiveX – это компоненты, которые могут использоваться другими программами и операционными системами вызывающими их. Технология ActiveX используется вместе с программой Microsoft Internet Explorer для создания интерактивных страниц, которые выглядят и работают скорее как компьютерные программы, нежели как простые страницы. С помощью ActiveX пользователь может задавать и отвечать на вопросы, «нажимать» на кнопки и другим способом взаимодействовать с веб-страницей. Элементы ActiveX часто пишутся на языке Visual Basic.

Главный недостаток технологии ActiveX – полное отсутствие какой-либо защиты. Поэтому эксперты по компьютерной безопасности не одобряют их использование в сети Интернет.

Программы с рекламной информацией (Adware)

Программы Adware часто устанавливаются «в качестве нагрузки» к основным приложениям, которые предоставляются бесплатно, при условии что пользователь соглашается установить программу-adware. Поскольку adware-приложения обычно устанавливаются только после того, как пользователь принимает условия, указанные в соответствующем лицензионном соглашении, где указывается функция приложения, то их функционирование не является каким-либо нарушением прав пользователя.

Однако, всплывающие рекламные объявления могут причинять неудобства пользователю, а в некоторых случаях и ухудшать операционные характеристики системы. Кроме того, пользовательская информация, собираемой некоторыми из этих приложений, может показаться недопустимой для разглашения теми пользователями, которые недостаточно полно изучили условия лицензионного соглашения.

Архив

Диск или директория, содержащие файлы - резервные копии.

Файл, содержащий один или несколько файлов в сжатом формате.

Брешь в системе (Backdoor)

Брешь в защите системы, специально оставленная разработчиками. Это не всегда делается со злым умыслом: например, в некоторых операционных системах предусмотрены учетные записи, которые могут использоваться персоналом службы технической поддержки или программистами разработчика.

Загрузочный сектор

Сектор в начале каждого диска, в котором хранится информация об архитектуре диска: размер сектора, размер папки и т.д. Загрузочный сектор загрузочного диска содержит еще и программу, загружающую операционную систему.

Загрузочный вирус

Вирус, заражающий загрузочный сектор жесткого или гибкого диска. Попытка загрузиться с зараженной дискеты приводит к тому, что вирус активируется в памяти. Всякий раз, когда Вы загружаете систему с этого места, вирус будет активироваться в памяти.

Браузер

Сокращение от Web browser – приложение, которое ищет и показывает на экране Веб-страницы. Два самых популярных браузера - это Netscape Navigator и Microsoft Internet Explorer. Это графические браузеры, то есть, они показывают и рисунки, и текст. Кроме того, большинство современных браузеров могут отображать мультимедийную информацию, включая звук и видеоизображение, хотя они и требуют установки дополнительных программ.

Командная строка

В командной строке пользователь вводит в специальном поле нужные команды на специальном командном языке.

Файлы истории обращений - Cookie

В сфере Интернет технологий под названием «файлы истории обращений (cookies)» понимаются маленькие файлы, содержащие информацию о компьютере, которую можно проанализировать и использовать для того, чтобы выяснить Ваши интересы и предпочтения. Поэтому технология создания таких файлов процветает, и сейчас Вы можете получить рекламу товаров, основанную на Ваших интересах. Это палка о двух концах. С одной стороны, Вы видите именно то, что Вам может пригодиться. Но с другой – за Вами постоянно следят, и знают, на какой странице Вы находитесь, и на какой кнопке щелкаете мышкой. Понятно, почему сейчас так широко обсуждается конфиденциальность данных пользователей, и многие чувствуют себя ущемленными в своих правах, будучи уверенными, что их «считывают» как кассир в магазине считывает штрих-код на этикетке. Порой эта точка зрения кажется крайностью, но иногда она полностью отражает действительность.

Дисковод

Это оборудование, считывающее данные с диска и записывающее их на диск.

Накопитель на жестких дисках считывает данные и записывает их на жесткие диски.

Накопитель на гибких магнитных дисках работает с гибкими дисками - дискетами.

Дисковод может быть встроенным (в корпусе компьютера), или же внешним (в отдельном корпусе и подключаться к компьютеру).

Загрузка

Копирование данных (обычно целых файлов) из основного местоположения на внешнее устройство. Обычно этот термин используется по отношению к копированию файла из источника в сети на свой компьютер. Загрузкой также называют копирование файла с сетевого файлового сервера на компьютер в сети.

Электронная почта

Электронная почта. Отправка сообщений на другие компьютеры через локальную или глобальную сеть.

События

Действие или событие, обнаруженное программой. Событиями могут быть действия пользователя, например щелчок кнопки мыши, или нажатие на клавишу, или системные события, например, переполнение памяти.

Ложная тревога

Событие «ложная тревога» появляется, когда программа считает зараженным файл, который таковым на самом деле не является.

Расширение файла

Часть названия файла после точки, обозначающая тип данных, хранящихся в нем.

Многие операционные системы, такие как Unix, VMS, и MSDOS, используют расширения имени файла. Обычно они состоят из трех букв, потому что старые ОС не поддерживают более длинные расширения. Например, "c" текст программы на языке C (C source code), "ps" – язык PostScript, а "txt" – любой текстовый файл.

Эвристический метод

Способ обнаружения новых вирусов, основанный на правилах. Этот способ проверки не связан напрямую с определенными образами вирусов. Преимущество эвристической проверки состоит в том, что новый вирус не может обмануть фильтр. Однако он может принять подозрительный код в обычных программах за вирус и выдать так называемую «ложную тревогу».

IP

Сокращение от Internet Protocol – Интернет Протокол – маршрутизируемый протокол семейства TCP/IP, отвечающий за адресацию, маршрутизацию, фрагментацию и повторную компоновку IP пакетов.

Прикладная минипрограмма Java апплет

Программа, написанная на языке Java, работающая только на страницах в сети. Чтобы использовать апплет на странице, Вы должны указать его название и размер (длину и ширину в пикселях), которые он может использовать. При открывании страницы браузер загружает эту программу с сервера и запускает ее на компьютере пользователя (который в этом случае называется «клиент»). Апплеты отличаются от приложений, которыми они управляются, более строгим протоколом обеспечения безопасности.

Например, даже если минипрограмма запускается на компьютере-клиенте, она не может считывать или записывать данные на этот компьютер. Кроме того, апплеты могут считывать и записывать данные только с того домена, которым они обслуживаются.

Макро-вирус

Компьютерный вирус, который кодируется как встроенный в документ макрос. Многие приложения, такие как Microsoft Word и Excel поддерживают сложные макроязыки.

Эти приложения позволяют встраивать макросы в документ, и эти макросы выполняются всякий раз, когда Вы открываете документ.

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 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-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 (Phishing)

Действие, сводящееся к отправке пользователю электронного письма якобы от имени реально существующей организации с целью получения обманным путем конфиденциальной информации о пользователе и ее последующего присвоения в корыстных целях. В получаемом пользователем сообщении по электронной почте его с помощью ссылки приглашают посетить якобы официальный веб-сайт реально существующей организации, где его просят подтвердить или обновить личные данные. Например, пароли и номера банковского счета, кредитной карточки, карточки социального обеспечения. Однако на самом деле такого рода веб-сайт является поддельным и создается для кражи конфиденциальной информации пользователей.

Полиморфный вирус

Вирус, изменяющий свою форму всякий раз, заражая новый файл. Поскольку у таких вирусов нет бинарной закономерности, их трудно обнаружить.

Порт

Компьютерный интерфейс, с помощью которого подключается внешнее устройство. У персональных компьютеров есть несколько видов портов. Внутри корпуса есть несколько портов для подключения дисководов, монитора и клавиатуры. Снаружи есть порты для подключения модемов, принтеров, мыши и других внешних устройств.

В сетях на базе протоколов TCP/IP и UDP порт – это конечная точка логического подключения. Номер порта указывает на его тип. Например, порт номер 80 используется для HTTP трафика.

Файл отчета

Файл, содержащий список совершенных действий. BitDefender включает в отчеты путь к проверенным файлам, папки, количество проверенных архивов

и файлов, а также сколько подозрительных и зараженных файлов обнаружено.

Руткит

Руткиты - это набор программных инструментов, позволяющих получить доступ к системе на уровне администратора. Термин впервые использовался для операционных систем UNIX и относился к инструментам перекомпиляции, которые позволяли получить права администратора, при этом их присутствие оставалось скрытым для системных администраторов.

Основной целью руткитов является скрывать процессы, файлы, логины и журналы. Они также могут перехватывать данные с терминалов, сетевых соединений или перифирийных устройств, если их встроить в соотвествующее программное обеспечение.

По своей природе руткиты не вредоносны. Например, системы и даже некоторые приложения скывают важные файлы при помощи руткитов. Однако, чаще всего их все-таки используют как вредоносные порграммы, либо чтобы скрыть присутствие в системе. При совмещении с вредоносными программами, руткиты представляют значительную угрозу для целостности и безопасности системы. Они могут отслеживать трафик, создавать бреши в системе, изменять файлы и журналы, избегая выявления.

Сценарий или скрипт

Еще один термин, обозначающий макрос или командный файл. Сценарий – это набор команд, выполняющихся без участия пользователя.

Spam

Рекламное сообщение или новостная рассылка по электронной почте. Обычно под спамом понимают незаконную рассылку электронных писем, часто коммерческого содержания.

Программа-шпион - Spyware

Любого рода программа-шпион, которая тайно и без ведома пользователя - чаще всего в рекламных целях - собирает информацию о пользователе во время его с соединения с Интернетом. Шпионские программы обычно маскируют как скрытые компоненты бесплатных или условно бесплатных (shareware) приложений, которые можно скачать с Интернета, хотя следует отметить, что большинство бесплатных или условно бесплатных приложений не содержит программ-шпионов. Программа-шпион после своей установки отслеживает адреса в Интернете, к которым обращается пользователь и тайно пересылает эту информацию третьим лицам. Кроме того, программы-шпионы могут собирать информацию об адресах электронной почты, паролях и даже номерах кредитных карточек пользователей.

Программы-шпионы аналогичны вирусам-троянам в том смысле, что и те и другие устанавливаются самими пользователями во время установки других программ. Жертвами программ-шпионом обычно становятся при скачивании известных программных продуктов из файлообменных сетей.

Действия программ-шпионы являются не только нарушением этики и конфиденциальности, но и кражей ресурсов компьютерной памяти пользователей и ресурсов канала соединения с Интернетом за счет передачи информации программой-шпионом своему источнику при подключении пользователя к Интернету. За счет потребления памяти и системных ресурсов программами-шпионами, работа последних в фоновом режиме может приводить к неустойчивой работы системы и ее сбоям.

Элементы запуска

Все файлы, помещенные в эту папку будут открываться при запуске компьютера. Это могут быть, например, экран запуска, звуковой файл, проигрываемый при первом запуске компьютера, ежедневник с напоминаниями или другие приложения. Обычно в эту папку помещается не сам файл, а его ярлык.

Системный трей

Системный трей или область уведомлений впервые появился в операционной системе Windows 95. Он расположена на панели задач Windows, обычно в нижней части экрана, рядом с часами и содержит маленькие иконки, обеспечивающие быстрый доступ к таким функциям, как факс, принтер, модем, регулировка громкости и т.д. Чтобы просмотреть подробную информацию о программе и ее настройки, просто дважды щелкните мышкой на иконке.

TCP/IP

Протокол управления передачей/Интернет протокол (Transmission Control Protocol/Internet Protocol) – набор сетевых протоколов, широко используемых в Интернете. Они объединяют в одну большую сеть множество взаимосвязанных сетей, состоящих из компьютеров с различной архитектурой и с различными операционными системами. Протокол TCP/IP включает в себя стандарты связи между компьютерами и общепринятые правила объединения сетей и трафик маршрутизации.

Вирус класса Троян

Вредоносная программа, маскирующаяся под безвредное приложение. В отличие от обычных вирусов, вирус класса Троян не копирует себя, однако, он может быть не менее разрушительным. Вирусы одного из наиболее опасных типов обещают избавить Ваш компьютер от всех вирусов, но на самом деле загружают вирусы на компьютер.

Этот термин взят из поэмы Гомера «Илиада», где в одной из глав описывается, как греки подарили своим врагам, жителям Трои, огромного деревянного коня, якобы в знак мира. Но после того, как троянцы втащили статую в город, греческие солдаты выскочили из полости в теле коня и открыли городские врата, после чего их соратники ворвались в Трою и захватили город.

Обновление

Новая версия программного обеспечения или оборудования, разработанная на замену устаревшей версии этого продукта. Кроме того, многие обновления часто определяют, установлена ли на компьютере старая версия данного программного продукта. Если нет – обновление невозможно.

У программы BitDefender есть свой собственный модуль обновления, который позволяет вручную проверять наличие или автоматически обновлять программный продукт.

Вирус

Программа или часть кода, которая загружается на Ваш компьютер без Вашего ведома и запускается против Вашего желания. Многие вирусы также могут копировать себя. Все компьютерные вирусы созданы людьми. Очень легко написать простой вирус, который копирует себя снова и снова. Даже такой простой вирус очень опасен, так как он быстро использует всю свободную память и система зависает. Более опасные вирусы могут передавать себя по сети и прорываться через системы защиты.

Образ вируса

Двоичный образец вируса, используемый программой защиты от вирусов для обнаружения и уничтожения этого вируса.

Вирус класса червь

Программа, которая распространяется по сети, копируя и отправляя себя дальше. Она не может присоединяться к другим программам.