bitdefender

INTERNET SECURITY 2008

Руководство пользователя

BitDefender Internet Security 2008

Руководство пользователя

Опубликовано 2008.04.02

Правовые положения


bitdefender

Содержание

Лицензии и гарантии

ЕСЛИ ВЫ НЕ СОГЛАСНЫ С УСЛОВИЯМИ ДАННОГО СОГЛАШЕНИЯ, НЕ УСТАНАВЛИВАЙТЕ ДАННОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ВЫБИРАЯ "ПРИНЯТЬ УСЛОВИЯ","ОК","ДАЛЕЕ","ДА", УСТАНАВЛИВАЯ ИЛИ ИСПОЛЬЗУЯ ЛЮБЫМ ДРУГИМ ОБРАЗОМ 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, и включают, документацию и обновления любых приложений, приобретенных согласно лицензии, либо любое другое сервисное соглашение, определенное в документации, или их копии.

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

Если Вы не согласны с условиями данного соглашения, не устанавливайте и не используйте программное обеспечение 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 BITDEFENDER предоставляет Вам и только Вам следующую неисключительную, ограниченную, без права передачи, лицензию на использование программного продукта BitDefender.

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

ЛИЦЕНЗИЯ ПЕРСОНАЛЬНОГО ПОЛЬЗОВАТЕЛЯ. Данная лицензия относится к программному обеспечению BitDefender, которое может быть установлено на персональном компьютере и которое не имеет серверных функций. Каждый пользователь может установить данный программный продукт на персональном

компьютере, а также может сделать дополнительную резервную копию на другом устройстве.

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

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

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

АВТОРСКИЕ ПРАВА. Все права, в том числе и авторское право, на программный продукт BitDefender (включая, но не ограничивая: изображения, фотографии, логотипы, анимированные изображения, видео, звук, тексты и прикладные мини программы, входящие в программный продукт BitDefender), сопутствующие печатные материалы и любые копии программного продукта BitDefender являются собственностью компании BITDEFENDER. BitDefender защищен законом об авторском праве и международными соглашениями. Поэтому Вы должны обращаться с ним как и с любым другим лицензионным продуктом. Вы не имеете права копировать сопутствующие печатные материалы. На всех копиях должна стоять пометка об авторских правах, независимо от того, на каком носителе или в какой форме существует продукт BitDefender. Вы не имеете права выдавать сублицензии, сдавать в аренду или продавать BitDefender. Вы не имеете права восстанавливать алгоритм работы, вносить изменения, раскодировать, создавать свои продукты на основе BitDefender, изменять, переводить или предпринимать какие-либо попытки дешифровать исходный код программного продукта BitDefender.

ОГРАНИЧЕННАЯ ГАРАНТИЯ. Компания BITDEFENDER дает тридцатидневную гарантию со дня покупки на то, что все носители, на которых распространяется

программный продукт BitDefender, не имеют дефектов. При нарушении гарантии компания BITDEFENDER может заменить поврежденный экземпляр. Компания BITDEFENDER не гарантирует, что программный продукт BitDefender будет работать без ошибок или сбоев, или что ошибки будут исправлены. Компания BITDEFENDER не гарантирует, что программный продукт BitDefender будет отвечать всем Вашим требованиям.

КРОМЕ ОГОВОРЕННЫХ В ДАННОМ СОГЛАШЕНИИ, BITDEFENDER ОТКАЗЫВАЕТСЯ ОТ ПРЕДОСТАВЛЕНИЯ ЛЮБЫХ ГАРАНТИЙ В ОТНОШЕНИИ ПРОГРАММНОГО ПРОДУКТА, УСОВЕРШЕНСТВОВАНИЙ, ПОДДЕРЖКИ И ДРУГИХ ОТНОСЯЩИХСЯ МАТЕРИАЛОВ ИЛИ УСЛУГ. НАСТОЯЩИМ СОГЛАШЕНИЕМ BITDEFENDER ОТКАЗЫВАЕТСЯ ОТ ГАРАНТИЙ, ВКЛЮЧАЯ БЕЗ ОГРАНИЧЕНИЯ ЛЮБЫЕ ПОДРАЗУМЕВАЕМЫЕ ГАРАНТИИ КАЧЕСТВА И ПРИГОДНОСТИ ПРОГРАММЫ ДЛЯ ИСПОЛЬЗОВАНИЯ ПО НАЗНАЧЕНИЮ ИЛИ ДЛЯ КАКОЙ-ЛИБО ДРУГОЙ ЦЕЛИ. НАСТОЯЩИМ СОГЛАШЕНИЕМ BITDEFENDER ОТКАЗЫВАЕТСЯ ОТ ГАРАНТИЙ ЗА ТОЧНОСТЬ ДАННЫХ И 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 ПРОЧЕГО.

ОТКАЗ ОТ ОТВЕТСТВЕННОСТИ ЗА ПОВРЕЖДЕНИЯ. Любое лицо, использующее, тестирующее или оценивающее программный продукт BitDefender несет все риски, касающиеся качества его работы. Компания BITDEFENDER не несет никакой ответственности за любой ущерб, включая и не ограничиваясь прямым и непрямым ущербом, возникшим в результате неправильного использования, работы или доставки BitDefender, даже если компания BITDEFENDER 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 BITDEFENDER НЕ ДОЛЖНА ПРЕВЫШАТЬ СУММЫ, УПЛАЧЕННОЙ ЗА ПРОГРАММНЫЙ ПРОДУКТ BITDEFENDER. Перечисленные отказы и ограничения действуют независимо от того, принимаете ли Вы их, а также действуют в том случае, если 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 ВООРУЖЕНИЯ, В СИСТЕМАХ ПРЯМОГО ИЛИ НЕПРЯМОГО ЖИЗНЕОБЕСПЕЧЕНИЯ, В УПРАВЛЕНИИ ПОЛЕТАМИ ИЛИ В ЛЮБЫХ ДРУГИХ ВИДАХ ДЕЯТЕЛЬНОСТИ, ГДЕ ОШИБКА МОЖЕТ ПОВЛЕЧЬ ЗА СОБОЙ СМЕРТЬ, СЕРЬЕЗНЫЕ ПОВРЕЖДЕНИЯ ИЛИ БОЛЬШОЙ УЩЕРБ.

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

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

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

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

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

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

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

Адрес российского Издательства BitDefender: 125284, Москва, ул.Беговая, д.13. Телефон: +7 (495) 935-8276 info@bitdef.ru www.bitdef.ru Компания-изготовитель: BitDefender. Юридический адрес компании-изготовителя: 5, Fabrica de Glucoza street, 72322-Sector2, Bucharest, RomaniaТелефон: 40-21-2330780, Факс:40-21-2330763,элетронная почта: office@bitdefender.com. www.bitdefender.com

Предисловие

Данное пособие предназначено для всех пользователей, которые предпочли **BitDefender Internet Security 2008** в качестве решения обеспечения безопасности для персонального компьютера. Информация, представленная в данном пособии, предназначена не только для опытных пользователей, но и для всех, кто может работать с операционной системой Windows.

Данное пособие расскажет Вам о **BitDefender Internet Security 2008**, Компании и команде, создавшей его, а так же поможет провести процесс установки, обучит методам настройки. Вы узнаете, как пользоваться **BitDefender Internet Security 2008**, обновлять, тестировать и настраивать его. Вы узнаете, как получить максимум пользы от BitDefender.

Мы желаем Вам приятного и полезного чтения.

1. Соглашения, используемые в данной книге

1.1. Типографские обозначения

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

Виды шрифтов и стилей	Описание
`sample syntax`	Образцы написания напечатаны `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. xii)	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 внимание к дополнительной информации, имеющей отношение к содержанию текущего раздела руководства.

Замечание

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

Важно

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

Внимание

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

2. Структура книги

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

Установка. Пошаговые инструкции по установке BitDefender на рабочей машине. Это развернутое пособие по установке **BitDefender Internet Security 2008**. Начиная с необходимых требований для успешной установки, Вам помогут пройти процесс инсталляции продукта. Наконец, описана процедура удаления, в случае, если Вам понадобилось удалить BitDefender.

Основны администрирования. Описание основных процедур администрирования и обслуживания BitDefender.

Детальное описание администрирования. Детальное описание всех возможностей обеспечения безопасности при помощи продукта BitDefender. Данная глава подробно объясняет все опции, доступные в консоли настройки. Вас научат настраивать и пользоваться всеми модулями BitDefender для эффективной защиты Вашего компьютера от всевозможных угроз (вредоносных программ, спама, атак хакеров, неадекватного содержимого и т.д.).

BitDefender Rescue CD. 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 рады Вашим замечаниям по улучшению данного руководства. 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 русском языке, чтобы мы могли оперативно их обработать.

Установка

1. Установка BitDefender Internet Security 2008

Глава **Установка BitDefender Internet Security 2008** этого руководства для пользователя содержит следующие темы:

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

1.1. Системные требования

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

- Windows 2000 SP4 / XP SP2 32b & 64b / Vista 32b & 64b; Internet Explorer 6.0 (или выше)
- Поддерживаемые почтовые клиенты: Microsoft Outlook 2000 / 2003 / 2007; Microsoft Outlook Express; Microsoft Windows Mail; Thunderbird 1.5 and 2.0

Windows 2000

- 800 Мгц процессор или выше
- Минимум 256 Мб оперативной памяти (рекомендуется 512 Мб)
- Минимум 60 Мб свободного места на жестком диске

Windows XP

- 800 Мгц процессор или выше
- Минимум 512 Мб оперативной памяти (рекомендуется 1 Гб)
- Минимум 60 Мб свободного места на жестком диске

Windows Vista

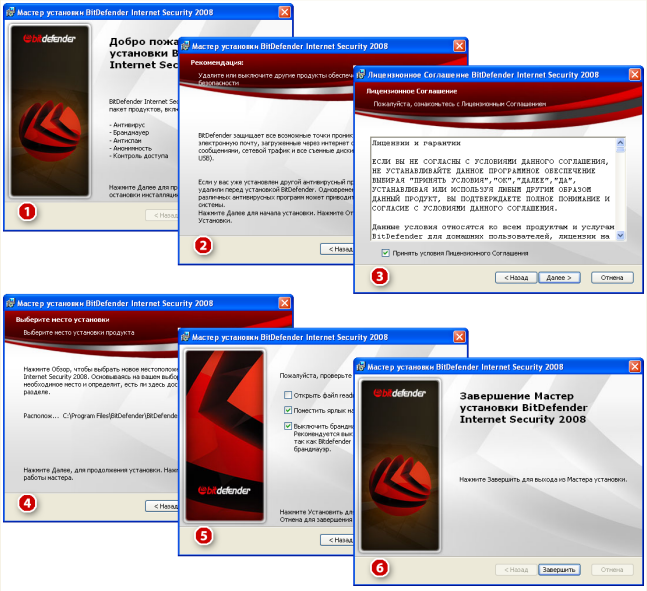
- 800 Мгц процессор или выше
- Минимум 512 Мб оперативной памяти (рекомендуется 1 Гб)
- Минимум 60 Мб свободного места на жестком диске

BitDefender Internet Security 2008 может быть скачен для ознокомления с веб-сайта BitDefender: http://www.bitdef.ru.

1.2. Пошаговая установка

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

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



Пошаговая установка

Следуйте за этими шагами, чтобы установить BitDefender Internet Security 2008:

1. Нажмите **Далее** чтобы продолжить, или **Отменить** если Вы хотите прервать установку.
2. Нажмите **Далее**.

BitDefender Internet Security 2008 предупредит Вас, если на Вашем компьютере установлена какая-либо другая антивирусная программа. Нажмите **Удалить**, чтобы деинсталлировать соответствующий продукт. Если Вы хотите продолжить, не удаляя обнаруженные продукты, нажмите **Далее**.

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

3. Пожалуйста, 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.
4. По умолчанию, BitDefender Internet Security 2008 будет установлен в `C:\Program Files\Softwin\BitDefender 10`. Если Вы хотите выбрать другой путь установки, нажмите **Обзор** и в открывшемся окне выберите каталог, куда необходимо установить BitDefender Internet Security 2008.

   Нажмите **Далее**.
5. Выберите опции, имеющие отношения к процессу установки. Некоторые из них будут выбраны по умолчанию:
   - **Открыть файл readme** - открывает ознакомительный файл в конце установки.
   - **Создать ярлык на рабочем столе** - добавляет ярлык BitDefender Internet Security 2008 на Ваш рабочий стол после окончания процесса установки.
   - **Извлечь CD из привода после окончания установки** - позволяет извлечь диск из привода после окончания установки; данная опция появляется при установке продукта с CD.
   - **Выключить Брандмауэр Windows** - выключает Брандмауэр Windows.

Важно
Мы рекомендуем Вам выключить Брандмауэр Windows, так как BitDefender Internet Security 2008 уже включает усовершенствованный Брандмауэр. Выполнение двух брандмауэров на одном компьютере может вызвать проблемы.

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

   Нажмите **Установить**, чтобы начать установку программы.

Важно

Во время установки будет запущен мастер установки. Этот мастер поможет Вам зарегистрировать **BitDefender Internet Security 2008**, создать учетную запись BitDefender и настроить BitDefender на выполнение важных задач по обеспечению безопасности.

Завершите процесс установки при помощи мастера, чтобы перейти к следующему шагу.

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

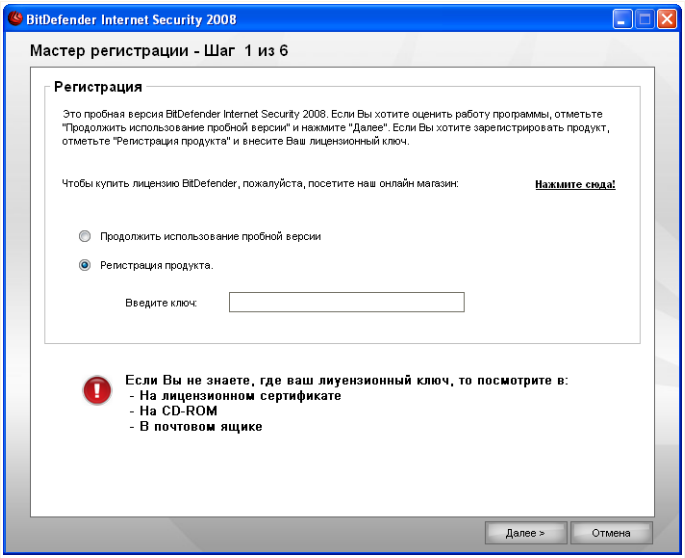
   Если вы приняли установки по умолчанию, вы можете увидеть в `Program Files` новую папку `BitDefender`, в которой будет находиться подкаталог `BitDefender 2008`.

1.3. Мастер начальной настройки

Во время процесса установки будет запущен мастер.Этот мастер поможет Вам зарегистрировать **BitDefender Internet Security 2008**, создать учетную запись и настроить BitDefender на выполнение важных задач обеспечения безопасности.

Завершение всег шагов мастера необязательно; однако, рекомендуется пройти все шаги, чтобы сэкономить время и убедиться, что Ваша система в безопасности еще до установки BitDefender Internet Security 2008.

1.3.1. Шаг 1/6 - Регистрация BitDefender Internet Security 2008



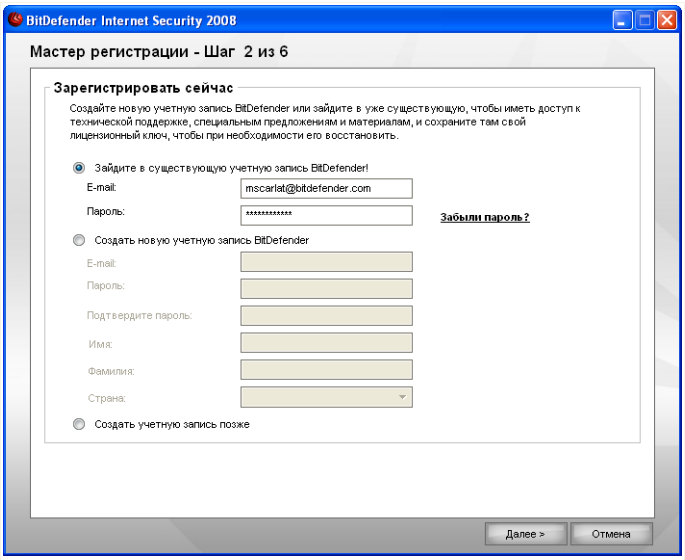
Регистрация

Выберите **Зарегистрировать продукт**, чтобы зарегистрировать **BitDefender Internet Security 2008**. Введите лицензионный ключ в поле **Новый ключ**.

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

Нажмите **Далее**.

1.3.2. Шаг 2/6 - Создание учетной записи BitDefender



Создание учетной записи

У меня нет учетной записи BitDefender

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

Замечание
Если Вы хотите создать учетную запись позднее, выберите соответствующую опцию.

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

- **E-mail** - введите свой адрес электронной почты.
- **Пароль** - введите пароль Вашей учетной записи BitDefender.

Замечание
Пароль должен состоять минимум из четырех символов.

- **Повторите пароль** - снова введите набранный ранее пароль.
- **Имя** - введите Ваше имя.
- **Фамилия** - введите Вашу фамилию.
- **Страна** - выберите страну постоянного проживания.

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

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

Для продолжения нажмите **Далее**.

У меня уже есть учетная запись BitDefender

BitDefender автоматически определит, если вы решистрировали учетную запись BitDefender ранее на этом компьютере. В этом случае все, что Вам нужно сделать - это нажать **Далее**.

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

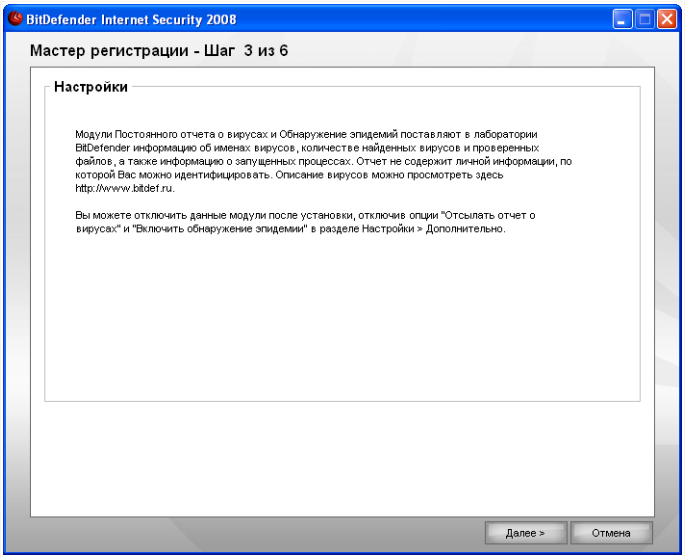
Замечание

Если Вы введете неправильный пароль Вам будет предложено ввести его еще раз и нажмите **Далее**. Нажмите **Ok**, чтобы ввести пароль еще раз или **Отменить**, чтобы прервать работу мастера.

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

Для продолжения нажмите **Далее**.

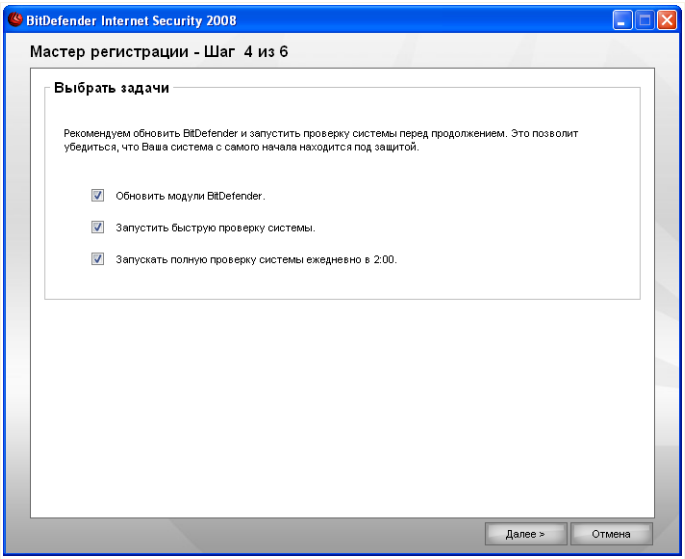
1.3.3. Шаг 3/6 - Узнайте о системе слежения за вирусами в реальном времени (RTVR)



Информация о Системе слежения за вирусами в реальном времени

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

1.3.4. Шаг 4/6 - Выбор задач для запуска



Выбор задачи

Настройте BitDefender Internet Security 2008 на выполнение важных задач обеспечения безопасности Вашей системы.

Доступны следующие варианты:

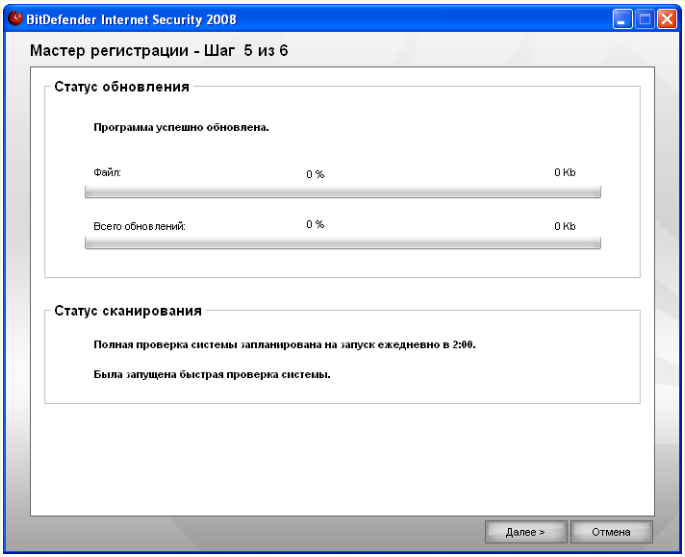
- **Обновить модули BitDefender (может потребоваться перезагрузка)** - на следующем шаге будет произведено обновление модулей BitDefender, чтобы обеспечить защиту Вашего компьютера от новых вирусов и угроз.
- **Запустить быструю проверку системы** - на следующем шаге будет проведена быстрая проверка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

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

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

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

1.3.5. Шаг 5/6 - Ожидание завершения задач

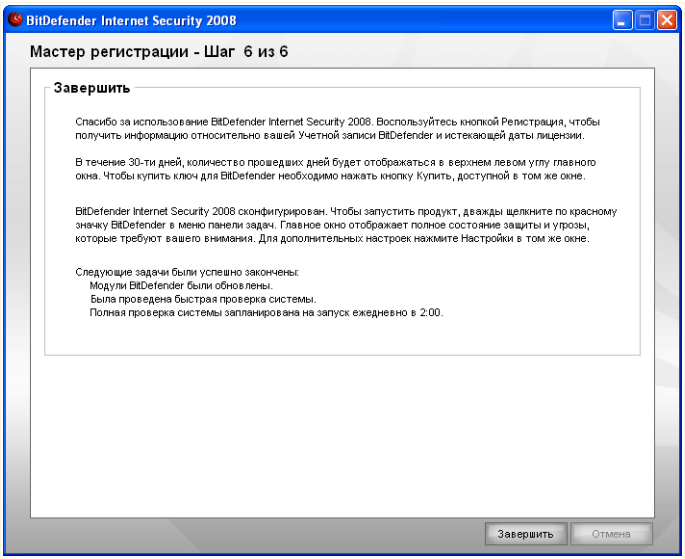


Статус задачи

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

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

1.3.6. Шаг 6/6 – Итоговый отчет



Завершение

Это последний шаг мастера установки.

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

1.4. Обновление

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

- **Установить, не удаляя предыдущую версию, - возможно для BitDefender v8 и выше, кроме версии Internet Security**.

  Дважды щелкните на файле установки и следуйте указаниям мастера установки, описанным в разделе «*Пошаговая установка*» (p. 3).

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. 3).

Важно

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

1.5. Удаление или восстановление BitDefender.

Если Вы хотите восстановить или удалить **BitDefender Internet Security 2008**, в меню Windows пуск выберите следующее: **Пуск → Программы → BitDefender 2008 → Восстановить или Удалить**.

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

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

Важно

Перед тем, как восстанавливать продукт, рекомендуем Вам сохранить Список Друзей и Спамеров. Также сохраните параметры настройки BitDefender и базу данных Bayesian. После окончания процеса восстановления вы сможете их снова загрузить.

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

  Перезагрузите компьютер, при поступлении соответствующего запроса системы и после этого, нажмите **Установить**, чтобы переустановить BitDefender Internet Security 2008.

  Как только процесс установки завершен, появится новое окно. Нажмите **Завершить**.
- **Удалить** - удаление всех установленных компонентов.

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

Если Вы выбираете удалить BitDefender, появится новое окно.

Важно
Удаляя BitDefender, вы лишаетесь защиты от вирусов, программ-шпионов и атак хакеров. Если Вы хотите, чтобы Брандмауэр Windows и Защита Windows (только для Windows Vista) были включены после деинсталляции BitDefender, выберите соответствующие флажки.

Нажмите **Удалить**, чтобы начать удаление BitDefender Internet Security 2008 с Вашего компьютера.

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

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

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

При удалении BitDefender возникла проблема.

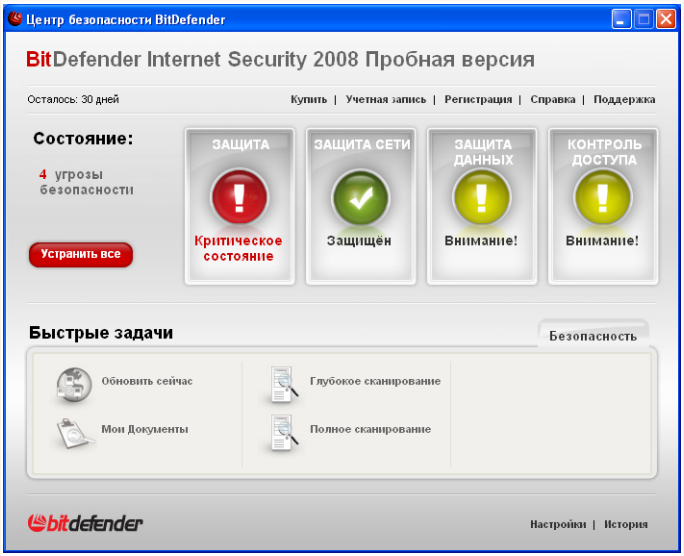
Если во время удаления BitDefender возникла ошибка, процесс будет отменен, и появится новое окно. Чтобы убедиться, что BitDefender полностью удален с Вашего компьютера, нажмите **Запустить инструмент удаления**. Он удалит все файлы и записи в реестре, которые не были удалены во время автоматического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

Основны администрирования

2. Начало работы

Как только вы установили BitDefender, Ваш компьютер находится под защитой. Теперь Вы можете открыть Центр безопасности BitDefender и проверить состояние системы защиты, принять превентивные меры или полностью настроить продукт.

Открыть Центр безопасности BitDefender можно через меню Пуск, по следующей схеме **Пуск → Программы → BitDefender 2008 → BitDefender Internet Security 2008** или еще быстрее, дважды щелкнув мышкой по значку **BitDefender** в области уведомлений на панели задач.



Центр безопасности BitDefender

Центр безопасности BitDefender состоит из двух областей:

- Область **Состояние**: содержит информацию о текущем состоянии компьютера и помогает устранить уязвимости. Здесь Вы можете просмотреть список проблем, которые могут влиять на Ваш компьютер. Нажав соответствующую красную кнопку **Исправить все**, уязвимости Вашего компьютера будут либо

тут же устранены, либо Вы получите инструкции, объясняющие, что необходимо сделать, чтобы их устранить. Кроме того, есть четыре кнопки состояния, соотвествующие четырем категориям безопасности. Зеленый цвет означает полное отсутствие проблем. Желтый и красный цвета сигнализируют о среднем и высоком уровне угрозы безопасности Вашему компьютеру. Чтобы исправить эти проблемы, нажмите желтую/красную кнопку, а затем кнопку **Исправить** одну за другой, или кнопку **Исправить все**. Серый цвет означает, что компонент ненастроен.

- Область **Быстрых задач**: помогает поддерживать безопасность Вашей системы и защищать данные.

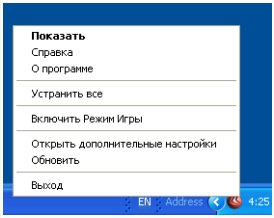
Кроме того, Центр безопасности BitDefender содержит несколько полезных ссылок.

Ссылка	*Описание*
Купить	Открывает страницу, где можно приобрести продукт.
Моя учетная запись	Открывает страницу с учетной записью BitDefender
Зарегистрировать	Запускает мастера регистрации.
Помощь	Открывает файл справочника.
Поддержка	Открывает страницу службы поддержки BitDefender.
Настройки	Открывает консоль дополнительных настроек.
История	Открывает страницу событий BitDefender.

2.1. Значок BitDefender в системном трее.

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

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



Значок BitDefender

- **Показать** - открывает Центр безопасности BitDefender.
- **Помощь** - открывает файл справочника.
- **О компании** - открывает веб-страницу BitDefender
- **Исправить все проблемы** - помогает устранить имеющиеся уязвимости в безопасности компьютера.
- **Включить / выключить режим игры** - переключает Режим Игры вкл / выкл.
- **Дополнительные настройки** - доступ к консоли дополнительных настроек.
- **Обновить сейчас** - запускает немедленное обновление. Когда проверка завершится, откроется новое окно, где Вы можете увидеть результаты проверки.
- **Выйти** - выключает приложение.

Всякий раз, когда включен Режим игры идет, то Вы можете видеть символ G на значке BitDefender.

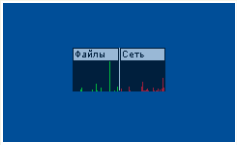
Если есть критические проблемы, которые затрагивают безопасность Вашей системы, то на значке BitDefender будет отображен восклицательный знак Вы можете подвести курсор мыши к значку, чтобы увидеть число проблем.

2.2. Строка состояния сканирования

В окне **Панель активной проверки** графическое отображение процесса проверки Вашей системы.

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

Красные полоски в **Зоне Сети** показывают, сколько килобайт информации передается и скачивается из Интернета в секунду, по шкале от 0 до 100.



Строка состояния

Замечание
Панель активной проверки уведомит о том, что антивирусная защита или Брандмауэр отключены, отображая красный крест поверх соответствующей области (**Файловая зона** или **Зона сети**).

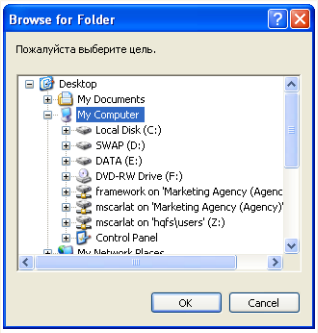
Вы можете использовать **Панель активной проверки** для проверки объектов. Для этого перетащите объекты, которые Вы желаете проверить, прямо на нее. Для дополнительной информации, перейдите к «*Проверка перетаскиванием*» (p. 71).

Чтобы убрать это окно с экрана, просто щелкните правой кнопкой мышки на нем и выберите пункт меню **Скрыть**. Чтобы полностью скрыть это окно, в консоли настроек нажмите **Дополнительно**, а затем уберите отметку из поля, соответствующего пункту **Включить панель активной проверки (график активности программы)**.

2.3. Ручная проверка BitDefender

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

Чтобы воспользоваться ручной проверкой BitDefender, откройте меню Пуск и последовательно откройте **Пуск** → **Программы** → **BitDefender 2008** → **BitDefender Manual Scan** Появится следующее окно:



Ручная проверка BitDefender

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

2.4. Режим Игры

Новый Режим Игры изменяет параметры настроек системы защиты для того, чтобы снизить к минимуму воздействие на компьютер во время игры, при этом поддерживая безопасность на высоком уровне. Когда Вы включаете Режим Игры, будут установлены следующие настройки:

- Все предупреждения и всплывающие окна BitDefender будут отключены.
- Режим защиты BitDefender в реальном времени будет установлен, как **Разрешен**.
- Брандмауэр BitDefender установлен в **Режим Игры**.

Всякий раз, когда включен Режим игры идет, то Вы можете видеть символ `G` на значке BitDefender.

2.4.1. Использование Режима Игры

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

- Кликните правой кнопкой мыши на иконке BitDefender в системном трее и установите **Включить Режим Игры**.
- Нажмите `Alt+G` (установлено по умолчанию).

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

2.4.2. Изменение Горячих клавиш Режима Игры

Чтобы изменить Горячие клавиши, необходимо выполнить следующие шаги:

1. Кликните **Установки**, чтобы открыть панель установок Центра безопасности BitDefender.

Замечание
Вы также можете кликнуть значок BitDefender в системном трее правой кнопкой и выберать **Открыть расширенные настройки**.

2. Нажмите **Дополнительно**.
3. В пункте **Горячие клавиши для Режима Игры** установите желаемые Горячие клавиши:
   - Выберите клавиши, которые Вы хотите изменить, используя следующие: клавиша Control (`Ctrl`), клавиша Shift (`Shift`) или клавиша Alternate (`Alt`).

- В поле редактирования укажите букву с клавишей, которую Вы хотите использовать.

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

Замечание
Удалив отметку рядом с **Горячие клавиши Режима Игры**, Вы отключите Горячие клавиши.

3. Статус безопасности

Функция состояния безопасности отображает систематизированный список уязвимостей Вашего компьютера, которым можно легко пользоваться. BitDefender Internet Security 2008 позволяет сделать вывод, повлияет ли существующая проблема на безопасность Вашего компьютера.

Имеется четыре кнопки состояния безопасности:

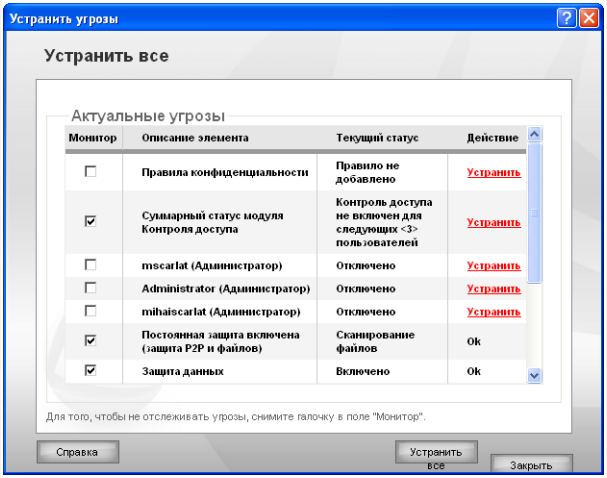
- **БЕЗОПАСНОСТЬ PC**
- **БЕЗОПАСНОСТЬ СЕТИ**
- **КОНТРОЛЬ КОНФИДЕНЦИАЛЬНОСТИ**
- **КОНТРОЛЬ ДОСТУПА**

Одновременно, слева можно видеть список проблем, влияющих на безопасность Вашей системы, а также красную кнопку **Исправить все проблемы**.

Четыре кнопки состояния могут быть зеленого, желтого, красного или серого цвета в зависимости от текущего уровня защиты.

- **Зеленый** цвет обозначает низкий уровень угроз для безопасности Вашего компьютера.
- **Желтый** цвет обозначает средний уровень угроз для безопасности Вашего компьютера.
- **Красный** цвет обозначает высокий уровень угроз для безопасности Вашего компьютера.
- **Серый** цвет обозначает ненастроенные компоненты.

Устранение существующих проблем безопасности не требует от Вас никаких усилий, кроме необходимости нажать кнопку **Исправить все проблемы**. Появится новое окно.



Проблемы безопасности

Вы увидите список проблем, а также краткое описание их состояния.

Для того, чтобы исправить только конкретную проблему, нажмите соответствующую кнопку **Исправить**. Проблема будет решена сразу же, либо после того, как Вы выполните все шаги мастера. Если Вы решите исправить сразу все проблемы. нажмите кнопку **Исправить все проблемы** и следуйте указаниям мастера.

Если Вам необходимо дополнительная помощь, то нажмите кнопку **Больше Помощи**, которая находится в нижней части края окна. Страница контекстной справки предоставляет Вам детальную информацию о данной проблеме и о том, как ее исправить.

Важно

Для каждой проблемы имеется специальное поле, отмеченное галочкой по умолчанию. Если Вы не хотите, чтобы тот или иной фактор принимался во внимание при расчете уровня риска, уберите отметку из соответствующего поля. Будьте осторожны, используя данную функцию, поскольку это может привести к значительному увеличению количества угроз, с которыми придется столкнуться Вашему компьютеру.

Чтобы исправить данные проблемы позднее, нажмите **Закрыть**.

3.1. Кнопка статуса Контроля доступа

Если кнопка статуса Контроля доступа зеленого цвета, то Контроль доступа включен. Если серого цвета, то выключен.

Для подключения Контроля доступа выполните следующие шаги:

1. Нажмите на кнопку состояния контроля доступа.
2. Сделайте одно из следующего:
   - Чтобы включить Контроль доступа для всех пользователей, нажмите **Исправить все**.
   - Чтобы включить Контроль доступа для определенных пользователей, нажмите **Исправить** напротив соответствующих пользователей.

3.2. Кнопка состояние Безопасности компьютера

Если кнопка состояния безопасности зеленого цвета, то повода для беспокойств нет. Если же кнопка желтого, красного или серого цвета, то уровень угнозы безопасности Вашему компьютеру средний или значительный.

Цвет кнопки состояния может изменяться не только, когда Вы изменяете настройки, влияющие на безопасность Вашего компьютера, но и когда Вы забываете выполнять некоторые важные действия. Например, если последняя проверка системы выполнялась давно, кнопка будет желтой, если очень давно - красной.

Следующая таблица расскажет Вам о том, какие элементы принимаются во внимание при расчете угрозы безопасности.

Проблема	*Цвет*
Последняя проверка системы выполнялась давно	Желтый
Последняя проверка системы выполнялась очень давно	Красный
Защита в реальном времени отключена	Красный
Уровень защиты антивируса установлен как разрешающий	Желтый
Автоматическое обновление выключено	Красный
Последнее обновление сделанно день назад	Красный

Проблема	Цвет
Антиспам выключен	Серый

Чтобы исправить проблемы, выполните следующие действия:

1. Нажмите на кнопку состояние безопасности
2. Нажмите кнопку **Исправить**, если Вы хотите исправлять их одну за другой, либо кнопку **Исправить все**, если Вы хотите исправить все сразу.
3. Если проблему не удается решить сразу же, то выполните все действия мастера, чтобы исправить данную проблему.

3.3. Сотояние кнопки Безопасность Сети

Если кнопка состояния безопасности сети зеленого цвета, то повода для беспокойств нет. Если же кнопка красного цвета, то существует значительная угроза безопасности Вашего компьютера.

Следующая таблица расскажет Вам о том, какие элементы принимаются во внимание при расчете угрозы безопасности.

Проблема	Цвет
Брандмауэр выключен	Красный
Режим "Невидимости" выключен	Красный
Беспроводное соединение не защищено	Красный

Чтобы исправить проблемы, выполните следующие действия:

1. Нажмите на кнопку сотояния Безопасность Сети
2. Нажмите кнопку **Исправить**, если Вы хотите исправлять их одну за другой, либо кнопку **Исправить все**, если Вы хотите исправить все сразу.
3. Если проблему не удается решить сразу же, то выполните все действия мастера, чтобы исправить данную проблему.

3.4. Кнопка статуса Контроля конфиденциальности

Если кнопка состояния модуля Контроля конфиденциальности зеленого цвета, то повода для беспокойств нет. Если же кнопка красного или серого цвета, то существует значительная угроза безопасности Вашего компьютера.

Следующая таблица расскажет Вам о том, какие элементы принимаются во внимание при расчете угрозы безопасности.

Проблема	*Цвет*
Защита личных данных установлена и включена	Зеленый
Защита личных данных установлена и выключена	Красный
Защита личных данных не установлена	Серый

Чтобы исправить проблемы, выполните следующие действия:

1. Нажмите на кнопку состояния личных данных.
2. Нажмите кнопку **Исправить**, если Вы хотите исправлять их одну за другой, либо кнопку **Исправить все**, если Вы хотите исправить все сразу.
3. Если проблему не удается решить сразу же, то выполните все действия мастера, чтобы исправить данную проблему.

4. Быстрые задачи

Под четырьмя кнопками состояния расположена область **Быстрых задач**

4.1. Безопасность

BitDefender снабжен модулем безопасности, который помогает поддерживать саму программу всегда в обновленном состоянии, и надежно защищать Ваш компьютер от вирусов.

Чтобы войти в модуль безопасности, нажмите вкладку **Безопасность**

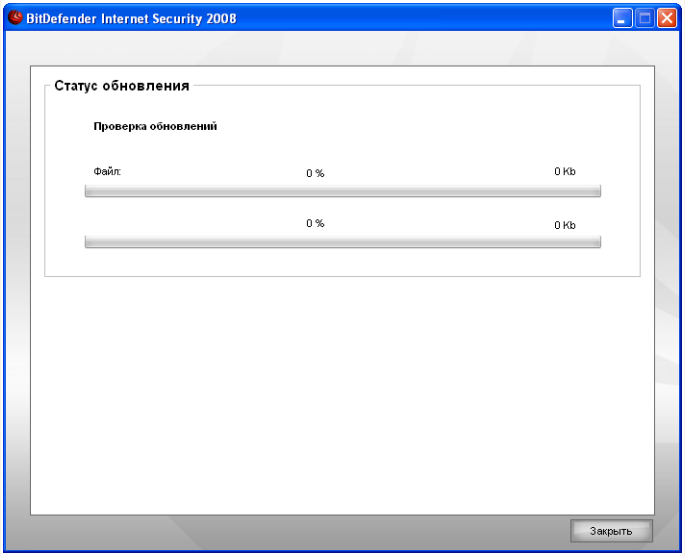
Доступны следующие варианты:

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

4.1.1. Обновление BitDefender

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

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



Обновление BitDefender

В этом окне Вы можете видеть статус процесса обновления.

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

Если Вы хотите закрыть это окно, нажмите **Завершить**. Это не будет останавливать процесс обновления.

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

Если требуется, то перезагрузите компьютер. В случае основного обновления, Вас попросят перезагрузить компьютер. Если Вы не хотите, чтобы больше не было подтверждения, когда обновление требует перезагрузки, отметьте **Ждать перезагрузки, а не показывать подтверждение**. Таким образом, в следующий раз, когда обновление требует перезагрузки, продукт, будет продолжать работать со старыми файлами, пока Вы не перезагрузите систему добровольно.

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

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

4.1.2. Сканирование с помощью BitDefender

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

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

Замечание

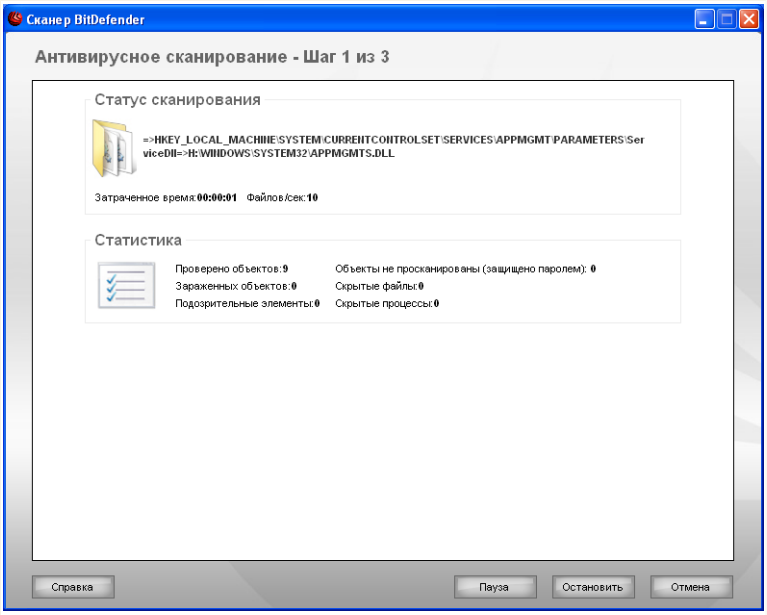
Поскольку задания **Глубокая проверка системы** и **Полная проверка системы** проводят анализ всей системы, их выполнение может занять определенный промежуток времени. Поэтому, рекомендуем выполнять эти задачи с небольшим приоритетом, либо когда Ваша система не загружена.

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

Чтобы завершить процесс проверки выполните последовательность из трех шагов.

Шаг 1/3 - Сканирование

BitDefender начнет проверку выбранных объектов.



Сканирование

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

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

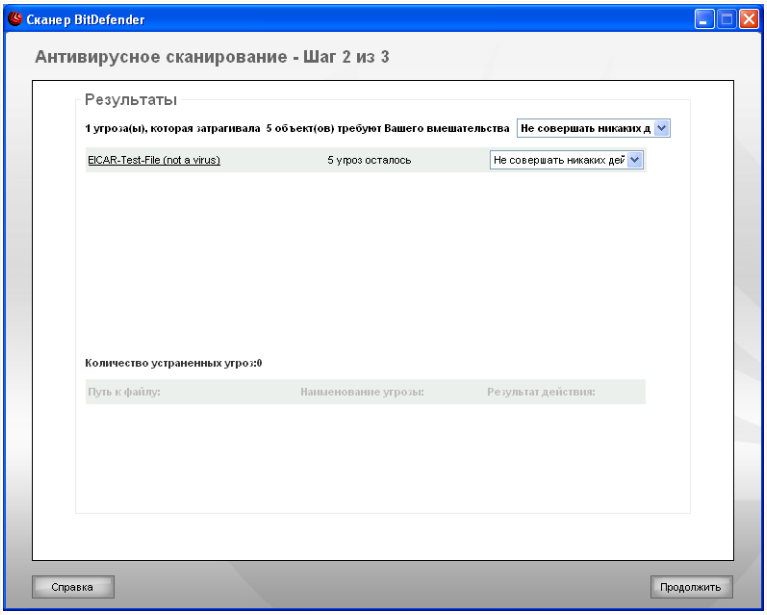
Чтобы временно приостановить процесс проверки, нажмите **Пауза**. Чтобы продолжить проверку, нажмите **Возобновить**.

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

Дождитесь окончания сканирования BitDefender

Шаг 2/3 - Выберите Действия

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



Действия

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

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

Для каждой группы проблем Вы можете выбрать общее действие, либо есть возможность выбрать отдельное действие для каждой проблемы.

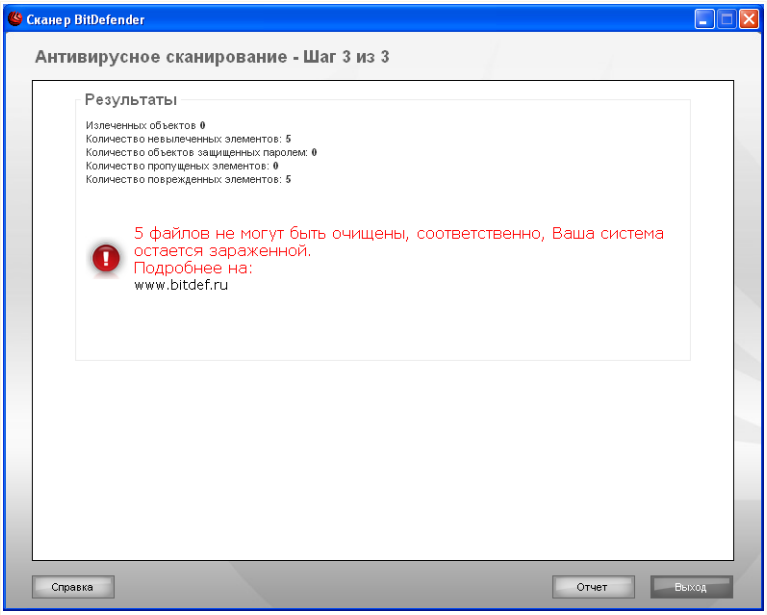
Доступны следующие варианты:

Действие	Описание
Ни чего не делать	Над обнаруженными файлами не будет производиться никаких действий.
Вылечить	Выполняется лечение зараженных файлов.
Удалить	Удаление обнаруженных файлов.
Раскрыть	Сделать скрытые объекты видимыми.

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

Шаг 3/3 - Просмотр результатов

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



Краткий обзор

Здесь Вы можете просмотреть краткий обзор. Отчеты автоматически сохраняются в разделе Журнал событий в окне **Свойства** соответствующей задачи.

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

Нажмите **Выход**, чтобы закрыть окно.

BitDefender не может исправить некоторые проблемы

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

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

Обнаруженные BitDefender элементы, защищенные паролем

Категория защищенных паролем включает в себя два типа элементов: архивы и инсталляторы. Они не представляют реальной угрозы безопасности системы, только если не содержат зараженных файлов, да и в этом случае опасны, только если их запустить.

Чтобы убедиться, что эти элементы являются чистыми:

- Если защищенный паролем элемент - это архив, то распакуйте его и проверьте содержащиеся в нем файлы с помощью выборочного сканирования. Самый простой способ их просканировать - это щелкнуть правой кнопкой мышки на них и выберать **BitDefender Antivirus 2008** из меню.
- Если защищенный паролем элемент - это инсталлятор, то убедитесь, что функция защиты в режиме реального времени включена, перед тем, как запустить его. Если файл-инсталлятор заражен, BitDefender обнаружит и изолирует инфекцию.

Если Вы не хотите, чтобы BitDefender снова обнаруживал эти объекты, Вы должны добавить их в список исключений для процесса сканирования. Чтобы добавить исключение при сканировании, откройте консоль настроек, нажав **Настройки**, и затем перейдите на **Антивирус > Исключения** . Для просмотра дополнительной информации перейдите по ссылке Объекты, исключенные из сканирования.

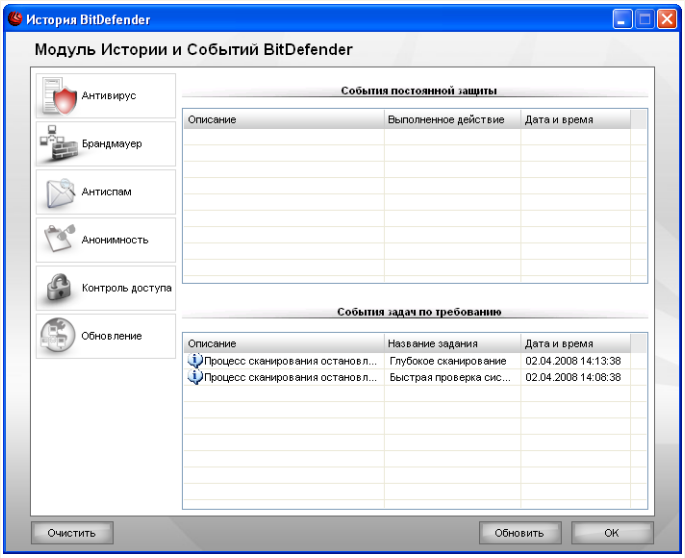
Обнаруженные BitDefender подозрительные файлы

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

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

5. Архив

Ссылка **Архив** внизу окна центра безопасности BitDefender открывает окно с прошлыми событиями BitDefender. Здесь представлен обзор всех событий, связанных с безопасностью. Например, Вы можете проверить, было ли успешным последнее обновление, были ли найдены на Вашем компьютере вредоносные программы, успешно ли были выполнены задачи создания резервной копии данных, и т.д.



События

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

- **Антивирус**
- **Брандмауэр**
- **Антиспам**
- **Контроль личных данных**
- **Контроль доступа**
- **Обновление**

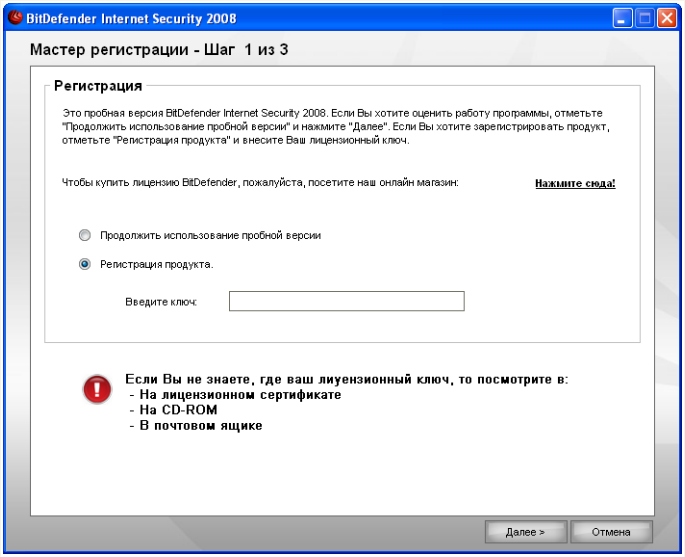
Для каждой категории имеется список событий. Для каждого события отображается следующая информация: краткое описание, действие, выполненное BitDefender при появлении события, дата и время события. Если Вы хотите узнать больше о каком-то определенном событии, дважды нажмите на нем.

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

6. Регистрация

BitDefender Internet Security 2008 предоставляется с 30-ти дневным периодом пробного использования. Если Вы хотите зарегистрировать BitDefender Internet Security 2008, изменить лицензионный ключ или создать учетную запись BitDefender, нажмите ссылку **Регистрация**, которая находится в верхней части окна Центра Безопасности BitDefender. Появится Мастер регистрации.

6.1. Шаг 1/3 - Регистрация BitDefender Internet Security 2008



Регистрация

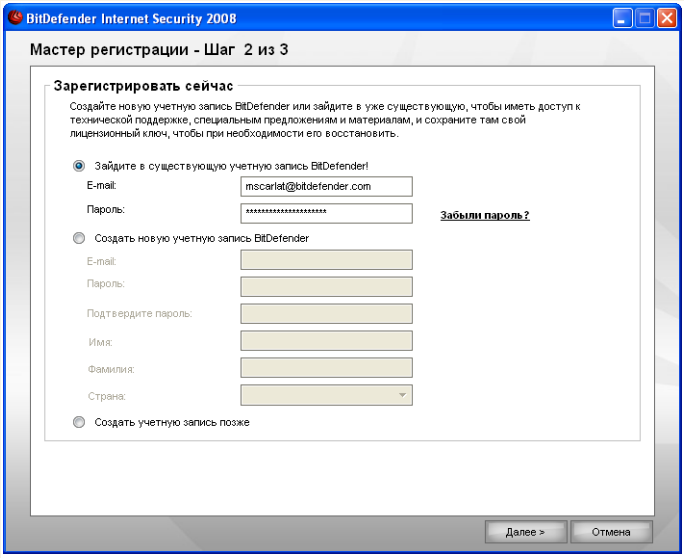
Если у Вас нет лицензии BitDefender, нажмите соответствующую ссылку для перехода в онлайн-магазин BitDefender и приобретите лицензионный ключ.

Для регистрации BitDefender Internet Security 2008 выберите **Зарегистрировать продукт** и введите лицензионный ключ в поле**Введите новый ключ**.

Если период пробного использования еще не истек, и Вы хотите продолжить использовать пробную версию, выберите **Продолжить пользоваться пробной версией**.

Для продолжения нажмите **Далее**.

6.2. Шаг 2/3 - Создание учетной записи BitDefender



Создание учетной записи

У меня нет учетной записи BitDefender

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

Замечание
Если Вы хотите создать учетную запись позднее, выберите соответствующую опцию.

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

- **E-mail** - введите свой адрес электронной почты.
- **Пароль** - введите пароль Вашей учетной записи BitDefender.

> ***Замечание***
> Пароль должен состоять минимум из четырех символов.

- **Повторите пароль** - снова введите набранный ранее пароль.
- **Имя** - введите Ваше имя.
- **Фамилия** - введите Вашу фамилию.
- **Страна** - выберите страну постоянного проживания.

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

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

Для продолжения нажмите **Далее**.

У меня уже есть учетная запись BitDefender

BitDefender автоматически определит, если вы решистрировали учетную запись BitDefender ранее на этом компьютере. В этом случае все, что Вам нужно сделать - это нажать **Далее**.

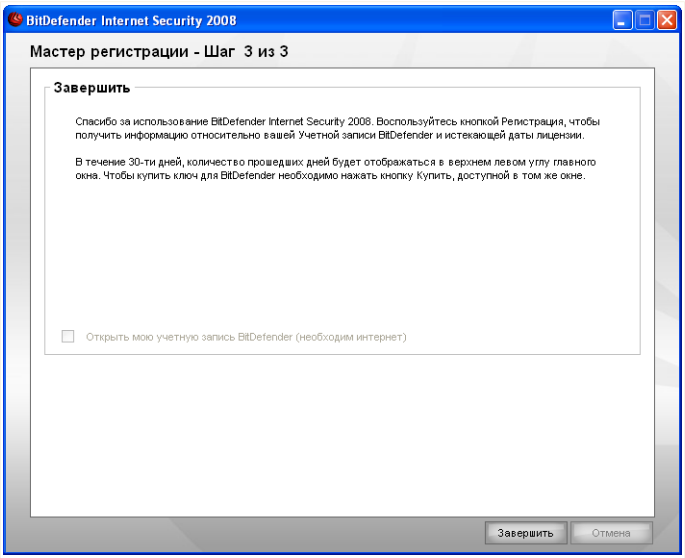
Если у Вас уже есть активная учетная запись, но BitDefender не определяет ее, выберите **Использовать существующую учетную запись BitDefender** и укажите e-mail и пароль Вашей учетной записи.

> ***Замечание***
> Если Вы введете неправильный пароль Вам будет предложено ввести его еще раз и нажмите **Далее**. Нажмите **Ok**, чтобы ввести пароль еще раз или **Отменить**, чтобы прервать работу мастера.

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

Для продолжения нажмите **Далее**.

6.3. Шаг 3/3 - Регистрация BitDefender Internet Security 2008



Краткий обзор

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

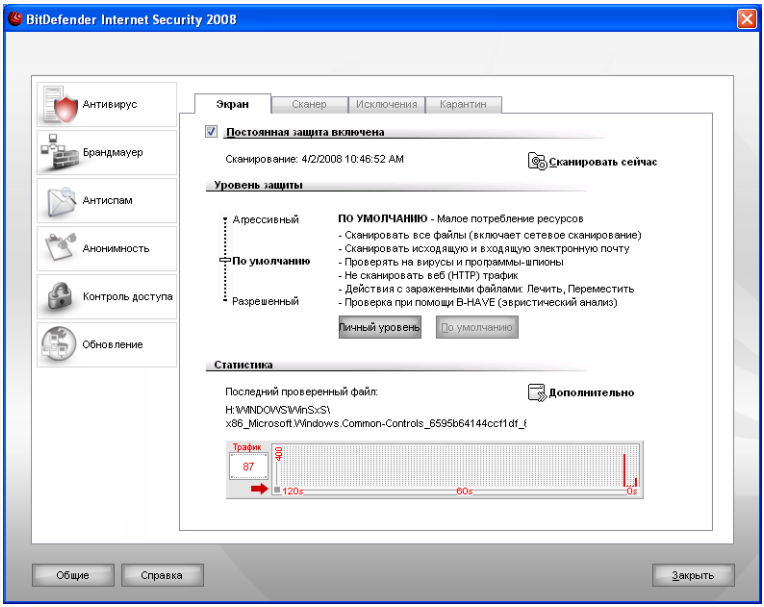
Нажмите **Завершить**, чтобы закрыть окно.

Детальное описание администрирования

7. Консоль настроек

идет с централизованной консолью управления, который позволяет быстро настраивать и администрировать BitDefender.

Попасть в консоль настроек можно при помощи ссылки **Настройки**, расположенной внизу окна центра безопасности.



Консоль настроек

Консоль управления состоит из: **Антивирус**, **Брандмауэр**, **Антиспам**, **Контроль личных данных**, **Контроль доступа** и **Обновление**. Это позволяет Вам легко управлять BitDefender, основываясь на типе решаемой проблемы безопасности.

В левой части консоли настроек видеть выбор необходимого модуля:

- Антивирус - в данном разделе вы можете настроить модуль **Антивирус**.
- Брандмауэр - в этом разделе вы можете сконфигурировать **Брандмауэр**.
- Антиспам - в этом разделе вы можете настраивать модуль **Антиспама**.

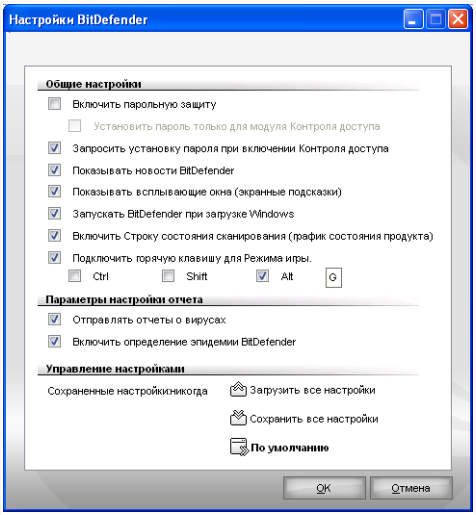
- Контроль личных данных - в этом разделе Вы можете конфигурировать модуль **Контроль личных данных**.
- Контроль доступа - в этом разделе Вы можете конфигурировать модуль **Контроль доступа**.
- Обновление - в этом разделе Вы можете конфигурировать модуль **Обновление**.

В нижней части консоли настроек есть кнопка **Больше помощи**, которая открывает страницу контекстной справки. Нажмите эту кнопку, чтобы получить больше информации о той секции, где Вы находитесь, когда бы Вам ни потребовалась дополнительная помощь.

Если Вам необходимо дополнительная помощь, то нажмите кнопку **Больше Помощи**, которая находится в нижней части края окна. Страница контекстной справки предоставляет Вам детальную информацию о секции, в которой Вы находитесь.

7.1. Конфигурация основных настроек

Нажмите ссылку **Дополнительно**, чтобы получить доступ и управление к общим настройкам BitDefender Internet Security 2008. Появится новое окно.



Основные настройки

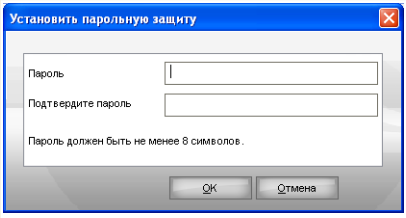
Здесь Вы можете настроить общее поведение Bitdefender. По умолчанию, Bitdefender загружается при запуске Windows и затем работает в свернутом виде в панели задач.

7.1.1. Основные настройки

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

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

  Если Вы выбираете эту опцию, появится следующее окно:



Введите пароль

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

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

Если Вы хотите, чтобы были запросы пароля только тогда, когда изменяются настройки модуля Контроль доступа, Вы должны так же выбрать **Спрашивать/применять пароль только для модуля Контроль доступа**. С другой стороны, если пароль был установлен только на Контроль доступа, и Вы неотметили эту опцию, то соответствующий пароль будет запрашиваться при изменении любой опции BitDefender.

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

- **Запрашивать пароль при включении модуля Контроль доступа** - если эта опция включена и не установлен пароль, то Вы должны установить его при включении модуля Контроль доступа.

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

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

- **Включить "горячую клавишу" для Режима игры** - разрешает использование клавишы для включения / выключения Режима игры. По умолчанию это `Alt+G`

  Чтобы изменить "горячую клавишу", сделайте следующее:

  1. Отметьте клавиши модификатора, которые Вы хотите использовать: Control key (`Ctrl`), Shift key (`Shift`) or Alternate key (`Alt`).
  2. В поле редактирования укажите букву с клавишей, которую Вы хотите использовать.

7.1.2. 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.

7.1.3. 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 BitDefender.

Важно
Только пользователи с правами администратора могут сохранять и загружать настройки.

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

8. Антивирус

BitDefender защищает Ваш компьютер от всех типов вредоносных программ (вирусов, троянов, программ-шпионов, руткитов и т.д.).

Помимо классической проверки, основывающейся на образах вредоносных программ, BitDefender также выполняет эвристический анализ проверяемых файлов. Целью эвристического анализа является выявление новых вирусов, основываясь на определенных шаблонах и алгоритмах, до того, как найдено определение вируса. Здесь могут проявляться ложные срабатывания. Когда такие файлы обнаруживаются, они обозначаются как подозрительные. В этом случае, рекомендуем отправить их в Лабораторию BitDefender для анализа.

Настройки защиты BitDefender разделены на две категории:

- **Входная проверка** - предотвращает доступ в систему новых вредоносных программ. Эта категория также называется постоянная защита - файлы сканируется по мере того, как пользователь ими пользуется. К примеру, BitDefender проверяет текстовый файл на наличие известных угроз при его открытии, а также электронные сообщение, когда Вы их получаете.
- **Проверка по требованию** - обнаруживает и удаляет вредоносные программы, которые уже находятся на вашем компьютере. Это классический тип проверки по желанию пользователя, когда Вы выбираете диск, папку, или файл для проверки BitDefender, а BitDefender проверяет их по Вашему требованию. Задачи проверки позволяют создавать распланированые действия, которые регулярно запускаются по расписанию.

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

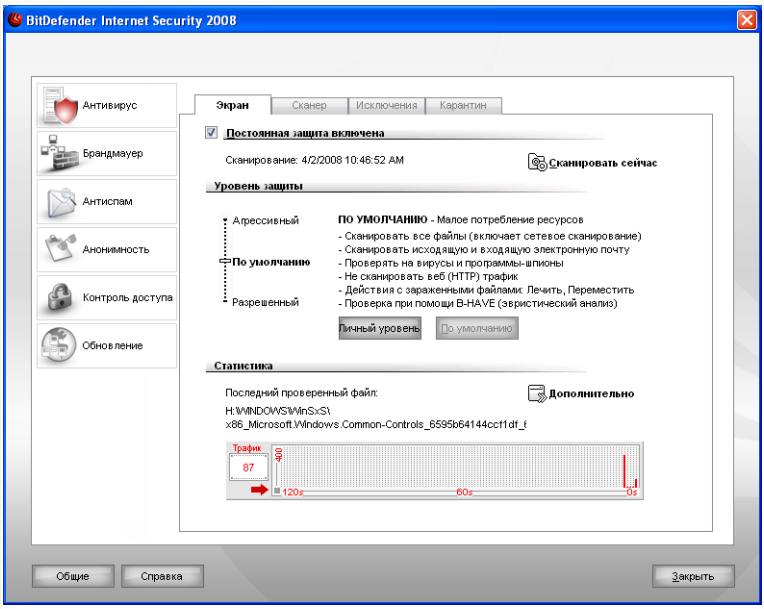
- Входное сканирование
- Сканирование по требованию
- Объекты, исключенные из сканирования
- Карантин

8.1. Входное сканирование

Входная проверка, также называемая постоянной защитой, защищает Ваш компьютер от всех типов угроз, проверяя все открываемые файлы, электронные

сообщения и сообщения так называемых программ-мессенджеров (ICQ, NetMeeting, Yahoo Messenger, MSN Messenger).

Чтобы настроить и следить за работой постоянной защиты, нажмите ссылку **Антивирус>Монитор** в консоли настроек. Появится следующее окно:



Постоянная защита

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 просмотреть более детальную информацию.

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

8.1.1. Конфигурация уровня защиты

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

Существует 3 уровня защиты:

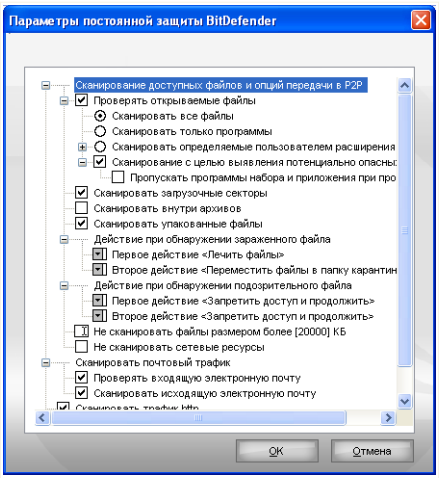
Уровень защиты	*Описание*
Разрешающий	Выполняет основные процессы безопасности. Потребляет малое количество ресурсов. Программы и входящие электронные сообщения проверяются только на наличие вирусов. Кроме классического сканирования при помощи базы образов, также используется эвристический анализ. К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

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

8.1.2. Настройка уровня защиты

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

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



Настройки защиты

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

Замечание

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

- Выберите настройку **Проверять открываемые и закачиваемые напрямую (P2P) файлы** - чтобы проверять все открываемые файлы и обмен данными

с помощью 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 ";".
	Проверка на наличие других угроз	Проверка на наличие других угроз. Обнаруженные файлы будут считаться зараженными. Программное обеспечение, которое включает компоненты рекламного ПО, может прекратить работу, если выбрана эта настройка. Поставьте значок в поле **Пропускать программы дозвона и приложения при сканировании**, если Вы хотите пропускать подобные файлы при сканировании.
Сканировать начальную загрузку		Проверка загрузочных секторов системы.
Проверять внутри архивов		Проверяются также архивы. Включение данной опции замедлит работу компьютера.
Проверить запакованные файлы		Проверяются все запакованные файлы.

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

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

Доступны следующие варианты:

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

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

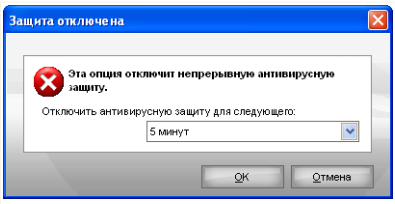
  Предупреждение об обнаружении зараженного вирусом файла содержит название вируса, путь к зараженному файлу, действие BitDefender, выполненного с этим файлом, и ссылку на сайт BitDefender, где Вы сможете получить более подробную информацию об этом вирусе. В случае обнаружения вируса в электронной почте, 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.

8.1.3. Отключение постоянной защиты

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



Включенная постоянная защита

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

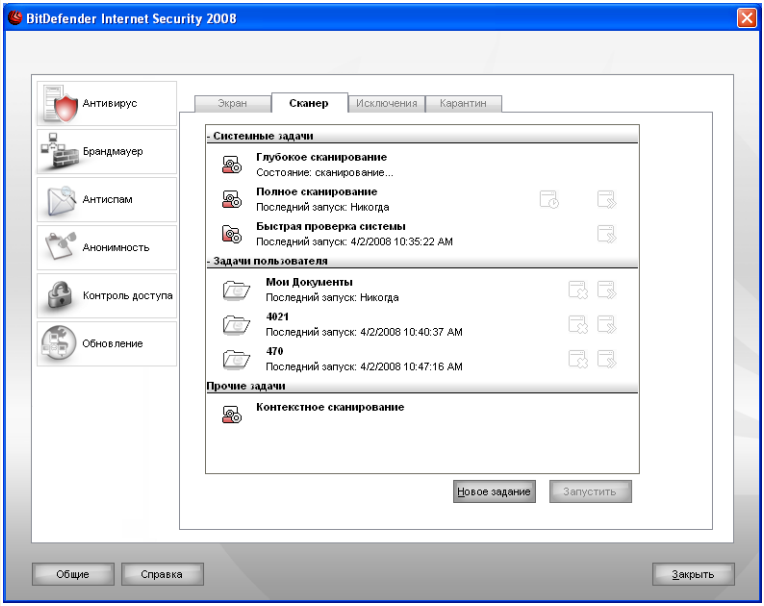
Внимание
Этот аспект является критическим с точки зрения безопасности. Рекомендуем Вам отключать постоянную защиту на как можно меньший промежуток времени. Если постоянная защита отключена, Вы не защищены от угроз вредоносных программ.

8.2. Сканирование по требованию

Главное назначение программного продукта BitDefender - защищать Ваш компьютер от вирусов. В первую очередь BitDefender не позволяет новым вирусам проникнуть на компьютер, проверяя электронные письма и новые загружаемые и копируемые файлы.

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

Нажмите **Антивирус>Проверка** в консоли настроек, чтобы настроить и запустить проверку по требованию. Появится следующее окно:



Задачи сканирования

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

8.2.1. Задачи сканирования

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

У каждого задания есть окно **Свойства**, позволяющее Вам настроить данное задание и просматривать результаты его работы. Более подробную информацию можно найти здесь: «*Настройка задач проверки*» (p. 59).

Существует три категории задач сканирования:

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

Стандартные задачи	*Описание*
Глубокая проверка системы	Проверка всей системы В конфигурации по умолчанию проверка производится на все виды вредоносных программ, угрожающих безопасности Вашей системы, а именно на наличие вирусов, программ-шпионов, рекламного ПО, руткитов и проч.
Полная проверка системы	Проверка всей системы кроме архивов. В конфигурации по умолчанию проверка производится на все виды вредоносных программ, угрожающих безопасности Вашей системы, а именно на наличие вирусов, программ-шпионов, рекламного ПО, руткитов и проч.
Быстрая проверка системы	Сканирование `Windows`, `Program Files` и `Всех пользователей` папки. В конфигурации по умолчанию проверка производится на все виды вредоносных программ, кроме руткитов. Не производится проверка памяти, реестра и записей cookies.

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

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

  Задача под названием `Мои документы` обеспечивается. Используйте данное задание для проверки основных папок пользователя: `Мои документы`, `Рабочий стол` and `Автозагрузка`. Это позволит обеспечить безопасность Ваших документов, безопасность рабочего пространства и запуск незараженных программ при загрузке.
- **Прочие задачи** - содержит список мелких задач. Эти задачи проверки включают альтернативные типы сканирования, которые не могут быть запущены из

данного окна. Вы можете только изменить их настройки или просмотреть отчеты о проверке.

Справа от каждой задачи доступны три кнопки:

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

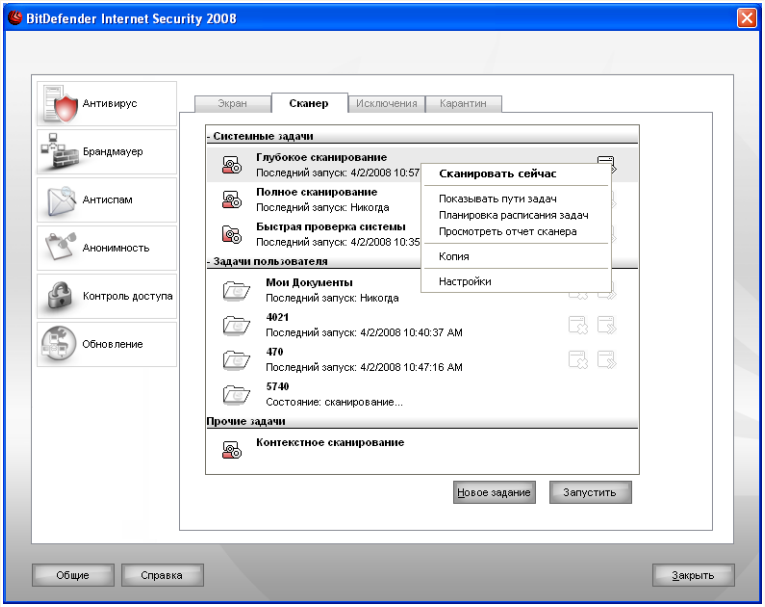
Замечание
Недоступно для системных задач. Вы не можете удалить системные задачи.

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

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

8.2.2. Использование Выпадающего меню

Для каждой задачи имеется



Выпадающее меню

выпадающее меню, открывающееся щелчком правой кнопки мыши по выбранной задаче.

В выпадающем меню имеются следующие команды:

- **Проверить сейчас** - запуск выбранной задачи, немедленное начало процесса проверки.
- **Сменить объект сканирования** - открывает окно **Свойства**, вкладку **Путь проверки**, где можно изменить объект проверки для выбранной задачи.

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

- **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.

- **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.

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

8.2.3. Создание задач сканирования

Создать задачу сканирования, использую один из следующих способов:

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

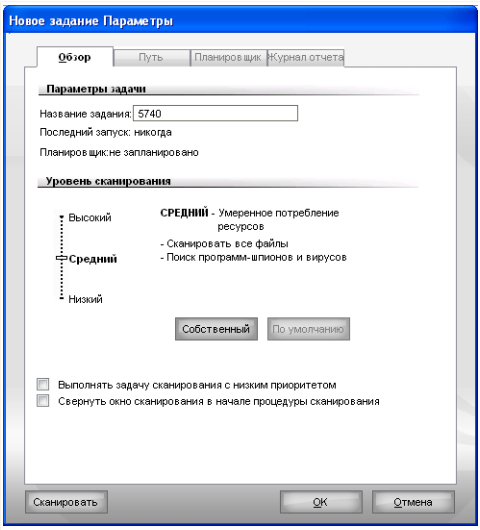
8.2.4. Настройка задач проверки

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

Замечание
Чтобы получить больше информации, просмотрите журналы и таблицу **Журналы**, обратитесь к «*Просмотр журнала проверок*» (p. 77).

Конфигурация настроек сканирования

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



Краткий обзор

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

Выбор уровеня проверки

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

Существует 3 уровня проверки:

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

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

Имеется ряд общих настроект для процесса проверки:

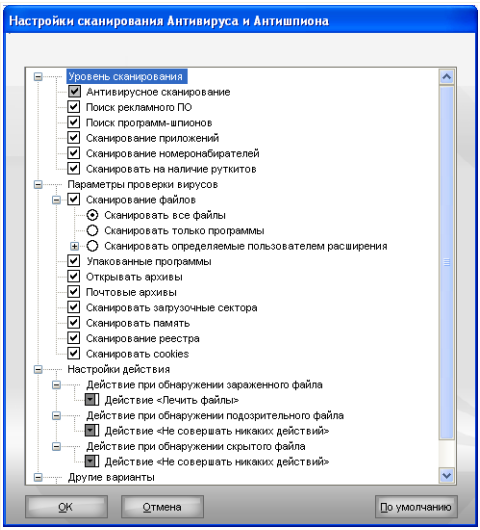
Настройка	*Описание*
Выполнить задачу с низким приоритетом	Уменьшается приоритет процесса проверки. Таким способом Вы ускоряете работу других программ, но увеличиваете время, необходимое для завершения процесса проверки.
Свернуть окно проверки в панель задач при запуске	Окно проверки свертывается в системный трей. Чтобы открыть его, следует дважды щелкнуть на значке BitDefender.

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

Настройка уровеня проверки

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

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



Настройки проверки

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

Опции сканирования сгруппированы в пять категорий:

- **Уровень проверки**
- **Опции проверки на вирусы**
- **Настройки действий**
- **Другие настройки**

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

  Доступны следующие варианты:

Настройка	Описание
Проверка на вирусы	Сканирование на известные вирусы. BitDefender также обнаруживает неполные или поврежденные тела вирусов, удаляя любую потенциально опасную угрозу безопасности Вашей системы.
Проверка на вредоносное рекламное ПО	Проверка на вредоносное рекламное ПО. Эти файлы будут считаться зараженными. Программное обеспечение, которое включает компоненты этого ПО, может прекратить работу, если выбрана эта настройка.
Проверка на шпионы	Проверка на известные программы-шпионы. Обнаруженные файлы будут считаться инфицированными.
Проверка на приложения	Сканирование приложений (`.exe` и `.dll` файлов).
Проверка на номеронабирателей	Проверка на приложения, набирающие дорогие телефонные номера. Обнаруженные файлы будут считаться инфицированными. Программное обеспечение, включающее в себя компоненты, осуществляющие набор номеров, могут перестать работать при включении данной опции.
Проверка на руткиты	Проверка на скрытые объекты (файлы и процессы), известные как руткиты.

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

  Доступны следующие варианты:

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`;

Настройка		Описание
		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 ";".
Открыть запакованные программы		Проверяются запакованные файлы.
Открыть архивы		Проверка внутри архивов.
Открыть почтовые архивы		Проверка внутри почтовых архивов.
Проверить загрузочные секторы		Проверка загрузочных секторов системы.
Проверка памяти		Проверка памяти на вирусы и прочие вредоносные программы.
Проверка записей системного реестра		Проверка записей системного реестра.
Проверка файлов Cookies		Проверка файлов Cookies.

- Укажите действие, которое следует предпринять по отношению к зараженным или подозрительным файлам в **Настройка действий**. Вы можете указать различные действия для разных категорий.
  - Выбрерите действие, которое будет применено над зараженными файлами. Доступны следующие варианты:

Действие	Описание
Никаких (только объекты)	Не выполняются никакие действия с зараженными файлами. Названия этих файлов появятся в файле отчета.
Вылечить файлы	Выполняется лечение зараженных файлов.
Удалить файлы	Зараженный файл удаляется немедленно, без предупреждения.

Действие	Описание
Переместить файлы в карантин	Зараженные файлы перемещаются в Карантин.

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

Действие	Описание
Никаких (только объекты)	Не выполняются никакие действия с подозрительными файлами. Названия этих файлов появятся в файле отчета.
Удалить файлы	Подозрительные файлы удаляются немедленно, без предупреждения.
Переместить файлы в карантин	Подозрительные файлы перемещаются в Карантин.

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

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

Действие	Описание
Никаких (только объекты)	Не выполняются никакие действия со скрытыми файлами. Названия этих файлов появятся в файле отчета.
Переместить файлы в карантин	Скрытые файлы перемещаются в Карантин.
Сделать видимым	Выявить скрытые файлы, так что Вы сможете их просмотреть.

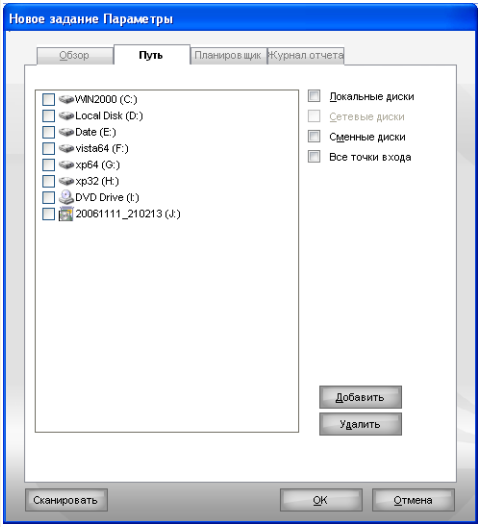
Замечание
Если Вы выберите опцию игнорировать обнаруженные файлы, или выбранное Вами действие не будет выполнено, Вам будет предложено выбрать действие при помощи мастера проверки.

- Чтобы запрашивать разрешение на отправку всех подозрительных файлов в Лабораторию BitDefender после окончания процесса проверки, отметьте поле **Отправлять подозрительные файлы в Лабораторию BitDefender** в категории **Прочие опции**.

Чтобы загрузить настройки по умолчанию, нажмите **По умолчанию**. Нажмите **OK**, чтобы сохранить изменения и закройте окно.

Настройка сканирования

Чтобы увидеть результаты сканирование после запуска выберите и нажмите на **Просмотр журнала проверок**. Появится следующее окно:



Сканировать

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

В этом разделе находятся следующие кнопки:

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

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

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

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

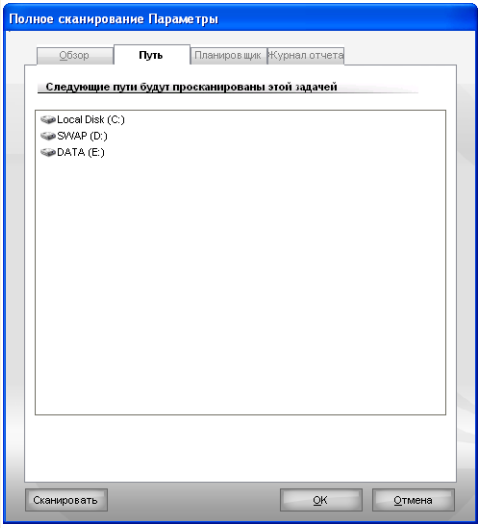
Замечание
Если Вы хотите проверить на наличие вирусов весь компьютер, поставьте значок в поле **Все объекты**.

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

Просмотр цели сканирования системных задач

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

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



Цель сканирования из задачи "Полное сканирование системы"

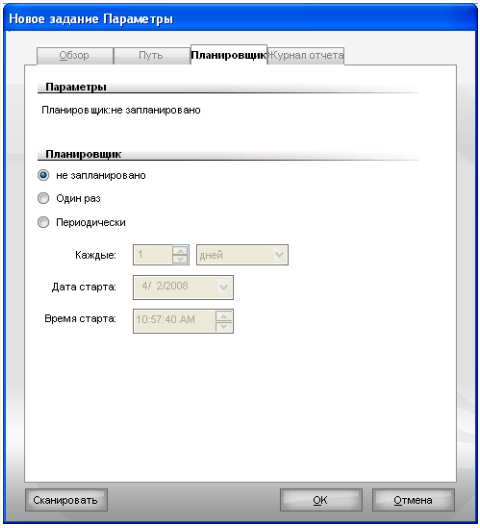
Полное сканирование системы и **Глубокое сканирование системы** просканирует все локальные диски, в то время как **Быстрое сканирование системы** просканирует только папки `Windows` и `Program Files`.

Нажмите **OK**, чтобы закрыть окно. Чтобы запустить задачу, нажмите **Сканировать**.

Планирование задач сканирования

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

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



Планировщик

Вы можете просмотреть запланированные задачи, если такие есть.

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

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

8.2.5. Сканирование объектов

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

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

Методы сканирования

BitDefender имеет четыре типа сканирования по требованию:

- Немедленная проверка - запуск задачи проверки из списка системных / определенных пользователем.
- Контекстная проверка - щелкните правой клавишей мыши на файле или папке и выберите BitDefender Antivirus 2008.
- Проверка с перетаскиванием - перетащите файл или папку на Панель состояния проверки;
- Ручная проверка - непосредственный выбор файлов и папок для сканирования.

Немедленная проверка

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

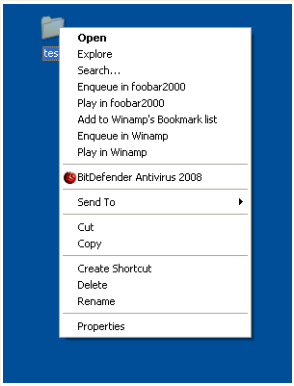
Чтобы запустить задачу сканирования, используйте один из следующих методов:

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

Появится Сканер BitDefender и начется сканирование. Больше информации найдете «*Сканер BitDefender*» (p. 72).

Проверка через контекстное меню

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



Проверка через контекстное меню

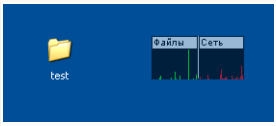
Щелкните правой кнопкой мышки на файле или папке, которые необходимо проверить, и выберите **BitDefender Antivirus 2008**.

Появится Сканер BitDefender и начется сканирование. Больше информации найдете «*Сканер BitDefender*» (p. 72).

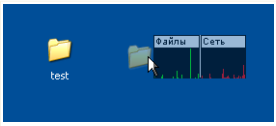
Вы можете изменить настройки проверки и просмотреть файл отчета с помощью **Свойств** в окне задачи **Проверка через контекстное меню**.

Проверка перетаскиванием

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



Тяните Файл



Переместите файл

Появится Сканер BitDefender и начется сканирование. Больше информации найдете «*Сканер BitDefender*» (p. 72).

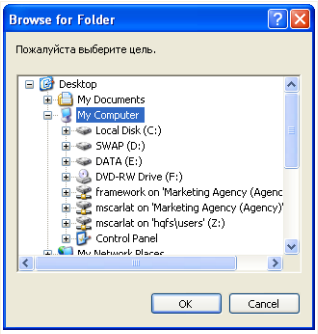
Ручное сканирование

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

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

Чтобы выбрать объект, который будет просмотрен BitDefender, надо зайти в **Пуск → Программы → BitDefender 2008 → BitDefender Manual Scan**.

Появится следующее окно:



Ручное сканирование

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

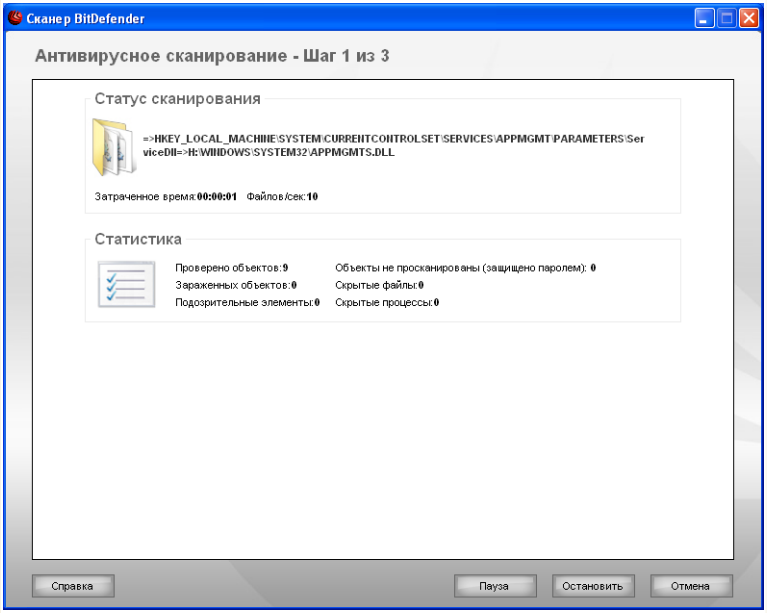
Появится Сканер BitDefender и начется сканирование. Больше информации найдете «*Сканер BitDefender*» (p. 72).

Сканер BitDefender

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

Шаг 1/3 - Сканирование

BitDefender начнет проверку выбранных объектов.



Сканирование

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

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

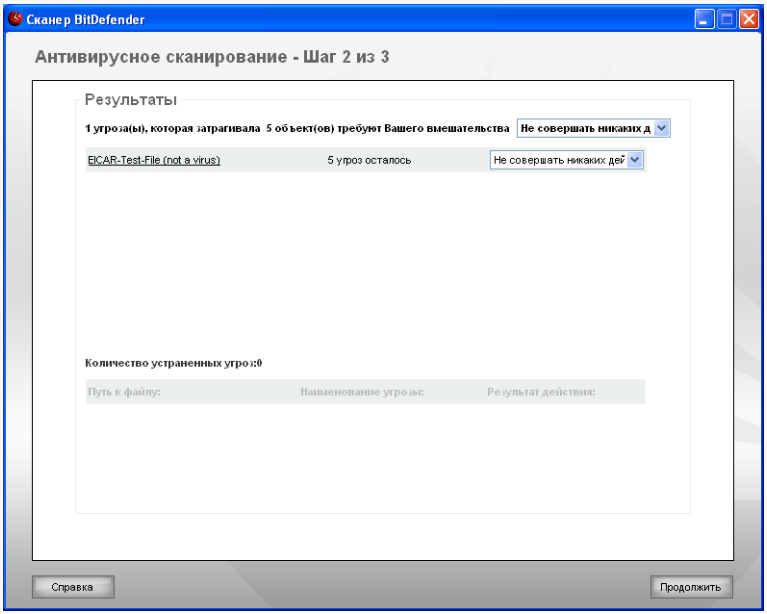
Чтобы временно приостановить процесс проверки, нажмите **Пауза**. Чтобы продолжить проверку, нажмите **Возобновить**.

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

Дождитесь окончания сканирования BitDefender

Шаг 2/3 - Выберите Действия

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



Действия

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

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

Для каждой группы проблем Вы можете выбрать общее действие, либо есть возможность выбрать отдельное действие для каждой проблемы.

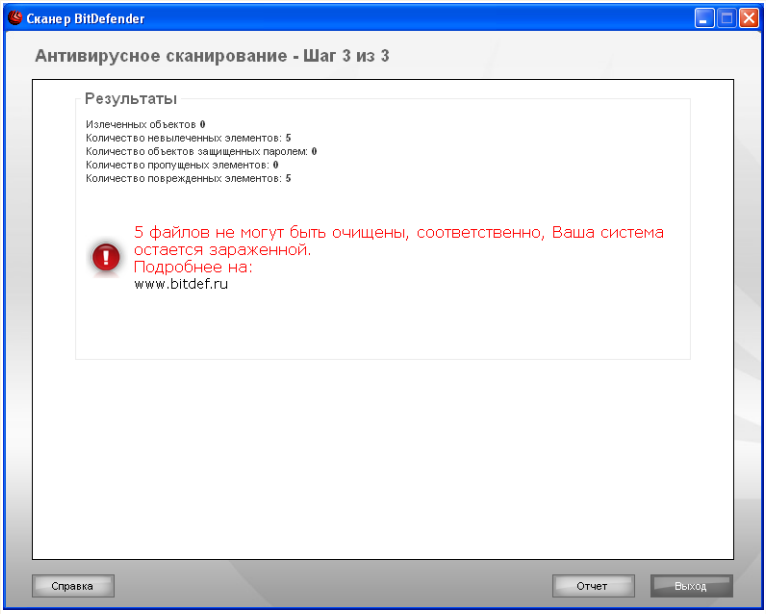
Доступны следующие варианты:

Действие	Описание
Ни чего не делать	Над обнаруженными файлами не будет производиться никаких действий.
Вылечить	Выполняется лечение зараженных файлов.
Удалить	Удаление обнаруженных файлов.
Раскрыть	Сделать скрытые объекты видимыми.

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

Шаг 3/3 - Просмотр результатов

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



Краткий обзор

Здесь Вы можете просмотреть краткий обзор. Отчеты автоматически сохраняются в разделе Журнал событий в окне **Свойства** соответствующей задачи.

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

Нажмите **Выход**, чтобы закрыть окно.

BitDefender не может исправить некоторые проблемы

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

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

Обнаруженные BitDefender элементы, защищенные паролем

Категория защищенных паролем включает в себя два типа элементов: архивы и инсталляторы. Они не представляют реальной угрозы безопасности системы, только если не содержат зараженных файлов, да и в этом случае опасны, только если их запустить.

Чтобы убедиться, что эти элементы являются чистыми:

- Если защищенный паролем элемент - это архив, то распакуйте его и проверьте содержащиеся в нем файлы с помощью выборочного сканирования. Самый простой способ их просканировать - это щелкнуть правой кнопкой мышки на них и выберать **BitDefender Antivirus 2008** из меню.
- Если защищенный паролем элемент - это инсталлятор, то убедитесь, что функция защиты в режиме реального времени включена, перед тем, как запустить его. Если файл-инсталлятор заражен, BitDefender обнаружит и изолирует инфекцию.

Если Вы не хотите, чтобы BitDefender снова обнаруживал эти объекты, Вы должны добавить их в список исключений для процесса сканирования. Чтобы добавить исключение при сканировании, откройте консоль настроек, нажав **Настройки**, и затем перейдите на **Антивирус > Исключения** . Для просмотра дополнительной информации перейдите по ссылке Объекты, исключенные из сканирования.

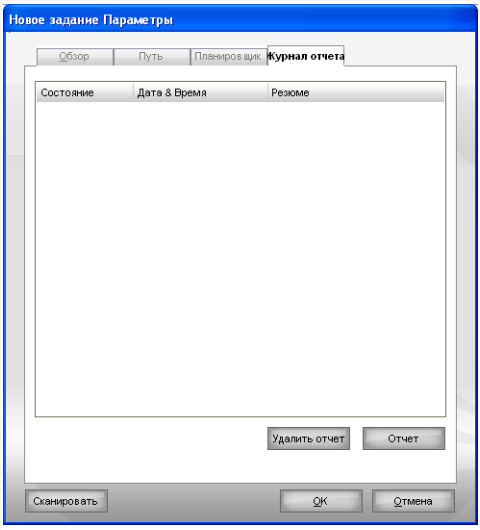
Обнаруженные BitDefender подозрительные файлы

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

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

8.2.6. Просмотр журнала проверок

Чтобы увидеть результаты сканирование после запуска выберите и нажмите на **Просмотр журнала проверок**. Появится следующее окно:



Журнал проверок

Здесь Вы можете увидеть файлы отчетов, которые генерировались каждый раз, когда выполнялась задача.

Для каждого файла Вам предоставляют информацию, относительно состояния записанного процесса сканирования, даты и времени, из отчета результатов сканирования.

Доступны две кнопки:

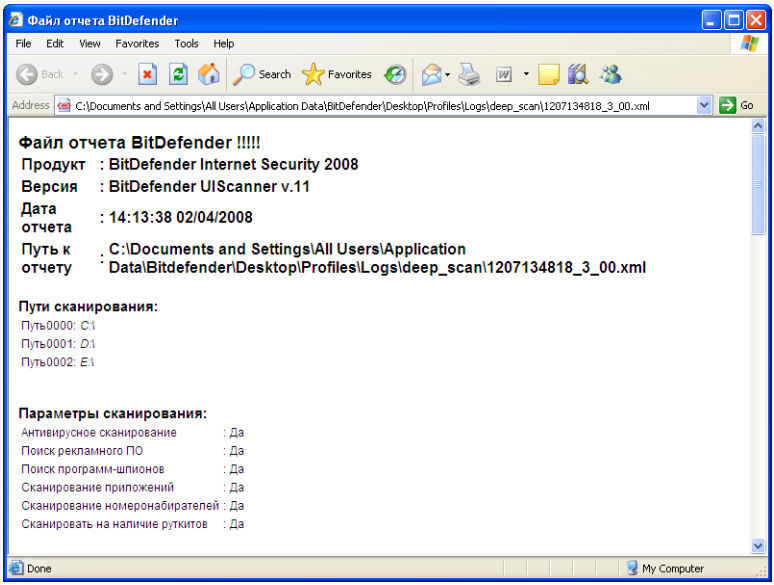
- **Удалить отчет** - удаление выбранного файла отчета.
- **Показать отчет** - просмотр выбранного файла отчета. Отчет сканирования откроется в вашем web-браузере по умолчанию.

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

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

Пример отчета проверок

Следующий рисунок представляет собой пример файла отчета сканирования:



Пример отчета проверок

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

8.3. Объекты, исключенные из сканирования

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

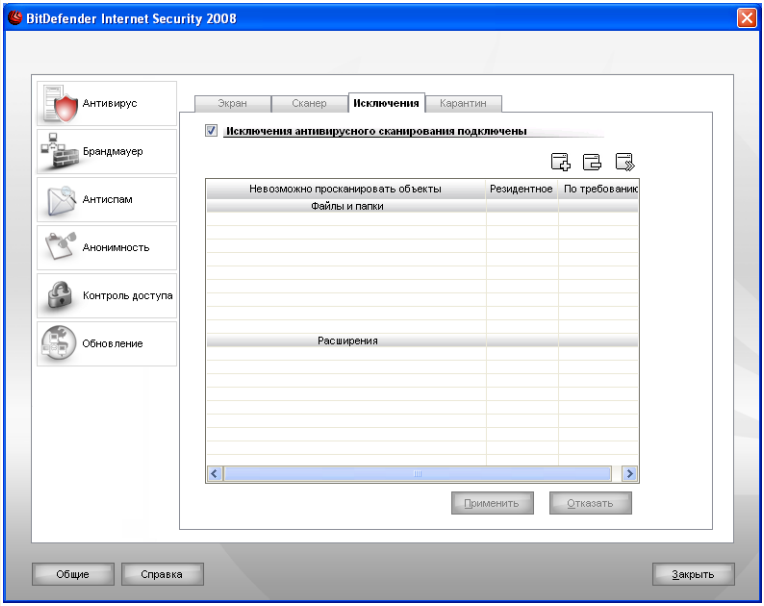
BitDefender позволяет исключать объекты при входной проверке и/или проверки по требованию. Данная функция предназначена для уменьшения времени на проверку и исключения вмешательства в процесс Вашей работы.

Два типа объектов могуть быть исключены из сканирования:

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

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

Чтобы просмотреть и изменить список исключаемых объектов, в консоли настроек нажмите **Антивирус>Исключения** Появится следующее окно:



Исключения

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

Замечание
Указанные здесь исключения НЕ распространяются на контекстную проверку.

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

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

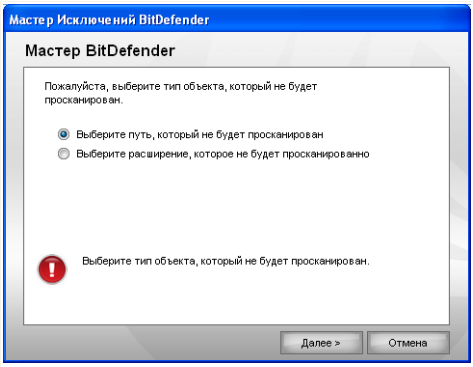
Замечание
Вы также можете нажать правой кнопкой мыши на объекте и воспользоваться пунктами меню для его редактирования или удаления.

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

8.3.1. Исключение путей для сканирования

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

Шаг 1/3 - Выберите тип объекта

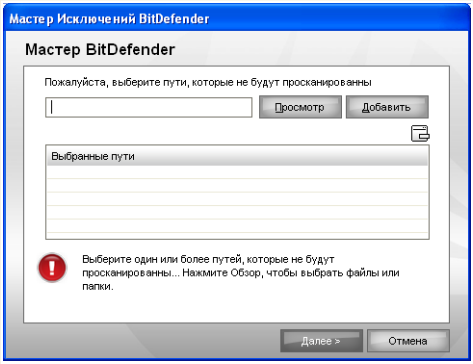


Тип объекта

Выберите опцию для исключения пути из сканирования.

Нажмите **Далее**.

Шаг 2/3 - Задайте пути исключения



Пути исключения

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

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

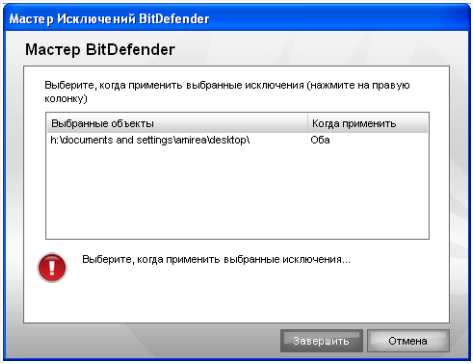
Замечание
Если указанный путь не существует, появится сообщение об ошибке. Нажмите **OK** и проверьте правильность пути.

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

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

Нажмите **Далее**.

Шаг 3/3 - Выберите тип сканирования



Тип сканирования

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

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

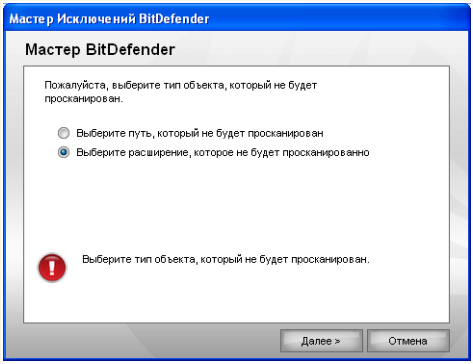
Нажмите **Завершить**.

Нажмите **Применить**, чтобы сохранить изменения.

8.3.2. Исключение расширений из сканирования

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

Шаг 1/3 - Выберите тип объекта

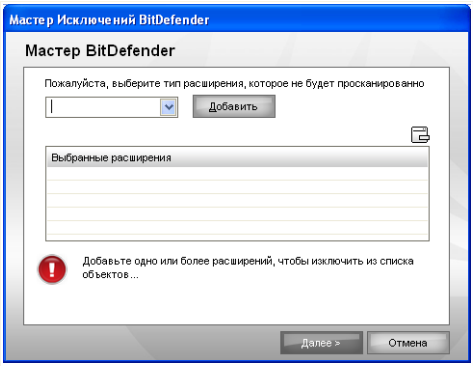


Тип объекта

Выберите опцию, которая исключает расширение из сканирования.

Нажмите **Далее**.

Шаг 2/3 - Задайте расширения, которые необходимо исключить



Исключение расширений

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

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

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

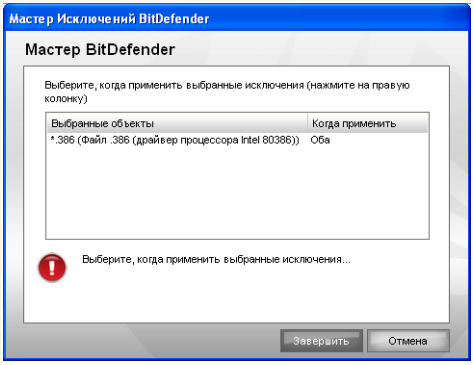
- Тип расширения, которое должно быть исключенно из сканирования, в редактирующей области и нажмите **Добавить**.

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

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

Нажмите **Далее**.

Шаг 3/3 - Выберите тип сканирования



Тип сканирования

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

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

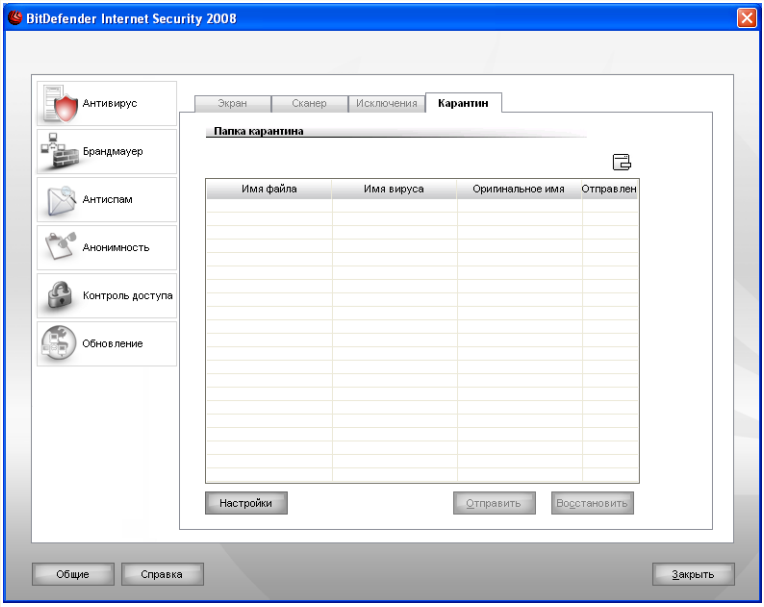
Нажмите **Завершить**.

Нажмите **Применить**, чтобы сохранить изменения.

8.4. Область Карантина

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

Нажмите **Антивирус>Карантин** в консоли настроек, чтобы просмотреть и выполнить действия над файлами в карантине, а также установить настройки карантина.



Карантин

8.4.1. Управление изолированными файлами

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.

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

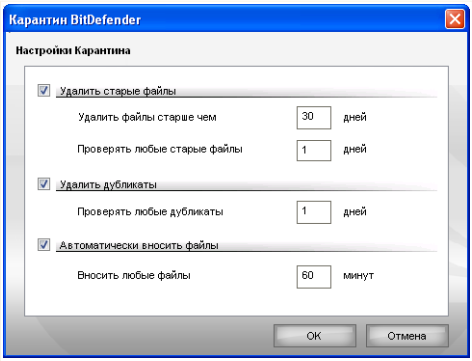
Чтобы удалить выбранный файл из карантина, нажмите кнопку **Удалить**. Если Вы хотите восстановить выбранный файл в его первоначальное местоположение, нажмите **Восстановить**.

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

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

8.4.2. Конфигурация настроек Карантина

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



Настройки карантина

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

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

Замечание
По умолчанию, BitDefender ежедневно проверяет старые файлы и удаляет файлы, старше 10 дней.

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

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

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

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

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

9. Брандмауэр

Брандмауэр защищает ваш компьютер от несанкционированных проникновений и передачи информации. Как страж у ворот, он бдительно следит за вашими подключениями к сети Интернет и определяет, какие данные пропускать в Интернет, а какие блокировать.

Замечание
Брандмауэр просто необходим, если Вы пользуетесь широкополосным подключением или подключением по цифровой абонентской линии DSL.

В "невидимом режиме" Ваш компьютер скрыт от вредоносным программ и хакеров. Модуль брандмауэра может автоматически определять и защищать от сканирования портов (поток пакетов, отправляемых на компьютер с целью выявления "точек доступа", часто является подготовкой для сетевых атак).

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

- Ознакомление с Брандмауэром
- Статус Брандмауэра
- Защита трафика
- Дополнительные настройки
- Активность Брандмауэра
- Сетевые зоны

9.1. Ознакомление с Брандмауэром

Брандмауэр BitDefender разработан для того, чтобы обеспечить лучшую защиту для Ваших сетевых и Интернет соединений, без необходимости ручной настройки. Независимо от того, подключены ли Вы напрямую к сети Интернет. К одной сети или к нескольким локальным сетям (Ethernet, беспроводная сеть, VPN или другой тип сетевого соединения), в надежной или не надежной зоне, брандмауэр произведет самостоятельную настройку, чтобы приспособиться к соответствующей ситуации.

По умолчанию BitDefender автоматически определяет настройки сетевых соединений на Вашем компьютере и создает соответствующий профиль брандмауэра. Он также добавляет обнаруженные сетевые соединения в профиль в виде надежных или не надежных зон, в зависимости от их настройки.

9.1.1. Что такое профили брандмауэра?

Профиль брандмауэра - ряд правил, которые контролируют сетевые приложения / Доступ в Интернет.

В зависимости от настройки сетевых соединений на Вашем компьютере, BitDefender автоматически создает определенный тип профиля. Создаваемый профиль содержит правила доступа в сеть и элементарные правила доступа в Интернет, необходимые системным приложениям и компонентам BitDefender.

Замечание
Независимо от количества сетевых соединений на Вашем компьютере, создается единый профиль брандмауэра.

Существует три типа базовых профиля:

Профиль	*Описание*
Прямое подключение	Содержит элементарные правила доступа в Интернет, рекомендованные для конфигурации сетевого соединения, чтобы обеспечить прямой доступ в Интернет. Правила не позволяют сетевым пользователям получать доступ к Вашему компьютеру, либо Вам получать доступ к сетевым ресурсам.
Ненадежная	Содержит правила доступа к сети, рекомендованные для настройки сетевого соединения, связанного с ненадежной сетью. Правила позволяют Вам просматривать сетевые ресурсы, но не позволяют другим сетевым пользователям получить доступ на Ваш компьютер.
Надежная	Содержит правила доступа к сети, рекомендованные для настройки сетевого соединения, связанного с надежной сетью. Никаких ограничений на доступ по сети нет. Это означает, что Вы имеете доступ ко всем общим сетевым ресурсам, сетевым принтерам и прочим сетевым ресурсам. В то же время, пользователи сети могут получить доступ к Вашему компьютеру и к Вашим ресурсам общего пользования.

По мере того, как приложения осуществляют попытку соединений с Интернет, соответствующие правила дополняются в Вашем профиле Вы можете выбрать, разрешать или запрещать доступ в Интернет по умолчанию приложений, правила для которых не были созданы, либо разрешать доступ по умолчанию только приложениям из списка разрешенных, а для всех остальных запрашивать разрешение.

Замечание

Чтобы указать правила доступа для приложений, которые пытаются соединиться с Интернет в первый раз, перейдите в раздел Статус и установите уровень защиты. Чтобы редактировать существующий профиль, перейдите в раздел Трафик и нажмите **Редактировать профиль**.

9.1.2. Что такое сетевые зоны?

Зоной сети является либо компьютер в сети, либо вся сеть в целом, полностью изолированные от Вашего компьютера или, наоборот, имеющие возможность обнаружить Ваш компьютер и подключиться к нему. С практической точки зрения, зона - это IP-адрес или диапазон IP-адресов, доступ с которых к Вашему компьютеру разрешен или запрещен.

По умолчанию, BitDefender автоматически добавляет зоны для определенных сетевых соединений. Зона создается путем создания в текущем профиле соответствующего правила доступа, применимого ко всей сети.

Существует два типа зон:

Тип зоны	*Описание*
Надежная зона	Компьюрепы из надежной сети могут получить доступ к Вашему компьютеру, а Вы к их. Все попытки соединений из этой зоны, а также все попытки соединения с Вашего компьютера к этой зоне разрешены. Если сеть добавляется как надежная зона, Вы имеете неограниченный доступ ко всем общим ресурсам, сетевым принтерам и прочим сетевым ресурсам. В то же время, пользователи сети могут получить доступ к Вашему компьютеру и к Вашим ресурсам общего пользования.

Тип зоны	Описание
Ненадежная зона	Компьютеры из не надежной сети не могут получить доступ к Вашему компьютеру, так и Вы не сможете получить доступ к их компьютерам. Все попытки соединений из этой зоны, а также все попытки соединения с Вашего компьютера к этой зоне заблокированы. Поскольку в "невидимом" режиме обмен пакетов по протоколу ICMP запрещен, Ваш компьютер становится практически невидимым для других компьютеров в данной зоне.

Замечание

Чтобы редактировать зоны, перейдите в раздел Зоны. Чтобы изменить правило для соответствующей зоны, перейдите в раздел Трафик и нажмите **Редактировать профиль**.

9.1.3. Команды Брандмауэра

При перезагрузке системы после установки, BitDefender автоматически определяет сетевые настройки Вашего компьютера, создает соответствующий базовый профиль и добавляет зоны, в зависимости от найденных сетей.

Замечание

Если Вы соединяетесь непосредственно к Интернет, то никакая зона сети не создана для соответствующей настройки сети. Если Вы связаны с более чем одной сетью, то зоны добавляются в зависимости от конкретной сети.

Каждый раз при изменении настроек сетевых соединений, независимо от того, подключились ли Вы к другой сети, либо отключили существующее соединение, создается новый профиль брандмауэра. Соответственно, в это же время корректируются и сетевые зоны.

При создании нового профиля брандмауэра старый сохраняется, так что его можно снова использовать, когда Вы возвратитесь к соответствующей конфигурации сетевых соединений.

В зависимости от конфигурации сети, BitDefender будет настраивать себя соответственно. Как Брандмауэр BitDefender нестраивается по умолчанию:

- Если Вы подключаетесь к Интернет напрямую, независимо от того, подключены ли Вы еще и к другим сетям, создается профиль Прямого соединения. В противном случае, BitDefender создаст профиль брандмауэра для ненадежных сетей.

Замечание

фактически безопасность для надежных профилей, по умолчанию не создано. Чтобы создать надежный профиль, Вы должны перезагрузить существующий профиль. Более подробную информацию найдете здесь *«Переопределение профилей»* (p. 104).

- Зоны добавлены в зависимости от конфигурации сети.

Тип зоны	*Конфигурация сети*
Надежная зона	**Частный IP-адрес без шлюза** - компьютер является частью локальной сети (LAN) и не подключен к Интернет. Примером такой конфигурации является домашняя сеть, созданная для того, чтобы члены семьи могли совместно использовать файлы, принтеры и другие ресурсы.
	Частный IP с домен-контроллером - компьютер является частью локальной сети (LAN) и подключается к домену. Примером такой ситуации является офисная сеть, которая позволяет пользователям совместно использовать файлы или другие ресурсы внутри домена. Домен подразумевает существование ряда политик, к которым подчиняются компьютеры этого домена.
Ненадежная зона	**Открыть (не защищённое) беспроводное соединение** - Компьютер является частью беспроводной локальной сети (WLAN). Пример такой ситуации, когда Вы получаете доступ к интернет используя точку доступа в общественном месте.

Замечание

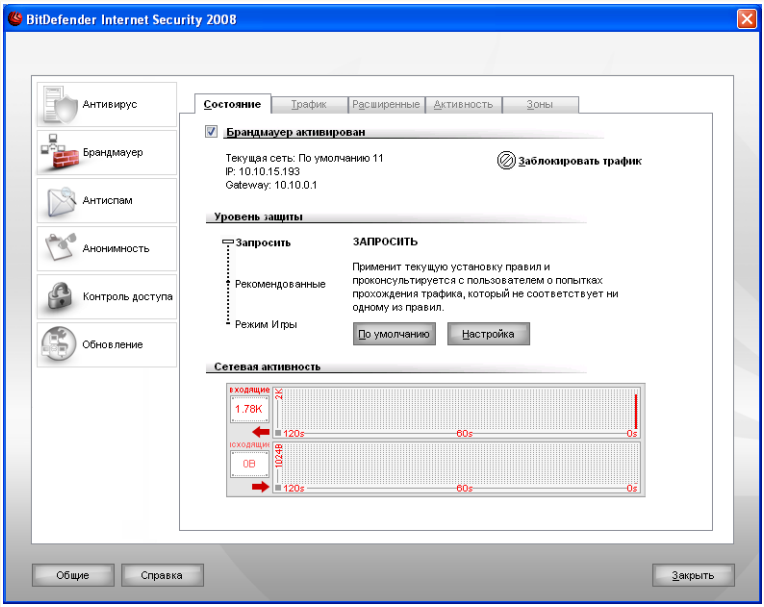
Зоны не создаются для некоторых конфигураций сети, таких как:

- **Внешний IP** - Компьютер напрямую выходит в Интернет.
- **Частный IP со шлюзом, но без домен-контроллера** - компьютер является частью локальной сети (LAN), но не является частью домена и подключается к Интернет через шлюз. Пример такой ситуации - школьная сеть, которая позволяет пользователям использовать обшие файлы или другие ресурсы.

- Режим Невидимости включен.
- VPN и удалённое подключение разрешены.
- ICS не разрешен для ненадежных зон.
- Приложениям из Списка разрешенных доступ предоставляется автоматически, в то время как для всех остальных приложений при первой попытке соединения будет запрос на подтверждение.

9.2. Статус Брандмауэра

Чтобы настроить защиту Брандмауэра, нажмите **Брандмауэр>Статус** в консоли настроек. Появится следующее окно:



Статус Брандмауэра

В этом разделе Вы можете включить/отключить модуль **Брандмауэр**, блокировать весь сетевой/интернет трафик и устанавливать поведения для новых событий.

Важно
Чтобы обезопасить компьютер от атак через Интернет, **Брандмауэр** должен быть включен.

Чтобы заблокировать весь трафик локальной сети/Интернет, нажмите **Блокировать трафик** и потом **Да**. Это позволит изолировать Ваш компьютер от любого другого компьютера в сети.

Чтобы разблокировать трафик, нажмите **Разблокировать трафик**.

В нижней части раздела Вы можете увидеть статистику BitDefender по входящему и исходящему трафику. График активности показывает объем трафика в сети Интернет за последние две минуты.

Замечание
График активности появляется даже в том случае, если **Брандмауэр** выключен.

9.2.1. Конфигурация уровня защиты

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

Существует 3 уровня защиты:

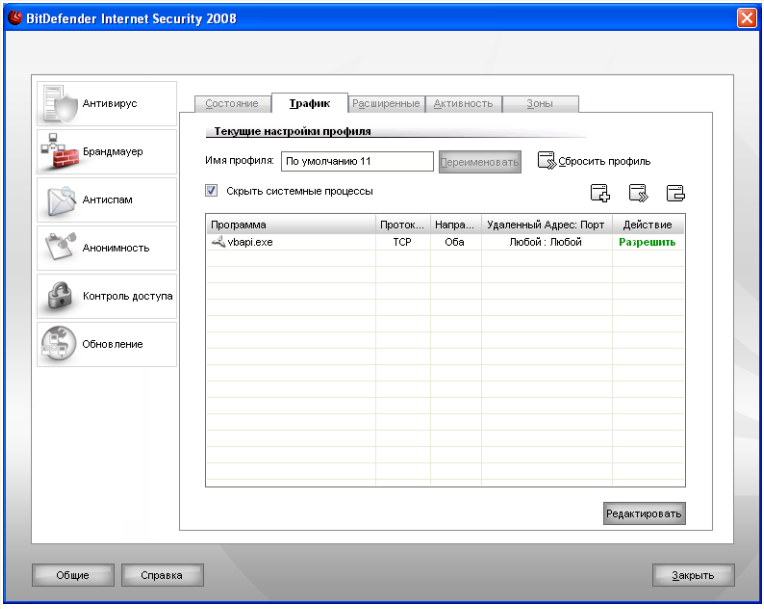
Уровень защиты	*Описание*
Режим Игры	Разрешает без предупреждения весь трафик, который не описан в установленных на данный момент правилах. Настоятельно не рекомендуем использовать этоту политику, но он может быть полезен системным администраторам и геймерам.
Разрешить рекомендованные	Разрешает все исходящие соединения от программ, известных BitDefender как легитимные. В разделе Трафик можно просмотреть все правила для них, по мере добавления. Пограммы из разрешенного списка - это в основном приложения, используемые во всем мире. Сюда входят самые распространенные браузеры, аудио и видео проигрыватели, программы общения и обмена файлами, а также серверные клиенты и операционные системы. Если Вы хотите просмотреть

Уровень защиты	Описание
	список программ в разрешенном списке, нажмите **Разрешенные**.
Запрашивать	Применяет текущие правила и консультируется с Вами обо всех попытках трафика, который не соответствуют ни одному из текущих правил.

Нажмите **По умолчанию**, чтобы установить правило по умолчанию (**Разрешать рекомендованные**).

9.3. Контроль трафика

Чтобы исправить правила брандмауэра текущего профиля, нажмите **Брандмауэр>Трафик** в консоли управления. Появится следующее окно:



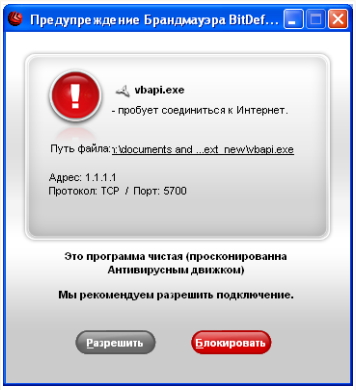
Контроль трафика

В этом разделе Вы можете определить, какие входящие или исходящие подключения следует разрешить/запретить, создавая правила с определенными протоколами, портами, приложениями и/или удаленными адресами.

Правила можно добавлять автоматически (с помощью окна предупреждения) или вручную (нажмите кнопку **Добавить** и выберите параметры для правила).

9.3.1. Автоматическое добавление правил

С включенным **Брандмауэром**, BitDefender будет спрашивать Вашего разрешения всякий раз, когда будет сделана попытка соединиться с Интернет:



Предупреждение брандмауэра

В появившемся окне Вы увидите следующее: приложение, пытающееся получить доступ в Интернет, использует протокол и порт через который оно пытается подключиться.

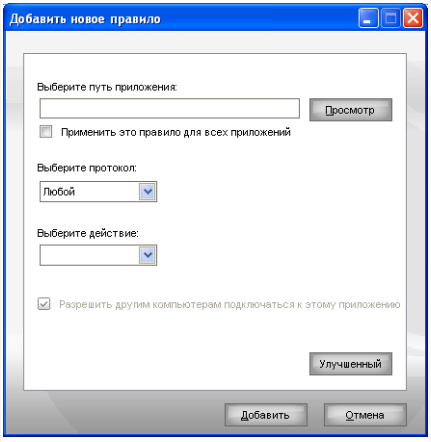
Нажмите **Разрешить**, чтобы разрешить всь трафик (входящий и исходящий) для данного приложения с локального компьютера или из любого другого места при помощи IP протокола и любого порта. Если Вы нажмете **Блокировать**, то возможность доступа в интернет через IP протокол для данного приложения будет полностью заблокирована.

В зависимости от Вашего ответа будет создано правило, которое тут же применится и запишется в таблицу. При следующей попытке соединения данного приложения по умолчанию будет использоваться это правило.

Важно
Разрешите входящие подключения только с IP-адресов или доменов, которым Вы полностью доверяете.

9.3.2. Добавление правил вручную

Нажмите **Добавить правило** и выберите параметры для правила. Появится следующее окно:



Добавление правил

Чтобы добавить новое правило для брандмауэра, следуйте следующим шагам:

1. Выберите приложение, для которого будет создано новое правило.

   Выберите приложение, нажмите **Обзор**, и нажмите **ОК**.

   Если Вы хотите создать правило для всех приложений, выберите **Применить это правило для всех приложений**.
2. Выберите протокол для которого примените правило.

   В окне появляется список наиболее часто употребляемых протоколов. Выберите нужный тип протокола (на который распространяется действие правила) из соответствующего раскрывающегося меню или выберите опцию **Любой**, чтобы выделить сразу все протоколы.

   Данная таблица содержит список протоколов, из которых Вы можете выбрать, а также небольшое описание каждого:

Протокол	*Описание*
ICMP	Internet Control Message Protocol - Протокол контрольных сообщений интернет – это расширенная версия Интернет-протокола (IP). ICMP поддерживает пакеты, содержащие сообщения об ошибках, а также контрольные и информационные сообщения. Например, команда PING

Протокол	Описание
	использует протокол ICMP для тестирования подключения к сети Интернет.
TCP	TCP - Протокол управления передачей позволяет двум устройствам установить соединение и начать обмен данными. TCP гарантирует доставку всех данных, а также то, что все пакеты данных будут доставлены в том порядке, в каком они были отправлены.
UDP	UDP (User Datagram Protocol) Протокол передачи дейтаграмм пользователя – это быстрый протокол транспортного уровня на основе IP. Он часто применяется в играх и других приложениях с использованием видео.

3. Выберите действие правила из соответствующего меню.

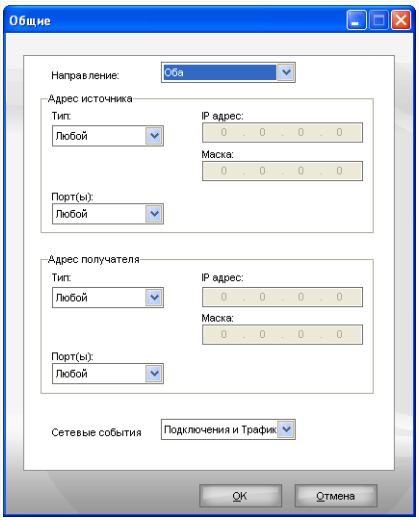
Действие	Описание
Разрешить	Указанному приложению будет разрешен доступ в сеть/Интернет при определенных обстоятельствах.
Запретить	Указанному приложению будет запрещен доступ в сеть/Интернет при определенных обстоятельствах.

4. Если ранее был выбран протокол TCP или UDP, вы можете указать, применимо ли данное правило тогда, когда приложения выступает в роли сервера.

   Отметьте поле **Позволять другим компьютерам осуществлять соединение с данным приложением**, чтобы применить действие ко всем сетевым событиям. Таким образом, Вы даете право или запрещаете приложению открывать порты.

   Если Вы хотите применить действие только для соединений по протоколу UDP или только для соединений по протоколу TCP, снимите галку из соответствующего поля.

Если Вы хотите изменить дополнительные параметры настройки для правила, нажмите**Дополнительно** . В появившемся окне можно выбрать следующее:



Дополнительные настройки правил

Вы можете конфигурировать следующее:

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

Тип	*Описание*
Исходящие	Правило применяется только к исходящему трафику.
Входящие	Правило применяется только к входящему трафику.
Входящие и исходящие	Правило применяется и ко входящему, и к исходящему трафику.

- **Источник адреса** - определяет источник адреса.

  Чтобы указать адрес источника, выберите тип адреса из меню и укажите необходимые данные. Доступны следующие варианты:

Тип	*Описание*
Любой	Правило применяется к любому адресу источника.

Тип	Описание
Хост	Правило применяется только, если источником служит указанный хост. Необходимо ввести IP-адрес хоста.
Сеть	Правило применяется только, если источником служит указанная сеть. Необходимо ввести IP-адрес и маску сети.
Собственная машина	Правило применяется только, если источником служит собственный компьютер. Если Вы используете несколько сетевых интерфейсов, выберите в меню сетевой интерфейс, по отношению к которому применяется правило. Если Вы хотите применить правило ко всем хостам - выберите **Любой**.
Локальная сеть	Данные правила применяются только в том случае, если источником является локальная сеть. Если Вы используете несколько сетевых интерфейсов, выберите в меню сетевой интерфейс, по отношению к которому применяется правило. Если Вы хотите применить правило ко всем локальным сетям - выберите **Любой**.

Если ранее был выбран протокол TCP или UDP, вы можете указать определенный порт или диапазон портов между 0 и 65535. Если Вы хотите применить правило ко всем портам - выберите **Любой**.

- **Адрес назначения** - укажите адрес назначения.

Чтобы указать адрес назначения, выберите тип адреса из меню и укажите необходимые данные. Доступны следующие варианты:

Тип	Описание
Любой	Данное правило применяется ко всем адресам назначения.
Хост	Данное правило применяется только, если адресом назначения является определенный хост. Необходимо ввести IP-адрес хоста.
Сеть	Данное правило применяется только, если адресом назначения является определенная сеть. Необходимо ввести IP-адрес и маску сети.

Тип	Описание
Собственная машина	Данное правило применяется только, если адресом назначения является собственный компьютер. Если Вы используете несколько сетевых интерфейсов, выберите в меню сетевой интерфейс, по отношению к которому применяется правило. Если Вы хотите применить правило ко всем хостам - выберите **Любой**.
Локальная сеть	Данное правило применяется только, если адресом назначения является локальная сеть. Если Вы используете несколько сетевых интерфейсов, выберите в меню сетевой интерфейс, по отношению к которому применяется правило. Если Вы хотите применить правило ко всем локальным сетям - выберите **Любой**.

Если ранее был выбран протокол TCP или UDP, вы можете указать определенный порт или диапазон портов между 0 и 65535. Если Вы хотите применить правило ко всем портам - выберите **Любой**.

- **Сетевые события** - если в качестве протоколов Вы выбрали TCP или UDP, выберите сетевые события , к которому применяется данное правило.

Нажмите **OK**, чтобы закрыть окно дополнительных настроек.

Нажмите **Добавить**, чтобы добавить правило брандмауэра.

9.3.3. Управление правилами

В таблице можно просмотреть уже существующие на данный момент правила для данного профиля.

Поставьте отметку в поле **Скрывать системные процессы**, чтобы скрыть правила, касающиеся системных процессов или процессов BitDefender.

Правила выведены в список в порядке приоритета, начиная сверху, причем первое правило имеет наибольший приоритет. Нажмите **Редактировать профиль**, чтобы перейти к виду **Подробнее**, где можно изменить приоритет правил, передвигая их вверх и вниз.

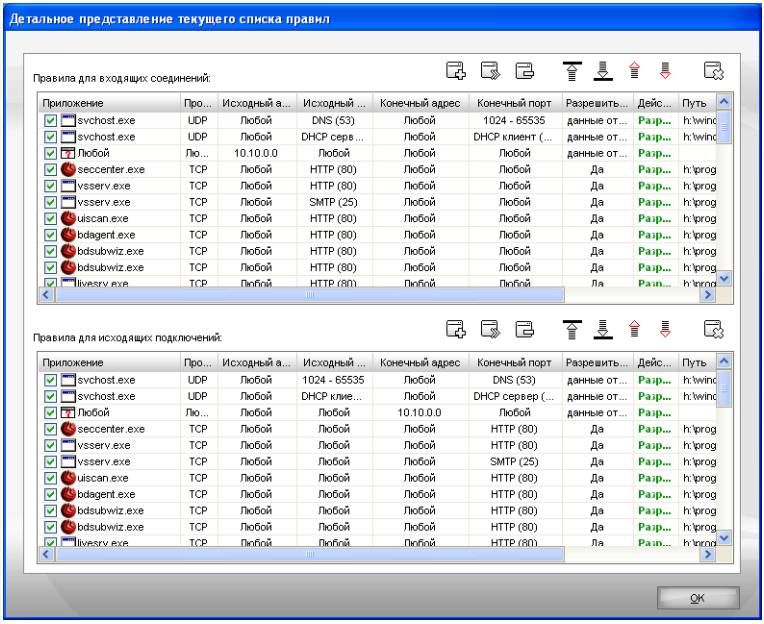
Чтобы удалить правило, выберите его и нажмите кнопку **Удалить правило**.

Чтобы изменить правило, выберите его и нажмите кнопку **Редактировать правило** или дважды нажмите на необходимом правиле.

Замечание
Имеется также контекстное меню, которое содержит следующие опции: **Добавить правило**, **Удалить правило** и **Редактировать правило**.

9.3.4. Модифицирование профилей

Вы можете изменить профиль, нажав **Редактировать профиль**. Появится окно следующего вида:



Подробный вид

Правила разделены на две категории: исходящие правила и входящие правила. Вы можете просмотреть название приложения и параметры правила для каждого правила (исходный адрес, адрес назначения, порты назначения, действие и т.д.).

Чтобы удалить правило, выберите его и нажмите кнопку **Удалить правило**. Чтобы удалить все правила, нажмите кнопку **Очистить список**. Чтобы изменить правило, либо выберите его и нажмите кнопку **Редактировать правило**, либо

дважды нажмите его. Чтобы временно отключить правило, не удаляя его, уберите галочку в соответствующем поле.

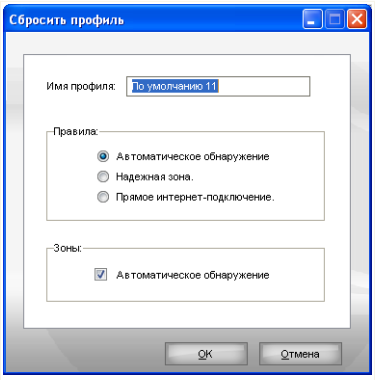
Вы можете увеличить или уменьшить приоритет правила. Нажмите кнопку **Передвинуть выше в списке**, чтобы увеличить приоритет выбранного правила на один уровень, или нажмите клавишу **Передвинуть ниже в списке**, чтобы уменьшить приоритет выбранного правила на один уровень. Чтобы назначить для правила наивысший приоритет, нажмите кнопку **Сделать первым**. Нажмите кнопку **Сделать последним**, чтобы назначить правилу наименьшей приоритет.

Замечание
Имеется также контекстное меню, оно содержит следующие опции: **Добавить правило**, **Редактировать правило**, **Удалить правило**, **Передвинуть выше**, **Передвинуть ниже** и **Очистить список**.

Нажмите **OK**, чтобы закрыть окно.

9.3.5. Переопределение профилей

Опытные пользователи могут воспользоваться возможностью изменить конфигурацию профиля брандмауэра, чтобы оптимизировать защиту брандмауэра или настроить ее с учетом собственных пожеланий. Чтобы переопределить настройки профиля брандмауэра, нажмите кнопку **Переопределить профиль**. Появится следующее окно:



Переопределить профилей

Вы можете конфигурировать следующее:

- **Имя профиля** - в соответствующем поле введите новое имя.
- **Правила** - укажите, какие типы правил должны быть созданы для системных приложений.

  Доступны следующие варианты:

Настройка	*Описание*
Автоматическое определение	Позволяет BitDefender самостоятельно обнаружить текущую сетевую конфигурацию и создать соответствующий набор элементарных правил.
Надежная сеть	Создает набор элементарных правил, соответствующих надежной сети.
Прямое подключение к Интернет	Создает набор элементарных правил, соответствующих прямому подключению к Интернет.

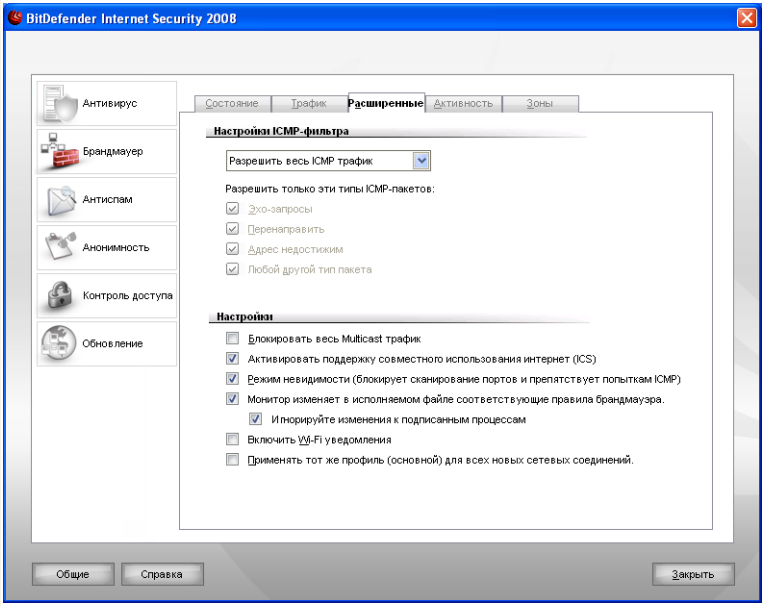
- **Зоны** - отметьте опцию **Автоматическое определение**, чтобы позволить BitDefender создать соответствующие зоны для выявленных сетей.

Нажмите **OK**, чтобы закрыть окно и переопределить профиль.

Важно
Все правила, которые Вы добавили в данном разделе будут потеряны, если Вы решите переопределить профиль брандмауэра.

9.4. Дополнительные настройки

Чтобы изменить дополнительные настройки брандмауэра BitDefender, нажмите **Брандмауэр>Дополнительно** в консоли настроек. Появится следующее окно:



Дополнительные настройки

В данном разделе вы можете изменить дополнительные настройки брандмауэра BitDefender. Дополнительные настройки позволяют Вам назначить правила фильтров для ICMP трафика (ICMP Настройки) и заблокировать многопотоковы трафик, расшарить Интернет соединение или сделает Ваш компьютер невидимым вредоносных программ и хакеров(Настройки).

9.4.1. Настройки ICMP фильтра

Из меню Вы можете выбрать одно из следующих правил фильтрации ICMP трафика:

- **Разрешить весь ICMP трафик** - разрешает весь ICMP трафик.
- **Блокировать весь ICMP трафик** - блокировка всего ICMP трафика.
- **Настроить фильтр ICMP** - настройка фильтрации CMP трафика. Здесь Вы можете выбрать, какие типы ICMP пакетов разрешить.

  Доступны следующие варианты:

Настройка	Описание
Отклик	Выбор этой опции позволяет использовать сообщения типа запрос отклика и ответный отклик. Запрос отклика– это ICMP сообщение, которое содержит пакет данных, передаваемых на сервер (хост), в ответ на которое должен последовать ответный отклик, также содержащий пакет данных. На все запросы отклика сервер должен дать ответные отклики, содержащие точные данные, полученные в сообщении запроса отклика. Ответный отклик- это ICMP сообщение, сгенерированное в ответ на ICMP сообщение запроса отклика, причем его использование является обязательным для всех серверов и маршрутизаторов.
Переадресовка	Это ICMP сообщение, в котором дается указание передающему серверу относительно переадресования его данных маршрутизации (чтобы передавать пакеты по альтернативному маршруту). Если для достижения принимающего сервера передающий сервер пробует отправлять данные через маршрутизатор (R1), а затем через другой маршрутизатор (R2), но при этом доступен также прямой путь от сервера до маршрутизатора R2, то переадресовка укажет этот альтернативный маршрут передающему серверу. При этом маршрутизатор будет продолжать передавать исходную дейтаграмму прежнему адресату. Однако, если дейтаграмма содержит данные маршрутизации, то сообщение переадресовки не будет посылаться даже при доступности лучшего маршрута.
Адресат недоступен	Это ICMP сообщение, которое сгенерировано маршрутизатором, чтобы сообщить клиенту, что сервер адресата является недостижимым, если дейтаграмма не имеет многоадресного адреса. Появление такого рода сообщений может быть вызвано следующими причинами: отсутствием

Настройка	Описание
	физического подключения к передающему серверу (бесконечное расстояние), неактивным состоянием указанного протокола или порта, а также необходимостью фрагментирования данных, защищенных от фрагментирования специальным флажком 'не фрагментировать'.
Пакеты любого другого типа	При выборе этой опции допускается прохождение любого другого пакета, помимо пакетов **Отклик**, **Адресат недоступен** или **Переадресовка**.

9.4.2. Конфигурация дополнительных настроек брандмауэра

Доступны следующие дополнительные настройки брандмауэра:

- **Блокировать весь многоадресный трафик** - блокировка всего получаемого многоадресного трафика .

  Многоадресный трафик - это трафик, адресуемый конкретной группе в сети. Пакеты отсылаются на специальный адрес, откуда клиенты могут их получать, в случае их согласия.

  Например, пользователь сети, у которого есть ТВ-тюнер, может транслировать видео-поток (отсылать каждому пользователю сети) или пользоваться многоадресной рассылкой (посылать его на специальный адрес). Компьютеры, прослушивающие многопользовательские адреса могут принимать или отказывать принимать пакеты. Если пакеты принимаются, видео-поток могут просмотреть все многоадресные клиенты.

  Значительное количество многоадресного трафика потребляет ресурсы и загружает канал. При включении данной опции все получаемые многоадресные пакеты будут игнорироваться. Однако, выбирать данную опцию не рекомендуется.
- **Включить общий доступ к подключению интернета (ICS)** - включает поддержку Общего доступа к подключению интернет (ICS).

Замечание
Эта опция не включает автоматически функцию ICS на Вашей системе, а только позволяет устанавливать соединения подобного типа, если данная функция включена в операционной системе.

Общий доступ к подключению интернет (ICS) позволяет пользователям локальной сети подключаться к интернет через Ваш компьютер. Эта функция полезна, если у Вас есть определенное подключение к Интернет (например, беспроводное), и Вы хотите позволить другим пользователям Вашей локальной сети им пользоваться.

Разделение доступа в Интернет с пользователями локальной сети приводет к повышенному потреблению ресурсов и имеет определнный риск. Он также занимает некоторые Ваши порты (открытые пользователями, использующими Ваше сетевое соединение).

- **Режим невидимости** - позволяет Вашему компьютеру быть "невидимым" для вредоносных программ и хакеров.

  Самым простым методом проверки того, что Ваш компьютер уязвим, является подключение к портам и ожидание ответов от них. Этот метод называется сканированием портов.

  Желательно, чтобы о существовании вашего компьютера, а тем более о его работе в сети Интернет, не знали ни хакеры, ни какие-либо хакерские программы. Опция **Режим «Невидимка»** будет блокировать ответ Вашего компьютера на все запросы о том, какие порты являются открытыми, или о местоположении Вашего компьютера.
- **Отслеживать изменения в файлах программ, которые соответствуют правилам брандмауэра** - проверка каждого приложения, осуществляющего попытку подключения к Интернет на наличие каких либо изменений в них с момента, когда было добавлено соответствующее правило, регулирующее доступ данного приложения. Если приложение было изменено, Вы будете предупреждены сообщением с просьбой уточнить стоит ли разрешать или запрещать данному приложению выход в Интернет.

  Обычно при обновлениях приложения изменяются. Но существует также вероятность, что они были изменены какими-либо вредоносными программами с целью заражения Вашего компьютера или других компьютеров в Вашей сети.

Замечание
Рекомендуем включать эту опцию и позволять доступ в Интернет только тем приложениям, которые, на Ваш взгляд, действительно могли измениться с

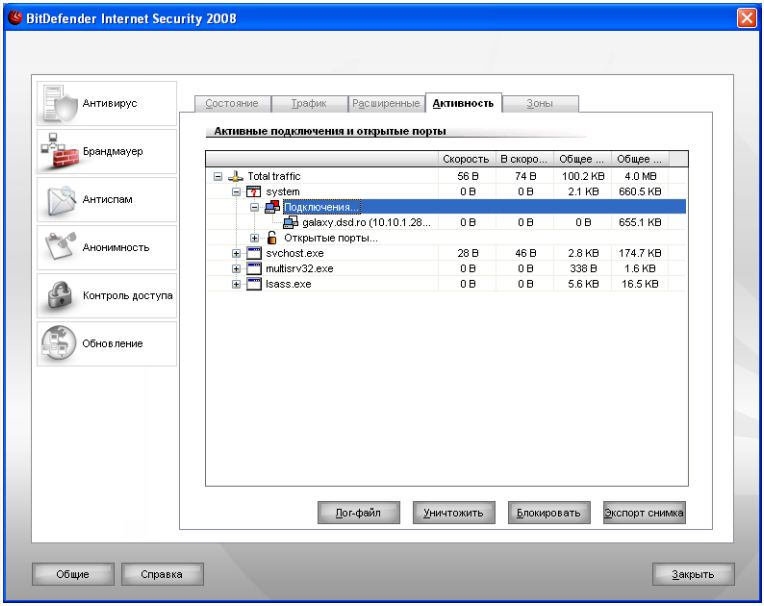
момента, когда было создано соответствующее правило доступа данного приложения в Интернет.

Зарегистрированным приложениям обычно стоит доверять больше. Вы можете выбрать опцию **Игнорировать изменения для зарегистрированных процессов** для того, чтобы разрешить зарегистрированным приложениям, которые были изменены, доступ в Интернет без Вашего уведомления о данном событии.

- **Включить уведомления Wi-Fi** - включение уведомлений Wi-Fi.
- **Применить тот же (основной) профиль ко всем новым сетям** - создает профиль брандмауэра по умолчанию (основной), дает ему название`Основная сеть`, и применяет его всегда, когда обнаруживает новую конфигурацию сети. Если Вы вернетесь к старой конфинурации сети, для которой задан профиль брандмауэра, то соответствующий профиль брандмауэра будет загружен вместо основного профиля.

9.5. Контроль соединений

В данном разделе можно просмотреть текущую сетевую/интернет активность (по TCP и UDP) по каждому приложению. Здесь также можно получить доступ к журналу брандамауэра BitDefender, нажмите в консоли упраления **Брандмауэр>Активность**. Появится следующее окно:



Контроль соединений

Здесь можно просмотреть общую информацию о соединениях приложений. Для каждого приложения отображаются его соединения и открытые порты, а также статистика относительно скорости входящего и исходящего трафика и общего количества отосланных/полученных данных.

Это окно отображает активность сетевого соединения/соединения с Интернет в реальном времени. По мере того, как соединения или порты закрываются, соответствующие пункты вначале тускнеют, а затем и вовсе исчезают из списка. То же самое происходит и со статистическими данными для определенного приложения, которое генерирует трафик или имеются открытые порты и которые Вы закрыли.

Нажмите **Блокировать**, чтобы создать правила и ограничить трафик данного приложения, порта или соединения. Вам нужно будет подтвердить Ваш выбор. Правила можно просмотреть в разделе Трафик, а также внести в них изменения.

Замечание
Для блокировки приложения, порта или соединения вы можете нажать на них правой кнопкой мыши и выбрать **Заблокировать**.

Нажмите **Уничтожить**, чтобы завершить все экземпляры выбранного процесса. Будет запрошено подтверждение вашего выбора.

Замечание
Для уничтожения процесса вы можете нажать на него правой кнопкой мыши и выбрать **Уничтожить**.

Нажмите **Экспортировать кадр** чтобы экспортировать список в файл с расширением `.txt`.

Для того, чтобы получить полный список событий, имеющих отношение к использованию модуля Брандмауэр (запуск/остановка брандмауэра, блокирование трафика, включение невидимого режима, изменение настроек, применение профиля), или событий, им обнаруженных (сканирование портов, блокирование попыток соединения согласно правил), обратитесь к Журналу событий брандмауэра Bitdefender, который можно просмотреть, нажав ссылку **Показать журнал**. Данный файл находится в папке Common Files текущего пользователя Windows, его можно найти здесь: `...BitDefender\BitDefender Firewall\bdfirewall.txt`.

9.6. Сетевые зоны

Зоной называется IP-адрес или диапазон IP-адресов, для которых создается отдельное правило в Вашем профиле. Данное правило может либо разрешать всем пользователям сети неограниченный доступ к Вашему компьютеру (надежные зоны) или, наоборот, полностью изолировать Ваш компьютер от других компьютеров в сети (ненадежная зона).

По умолчанию, BitDefender автоматически определяет, к каким сетям Вы подключены, и добавляет зоны в зависимости от конфигурации сети.

Замечание
Если Вы подключены к нескольким сетям, будет добавлены одна или несколько зон в зависимости от их конфигурации.

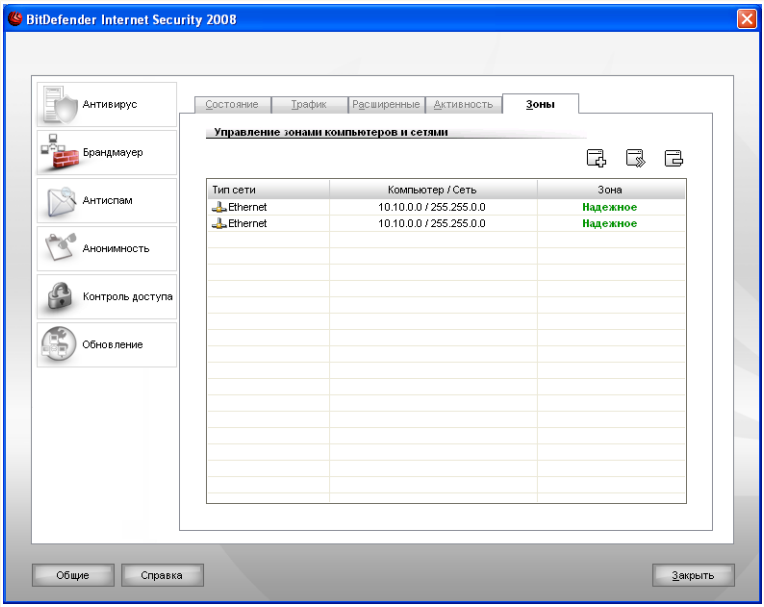
Надежные зоны по умолчанию добавляются для сетей следующих конфигураций:

- **Частный IP-адрес без шлюза** - компьютер является частью локальной сети (LAN) и не подключен к Интернет.
- **Частный IP с домен-контроллером** - компьютер является частью локальной сети (LAN) и подключается к домену.

Ненадежные зоны по умолчанию добавляются для сетей следующих конфигураций:

- **Открыть (не защищённое) беспроводное соединение** - Компьютер является частью беспроводной локальной сети (WLAN).

Чтобы настроить сетевые зоны, в консоли настроек нажмите **Брандмауэр>Зоны**. Появится следующее окно:



Сетевые зоны

В таблице приведен список всех сетевых зон, соответствующих Вашему профилю. Для каждой зоны отображается тип сети (Ethernet, беспроводная сеть, PPP и

т.д.), компьютер или сеть, которые связаны с этой зоной, а также информация о том, является ли данная зона надежной или ненадежной.

Чтобы редактировать зону, выберите ее и нажмите кнопку **Редактировать зону**, или дважды нажмите на названии зоны.

Замечание

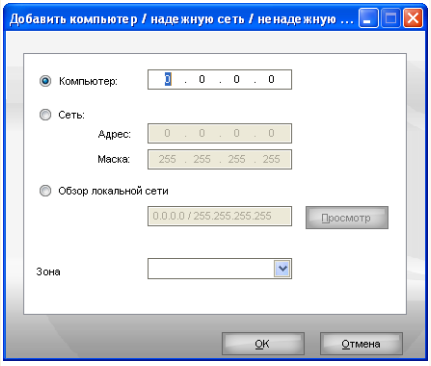
BitDefender по умолчанию добавляет открытые беспроводные сети к ненадежным зонам. Если Вы соединены с узкоспециализированной беспроводной сетью с надежными компьютерами (дома или с друзьями), вероятно, Вы захотите внести изменения в соответствующую зону. Чтобы иметь возможность совместно использовать ресурсы с другими пользователями данной сети, Вам нужно назначить эту зону надежной.

Чтобы удалить зону, выберите ее и нажмите кнопку **Удалить зону**.

9.6.1. Добавление зон

Добавление зон вручную. С помощью этой операции Вы можете, например, организовать совместное использование файлов с друзьями внутри открытой беспроводной сети (добавив их компьютеры в надежную зону), или блокировать один из компьютеров в надежной зоне (добавив его в ненадежную зону).

Чтобы добавить новую зону, нажмите кнопку **Добавить зону**. Появится следующее окно:



Добавить зону

Чтобы добавить, зону необходимо выполнить следующие шаги:

1. Укажите компьютер из локальной сети или всю локальную сеть, которую Вы хотите добавить в качестве зоны. Можно воспользоваться одним из следующих методов:
   - Чтобы добавить конкретный компьютер, выберите опцию **Компьютер** и впишите IP-адрес.
   - Чтобы добавить конкретную сеть, выберите опцию **Сеть** и впишите IP и маску сети.
   - Чтобы найти и добавить компьютеры или сети воспользуйтесь обзором локальных сетей.

     Чтобы произвести обзор локальных сетей, выберите **Обзор локальных сетей**, а затем нажмите **Обзор**. Появится новое окно, где Вы можете просмотреть все сети, к которым Вы подключены, а также членов каждой сети.

     Выберите компьютер или сеть, которую Вы хотите добавить в зону, из списка и нажмите **OK**
2. В меню выберите тип зоны (надежная или ненадежная), которую Вы хотите создать.
3. Нажмите **OK**, чтобы добавить зону.

10. Антиспам

BitDefender Antispam использует передовые технологические достижения и стандарты соответствующие в этой сфере. Антиспам фильтры отсеивают спам еще до того, как он попадает в Ваш почтовый ящик.

Раздел **Антиспам** данного руководства пользователя включает в себя следующие темы:

- Знакомство с антиспамом
- Статус Антиспама
- Настройка Антиспама
- Интеграция в почтовые клиенты

10.1. Знакомство с антиспамом

Проблема спама актуальна и для простых пользователей, и для больших компаний. Спам-сообщения раздражают, Вам не хотелось бы, чтобы некоторые из них попали на глаза вашим детям, а на работе Вас могут даже уволить за трату рабочего времени на спам или за получение Вами почтовых рассылок сексуального содержания на Ваш рабочий адрес электронной почты. И Вы не можете остановить этот поток! Лучшее, что можно сделать – это, очевидно, не получать таких писем вообще. К сожалению, существует множество разновидностей спама, и их количество день ото дня все увеличивается.

10.1.1. Антиспам-фильтры

Модуль Антиспама BitDefender включает семь различных фильтров, чтобы обеспечить непопадание в Ваш почтовый ящик Спама: (Белый список, Черный список, Фильтр символов, Фильтр изображения, Фильтр URL, Эвристический фильтр и Байесовский фильтр)

Замечание
Вы можете включить/отключить каждый из этих фильтров в модуле **Антиспам**, раздел Настройки.

Белый / черный список

Большинство людей переписываются с определенной группой людей или вообще получают письма от компаний, чей адрес находится на одном с ними домене.

Используя **списки друзей или спамеров**, Вы легко можете выделить людей, от которых Вы хотите получать письма независимо от их содержания (друзья) и людей, от которых Вы не хотите получать ни строчки (спамеры)."

Замечание
Белый / черный список также известны как **Списки Друзей / Спамеров**.

Вы можете работать со списками друзей/ спамеров через Консоль управления или с помощью Панели инструментов Антиспам, который интегрируется и используется в месте с почтовым клиентом.

Замечание
Мы рекомендуем записывать имена и адреса электронной почты друзей в **Список друзей**. BitDefender пропускает сообщения от адресатов из этого списка. Таким образом, Вы будете уверены, что получите ожидаемые письма.

Фильтр символов

Большинство спам-сообщений написаны кириллицей или азиатскими символами. Фильтр кодировки определяет подобные сообщения и отмечает их как SPAM.

Фильтр изображений

Поскольку спам-сообщениям становится все сложнее избежать распознавания с помошью эвристического фильтра, в последнее время в папках входящей почты все чаще можно найти сообщения, не содержащие ничего, кроме изображений со спамерским содержанием. Чтобы решить эту все более актуальную проблему, Bitdefender впервые использовал **Фильтр изображений**, который сравнивает образ изображений, полученных по электронной почте, с теми, которые имеются в базе данных Bitdefender. В случае соответствия электронная почта будет отмечена как SPAM.

Фильтр URL

Практически все спам-сообщения содержат ссылки на различные ресурсы. Обычно эти ресурсы содержат еще больше рекламы, а так же дают возможность приобрести товары, но иногда, они используются для фишинга.

BitDefender имеет базу данных подобных ссылок. Фильтр URL проверяет каждую ссылку в сообщении на ее наличие в базе данных. Если совпадение найдено, то сообщение отмечается как SPAM.

NeuNet (эвристический) фильтр

Нейросетевой (эвристический) фильтр производит ряд тестов над всеми компонентами сообщения (т.е. не только над заголовком, но и над текстом сообщение либо в текстовом или в HTML формате), в поиске слов, фраз, ссылок и прочих компонентов, характерных для спама. Основываясь на результатах анализа, этот фильтр добавляет сообщения в Спам.

Фильтр также обнаруживает сообщения, которые в теме сообщения отмечены как `Содержащее информацию сексуального характера:`, и также отмечает их как SPAM.

Замечание

С 19 мая 2004 года согласно федеральным законам спам-сообщения, содержащие информацию сексуального характера, должны содержать предупреждение `Содержащее информацию сексуального характера (SEXUALLY-EXPLICIT):` в заголовке или в первых строках сообщений.

Байесовский фильтр

Модуль **Байесовский фильтр** классифицирует сообщения согласно статистической информации о повторах определенных слов в сообщениях, помеченных как спам, в сравнении с письмами, помеченными Вами или эвристическим фильтром как Не-спам.

Например, если некое слово из четырех букв чаще всего появляется в Спаме, естественно предположить, что следующее письмо, в котором встречается это слово, ТОЧНО БУДЕТ спамом. В расчет принимаются и все значимые слова в сообщении. На основе статистической информации высчитывается общая вероятность того, что письмо окажется спамом.

Этот модуль отличается еще одним интересным свойством: обучаемостью. Он быстро подстраивается под типы сообщений, получаемые пользователем, и хранит информацию о них. Чтобы фильтр работал эффективно, важно «обучать» его, то есть снабжать новыми образцами спама и нужных сообщений, так же как ищейку надо тренировать на определенный запах. Иногда приходится делать поправку фильтра, чтобы исправить допущенные им ошибки.

Важно

Можно скорректировать модуль Байесовский фильтр, используя кнопки **Спам** и **НЕ Спам** из Панели инструментов Антиспама.

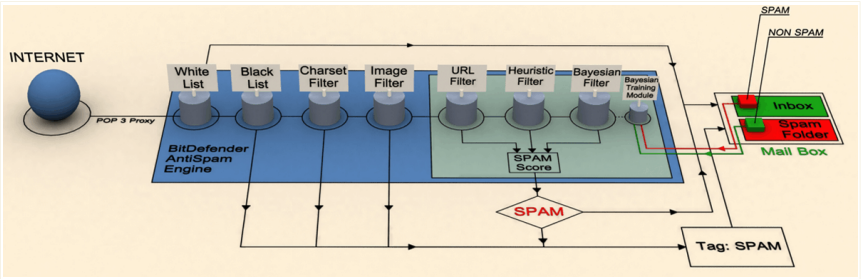
Замечание
Каждый раз, когда Вы выполняете обновление:

- новые образы изображения будут добавляться в **Фильтр изображения**;
- новые ссылки будут добавляться в **Фильтр URL**;
- новые правила будут добавляться в **Нейросетевой (эвристический) фильтр**;

Это поможет увеличивать эффективность вашего поискового движка Антиспам. Чтобы защитить Вас от спаммеров, Bitdefender может выполнить автоматические обновления. Для этого опция **Автоматическое обновление** должна быть включена.

10.1.2. Описание антиспама

На этой схеме показано, как работает BitDefender.



Описание антиспама

Как видно из схемы, фильтры антиспама (Белый список, Черный список, Фильтр символов, Фильтр изображений, Фильтр URL, нейросетевой (эвристический) фильтр и Байесовский фильтр) совместно используются Bitdefender для того, чтобы определить, следует ли направить некоторую часть электронной почты в Вашу папку **Входящие сообщения** или нет.

Каждое входящее электронное письмо вначале проверяется с помощью Белый список/Черный список. Если адрес отправителя находится в Списке разрешенных адресов, письмо попадает сразу же в папку **Входящие**.

В противном случае, сообщение будет проверено с помощью фильтра Черный список на наличие данного электронного адреса. Такие письма помечаются как СПАМ и перемещаются в папку **Спам** (расположенную в Microsoft Outlook).

Также, с помощью Фильтра символов отсеиваются письма, написанные кириллицей или иероглифами. Такие письма помечаются как СПАМ и перемещаются в папку **Спам**.

Письма, написанные не кириллицей или иероглифами, передаются в Фильтр изображений. **Фильтр изображений** обнаруживает все письма, содержащие приложения в виде графических изображений со спам-содержанием.

Затем фильтр URL сравнивает ссылки, обнаруженные в письме, с ссылками из базы данных BitDefender. В случае совпадения письмо добавляется к Спаму.

Затем Нейросетевой(эвристический) фильтр проведет ряд проверок компонентов сообщения, в поисках слов, фраз, ссылок или других характеристик Спама. В случае совпадения письмо добавляется к Спаму.

Замечание

Письма отмеченные как "ОТКРОВЕННО СЕКСУАЛЬНО" в теме письма BitDefender считает СПАМОМ.

Далее письмо анализируется с помощью Байесовского фильтра. На основе статистической информации о повторах определенных слов в сообщениях, помеченных как спам, в сравнении с письмами, помеченными Вами или эвристическим фильтром как Не-спам. В результате письмо добавляется к Спаму.

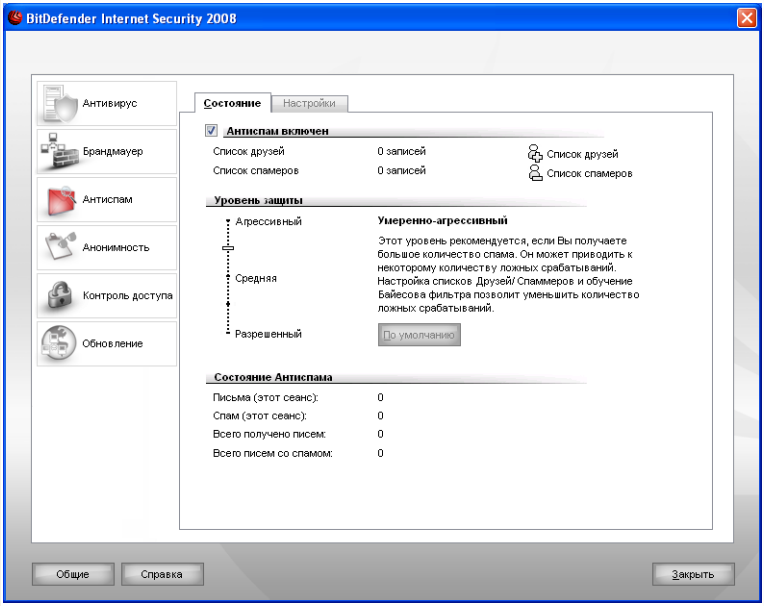
Если общий результат проверки (результат проверки URL + эвристичеким фильтром + Байесовским фильтром) превышает общий допустимый результат для сообщения (установленный пользователем в разделе Статус как предельный уровень), письмо считается Спамом.

Важно

Если Вы пользуетесь другим почтовым клиентом (не Microsoft Outlook или Microsoft Outlook Express), Вам необходимо создать правило для перемещения сообщений, отмесенных как Спам в определенный указанный каталог. BitDefender добавляет префикс `[СПАМ]` в тему сообщения, классифицированного как Спам.

10.2. Статус модуля Антиспам

Чтобы настроить защиту при помощи модуля Антиспам, нажмите **Антиспам>Состояние** в консоли настроек. Появится следующее окно:



Статус модуля Антиспам

В этом разделе Вы можете настраивать модуль **Антиспам** и просматривать информацию о его работе.

Важно
Чтобы Спам не попал в Ваш **Почтовый ящик**, **Фильтр Антиспама** должен быть постоянно включен.

В разделе **Статистика** Вы можете просмотреть статистику работы модуля Антиспам за текущий сеанс (с момента включения компьютера) или итоговую информацию (с момента установки BitDefender).

Чтобы настроить модуль **Антиспам** Вам следует выполнить следующие этапы настройки:

10.2.1. Шаг 1/2 - Настройка «уровня толерантности»

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

Существует 5 «уровней толерантности»

« Уровень толерантности»	*Описание*
Приемлемый	Предлагает защиту для учетных записей, которые получают много легитимных коммерческих электронных сообщений. Фильтр пропускает большинство электронных сообщений, но могут иметь место "ложная" классификация (попадание легитимных писем в категорию Спам).
Приемлемый умеренный	Предлагает защиту для учетных записей, которые получают некоторое количество легитимных коммерческих электронных сообщений. Фильтр пропускает большинство электронных сообщений, но могут иметь место "ложная" классификация (попадание легитимных писем в категорию Спам).
Умеренный	Предлагает защиту для обычных учетных записей. Фильтр блокирует основную часть спама, избегая "ложной" классификации.
Умеренно агрессивный	Предлагает защиту для учетных записей, регулярно получающих большое количество спама. Фильтр пропускает очень мало спама, но иногда может происходить "ложная" классификация (легитимные сообщения будут отмечены как Спам). Настройте **Список друзей/спаммеров** и "обучайте" **Обучаемый модуль (Байесовский)**, чтобы уменьшить количество "ложных" классификаций.
Агрессивный	Предлагает защиту для учетных записей, регулярно получающих очень большое количество спама.

« Уровень толерантности»	*Описание*
	Фильтр пропускает очень мало спама, но иногда может происходить "ложная" классификация (легитимные сообщения будут отмечены как Спам). Добавляйте Ваши контакты в **Список друзей**, чтобы уменьшить количество "ложных" классификаций.

Для выбора уровня по умолчанию(**Умеренно агрессивный**) нажмите **Уровень по умолчанию**.

10.2.2. Шаг 2/2 - Заполните список адресов

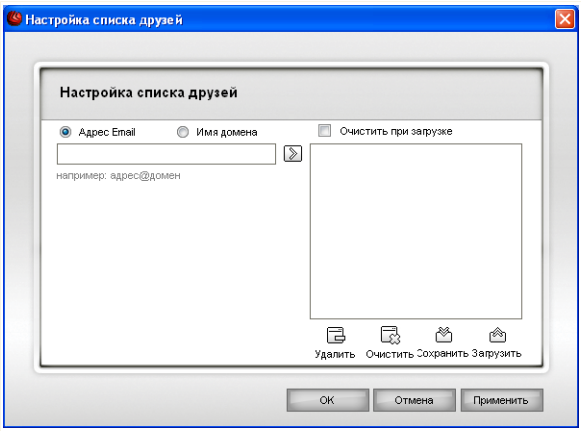
В этих списках содержатся электронные адреса, с которых вам отправляются легитимные сообщения или спам.

Список друзей

Список друзей - список адресов электронной почты, с которых Вы хотите получать письма независимо от их содержания. Сообщения от друзей не помечаются как Спам, даже если их содержание соответствует определению Спама.

Замечание
Все электронные письма, приходящие с адресов, указанных в списке друзей, автоматически попадут в вашу папку **Входящие** без обработки.

Чтобы управлять **Списком друзей**, нажмите (что соотвествует **Списку друзей**) или нажмите кнопку **Друзья** в Панели инструментов Антиспам.



Список друзей

Здесь Вы можете добавлять и удалять друзей из списка.

Если Вы хотите добавить адрес электронной почты, поставьте значок в поле **Адрес электронной почты** option, type in the address and click введите адрес и щелкнитемышкой на кнопке **Список друзей**.

Важно
Адрес должен иметь следующую структуру: name@domain.com.

Если Вы хотите добавить домен, поставьте значок в поле **Доменное имя** впишите его и нажмите . Домен появится в **списке друзей**.

Важно
Имя домена должно иметь следующий вид:

- @domain.com, *domain.com и domain.com - все письма, приходящие с domain.com попадут в вашу папку **Входящие** независимо от содержания;
- *domain* - все письма, приходящие с domain (независимо от доменного суффикса) попадут в вашу папку **Входящие** независимо от содержания;
- *com - все письма с доменным суффиксом com попадут в вашу папку **Входящие** независимо от содержания;

Чтобы удалить пункт из списка, выберите его и нажмите кнопку **Удалить**. Если Вы нажмете кнопку **Очистить**, то удалите все записи в списке и их восстановить возможности не будет.

Используйте кнопки **Сохранить**/ **Загрузить**, чтобы сохранить / загрузить **Список друзей** в необходимое место. Файл будет иметь расширение `.bwl`.

Чтобы сбросить текущее содержание списка при загрузки предварительно сохранненного, нажмите **Очистить текущий список при загрузке**.

Замечание
Мы рекомендуем записывать имена и адреса электронной почты друзей в **Список друзей**. BitDefender пропускает сообщения от адресатов из этого списка. Таким образом, Вы будете уверены, что получите ожидаемые письма.

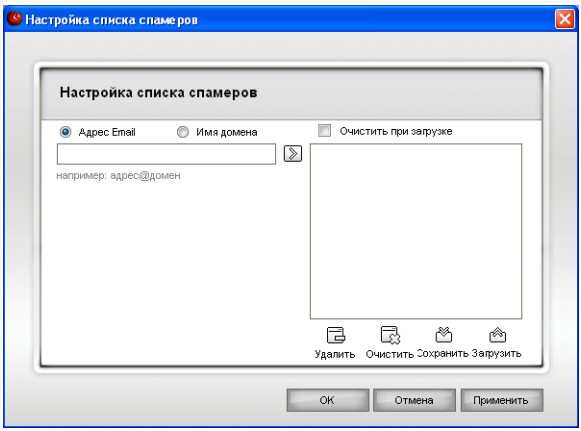
Нажмите **Применить** и **OK** чтобы сохранить и закрыть **список друзей**.

Список спаммеров

Список спаммеров - список адресов электронной почты, с которых Вы не хотите получать письма, независимо от их содержания.

Замечание
Все электронные письма, приходящие с адресов, указанных в **списке спаммеров** автоматически будут помечены как Спам без обработки.

Чтобы управлять **Списком спаммеров**, нажмите (что соотвествует **Списку спаммеров**) или нажмите кнопку **Спаммеры** в Панели инструментов антиспам.



Список спаммеров

Здесь Вы можете добавлять и удалять спаммеров из **Списка спаммеров**.

Если Вы хотите добавить адрес, поставьте значок в поле **Адрес электронной почты**, введите адрес и нажмите . Этот адрес появится в **Списке спаммеров**.

Важно
Адрес должен иметь следующую структуру: name@domain.com.

Если Вы хотите добавить домен, поставьте значок в поле **Доменное имя**, впишите его и нажмите . Домен появится в **Списке спаммеров**.

Важно
Имя домена должно иметь следующий вид:

- @domain.com, *domain.com и domain.com - все письма, приходящие с domain.com будут помечены как Спам;
- *domain* - все письма, приходящие с domain (независимо от доменного суффикса) будут помечены как Спам;
- *com - все письма с доменным суффиксом com будут помечены как Спам.

Чтобы удалить пункт из списка, выберите его и нажмите кнопку **Удалить**. Если Вы нажмете кнопку **Очистить**, то удалите все записи в списке и их восстановить возможности не будет.

Используйте кнопки **Сохранить**/ **Загрузить**, чтобы сохранить / загрузить **Список спаммеров** внеобходимое место. Файл будет иметь расширение `.bwl`.

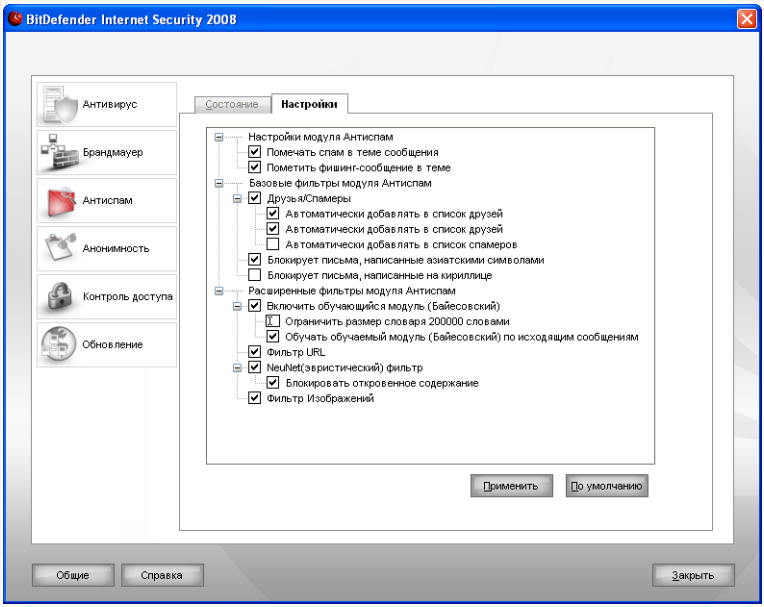
Чтобы сбросить текущее содержание списка при загрузки предварительно сохранненного, нажмите **Очистить текущий список при загрузке**.

Нажмите **Применить** и **OK** чтобы сохранить и закрыть **Список спаммеров**.

Важно
Перед переустановкой BitDefender сохраните списки **Друзей** и **Спаммеров** и после переустановки Вы сможете загрузить их.

10.3. Настройки антиспама

Чтобы изменить настройки модуля Антиспам, нажмите **Antispam>Настройки** в консоли настроек. Появится следующее окно:



Настройки антиспама

Здесь Вы можете подключить/отключить каждый фильтр Антиспам и установить некоторые другие настройки модуля Антиспам.

В окне Настройки обновления Вы можете увидеть три типа настроек: (**Настройки антиспама**, **Базовые фильтры антиспама** и **Дополнительные фильтры антиспама**), объединенные в разворачиваемое меню, похожее на все подобные меню операционной системы Windows.

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

10.3.1. Настройки антиспама

- **Помечать как Спам в поле «Тема»** - эта функция позволяет ставить пометку «Спам» в поле «Тема» письма, посчитанного Спамом.
- **Помечать как Спам все фишинг-сообщения в поле «Тема»** - эта функция позволяет ставить пометку «Спам» в поле «Тема» всех писем, определенных как фишинг-сообщения.

10.3.2. Базовые фильтры Антиспама

- **Список друзей/спаммеров** - включает/отключает Список друзей/спаммеров.
  - **Автоматически добавлять получателей в список друзей** - добавляет получателей в Список друзей.
  - **Автоматически добавлять в список друзей** - при нажатии кнопки **Не спам** в следующий раз в Панели инструментов антиспама отправитель будет автоматически добавлен в **Список друзей**.
  - **Автоматически добавлять в список спаммеров** - при нажатии кнопки **Спам** в следующий раз в Панели инструментов антиспама отправитель будет автоматически добавлен в **Список спаммеров**.

Замечание
Кнопки **Не Спам** и **Спам** используются для обучения Байесовского фильтра.

- **Блокировка писем написанных азиатскими символами** - блокировка сообщений, написанных Азиатскими символами.
- **Блокировка писем написанных кириллицой** - блокировка сообщений, написанных Символы Кириллицы.

10.3.3. Дополнительные фильтры Антиспама

- **Включить "обучающийся" модуль (Байесовский)** - включает/отключает "обучающийся" модуль (Байесовский).
  - **Ограничить длину словаря до 200 000 слов** - эта функция позволяет настраивать размер словаря Байесовского фильтра: чем меньше словарь, тем быстрее проверка, но чем больше словарь, тем точнее проверка.

Замечание
Мы рекомендуем размер словаря в 200 000 слов.

  - **Обучать "обучаемый" модуль (Байесовский) по исходящим сообщениям** - обучение "обучаемого" модуля (Байесовского) по исходящим сообщениям.
- **Фильтр URL** - включает/отключает Фильтр URL.
- **Нейросетевой (эвристический) фильтр** - включает/отключает Нейросетевой (эвристический) фильтр.
  - **Блокировка откровенного контента** - включает/отключает выявление сообщений с темой "СЕКСУАЛЬНО ОТКРОВЕННОЕ".
- **Фильтр изображений** - включает/отключает Фильтр изображений.

Замечание
Чтобы включить/отключить защиту, установите/снимите значок в соответствующем поле.

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

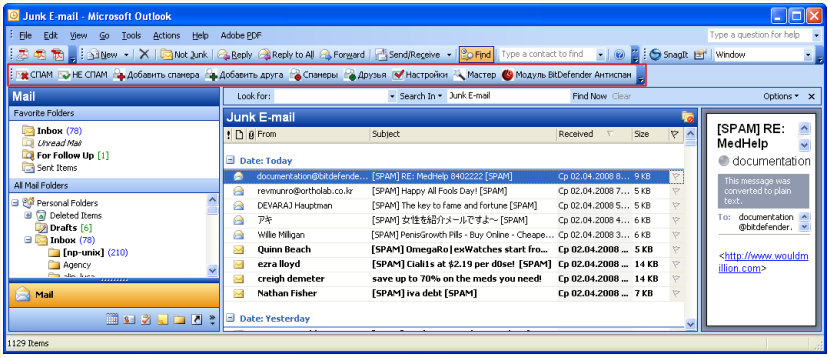
10.4. Интеграция в почтовые клиенты

BitDefender интегрируется в следующие почтовые программы при помощи интуитивно понятной и легкой в использовании панели инструментов:

- Microsoft Outlook
- Outlook Express
- Windows Mail
- Mozilla Thunderbird

10.4.1. Панель инструментов антиспама

Панель инструментов Antispam расположена в верхней части окна Вашего почтового клиента.



Панель инструментов антиспама

Важно

Основное различие в настройках Защиты от спама BitDefender для Microsoft Outlook и для Outlook Express / Windows Mail состоит в том, что в программе Microsoft Outlook спам-сообщения помещаются в папку **Спам**, а в Outlook Express / Windows Mail – в папку **Удаленные**. В обоих случаях в поле «Тема» письма добавляется пометка СПАМ.

В программе Microsoft Outlook папка **Спам** созданная BitDefender, находится в Списке папок на одном уровне с другими папками (такими, как Календарь, Контакты и т.д.).

Ниже приводится описание каждой кнопки:

- **Спам** - Щелчок мышки на этой кнопке отправляет выбранное письмо в модуль Байесовский фильтр, причисляя его к Спаму. Оно будет помечено как СПАМ и отправлен в папку **СПАМ**.

  В будущем сообщения, подходящие под эти характеристики, будут тоже помечены как СПАМ.

Замечание
Вы можете выбрать одно письмо или сразу несколько.

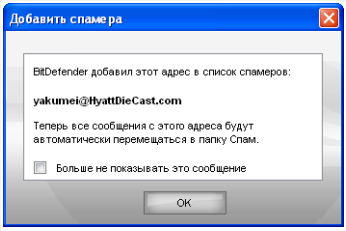
- **Не Спам** - Щелчок мышки на этой кнопке отправляет выбранное письмо в модуль Байесовский фильтр, не причисляя его к Спаму, и BitDefender не пометит его. Письмо будет перемещено из папки **Спам** в папку **Входящие**.

  В будущем сообщения, подходящие под эти характеристики тоже не будут помечены как СПАМ.

Замечание
Вы можете выбрать одно письмо или сразу несколько.

Важно
Кнопка **Не Спам** становится активной, когда Вы выделяете письмо, помеченное программой BitDefender как СПАМ. Обычно эти письма помещаются в папку **Спам**.

- **Добавить спамера** - нажмите на эту кнопку, тобы добавить отправителя выбранных сообщений в **Список спамеров**.



Добавить спаммера

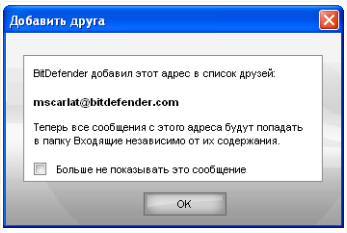
Поставьте значок в поле **Больше не показывать это сообщение** если Вы не хотите получать подтверждение при добавлении адреса спамера в список.

Нажмите **OK**, чтобы закрыть окно.

В будущем сообщения от этого адресата будут помечены как СПАМ.

Замечание
Вы можете выбрать одного отправителя или сразу нескольких.

- **Добавить друга** - нажмите на эту кнопку, чтобы добавить отправителя выбранных сообщений в **Список Друзей**.



Добавить друга

Выберите **Не показывать это сообщение** если вы не хотите делать подтверждения каждый раз, когда вы добавляете друга к списк.

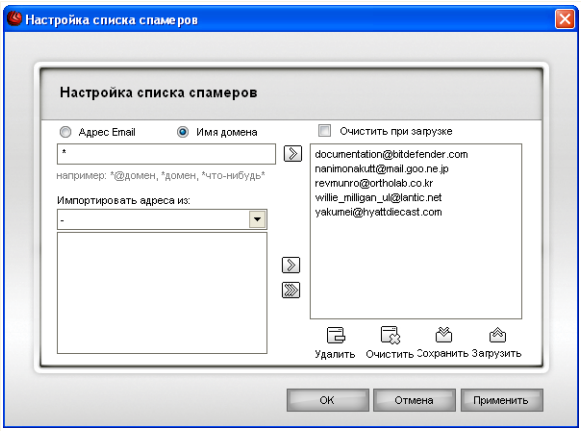
Нажмите **OK**, чтобы закрыть окно.

Вы всегда будете получать сообщения от этого адресата, независимо от их содержания.

Замечание
Вы можете выбрать одного отправителя или сразу нескольких.

- **Спамеры** - нажав эту кнопку Вы сможете редактировать Список спамеров – в нем содержатся электронные адреса, с которых Вы не хотите получать писем, независимо от их содержания.

Замечание
Все электронные письма, приходящие с адресов, указанных в **списке спаммеров** автоматически будут помечены как Спам без обработки.



Список спаммеров

Здесь Вы можете добавлять и удалять спаммеров из **Списка спаммеров**.

Если Вы хотите добавить адрес, поставьте значок в поле **Адрес электронной почты**, введите адрес и нажмите ⊡. Этот адрес появится в **Списке спамеров**.

Важно
Адрес должен иметь следующую структуру: name@domain.com.

Если Вы хотите добавить домен, поставьте значок в поле **Доменное имя**, впишите его и нажмите ⊡. Домен появится в **Списке спамеров**.

Важно
Имя домена должно иметь следующий вид:

- @domain.com, *domain.com и domain.com - все письма, приходящие с domain.com будут помечены как Спам;
- *domain* - все письма, приходящие с domain (независимо от доменного суффикса) будут помечены как Спам;
- *com - все письма с доменным суффиксом com будут помечены как Спам.

Чтобы импортировать электронные адреса из **Адресной книги Windows** / **папок Outlook Express** в **Microsoft Outlook** / **Outlook Express** / **Windows Mail**, выберите соотвествующий вариант из выпадающего меню **Импортировать электронные адреса из**

В программе **Microsoft Outlook Express / Windows Mail** появится новое окно, в котором Вы можете выбрать папку с адресами электронной почты, которые Вы хотите добавить в **Список спамеров**. Выбрав ее, нажмите кнопку **Выбрать**.

В обоих случаях электронные адреса появятся в списке импорта. Выберите нужные и нажмите Вы добавите их в **Список спамеров**. Если Вы сразу нажмите в список будут добавлены все адреса.

Чтобы удалить пункт из списка, выберите его и нажмите кнопку **Удалить**. Если Вы нажмете кнопку **Очистить**, то удалите все записи в списке и их восстановить возможности не будет.

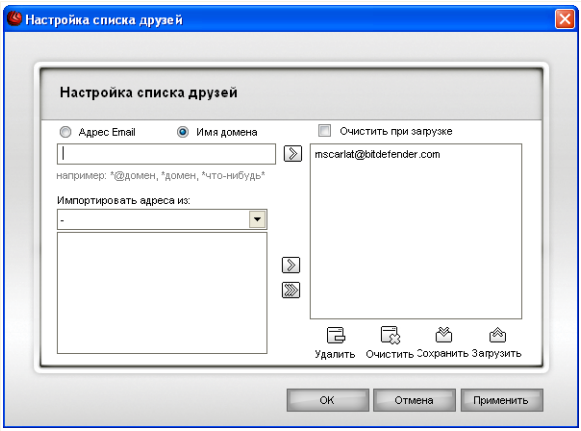
Используйте кнопки **Сохранить**/ **Загрузить**, чтобы сохранить / загрузить **Список спаммеров** внеобходимое место. Файл будет иметь расширение `.bwl`.

Чтобы сбросить текущее содержание списка при загрузки предварительно сохранненного, нажмите **Очистить текущий список при загрузке**.

Нажмите **Применить** и **OK** чтобы сохранить и закрыть **Список спаммеров**.

- **Список друзей** - список адресов электронной почты, с которых Вы хотите получать письма независимо от их содержания.

> ***Замечание***
> Все электронные письма, приходящие с адресов, указанных в списке друзей, автоматически попадут в вашу папку **Входящие** без обработки.



Список друзей

Здесь Вы можете добавлять и удалять друзей из списка.

Если Вы хотите добавить адрес, поставьте значок в поле **Адрес электронной почты**, введите адрес и нажмите кнопку . Этот адрес появится в **Списке друзей**.

Важно
Адрес должен иметь следующую структуру: name@domain.com.

Если Вы хотите добавить домен, поставьте значок в поле **Доменное имя** впишите его и нажмите . Домен появится в **списке друзей**.

Важно
Имя домена должно иметь следующий вид:

- @domain.com, *domain.com и domain.com - все письма, приходящие с domain.com попадут в вашу папку **Входящие** независимо от содержания;
- *domain* - все письма, приходящие с domain (независимо от доменного суффикса) попадут в вашу папку **Входящие** независимо от содержания;
- *com - все письма с доменным суффиксом com попадут в вашу папку **Входящие** независимо от содержания;

Чтобы импортировать электронные адреса из **Адресной книги Windows** / **папок Outlook Express** в **Microsoft Outlook** / **Outlook Express** / **Windows Mail**,

выберите соотвествующий вариант из выпадающего меню **Импортировать электронные адреса из**

В программе **Microsoft Outlook Express / Windows Mail** появится новое окно, в котором Вы можете выбрать папку с адресами электронной почты, которые Вы хотите добавить в **Список друзей**. Выбрав ее, нажмите кнопку **Выбрать**.

В обоих случаях электронные адреса появятся в списке импорта. Выберите нужные и нажмите Вы добавите их в **Список друзей**. Если Вы сразу нажмите в список будут добавлены все адреса.

Чтобы удалить пункт из списка, выберите его и нажмите кнопку **Удалить**. Если Вы нажмете кнопку **Очистить**, то удалите все записи в списке и их восстановить возможности не будет.

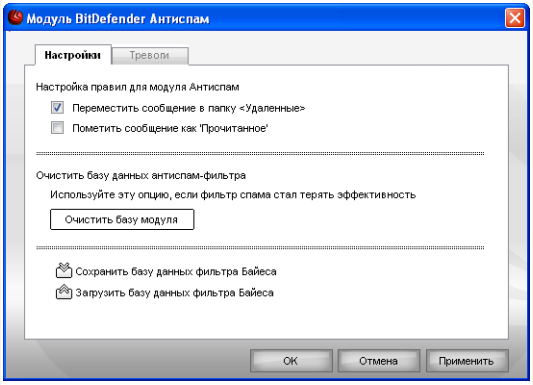
Используйте кнопки **Сохранить**/ **Загрузить**, чтобы сохранить / загрузить **Список друзей** в необходимое место. Файл будет иметь расширение `.bwl`.

Чтобы сбросить текущее содержание списка при загрузки предварительно сохранненного, нажмите **Очистить текущий список при загрузке**.

Замечание
Мы рекомендуем записывать имена и адреса электронной почты друзей в **Список друзей**. BitDefender пропускает сообщения от адресатов из этого списка. Таким образом, Вы будете уверены, что получите ожидаемые письма.

Нажмите **Применить** и **OK** чтобы сохранить и закрыть **список друзей**.

- **Настройки** - открывает окно **Настройки** в котором Вы можете выбрать различные опции для модуля **Антиспам**.



Настройки модуля Антиспам

Доступны следующие варианты:

- **Перемещать сообщения в папку удаленных** - перемещает спам-сообщения в папку **Удаленные** (только для Microsoft Outlook Express / Windows Mail);
- **Пометить как прочтенное** - помечает все спам-сообщения как прочтенные. При получении новых спам-сообщений старые письма не принимаются во внимание.

Если Вы заметили, что фильтр Антиспама стал работать неэффективно, Вам может потребоваться стереть базу данных и переобучить Байесовский фильтр. Нажмите **Очистить базу данных антиспама** чтобы очистить Байесовский фильтр.

Используйте кнопки **Сохранить Байес**/ **Загрузить Байес** чтобы сохранить/загрузить Базу данных Байесовского фильтра в необходимое место. Файл будет иметь расширение `.dat`.

Нажмите на закладке **Предупреждения** если Вы хотите получить доступ к разделу, в котором можно отключить появление подтверждений при работе с кнопками **Добавить спамера** и **Добавить друга**.

Замечание

В окне **Предупреждения** Вы можете включить/отключить появление предупреждения **Выберите электронное сообщение**. Это предупреждение появляется, когда Вы выбираете несколько сообщений, а не одно.

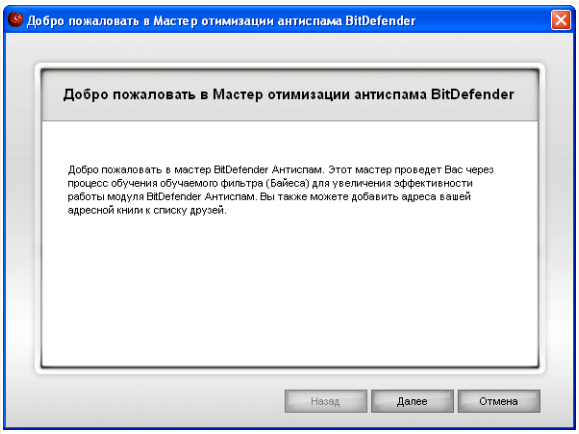
- **Программа-мастер** - Программа-мастер поможет Вам переобучить Байесовский фильтр, и со временем Антиспам BitDefender будет работать все лучше. Также Вы можете добавить адреса из вашей Адресной книги в **Список друзей** / **Список спамеров**.
- **BitDefender Антиспам** - Щелчок мыши на этой кнопке открывает Консоль управления.

10.4.2. Мастер настройки Антиспам

Когда Вы после установки BitDefender впервые запускаете почтовый клиент, появится программа-мастер, которая поможет Вам настроить Список друзей, Список спамеров и переобучить Байесовский фильтр для того, чтобы повысить эффективность работы фильров Антиспама.

Замечание
Мастера также можно запустить в любой момент, нажав кнопку **Мастер** в Панели инструментов Антиспам.

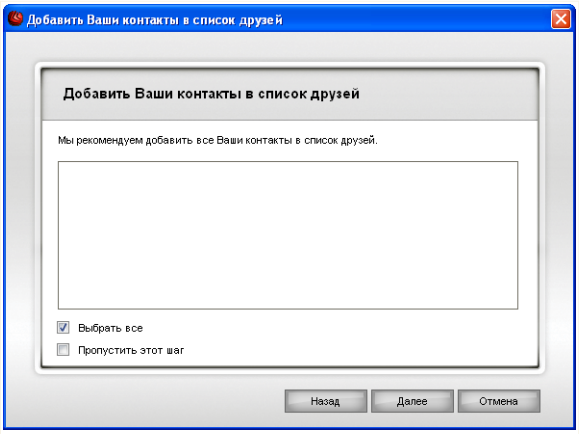
Шаг 1/6 - Экран приветствия



Окно приветствия

Нажмите **Далее**.

Шаг 2/6 - Заполните список друзей



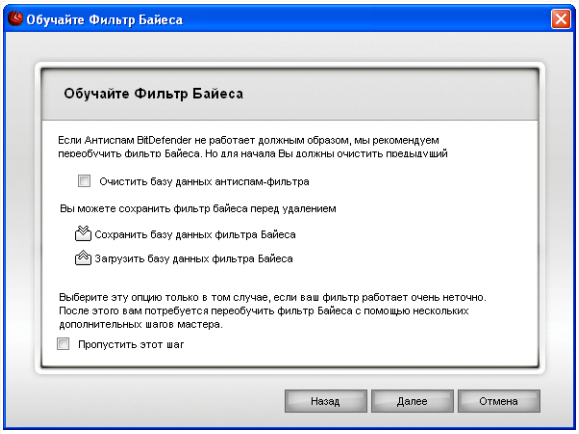
Заполните список друзей

Здесь Вы видите адреса из вашей **Адресной книги**. Выберите из них те, которые хотите занести в **Список друзей**. Мы рекомендуем занести все адреса. Вы будете получать письма от этих отправителей независимо от их содержания.

Чтобы добавить все Ваши контакты в Список друзей, нажмите **выбрать все**.

Поставьте галочку в поле **Пропустить этот этап** если Вы хотите пропустить этот этап. Нажмите **Назад** чтобы вернуться на предыдущий этап или **Далее** чтобы продолжить.

Шаг 3/6 - Удаление байесовой базы данных



Удаление байесовой базы данных

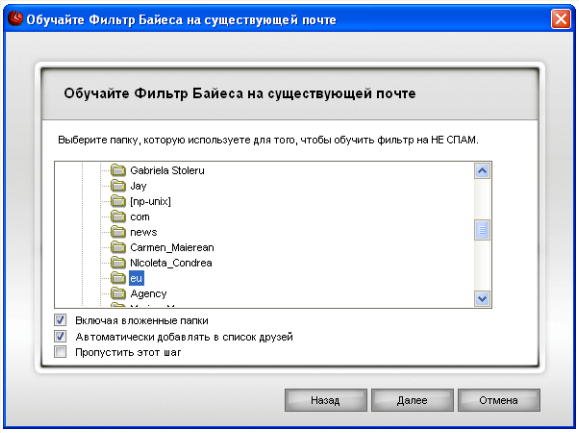
Вы можете заметить, что фильтр Защиты от спама стал работать хуже. Причиной этому может быть неверное обучение. Например, Вы по ошибке пометили нужные сообщения как Спам, или наоборот. В этом случае Вам нужно очистить базу данных фильтра и заново обучить его, следуя указаниям программы-мастера.

Поставьте значок в поле **Очистить базу данных фильтра Антиспам** если Вы хотите переустановить базу данных Байесовского фильтра.

Используйте кнопки **Сохранить фильтр Байеса**/ **Загрузить фильтр Байеса** чтобы сохранить этот фильтр в нужной директории или загрузить его.

Поставьте галочку в поле **Пропустить этот этап** если Вы хотите пропустить этот этап. Нажмите **Назад** чтобы вернуться на предыдущий этап или **Далее** чтобы продолжить.

Шаг 4/6 - Обучение байесова фильтра при помощи легетимных электронных сообщений



Обучение байесова фильтра при помощи легетимных электронных сообщений

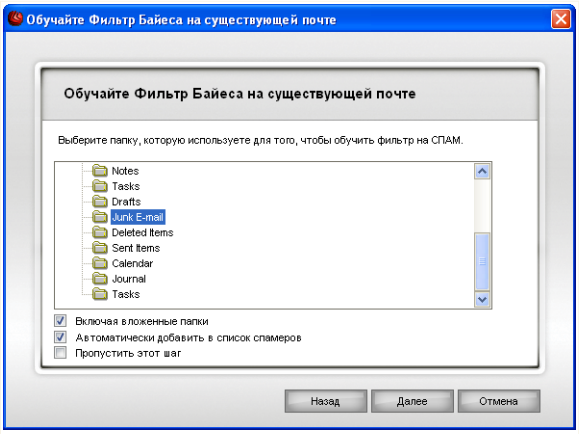
Выберите папку с разрешенными электронными письмами. Они будут использоваться для переобучения Байесовского фильтра.

Имеются два дополнительных параметра опции списка поддиректорий:

- **Включить подкаталоги** - включает в вашу выборку подкаталоги.
- **Автоматически добавлять в список друзей** - добавляет отправителей в **Список друзей**.

Поставьте галочку в поле **Пропустить этот этап** если Вы хотите пропустить этот этап. Нажмите **Назад** чтобы вернуться на предыдущий этап или **Далее** чтобы продолжить.

Шаг 5/6 - Обучение байесова фильтра при помощи спама



Обучение байесова фильтра при помощи спама

Выберите папку с электронными письмами, определенными как Спам. Они будутиспользоваться для обучения Байесовского фильтра.

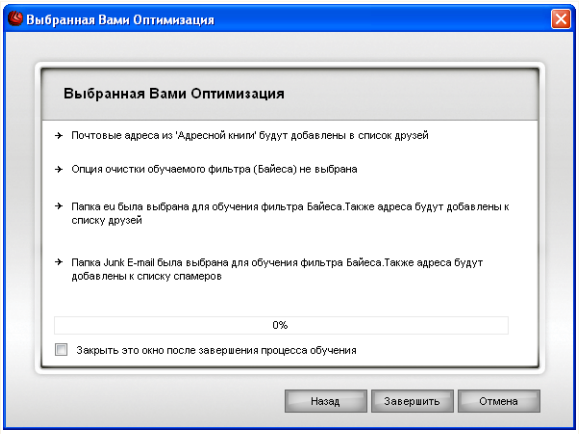
Важно
Пожалуйста, убедитесь в том, что выбранная Вами папка не содержит разрешенных почтовых сообщений. В противном случае, эффективность работы модуля Антиспам будет существенно снижена.

Имеются два дополнительных параметра опции списка поддиректорий:

- **Включить подкаталоги** - включает в вашу выборку подкаталоги.
- **Автоматически добавлять в список спамеров** - добавляет отправителей в **Список спамеров**.

Поставьте галочку в поле **Пропустить этот этап** если Вы хотите пропустить этот этап. Нажмите **Назад** чтобы вернуться на предыдущий этап или **Далее** чтобы продолжить.

Этап 6/6 – Краткий итоговый отчет



Краткий обзор

В этом окне Вы можете просмотреть все настройки, выполненные с помощью программы-мастера и можете внести необходимые изменения, вернувшись на предыдущие этапы нажав **Назад**).

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

11. Контроль личных данных

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

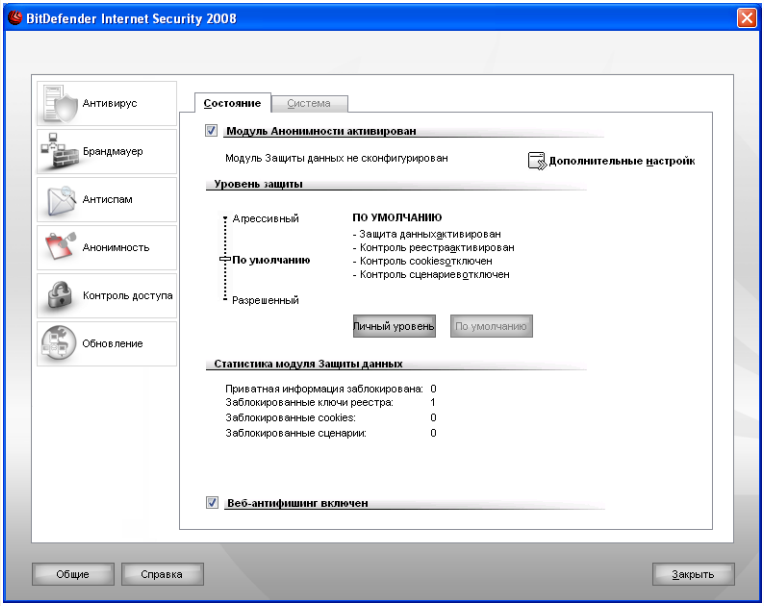
BitDefender также проверяет посещаемые Вами веб-сайты и предупреждает о любых попытках фишинга.

Раздел **Котроль личных данных** данного руководства пользователя включает в себя следующие темы:

- Состояние Контроля личных данных
- Дополнительные настройки - Контроль личных данных
- Дополнительные настройки - Контроль регистра
- Дополнительные настройки - Контроль cookie
- Дополнительные настройки - Контроль скриптов
- Информация о системе
- Инструменты Антифишинга

11.1. Состояние Контроля личных данных

Чтобы настроить и следить за работой модуля Контроля личных данных, нажмите **Контроль личных данных>Состояние** в консоли настроек. Появится следующее окно:



Состояние Контроля личных данных

11.1.1. Контроль личных данных

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

Контроль личных данных защищает Ваш компьютер используя 5 важных контролей защиты:

- Контроль личных данных - защищает Ваши персональные конфиденциальные данные, проверяя весь исходящий HTTP и SMTP трафик согласно правилам, созданным Вами в разделе Конфиденциальность

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

- Контроль регистра - спрашивает разрешения всякий раз, когда какая-либо программа будет пытаться менять запись в реестре, для того чтобы загружаться при запуске системы.
- 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.

Конфигурация уровня защиты

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

Существует 3 уровня защиты:

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

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

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

11.1.2. Антифишинговая защита

Фишинг - это криминальные действия в Интернет, которые используют психологические методы с целью выманивания у пользователей конфиденциальной информации.

В большинстве случаев, фишинг сводится к массовой рассылке поддельных электронных сообщений, утверждающих, что их автором является некая существующая, легитимная компания. Эти ложные сообщения отсылаются в

надежде, что хотя бы несколько пользователей, попадающих под критерии потенциальных жертв фишинга, раскроют конфиденциальную информацию о себе.

Стандартное сообщение при фишинге представляет собой текст, относительно Вашего счета в сети. В этом сообщении Вас пытаются убедить нажать на предоставляемую ссылку в сообщении, чтобы перейти на якобы легитимный веб-сайт (а на самом деле - поддельный), где запрашивается личная информация. Например, Вас могут попросить подтвердить информацию о Вашем счете, такую как имя пользователя и пароль, а также ввести номер Вашего банковского счета или номер социального страхования. Иногда, чтобы быть более убедительными, в письме сообщают, что Вашему счету якобы будет угрожать опасность или он будет заморожен, если Вы не воспользуетесь приведенной ссылкой.

Фишинг также использует программы-шпионы, например, кейлоггер (программа фиксирующая нажатые пользователем клавиши), чтобы украсть конфиденциальную информацию прямо с Вашего компьютера.

Основными объектами фишинга становятся пользователи всевозможных платежных сервисов в Интернете, таких как eBay и PayPal, а также банков и прочих услуг в сети. В последнее время, объектами фишинга с целью получения данных авторизации стали и пользователи социальных сетей в Интернет.

Чтобы защитить от попыток фишинга, когда Вы находитесь в Интернет, **Антифишинг** должен быть включен. Таким образом, BitDefender будет проверять каждый веб-сайт, перед тем, как Вы на него попадете, и предупредит Вас о существующей угрозе фишинга. Белый Список веб-сайтов, которых не надо просматривать BitDefender, можно формировать.

Чтобы легко управлять и настраивать защиту от фишинга и Белый список, воспользуйтесь панелью BitDefender антифишинг, интегрированной в Internet Explorer. Больше информации здесь «*Панель инструментов антифишинга*» (p. 164).

11.2. Дополнительные настройки - Контроль конфиденциальности

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

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

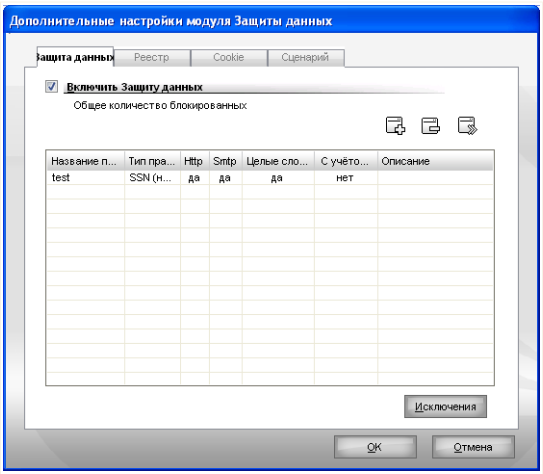
Контроль конфиденциальности позволяет безопасно хранить конфиденциальную информацию. Этот модуль проверяет HTTP или SMTP трафик в поисках указанных Вами строк. Если найдено совпадения, соотвествующая веб-страница или электронное сообщение блокируется.

Существует возможность работы нескольких пользователей, так что ни один из пользователей не имеет доступа к правилам установленными Вами.

Правила личных данных можно конфигурировать в разделе **Конфиденциальность**. Чтобы перейти в этот раздел, откройте окно **Дополнительные настройки Контроля личных данных** и нажмите вкладку **Конфиденциальность**.

Замечание

Открыть окно **Дополнительные настройки Контроля личных данных**, нажать **Контроль личных данных>Состояние** в консоли настроек и нажмите **Дополнительные настройки**.



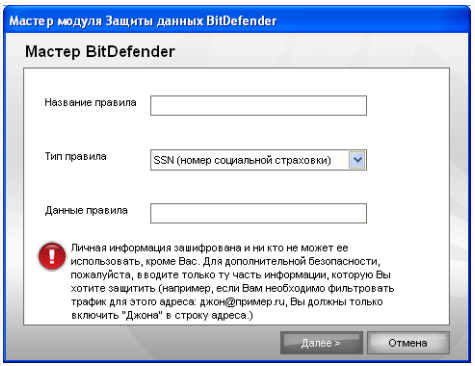
Контроль конфиденциальности

11.2.1. Создание правил конфиденциальности

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

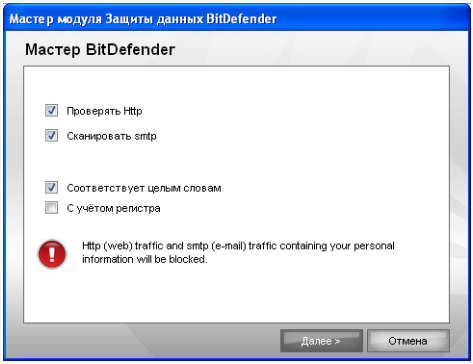
- **Тип правила** - выберите тип правила (адрес, имя, кредитная карта, PIN-код и т.д.).
- **Данные правила** - введите данные правила.

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

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

Нажмите **Далее**.

Шаг 2/3 - Выбор трафика



Выберите трафик

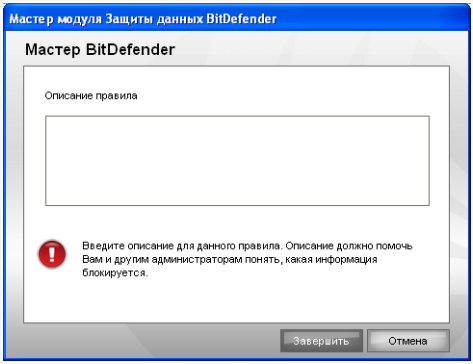
Выберите трафик, который будет проверяться BitDefender. Доступны следующие варианты:

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

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

Нажмите **Далее**.

Шаг 3/3 - Описание правила



Опишите правило

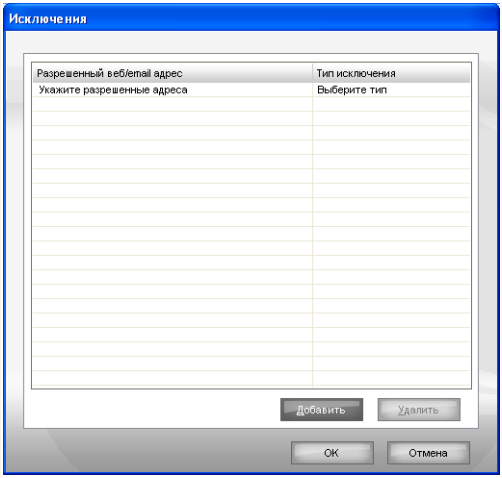
Введите краткое описание правила в поле редактирования.

Нажмите **Завершить**.

11.2.2. Определение исключений

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

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



Исключения

Добавить исключение, следуя по этим шагам:

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

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

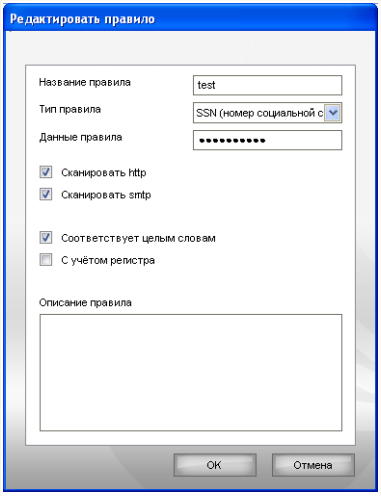
Нажмите **OK**, чтобы сохранить изменения.

11.2.3. 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.

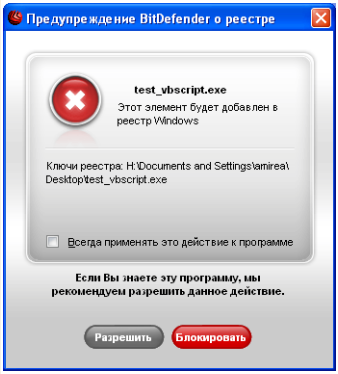
Нажмите **OK**, чтобы сохранить изменения и закройте окно.

11.3. Дополнительные настройки. Управление реестром

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

В **Реестре** также определяется, какие программы необходимо автоматически загружать при запуске Windows. Многие 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 **Всегда применять это действие к данной программе**. В этом случае будет создано правило, и то же самое действие будет применено для любой программы, которая попытается изменить запись в реестре, чтобы загружаться при запуске Windows.

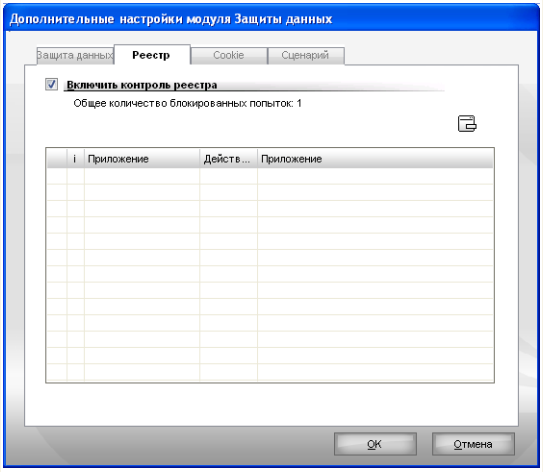
Замечание

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

Каждое правило, которое запомнили, можно найти для редактирования в разделе **Реестр**. Чтобы перейти в этот раздел, откройте окно **Дополнительные настройки Контроля личных данных** и нажмите на вкладку **Реестр**.

Замечание

Открыть окно **Дополнительные настройки Контроля личных данных**, нажать **Контроль личных данных>Состояние** в консоли настроек и нажмите **Дополнительные настройки**.



Контроль реестра

В этом окне Вы видите список правил в таблице.

Чтобы удалить правило, только выберите его и нажать кнопку **Удалить**. Чтобы временно отключить данное правила без его удаления, уберите отметку из соответствующего поля.

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

Нажмите **OK**, чтобы закрыть окно.

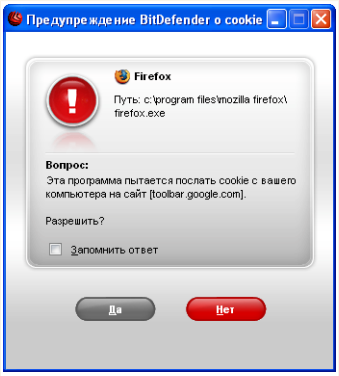
11.4. Дополнительные настройки. Контроль cookie

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

Но файлы cookie 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.

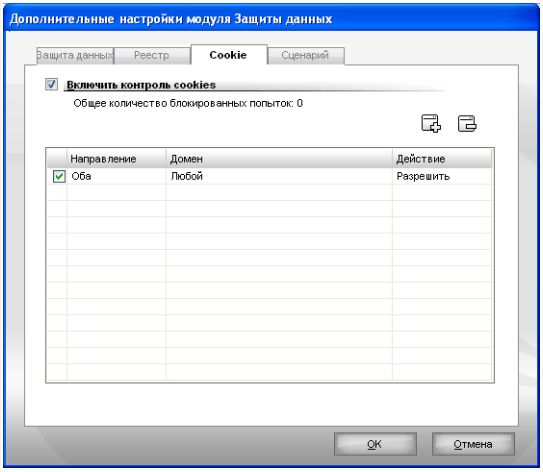
Замечание

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**. Чтобы перейти в этот раздел, откройте окно **Дополнительные настройки Контроля личных данных** и нажмите на вкладку **Cookie**.

Замечание

Открыть окно **Дополнительные настройки Контроля личных данных**, нажать **Контроль личных данных>Состояние** в консоли настроек и нажмите **Дополнительные настройки**.



Контроль cookie

В этом окне Вы видите список правил в таблице.

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.

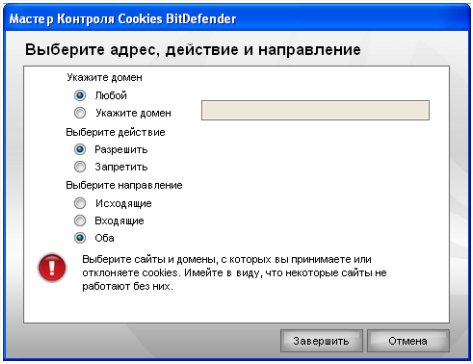
Чтобы удалить правило, достаточно выделить его и нажмите кнопку **Удалить**. Чтобы изменить параметр правила, дважды нажмите поле и внесите соответствующие изменения. Чтобы временно отключить правило без его удаления, уберите галочку в соответствующем поле.

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

11.4.1. 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**.

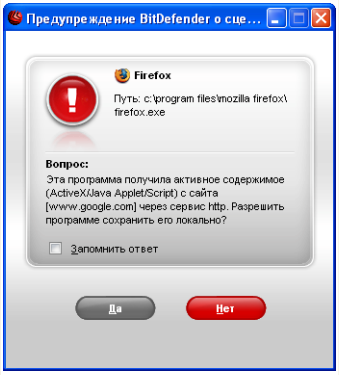
Нажмите **OK**, чтобы сохранить изменения и закройте окно.

11.5. Дополнительные настройки. 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

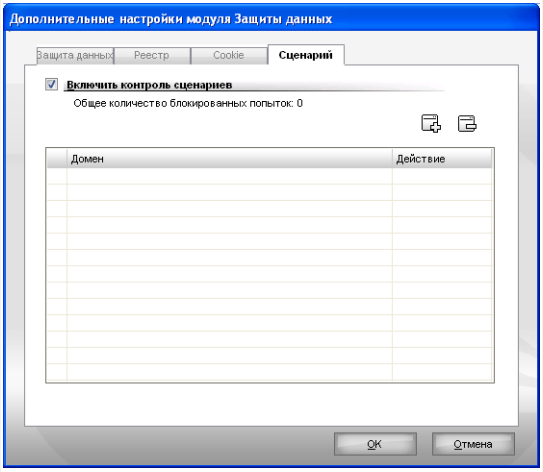
В этом окне Вы видите название ресурса.

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**. Чтобы перейти в этот раздел, откройте окно **Дополнительные настройки Контроля личных данных** и нажмите на вкладку **Сценарии**.

Замечание

Открыть окно **Дополнительные настройки Контроля личных данных**, нажать **Контроль личных данных>Состояние** в консоли настроек и нажмите **Дополнительные настройки**.



Контроль сценариев

В этом окне Вы видите список правил в таблице.

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.

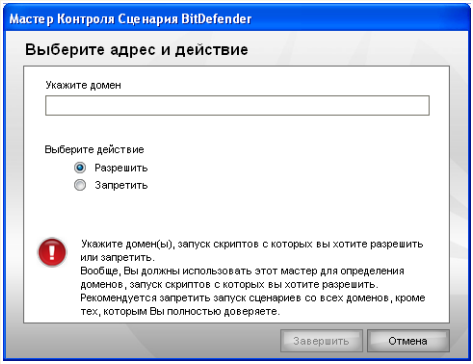
Чтобы удалить правило, достаточно выделить его и нажмите кнопку **Удалить**. Чтобы изменить параметр правила, дважды нажмите поле и внесите соответствующие изменения. Чтобы временно отключить правило без его удаления, уберите галочку в соответствующем поле.

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

11.5.1. 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.

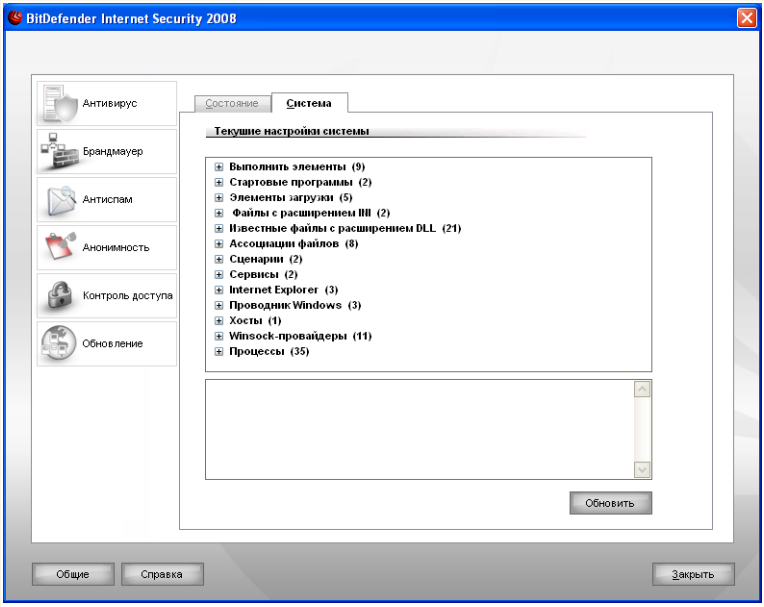
Нажмите **Завершить**.

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

11.6. Информация о системе

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

Чтобы получить информацию о системе, в консоли управления нажмите **Контроль личных данных>Информация о системе**. Появится следующее окно:



Информация 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. Вы должны нажать **Да** для подтверждения Вашего выбора.

> ***Замечание***
> Если Вы не хотите, чтобы постоянно появлялось подтверждение Вашего выбора, отметьте **Не спрашивать меня больше за этот сеанс**.

- **Перейти** - открывается окно, в которое помещается выбранный объект (например, **Регистр**).

■ **Обновить** - обновляется информация в разделе **Информация о системе**.

Замечание
В зависимости от выбранного элемента, один или оба из **Удалить** или **Перейти к**, кнопки не могут появится.

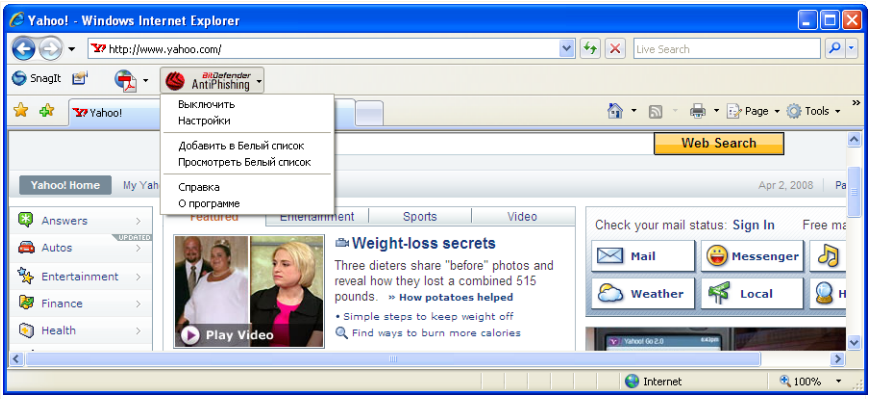
11.7. Панель инструментов антифишинга

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

Вы можете легко и эффективно управлять настройками антифишинга и Белым Списком при помощи панели BitDefender антифишинг, интегрируемой в Internet Explorer.

Панель антифишинга, **Иконка BitDefender**, он располагается в верхней части Internet Explorer. Нажмите на это, чтобы открыть меню панели инструментов.

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



Панель инструментов антифишинга

Следующие команды доступны в меню панели инструментов:

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

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

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

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

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

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

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

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

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

12. Контроль доступа

Модуль Контроля доступа может заблокировать доступ к:

- неприемлемые веб-страницы.
- Интернет, для определенных промежутков времени (например, когда время уроков).
- веб-страницы и почтовые сообщения, если они содержат ключевое слово.
- приложения, такие как игры, чаты, программы обмена файлами и другие.

Важно

Этот модуль могут просматривать и изменять только пользователи с правами администратора (системные администраторы). Если настройки защищены паролем, они могут быть изменены только если предоставлен правильный пароль. Администратор не может принудительно применить набор правил для пользователя, для которого набор правил уже был применен ранее другим администратором.

Раздел **Котроль доступа** данного руководства пользователя включает в себя следующие темы:

- Защита настроек Контроля доступа
- Состояние модуля Контроль доступа
- Веб-контроль
- Контроль приложений
- Фильтр ключевых слов
- Ограничитель времени в сети

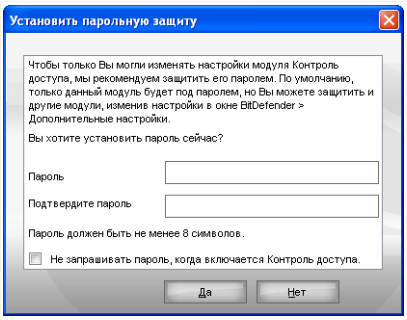
12.1. Защита настроек Контроля доступа

Если вы не единственный, кто имеет права администратора данного компьютера, рекомендуется защитить настройки Контроля доступа BitDefender паролем. Установив пароль, вы защитите сконфигурированные вами для определенных пользователей настройки модуля Контроля доступа от изменений другими пользователями, обладающими правами администратора.

При включении Контроля доступа BitDefender запросит у вас пароль (при настройках по умолчанию).

Для того, чтобы установить парольную защиту, проделайте следующее:

1. Введите пароль в поле **Пароль**.
2. Введите пароль еще раз в поле **Подтверждение пароля**.
3. Нажмите **OK**, чтобы сохранить пароль и закройте окно.



Установить парольную защиту

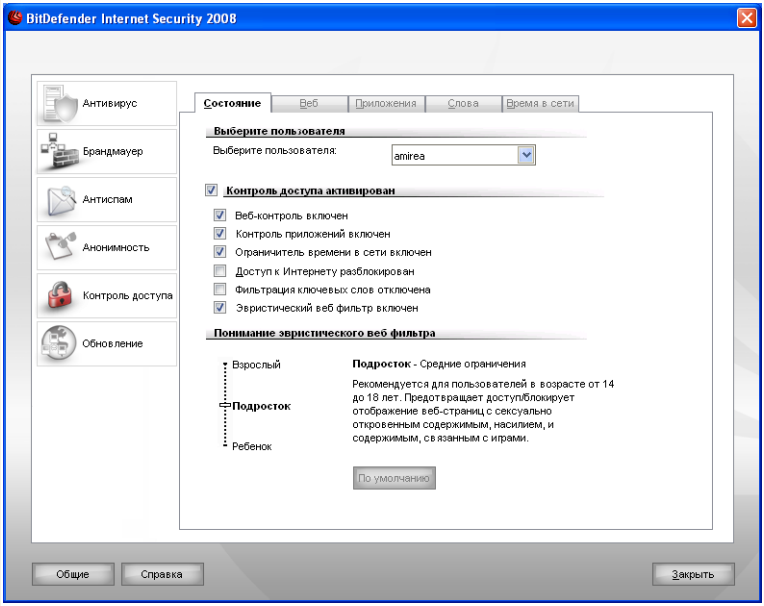
С этого момента всякий раз, когда Вы захотите изменить настройки Контроля доступа, Вы должны будете ввести пароль. Другие системные администраторы (если есть) также должны будут ввести пароль для изменения настроек Контроля доступа.

Замечание
Этот пароль не защитит другие настройки BitDefender.

Если Вы не хотите, чтобы постоянно появлялось это окно, отметьте **Не запрашивать пароль во время включения Контроля доступа**.

12.2. Статус Контроля доступа

Чтобы настроить Контроль доступа для выбранного пользователя, нажмите **Контроль доступа>Статус** в консоли настроек. Появится следующее окно:



Статус Контроля доступа

Важно

Всегда включайте **Контроль доступа**, чтобы оградить Ваших детей от неадекватного содержимого страниц при помощи настройки правил доступа на Вашем компьютере.

12.2.1. Выберите уровни защиты

Чтобы натсроить уровень защиты, прежде всего необходимо выбрать пользователя, для которого будут применяться эти настройки. Затем настройте уровень защиты при помощи следующих настроек:

- **Веб контроль** - включить **Веб контроль**, чтобы ограничивать передвижения в интернет согласно правилам, установленным Вами в разделе Веб.
- **Контроль приложений** - включите **Контроль приложений**, чтобы блокировать приложения на Вашем компьютере согласно правилам, установленным Вами в разделе Приложения.

- **Ограничитель времени в сети** - включен **Ограничитель времени в сети**, чтобы разрешить доступ в сеть согласно расписанию, установленному Вами в разделе Ограничитель времени.
- **Доступ в сеть** - включите данную опцию, чтобы заблокировать доступ ко всем веб-сайтам (не только к тем, которые указаны в разделе Веб).
- **Фильтр ключевых слов** - включите **Фильтр ключевых слов**, чтобы фильтровать доступ в интернет и почту согласно правилам, установленным Вами в разделе Ключевые слова.
- **Эвристический веб фильтр** - включите данную опцию, чтобы блокировать доступ в веб согласно ранее установленным правилам, основанным на возрастных категориях.

Замечание

В полной мере воспользоваться всеми преимуществами модуля Контроль доступа можно только, если Вы настроили следующие опции. Для того, чтобы узнать, как их настроить, обратитесь к следующим темам этой главы.

12.2.2. Конфигурация эвристического веб фильтра

Эвристический веб фильтр анализирует веб страницы и блокирует те из них, которые соответствуют шаблонам страниц с потенциально неадекватным содержимым.

Для того, чтобы ограничивать доступ к веб-ресурсам с помощью предустановленных установок на основе возраста пользователя, Вы должны выбрать соответствующий уровень толерантности. Перемещайте ползунок по шкале, чтобы выставить уровень толерантности, адекватный на Ваш взгляд для данного пользователя.

Существует 3 «уровня толерантности»

«Уровень толерантности»	*Описание*
Ребенок	Предполагает ограниченный доступ в интернет, рекомендуется для пользователей в возрасте до 14 лет. Блокируются веб-страницы с потенциально вредным для детей содержанием (порнография, сексуальность, наркотики, хакерство и т.п).

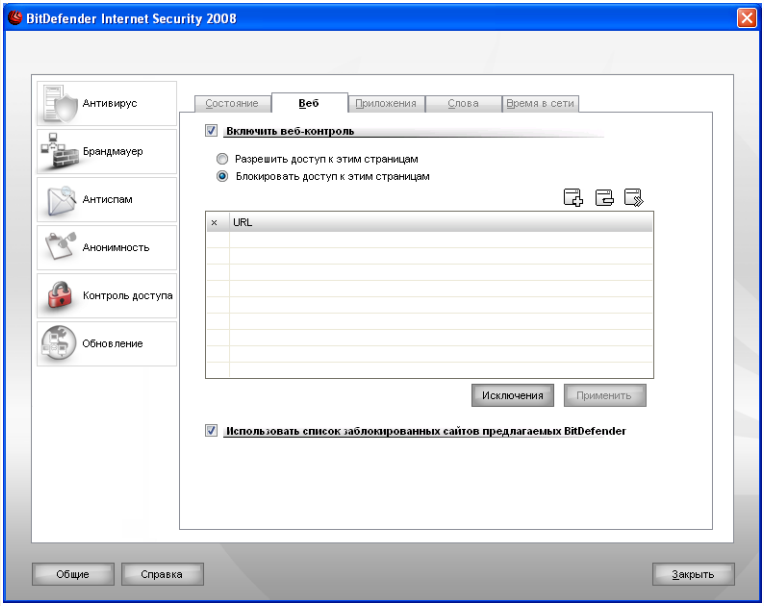
« Уровень толерантности»	*Описание*
Подросток	Предполагает ограниченный доступ в интернет, рекомендуется для пользователей в возрасте от 14 до 18 лет. Блокируются веб-страницы с контентом, содержащим элементы сексуальности, порнографии.
Взрослый	Предполагает неограниченный доступ ко всем веб-страницам, независимо от их содержания.

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

12.3. Веб-контроль

Веб-контроль дает Вам возможность блокировать доступ к сайтам с недопустимым, по вашему мнению, содержанием. BitDefender предоставляет пользователям и регулярно обновляет список сайтов-кандидатов на блокирование. Кроме того, по желанию пользователя можно блокировать доступ к веб-страницам, содержащим ссылки на помещенные в "черный список" сайты.

В данном разделе можно настроить Веб контроль, нажав **Контроль доступа>Веб** в консоли настроек. Появится следующее окно:



Веб-контроль

Чтобы включить эту защиту, установите значок в поле, соответствующем опции **Включить веб контроль**.

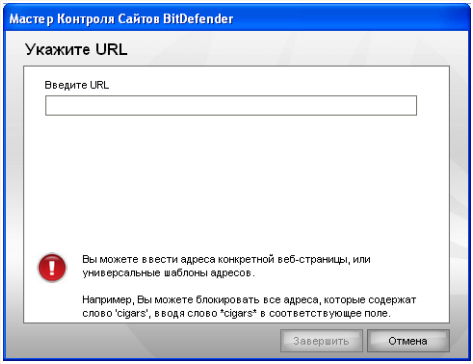
Выберите **Разрешить доступ к данным страницам/Запретить доступ к данным страницам**, чтобы просмотреть список разрешенных/заблокированных сайтов. Нажмите **Исключения...**, чтобы перейти к окну, где можно просмотреть дополнительный список.

Правила необходимо добавлять вручную. Прежде всего выберите **Разрешить доступ к данным страницам/Запретить доступ к данным страницам**,чтобы разрешить/запретить доступ к веб-сайтам, указанным Вами в мастере. Затем нажмите кнопку **Добавить...**, чтобы запустить мастера настройки.

12.3.1. Мастер конфигурации

Мастер конфигурации запускает процедуру из 1 шага.

Шаг 1/1 - Укажите веб-сайты



Укажите веб-сайты

Введите веб-сайты, для которых будет применяться правило, затем нажмите **Закончить**.

Важно
Имя домена должно иметь следующий вид:

- `*.xxx.com` - действие правила будет распространяться на все веб-сайты, оканчивающиеся на `.xxx.com`;
- `*porn*` - действие правила будет распространяться на все веб-сайты, адрес которых содержит `porn`;
- `www.*.com` - действие правила будет распространяться на все веб-сайты с доменным окончанием `com`;
- `www.xxx.*` - действие правила будет распространяться на все веб-сайты, адрес которых начинается с `www.xxx.`, независимо от доменного окончания.

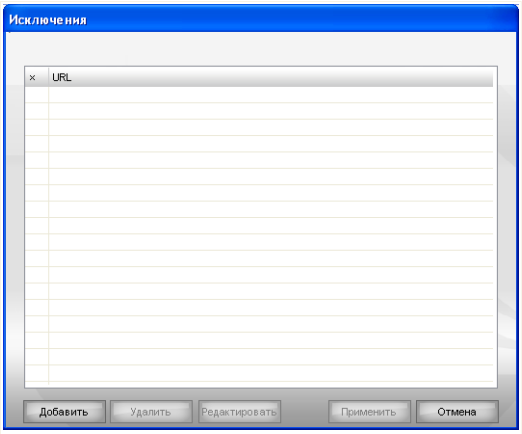
Нажмите **Применить**, чтобы сохранить изменения.

Чтобы удалить правило, выберите его и нажмите кнопку **Удалить**. Чтобы изменить правило, выберите его и нажмите кнопку **Редактировать...** или дважды нажмите на правило. Чтобы временно отключить правило, не удаляя его, уберите галочку из соответствующего поля.

12.3.2. Установка исключений

Иногда бывает необходимо указать исключения для определенного правила. Например, Вы создали правило, которое блокирует сайты, адреса которых содержат слово "killer" (синтаксис: `*killer*`). вы также знаете о существовании сайта `killer-music`, где пользователи могут слушать музыку. Чтобы создать исключение из ранее созданного правила, перейдите в окно **Исключения** и определите необходимые исключения.

Нажмите **Исключения...**. Появится окно следующего вида:



Определение исключений

Нажмите **Добавить...**, чтобы указать исключения. Появится мастер настройки. Завершите все шаги мастера, чтобы установить исключения.

Нажмите **Применить**, чтобы сохранить изменения.

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

12.3.3. Черный список сайтов BitDefender

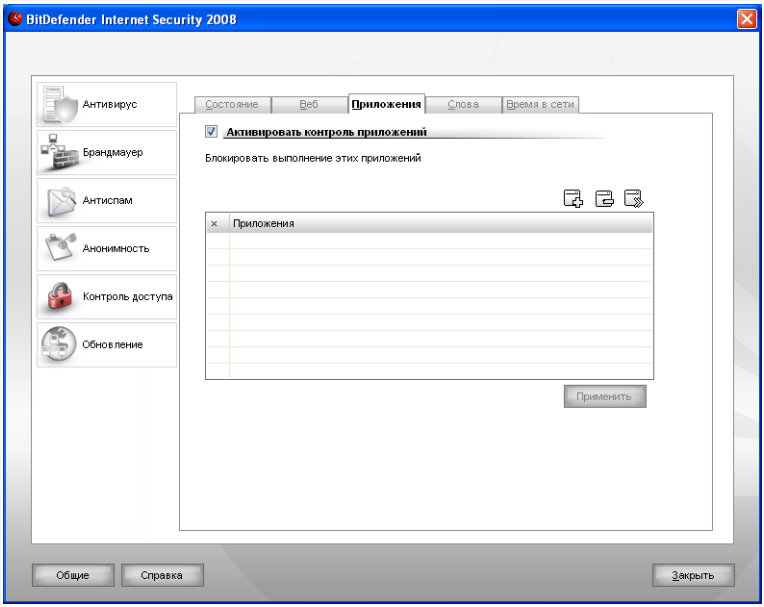
Чтобы помочь защитить Ваших детей, BitDefender предоставляет черный список вебсайтов с неадекватным или потенциально опасным содержанием. Чтобы

заблокировать сайты из данного списка, выберите **Использовать список блокируемых сайтов BitDefender**.

12.4. Контроль приложений

Контроль приложений позволяет Вам блокировать выполнение любого приложения. Таким образом можно заблокировать игровые, медийные и информационные программы, а также другие категории программного обеспечения и вредоносных кодов. Блокировка приложений таким способом одновременно защищает их от модификации, и поэтому они не могут быть скопированы или перемещены.

Чтобы настроить Контроль приложений, нажмите **Контроль доступа>Приложения** в консоли настроек. Появится следующее окно:



Контроль приложений

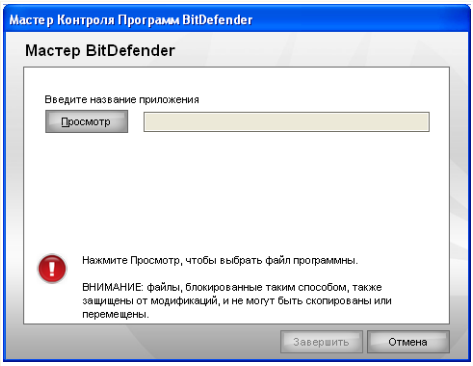
Чтобы включить эту защиту, установите значок на поле, соответствующем опции **Включить контроль приложений**.

Правила необходимо вводить вручную. Нажмите кнопку **Добавить...**, чтобы запустить мастера настройки.

12.4.1. Мастер конфигурации

Мастер конфигурации запускает процедуру из 1 шага.

Шаг 1/1 - Выбор приложения для блокировки



Выберите приложение для блокировки

Нажмите **Обзор**, выберите приложение для блокировки и нажмите **Завершить**.

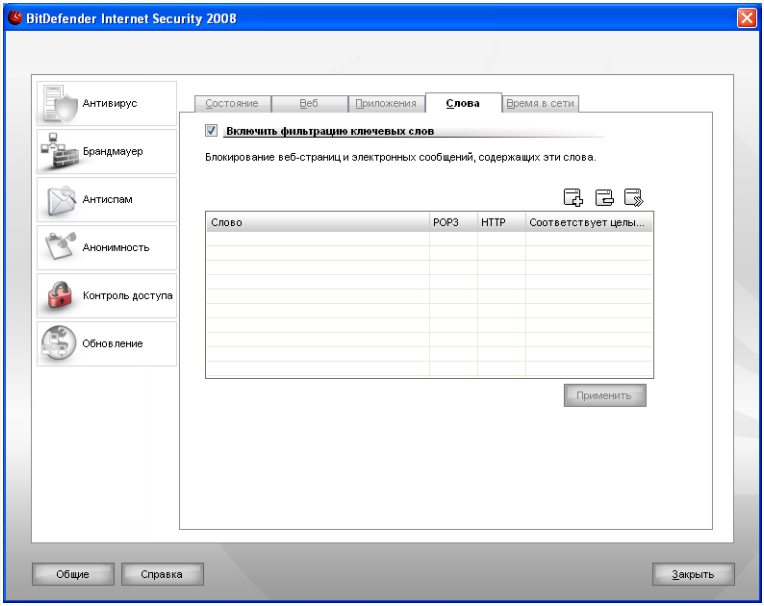
Нажмите **Применить**, чтобы сохранить изменения.

Чтобы удалить правило, выберите его и нажмите кнопку **Удалить**. Чтобы изменить правило, выберите его и нажмите кнопку **Редактировать...** или дважды нажмите на правило. Чтобы временно отключить правило, не удаляя его, уберите галочку из соответствующего поля.

12.5. Фильтрация ключевых слов

Фильтр ключевых слов помогает блокирвать электронные сообщения или веб-страницы, содержащие определенные слова. Таким образом, можно защитить пользователей от просмотра неадекватных слов или фраз.

тобы настроить Фильтр ключевых слов, нажмите **Контроль доступа>Ключевые слова** в консоли управления. Появится следующее окно:



Фильтрация ключевых слов

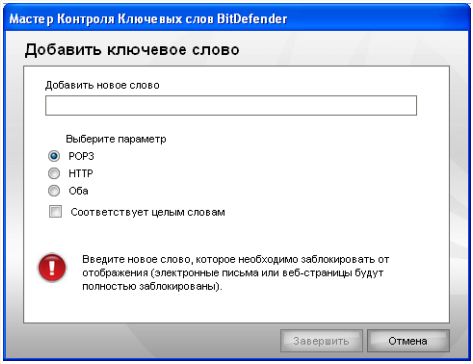
Чтобы включить эту защиту, установите значок на поле, соответствующем опции **Фильтрация ключевых слов**.

Правила необходимо вводить вручную. Нажмите кнопку **Добавить...**, чтобы запустить мастера настройки.

12.5.1. Мастер конфигурации

Мастер конфигурации запускает процедуру из одного шага.

Шаг 1/1 - Введите ключевое слово



Введите ключевое слово

Вы должны установить следующие параметры:

- **Ключевое слово** - введите в поле редактирование слово или фразу, которую Вы хотите блокировать.
- **Протокол** - выберите протокол, в котором BitDefender должен искать блокируемое слово.

  Доступны следующие варианты:

Настройка	Описание
POP3	Блокируются электронные сообщения, содержащие ключевое слово.
HTTP	Блокируются веб-страницы, содержащие ключевое слово.
Входящие и исходящие	Блокируются и электронные сообщения, и веб-страницы, содержащие ключевое слово.

Нажмите **Применить**, чтобы сохранить изменения.

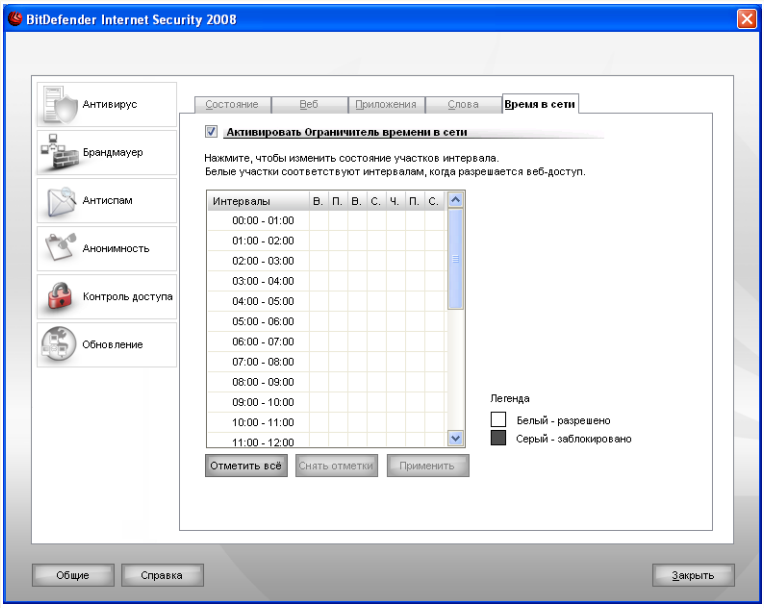
Чтобы удалить правило, выберите его и нажмите кнопку **Удалить**. Чтобы изменить правило, выберите его и нажмите кнопку **Редактировать...** или дважды нажмите на правило. Чтобы временно отключить правило, не удаляя его, уберите галочку из соответствующего поля.

12.6. Ограничитель времени в сети

Используя **Ограничитель времени в сети**, Вы можете разрешить или блокировать веб-доступ для пользователей или приложений в течение указанных интервалов времени.

Замечание
Независимо от настроек **Ограничителя времени в сети** программа BitDefender будет выполнять ежечасное автоматическое обновление продукта.

Чтобы настроить Ограничитель времени в сети, нажмите **Контроль доступа>Ограничитель времени** в консоли настроек. Появится следующее окно:



Ограничитель времени в сети

Чтобы включить эту защиту, установите значок на поле, соответствующем опции **Включить Ограничитель времени в сети**.

Выберите временные интервалы, в пределах которых будут заблокированы все соединения с сетью Интернет. Вы можете выбрать короткие интервалы, щелкая мышкой на соответствующих ячейках, а более продолжительные интервалы – наведя курсор, нажав левую кнопку мышки и, не отпуская ее, закрашивать несколько соседних ячеек. Также можно нажать **Выбрать все**, чтобы выбрать все ячейки, и, соответственно, полностью заблокировать доступ в интернет. После нажатия **Отменить все выделение**, доступ в интернет будет постоянно разрешен.

Важно
Ячейки, окрашенные серым цветом, соответствуют временным интервалам, в пределах которых заблокированы все соединения с сетью Интернет.

Нажмите **Применить**, чтобы сохранить изменения.

13. Обновление

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

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

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

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

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 защиты от спама** - к эвристическому и URL фильтрам будут добавлены новые правила, а фильтру изображений - новые изображения. Это поможет повысить эффективность вашей защиты от спама. Этот тип обновления также известен как **Обновление Антиспама**.
- **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**.

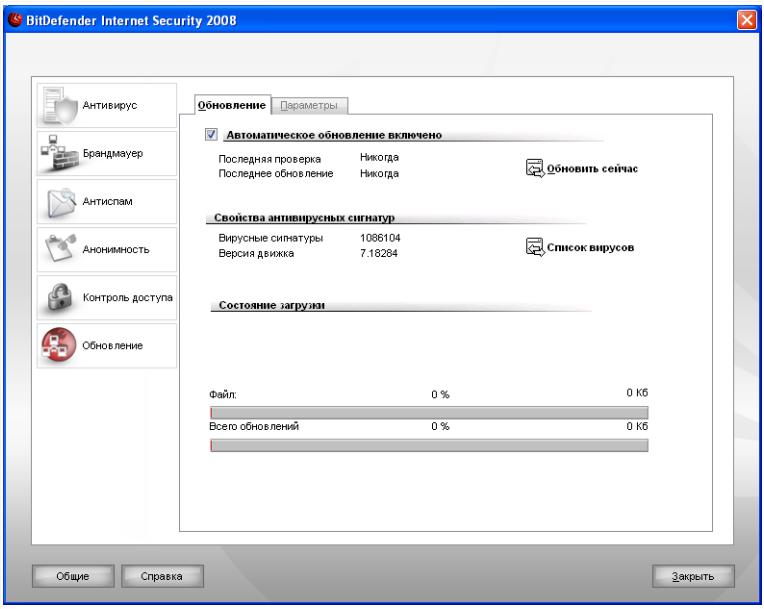
Раздел **Обновление** этого руководства пользователя содержит следующие темы:

- Автоматическое обновление

- Настройки обновления

13.1. Автоматическое обновление

Просматривать связанную с обновлением информацию и выполнять автоматические обновления, нажмите **Обновление>Обновление** в консоли настроек. Появится следующее окно:



Автоматическое обновление

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

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.

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

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

13.1.1. Требование к обновлению

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

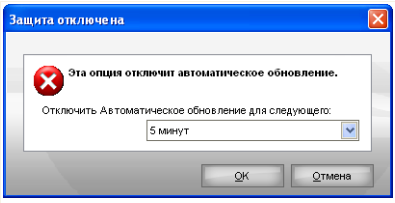
Модуль **Обновления** подключится к серверу обновления BitDefender и проверит наличие обновлений. Если программа обнаруживает новое обновление, то, в зависимости от настроек, установленных в разделе Опции обновления вручную. Вам будет предложено подтвердить загрузку обновления или обновление будет производиться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

13.1.2. Отключение автоматического обновления

Если Вы выберите эту опцию, то появится окно с предупреждением:



Отключить автоматическое обновление

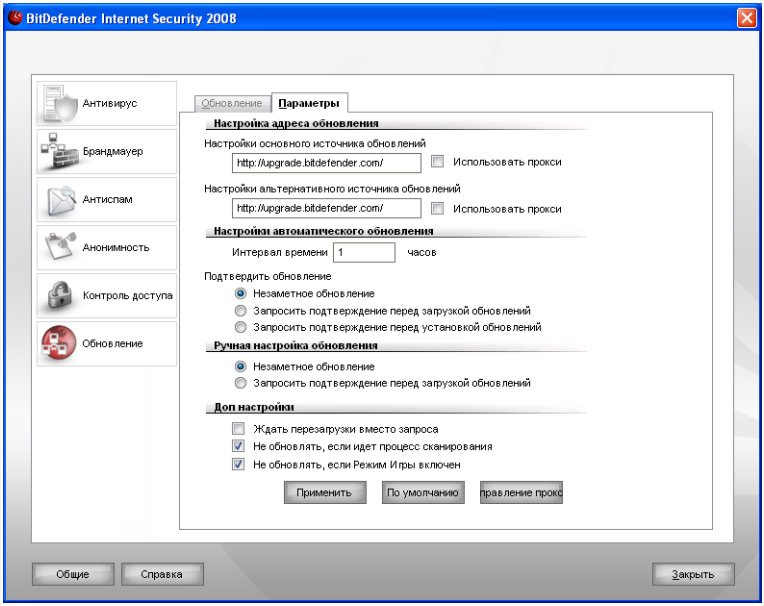
Вы должны подтвердить свое намерение, выбрав промежуток времени, на который Вы хотите отключить автоматическое обновление. Вы можете отключить на 5, 15 или 30 минут, на час, навсегда или до следующей перезагрузки системы.

Внимание
Этот аспект является критическим с точки зрения безопасности. Рекомендуем Вам отключать автоматическое обновление на как можно меньший промежуток времени. Если автоматическое обновление отключено, Вы не защищены от самых последних угроз.

13.2. Настройки обновления

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

Установить настройки обновлений и настроить прокси можно нажав **Обновления>Настройки** в консоли управления. Появится следующее окно:



Настройки обновления

В окне Настройки обновления Вы можете увидеть четыре типа настроек: (**Настройки местоположения обновления**, **Настройки автоматического обновления**, **Обновления вручную** и **Настройки интерфейса**).

13.2.1. Настройки местоположения обновления

Чтобы настроить местоположение обновлений, используйте опции для категории **Настройки местоположения обновления**.

Замечание
Изменять данные настройки нужно лишь в том случае, если Вы подключены к локальной сети, в которой хранятся обновления BitDefender, или если Вы осуществляете соединение с Интернет через прокси сервер.

Для более надежных и быстрых обновлений, Вы можете настроить 2 места обновления:**Основное местоположение обновлений** и **Альтернативное**

местоположение обновлений. По умолчанию, это: `http://upgrade.bitdefender.com`.

Чтобы изменить адрес источника, откуда берутся обновления, введите URL адрес локального зеркала в поле **URL**, соответствующем месту, которое Вы хотите изменить.

Замечание
Рекомендуем установить местное зеркало в качестве первоначального источника обновления и оставить альтернативный источник без изменений, в качестве запасного на случай, если местное зеркало станет недоступным.

Если компания использует прокси сервер для выхода в Интернет, поставьте отметку в поле **использовать прокси**, а затем нажмите **Настроить прокси**.

Замечание
Больше информации Вы найдете здесь «*Управление прокси*» (p. 187)

13.2.2. Конфигурирование автоматического обновления

Чтобы настроить автоматическое обновление, иисползуйте опции в разделе **Настройки автомотического обновления**.

Вы можете указать количество часов между запросами на наличие обновлений в поле **Интервал времени**. По умолчанию интервал составляет 1 час.

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

- **Обновление без предупреждения** - BitDefender автоматически скачивает и устанавливает обновления.
- **Запрос перед загрузкой обновлений** - каждый раз, когда появится новое обновление, BitDefender будет запрашивать ваше подтверждение перед загрузкой.

Замечание
Вам будет запрос о загрузке обновлений, даже если Вы вышли из Центра Безопасности.

- **Запрос перед установкой обновлений** - каждый раз, когда будет загружено обновление, Вам будет запрос об их загрузке.

Замечание
Вам будет запрос об установке обновлений, даже если Вы вышли из Центра Безопасности.

13.2.3. Конфигурация обновлений вручную

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

- **Обновление без предупреждения** - обновление вручную будет выполняться автоматически в фоновом режиме.
- **Запрос перед загрузкой обновлений** - каждый раз, когда появится новое обновление, BitDefender будет запрашивать ваше подтверждение перед загрузкой.

Замечание
Вам будет запрос о загрузке обновлений, даже если Вы вышли из Центра Безопасности.

13.2.4. Дополнительные настройки

Чтобы избежать того, когда процесс обновления BitDefender мешает Вашей работе на компьютере, настройте опции в категории **Дополнительные настройки**:

- **Ожидать перезагрузки без запроса** - Если для завершения установки обновления необходимо выполнить перезагрузку компьютера, то программа будет продложать работу со старыми файлами до перезагрузки системы. При этом сообщение с запросом пользователя о необходимости перезапуска системы появляться не будет, в связи с чем 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, этот процесс будет прерван.

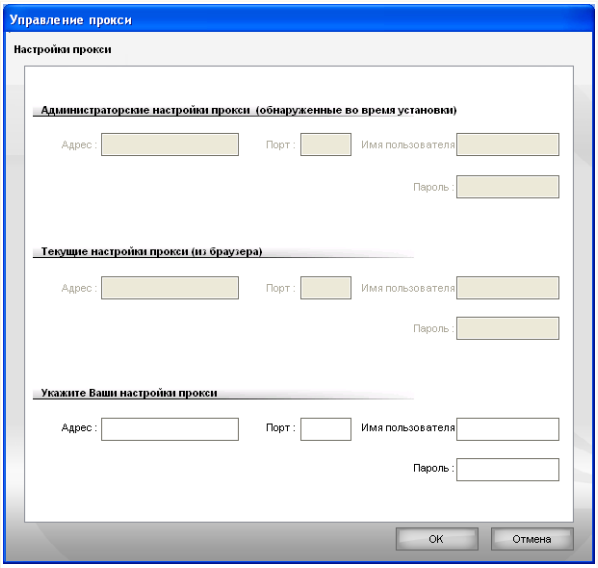
- **Не выполнять обновление, когда включен режим игры** - BitDefender не обновиться, пока включен режим игры. Таким образом, Вы можете минимизировать влияние продукта на работу системы в течение игр.

13.2.5. Управление прокси

Если Ваша компания использует прокси сервер для подсоединения к Интернет, Вам необходимо указать настройки прокси сервера, чтобы BitDefender имел возможность обновляться. В противном случае, он будет использовать настройки прокси администратора, устанавливавшего программу или настройки прокси текущего браузера, если таковые имеются.

Замечание
Настройки прокси сервера могут изменяться только пользователями с правами администратора компьютера или же пользователями, знающими пароль к настройкам программы.

Чтобы настроить прокси сервер, нажмите **Настроить прокси**. Откроется окно **Прокси менеджера**.



Прокси менеджер

Есть три параметра настройки для прокси:

- **Настройки прокси администратора (определены в процессе установки)** - настройки прокси сервера, определенные в процессе установки программы в учетной записи администратора, эти настройки могут быть изменены, только если Вы работаете под данной учетной записью. Если прокси сервер требует указания имени пользователя и пароля, укажите их в соответствующих полях.
- **Текущие настройки прокси (из браузера, используемого по умолчанию)** - настройки прокси сервера для текущего пользователя, полученные из браузера, используемого по умолчанию. Если прокси сервер требует указания имени пользователя и пароля, укажите их в соответствующих полях.

Замечание
Поддерживаемыми браузерами являются Internet Explorer, Mozilla Firefox и Opera. Если по умолчанию Вы используете другой браузер, BitDefender не сможет получить настройки прокси сервера для текущего пользователя.

- **Ваши собственные настройки прокси** - вы можете изменять настройки прокси, если зашли как администратор.

  Следующие настройки должны быть определены:
  - **Адрес** - введите IP-адрес к прокси серверу.
  - **Порт** - введите порт использующий BitDefender для подсоединения к прокси серверу.
  - **Пользователь** - введите имя пользователя, опознаваемого прокси-сервером.
  - **Пароль** - введите пароль пользователя, указанного ранее.

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

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

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

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

BitDefender Rescue CD

14. Краткий обзор

BitDefender Internet Security 2008 поставляется с загрузочным диском (BitDefender Rescue CD), который может проверить и вылечить все существующие жесткие диски перед запуском операционной системы.

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

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

BitDefender Rescue CD (диск-реаниматор BitDefender) - это измененный дистрибутив Knoppix, с интегрированным решением BitDefender для Linux на носителе GNU/Linux Knoppix Live CD, который представляет собой готовое к использованию антивирусное решение, которое можно использовать для проверки и "дезинфекции" жестких дисков (включая и разделы Windows NTFS). В то же время, диск-реаниматор BitDefender можно использовать для восстановления ценных данных в случаях, когда не возможно загрузить ОС Windows.

Замечание
Вы можете скачать BitDefender Rescue CD отсюда: http://download.bitdefender.com/rescue_cd/

14.1. Системные требования

Перед загрузкой BitDefender Rescue CD, необходимо сначала проверить соответствие вашей системы следующим требованиям.

Тип процессора
x86-совместимый процессор с минимальной тактовой частотой 166 МГц, что, однако, не гарантирует устойчивой работы программы. Процессор поколения i686, с тактовой частотой 800МГц.

Память
Минимум 512 Мб оперативной памяти (рекомендуется 1 Гб)

CD-ROM

BitDefender Rescue CD запускается с компакт-диска, поэтому необходимыми является наличие дисковода CD-ROM и настройка BIOS на загрузку системы с компакт-диска.

Подключение к сети Интернет

Хотя программа BitDefender Rescue CD выполняется без подключения к сети Интернет, для процедур обновления необходим доступ к активной ссылке HTTP, хотя бы через прокси-сервер. Поэтому для установки последнего обновления, подключение к сети Интернет является ОБЯЗАТЕЛЬНЫМ.

Графическая разрешающая способность

Стандартная SVGA-совместимая карта.

14.2. Включенное программное обеспечение

В компакт-диск BitDefender Реаниматор входят следующие пакеты программ.

Xedit

Это текстовый редактор.

Vim

Это мощный текстовый редактор, поддерживающий подсветку синтаксиса, графический интерфейс пользователя (GUI) и многое другое. Для более подробной информации смотрите Домашнюю страницу Vim .

Xcalc

Это калькулятор.

RoxFiler

RoxFiler - быстрый и мощный пакет для работы с графическими файлами.

Больше информации Вы найдете домашняя страница RoxFiler.

MidnightCommander

GNU Midnight Commander (mc) - файловый менеджер.

Более подробная информация домашняя страница MC.

Pstree

Pstree - показывает запущенные процессы.

Top

Top - показывает Linux задачи.

Xkill

Xkill - убивает клиента его X ресурсами.

Partition Image

Partition Image помогает сохранить разделы системных форматов EXT2, Reiserfs, NTFS, HPFS, FAT16 и FAT32 в файлы образов. Данная программа очень полезна при осуществлении резервного копирования данных.

Более подробная информация домашняя страница Partimage.

GtkRecover

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

Более подробная информация домашняя страница GtkRecover.

ChkRootKit

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

Более подробная информация домашняя страница ChkRootKit.

Nessus Network Scanner

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

Более подробная информация домашняя страница Nessus.

Iptraf

Iptraf – консольная утилита для сбора сетевой статистики.

Более подробная информациядомашняя страница Iptraf.

Iftop

Iftop - утилита позволяющая мониторить трафик в реальном времени.

Более подробная информация домашняя страница Iftop.

MTR

MTR - диагностический инструмент сети.

Более подробная информация домашняя страница MTR.

PPPStatus

PPPStatus отображает статистическую информацию о входящих и исходящих потоках трафика по TCP/IP.

Более подробная информация домашняя страница PPPStatus.

Wavemon

Wavemon - программа мониторинга для беспроводных сетевых устройств.

Более подробная информация домашняя страница Wavemon.

USBView

USBView показывает информацию об устройствах, связанных с USB.

Более подробная информация домашняя страница USBView.

Pppconfig

Pppconfig помогает автоматически настраивать dial-up ppp-соединение.

DSL/PPPoe

DSL/PPPoe настраивает PPPoE (ADSL) соединение.

I810rotate

I810rotate - переключатель видео сигналов на i810 аппаратном оборудование используя i810switch(1).

Более подробная информация домашняя страница I810rotate.

Mutt

Mutt - мощный почтовый клиент на текстовой основе MIME.

Более подробная информация домашняя страница Mutt.

Mozilla Firefox

Mozilla Firefox - один из лучших веб браузеров.

Более подробная информация домашняя страница Mozilla Firefox.

Elinks

Elinks - текстовый веб браузер.

Более подробная информация домашняя страница Elinks.

15. Реаниматор BitDefender

Данный раздел содержит информацию о том, как запускать и останавливать работу диска-реаниматора BitDefender, проверять Ваш компьютер на наличие вредоносных программ, а также сохранять данные с неработающей системы Windows на сменные носители. Однако, при помощи программ, имеющихся на данном диске, Вы можете выполнять гораздо больше действий, чем описано в данном руководстве.

15.1. Запуск BitDefender Rescue CD

Чтобы запустить BitDefender Rescue CD, установите настройки BIOS вашего компьютера на загрузку с дисковода, поместите CD в дисковод и перезагрузите компьютер.

Подождите, пока на экране монитора появится информация и выполняйте соответствующие инструкции для запуска BitDefender Rescue CD.

Экран загрузки

Обновление базы данных вирусных образов осуществляется автоматически без вмешательства пользователя.

После окончания загрузки на экране появится новый интерфейс - рабочий стол. Теперь Можно начинать работу с BitDefender Rescue CD.

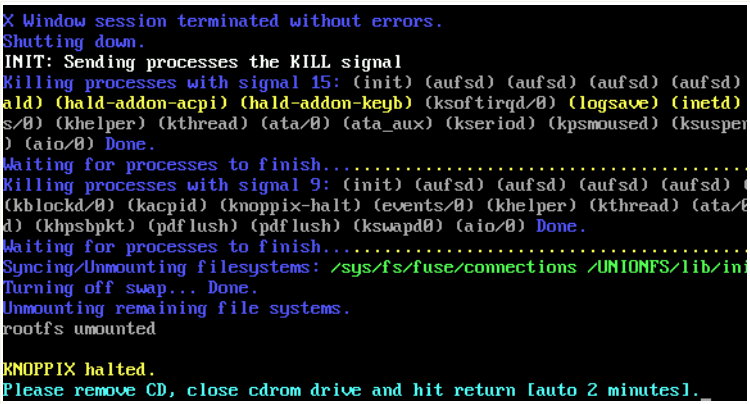
Рабочий стол

15.2. Остановка BitDefender Rescue CD

Вы можете выполнить безопасное отключение компьютера, для чего следует выбрать команду **Exit** в контекстном меню BitDefender Rescue CD (открывающееся после щелчка правой кнопкой мыши), либо использовать команду **halt** в терминале.

Выберите команду "EXIT"

Когда BitDefender Rescue благополучно закроет все программы, на экране появится новое изображение, соответствующее показанному на следующем рисунке. Теперь можно извлечь CD, чтобы последующую загрузку компьютера выполнить уже с жесткого диска. Теперь ваш компьютер можно выключить или перезагрузить.



Ожидайте появления этого сообщения на экране, сигнализирующего о завершении работы программы

15.3. Как выполнить антивирусную проверку?

Когда процесс загрузки завершен, откроется мастер, позволяющий произвести полную проверку Вашего компьютера. Все, что необходимо сделать для этого, - нажать кнопку **Старт**.

Замечание
Если разрешения вашего экрана недостаточно для корректного отображения, Вам будет предложено запустить проверку в текстовом режиме.

Чтобы завершить процесс проверки выполните последовательность из трех шагов.

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

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

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

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

Для каждой группы проблем Вы можете выбрать общее действие, либо есть возможность выбрать отдельное действие для каждой проблемы.

3. Здесь Вы можете просмотреть краткий обзор.

Если Вы хотите просканировать только определенную директорию, тогда необходимо:

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

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

```
# bdscan /path/to/scan/
```

15.4. Как я делаю обновление BitDefender через прокси?

Если есть прокси-сервер между вашим компьютером и Интернет, то необходимо сделать некоторые настройки конфигурации, чтобы обновить вирусные сигнатуры.

Чтобы выполнить обновление BitDefender через прокси-сервер, необходимо выполнить следующие шаги:

1. Щелкните правой кнопкой мыши по рабочей области. Появится контекстное меню BitDefender реаниматор CD.
2. Выберите опцию **Терминал (как root)**.
3. Тип команды: **cd /ramdisk/BitDefender-scanner/etc**.
4. Тип команды: **mcedit bdscan.conf**, чтобы редактировать этот файл используя GNU Midnight Commander (mc).
5. Раскомментируйте следующую строку: `#HttpProxy =` (просто удалите символ `#`) и задайте домен, имя пользователя, пароль и порт порт прокси-сервера. Например, эта строка может выглядеть так:

   ```
   HttpProxy = myuser:mypassword@proxy.company.com:8080
   ```
6. Нажмите **F2**, чтобы сохранить правильный файл, подтвердите сохранение и тогда нажмите **F10**, чтобы закрыть это.

7. Тип команды: **bdscan update**.

15.5. Как мне сохранить мои данные?

Предположим, Вы не можете запустить Ваш компьютер с ОС Windows из-за неизвестных проблем. В тоже время, Вам очень нужно получить доступ к данным на Вашем компьютере. Именно здесь пригодится диск-реаниматор BitDefender.

Выполните следующие шаги для того, чтобы скопировать данные с Вашего компьютера на сменный носитель, например, на модуль памяти USB:

1. Поместите диск-реаниматор BitDefender в привод, а модуль памяти подсоедините к USB порту, и перегрузите компьютер.
2. Ждите, пока BitDefender Rescue CD не загрузится. Появится следующее окно.

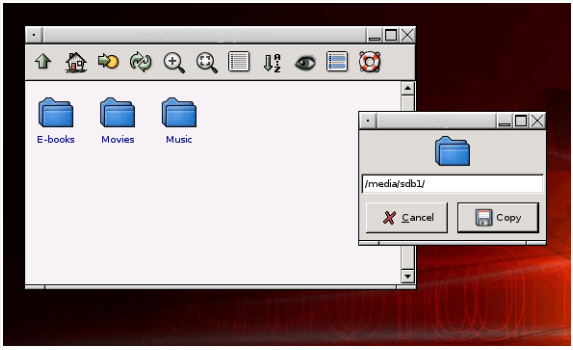
Экран рабочего стола

3. Нажмите два раза на раздел, где расположены данные, которые Вы хотите сохранить (например `[sda3]`).

Замечание

При работе с реаниматором BitDefender Вам придется столкнуться с обозначениями дисков, принятыми в Linux, Таким образом, `[sda1]` будет скорее всего соответствовать разделу `(C:)` диска в ОС Windows, `[sda3]` - `(F:)`, а `[sdb1]` - модулю памяти.

4. Просмотрите ваши папки и откройте желательную директорию. Например, `MyData` который содержит поддиректории `Видео`, `Музыка` и `Книги`.
5. Нажмите правой кнопкой мыши на выбранной папки и выберите **Копировать**. Появится следующее окно.



Сохранение данных

6. Введите `/media/sdb1/` в соответствующее текстовое поле и нажмите **Копировать**.

Получение справки

16. Поддержка

BitDefender заботится о своих клиентах и стремится предоставитьим быструю и полную техническую поддержку. Центр Поддержки всегда информирован о самых последних угрозах. Именно здесь Вы можете получить быстрый ответ на все Ваши вопросы.

Стремление сохранить время и деньги клиентов, предоставляя им самые последние продукты по самым оптимальным ценам, всегда было приоритетом BitDefender.

Вы можете в любое время обратиться за технической поддержкой по электронной почте support@bitdef.ru или по телефону **+7 495 987 4394**. Чтобы получить полный и оперативный ответ по электронной почте, пожалуйста, укажите в Вашем письме как можно больше информации о Вашем продукте BitDefender: версия, название, когда и где приобрели программу. Также опишите проблему, с которой Вы столкнулись как можно подробнее.

16.1. 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 куруглосуточно по адресу http://kb.bitdef.ru.

16.2. Просьба помощи

16.2.1. Перейти к самообслуживанию через веб

Возник вопрос? Наши специалисты готовы круглосуточно оказать Вам помощь по телефону, электронной почте или при помощи чата.

Перейдите по нижеследующим ссылкам:

Английский

http://www.bitdefender.com/site/KnowledgeBase/browseProducts/2195/

Немецкий

http://www.bitdefender.com/de/KnowledgeBase/browseProducts/2195/

Французский

http://www.bitdefender.com/fr/KnowledgeBase/browseProducts/2195/

Румынский

http://www.bitdefender.com/ro/KnowledgeBase/browseProducts/2195/

Испанский

http://www.bitdefender.com/es/KnowledgeBase/browseProducts/2195/

16.2.2. Откройте тикет техподдержки

Если Вы хотите создать уведомление для службы поддержки или получить помощь по электронной почте, просто перейдите по одной из этих ссылок:

Английский: http://www.bitdefender.com/site/Main/contact/1/
Немецкий: http://www.bitdefender.de/site/Main/contact/1/
Французский: http://www.bitdefender.fr/site/Main/contact/1/
Румынский: http://www.bitdefender.ro/site/Main/contact/1/
Испанский: http://www.bitdefender.es/site/Main/contact/1/

16.3. Контактная информация

Эффективная связь является залогом успешного бизнеса. За последние 10 лет компании BITDEFENDER удалось завоевать непререкаемый авторитет среди своих клинтов и партнеров за счет предвосхищения их ожиданий и постоянного улучшения связи с ними. Мы будем рады ответить на все ваши вопросы и решить ваши проблемы – не колеблясь, обращайтесь к нам за помошью.

16.3.1. Адреса веб-сайтов

Отдел продаж: sales@bitdef.ru
Техподдержка: 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

16.3.2. Офисы филиалов

Персонал компании BitDefender, ответственный за продукт, ответит на ваши вопросы коммерческого и общего характера, относящейся к сфере их деятельности и географической привязке. Ниже приведены адреса и контактная информация этих офисов.

США

BitDefender, LLC
6301 NW 5th Way, Suite 3500
Fort Lauderdale, Florida 33309
Веб сайт http://www.bitdefender.com
Техническая поддержка:

- E-mail: support@bitdef.ru
- Телефон:
  - +7 (495) 987-4394 (Только для зарегистрированных пользователей; доступен только в России)
  - 1-954-776-6262 (Только для зарегистрированных пользователей)

Служба поддержки клиентов:

- E-mail: customerservice@bitdef.ru
- Телефон:
  - +7 (495) 987-4394 (Только для зарегистрированных пользователей; доступен только в России)
  - 1-954-776-6262 (Только для зарегистрированных пользователей)

Германия

BitDefender GmbH
Headquarter Western Europe
Karlsdorferstrasse 56
88069 Tettnang
Германия
Телефон: +49 7542 9444 60
Факс: +49 7542 9444 99
Электронный адресinfo@bitdefender.com
Отдел продаж: sales@bitdefender.com
Веб сайт http://www.bitdefender.com
Техподдержка: support@bitdefender.com

Великобритания и Ирландия

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

Испания

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

Румыния

BITDEFENDER
5th Fabrica de Glucoza St.
Bucharest
Техподдержка: support@bitdef.ru
Отдел продаж: sales@bitdefender.com
Телефон: +40 21 4085600
Факс: +40 21 2330763
Веб-сайт продукта: http://www.bitdef.ru

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 агрессивной рекламной информацией

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.

Спам

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

Программа-шпион

Любого рода программа-шпион, которая тайно и без ведома пользователя - чаще всего в рекламных целях - собирает информацию о пользователе во время его с соединения с Интернетом. Шпионские программы обычно маскируют как скрытые компоненты бесплатных или условно бесплатных

(shareware) приложений, которые можно скачать с Интернета, хотя следует отметить, что большинство бесплатных или условно бесплатных приложений не содержит программ-шпионов. Программа-шпион после своей установки отслеживает адреса в Интернете, к которым обращается пользователь и тайно пересылает эту информацию третьим лицам. Кроме того, программы-шпионы могут собирать информацию об адресах электронной почты, паролях и даже номерах кредитных карточек пользователей.

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

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.