

bitdefender

INTERNET SECURITY v10



10th anniversary

Руководство пользователя



Антивирус
Брандмауэр
Антиспам
Антишпион
Доступ

BitDefender Internet Security v10

Руководство пользователя

BitDefender

Опубликовано 2007.05.09

Version 10.2

Copyright© 2007 SOFTWIN

Правовые положения

Все права защищены. Никакая часть этой публикации не может быть воспроизведена или передана в любой форме или любыми средствами, электронными или механическими, включая фотокопирование, перезапись, или использована в каких-либо информационных системах хранения данных и поисковых системах, без получения письменного разрешения от уполномоченного представителя компании SOFTWIN. Включение кратких цитат в обзорах разрешается только со ссылкой на цитируемый источник. Запрещено вносить какие-либо изменения в данный материал.

Предупреждение и условия отказа от ответственности. Данный программный продукт и документация к нему защищены авторским правом. Информация в этом документе предоставляется в состоянии «как есть», без гарантии полной достоверности. При подготовке этого документа авторы тщательно проверили точность и правовую чистоту содержащейся в нем информации, однако они не несут какой-либо ответственности перед физическими или юридическими лицами, которые могут предъявить претензии за какие-либо потери или ущерб, непосредственно или косвенно связанные с информацией, содержащейся в этой работе, или инкриминировать таковые.

Данная книга содержит ссылки на сторонние веб-сайты, которые не находятся под управлением SOFTWIN, поэтому SOFTWIN не несет ответственности за содержание какого-либо сайта, на который имеются ссылки в данном документе. Посещая любой сторонний веб-сайт, на который имеются ссылки в этом документе, Вы делаете это на свой страх и риск. Компания SOFTWIN приводит эти ссылки только для удобства читателя, но наличие этих ссылок не означает, что SOFTWIN берет на себя ответственность за содержание какого-либо стороннего веб-сайта.

Торговые марки. В этом документе могут упоминаться различные торговые марки. Компания Softwin подтверждает, что права собственности на все зарегистрированные и незарегистрированные торговые марки, упоминаемые в этом документе, принадлежат только их законным владельцам.





Содержание

| | |
|---|-----------|
| Лицензии и гарантии | xi |
| Предисловие | xv |
| 1. Соглашения, используемые в данной книге | xv |
| 1.1. Типографские обозначения | xv |
| 1.2. Замечания | xvi |
| 2. Структура книги | xvi |
| 3. Ваши комментарии | xvii |
| О программе BitDefender | 1 |
| 1. Что такое BitDefender? | 3 |
| 1.1. Почему именно BitDefender? | 3 |
| Установка программы | 7 |
| 2. Установка BitDefender Internet Security v10 | 9 |
| 2.1. Системные требования | 9 |
| 2.2. Пошаговая установка | 9 |
| 2.3. Мастер начальной настройки | 12 |
| 2.3.1. Шаг 1/8 - Мастер настройки BitDefender | 13 |
| 2.3.2. Шаг 2/8 - Регистрация BitDefender Internet Security v10 | 13 |
| 2.3.3. Шаг 3/8 - Создать учетную запись BitDefender | 14 |
| 2.3.4. Шаг 4/8 - Введите реквизиты учетной записи | 15 |
| 2.3.5. Шаг 5/8 - Информация о системе слежения за вирусами в реальном времени | 16 |
| 2.3.6. Шаг 6/8 - Выбор задач для запуска | 17 |
| 2.3.7. Шаг 7/8 - Ожидание завершения задач | 18 |
| 2.3.8. Шаг 8/8 - Итоговый отчет | 19 |
| 2.4. Обновление | 19 |
| 2.5. Удаление, восстановление или изменение BitDefender | 20 |
| Описание и особенности | 21 |
| 3. BitDefender Internet Security v10 | 23 |
| 3.1. Антивирус | 23 |
| 3.2. Брандмауэр | 24 |
| 3.3. Антиспам | 25 |
| 3.4. Антишпион | 25 |
| 3.5. Доступ | 26 |
| 3.6. Другие особенности | 27 |
| 4. Модули BitDefender | 29 |

| | |
|--|----|
| 4.1. Общий модуль | 29 |
| 4.2. Модуль Антивирус | 29 |
| 4.3. Модуль брандмауэр | 30 |
| 4.4. Модуль Антиспам | 30 |
| 4.4.1. Схема работы | 30 |
| 4.4.2. Антиспам-фильтры | 32 |
| 4.5. Модуль защиты от сетевых атак | 34 |
| 4.6. Модуль Контроль доступа | 34 |
| 4.7. Модуль обновлений | 35 |

Консоль управления 37

5. Краткий обзор 39

| | |
|--|----|
| 5.1. Системный трей | 40 |
| 5.2. Строка состояния сканирования | 41 |

6. Общий модуль 43

| | |
|---|----|
| 6.1. Центр Управления | 44 |
| 6.1.1. Быстрые задачи | 44 |
| 6.1.2. Уровни безопасности | 45 |
| 6.1.3. Статус регистрации | 46 |
| 6.2. Настройки консоли управления | 47 |
| 6.2.1. Общие настройки | 47 |
| 6.2.2. Настройки отчета о вирусах | 49 |
| 6.2.3. Настройки фона | 49 |
| 6.2.4. Управление настройками | 49 |
| 6.3. События | 50 |
| 6.4. Регистрация продукта | 51 |
| 6.4.1. Мастер регистрации | 52 |
| 6.5. О программе | 57 |

7. Модуль Антивирус 59

| | |
|--|----|
| 7.1. Входное сканирование | 59 |
| 7.1.1. Уровень защиты | 60 |
| 7.2. Сканирование по требованию | 65 |
| 7.2.1. Задачи сканирования | 65 |
| 7.2.2. Выпадающее меню | 67 |
| 7.2.3. Свойства задач проверки | 68 |
| 7.2.4. Типы проверки по требованию | 79 |
| 7.2.5. Сканирование на руткиты | 83 |
| 7.3. Карантин | 84 |

8. Модуль брандмауэр 87

| | |
|---|----|
| 8.1. Мастер Брандмауэра | 87 |
| 8.1.1. Шаг 1/7 - Экран приветствия | 88 |
| 8.1.2. Шаг 2/7 - Дополнительные настройки брандмауэра | 89 |
| 8.1.3. Шаг 3/7 - Настройки браузера интернет | 90 |
| 8.1.4. Шаг 4/7 - Настройки почтового клиента | 91 |



| | |
|--|------------|
| 8.1.5. Шаг 5/7 - Настройки прокси сервера | 92 |
| 8.1.6. Шаг 6/7 - Выбор типа сети | 93 |
| 8.1.7. Шаг 7/7 – Краткий итоговый отчет | 94 |
| 8.2. Статус Брандмауэра | 95 |
| 8.2.1. Уровень защиты | 96 |
| 8.3. Контроль трафика. | 97 |
| 8.3.1. Автоматическое добавление правил | 97 |
| 8.3.2. Добавление правил вручную | 99 |
| 8.3.3. Управление правилами | 101 |
| 8.3.4. Модифицирование профилей | 102 |
| 8.4. Дополнительные настройки | 104 |
| 8.4.1. Настройки ICMP фильтра | 104 |
| 8.4.2. Настройки модуля Антиспам | 106 |
| 8.5. Контроль подключений | 108 |
| 9. Модуль Антиспам | 111 |
| 9.1. Статус модуля Антиспам | 111 |
| 9.1.1. Заполните список адресов | 112 |
| 9.1.2. Настройка «уровня толерантности» | 115 |
| 9.2. Настройки антиспама | 117 |
| 9.2.1. Настройки антиспама | 117 |
| 9.2.2. Базовые фильтры Антиспама | 118 |
| 9.2.3. Дополнительные фильтры Антиспама | 118 |
| 9.3. Настройка Антиспама, встроенного в Microsoft Outlook/ Outlook Express / Windows Mail | 119 |
| 9.3.1. Панель инструментов антиспама | 119 |
| 9.3.2. Мастер настройки Антиспам | 126 |
| 10. Модуль защиты от сетевых атак | 133 |
| 10.1. Статус Антишпиона | 134 |
| 10.1.1. Уровень защиты | 135 |
| 10.2. Дополнительные настройки - Контроль конфиденциальности | 135 |
| 10.2.1. Мастер конфигурации | 136 |
| 10.2.2. Управление правилами | 139 |
| 10.3. Дополнительные настройки - Управление реестром | 140 |
| 10.4. Дополнительные настройки - Контроль дозвола | 142 |
| 10.4.1. Мастер конфигурации | 144 |
| 10.5. Дополнительные настройки - контроль cookie | 146 |
| 10.5.1. Мастер конфигурации | 149 |
| 10.6. Дополнительные настройки - Контроль сценариев | 150 |
| 10.6.1. Мастер конфигурации | 152 |
| 10.7. Информация о системе | 154 |
| 11. Модуль Контроль доступа | 155 |
| 11.1. Статус Контроль доступа | 156 |
| 11.1.1. Чувствительность эвристического веб фильтра | 157 |
| 11.2. Веб-контроль | 158 |
| 11.2.1. Мастер конфигурации | 159 |

| | |
|--|------------|
| 11.2.2. Установка исключений | 160 |
| 11.2.3. Черный список сайтов BitDefender | 160 |
| 11.3. Контроль приложений | 161 |
| 11.3.1. Мастер конфигурации | 161 |
| 11.4. Фильтрация ключевых слов | 163 |
| 11.4.1. Мастер конфигурации | 163 |
| 11.5. Ограничитель времени в сети | 165 |
| 12. Модуль обновлений | 167 |
| 12.1. Автоматическое обновление | 167 |
| 12.2. Обновление вручную | 168 |
| 12.2.1. Обновление вручную с использованием файла weekly.exe | 169 |
| 12.2.2. Обновление вручную при помощи zip архивов | 169 |
| 12.3. Настройки обновления | 171 |
| 12.3.1. Настройки местоположения обновления | 171 |
| 12.3.2. Опции автоматического обновления | 172 |
| 12.3.3. Настройки обновления вручную | 173 |
| 12.3.4. Дополнительные настройки | 173 |
| Практические приемы | 175 |
| 13. Практические приемы | 177 |
| 13.1. Как защитить Ваш компьютер, подключенный к Интернет | 177 |
| 13.2. Как защитить Ваш компьютер от угроз вредоносных программ | 178 |
| 13.3. Как настроить задачу проверки | 179 |
| 13.4. Как настроить модуль брандмауэра | 180 |
| 13.5. Как оградить Ваш компьютер от спама | 181 |
| 13.6. Как защитить Вашего ребенка от неадекватного контента | 182 |
| Реаниматор BitDefender | 185 |
| 14. Краткий обзор | 187 |
| 14.1. Что такое KNOPPIX? | 187 |
| 14.2. Системные требования | 187 |
| 14.3. Включенное программное обеспечение | 188 |
| 14.4. Антивирусный сканер BitDefender Linux | 188 |
| 14.4.1. BitDefender SMTP прокси-сервер | 189 |
| 14.4.2. Удаленный администратор BitDefender | 189 |
| 14.4.3. Антивирусный сканер BitDefender Linux | 190 |
| 15. Работа с LinuxDefender | 191 |
| 15.1. Запуск и остановка | 191 |
| 15.1.1. Запуск программы LinuxDefender | 191 |
| 15.1.2. Завершение работы LinuxDefender | 192 |
| 15.2. Настройка Интернет соединения | 193 |
| 15.3. Обновление BitDefender | 194 |
| 15.4. Проверка на вирусы | 195 |



| | |
|---|-----|
| 15.4.1. Как получить доступ к своим данным, записанным в Windows? | 195 |
| 15.4.2. Как выполнить вирусную проверку? | 196 |
| 15.5. Настройки фильтра почтовых сообщений | 196 |
| 15.5.1. Требования к системе | 196 |
| 15.5.2. Мгновенный почтовый фильтр | 197 |
| 15.6. Контролер сетевой защиты Nessus | 198 |
| 15.6.1. Поиск руткитов | 198 |
| 15.6.2. Сетевой сканер Nessus | 199 |
| 15.7. Проверка работоспособности RAM системы | 199 |

Получение справки 201

16. Тех. поддержка 203

| | |
|--|-----|
| 16.1. Отдел поддержки | 203 |
| 16.2. Поддержка в режиме «on-line» | 203 |
| 16.2.1. База знаний BitDefender | 203 |
| 16.3. Контактная информация | 204 |
| 16.3.1. Адреса веб-сайтов | 204 |
| 16.3.2. Офисы филиалов | 204 |

Глоссарий 207



Лицензии и гарантии

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

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

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

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

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

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

ПРИКЛАДНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ. Вы можете установить и использовать BitDefender на необходимом количестве компьютеров в рамках ограничения общего количества лицензированных пользователей. Вы можете сделать одну дополнительную резервную копию.

ЛИЦЕНЗИЯ ПЕРСОНАЛЬНОГО ПОЛЬЗОВАТЕЛЯ. Данная лицензия относится к программному обеспечению BitDefender, которое может быть установлено на персональном компьютере и которое не имеет сетевых функций. Каждый

пользователь может установить данный программный продукт на персональном компьютере, а также может сделать дополнительную резервную копию на другом устройстве. Дозволенное количество первичных пользователей - это количество пользователей лицензии.

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

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

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

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



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

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

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

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

В ЛЮБЫХ ДРУГИХ ВИДАХ ДЕЯТЕЛЬНОСТИ, ГДЕ ОШИБКА МОЖЕТ ПОВЛЕЧЬ ЗА СОБОЙ СМЕРТЬ, СЕРЬЕЗНЫЕ ПОВРЕЖДЕНИЯ ИЛИ БОЛЬШОЙ УЩЕРБ.

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

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

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

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

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

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

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

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



Предисловие

Данное пособие предназначено для всех пользователей, выбравших **BitDefender Internet Security v10** как решение для защиты персонального компьютера. Информация, представленная в данном руководстве, предназначена не только для опытных пользователей, но и для всех, кто может работать с операционной системой Windows.

Данное пособие описывает продукт **BitDefender Internet Security v10**, а также поможет пройти процесс установки, обучит, как настроить продукт. Вы узнаете, как использовать **BitDefender Internet Security v10**, как обновлять, тестировать и настраивать его. Вы узнаете, как получить максимальную выгоду от использования BitDefender.

Надеемся, что чтение будет увлекательным и полезным для Вас.

1. Соглашения, используемые в данной книге

1.1. Типографские обозначения

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

| Виды шрифтов и стилей | Описание |
|---|---|
| <code>sample syntax</code> | Образцы написания напечатаны шрифтом с фиксированной шириной СИМВОЛОВ. |
| http://www.bitdefender.com | Ссылки URL на внешние источники, http или ftp серверы. |
| <code><support@bitdefender.com></code> | Адреса электронной почты в тексте приводятся в качестве контактной информации. |
| «Предисловие» (р. xv) | 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. |
| <code>sample code listing</code> | Программные коды приводятся с помощью шрифтов с фиксированной ширины символов. |

1.2. Замечания

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



Замечание

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



Важно

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



Внимание

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

2. Структура книги

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

О программе BitDefender. Краткое введение в программу BitDefender.



Установка программы. Пошаговые инструкции по установке BitDefender на рабочем компьютере. Это полноценное пособие по установке **BitDefender Internet Security v10**. Начиная от первоначальных требований, необходимых для успешной установки, Вы пройдете весь процесс установки. Наконец, описана процедура удаления, в случае, если необходимо удалить BitDefender.

Описание и особенности. **BitDefender Internet Security v10**, его функции и модули представлены здесь.

Консоль управления. Описание базовых методов управления и поддержания BitDefender. Главы подробно поясняют все настройки **BitDefender Internet Security v10**, как регистрировать продукт, как проверять компьютер, как производить обновления. Вас научат настраивать и использовать все модули BitDefender.

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

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

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

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

3. Ваши комментарии

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

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



Важно

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



О программе BitDefender



1. Что такое BitDefender?

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

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

1.1. Почему именно BitDefender?

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

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

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

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

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

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

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

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



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

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



Установка программы



2. Установка BitDefender Internet Security v10

Глава **Установка BitDefender Internet Security v10** этого руководства пользователя содержит следующие разделы:

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

2.1. Системные требования

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

Microsoft Windows 2000 / XP 32-bit

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

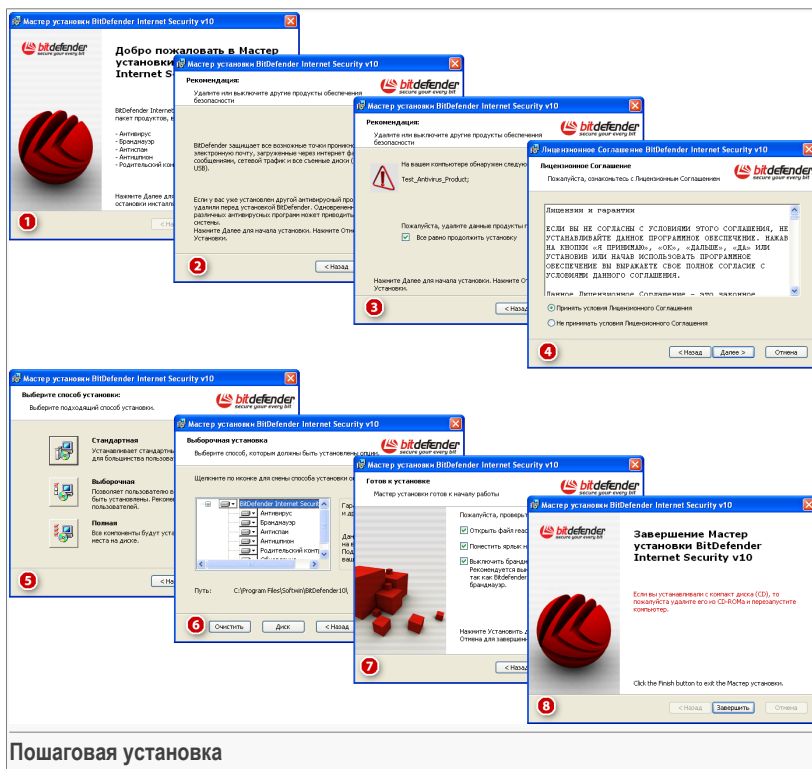
Microsoft Windows Vista 32-bit

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

Версию для оценки **BitDefender Internet Security v10** можно загрузить с <http://www.bitdef.ru> - вебсайта компании SOFTWIN, посвященного безопасности данных.

2.2. Пошаговая установка

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



Пошаговая установка

1. Нажмите **Далее** чтобы продолжить, или **Отменить** если Вы хотите прервать установку.
2. Нажмите **Далее** чтобы продолжить, или **Назад** если Вы хотите вернуться к первому шагу.
3. BitDefender Internet Security v10 предупредит, если на Вашем компьютере установлены другие антивирусные программы.

Внимание



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



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

Замечание



Если BitDefender Internet Security v10 не обнаружит другие антивирусные программы на Вашем компьютере, Вы пропустите этот шаг.

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

Обычная

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

Выборочная

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

Полная

Полная установка продукта. Будут установлены все модули BitDefender.

Выбрав вариант **Обычная** или **Полная**, вы пропустите шаг 6.

6. При **Выборочной** установке появится новое окно со списком всех компонентов BitDefender, из которых Вы сможете выбрать необходимые для установки.

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

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

Если вы хотите выбрать другой каталог, нажмите **Обзор**, а затем в открывшемся окне выберите каталог, куда хотите установить BitDefender Internet Security v10. Нажмите **Далее**.

7. Существуют две опции, выбранные по умолчанию:

- **Открыть файл readme** - открывает ознакомительный файл в конце установки.
- **Создать ярлык на рабочем столе** - создает ярлык BitDefender Internet Security v10 на вашем рабочем столе в конце установки.

- **Выключить Брандмауэр Windows** - выключает Брандмауэр Windows.

**Важно**

Мы рекомендуем Вам выключить Брандмауэр Windows, так как BitDefender Internet Security v10 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**

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

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

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

**Замечание**

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

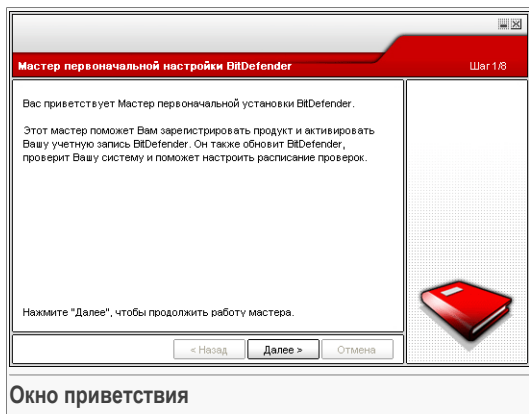
2.3. Мастер начальной настройки

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

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

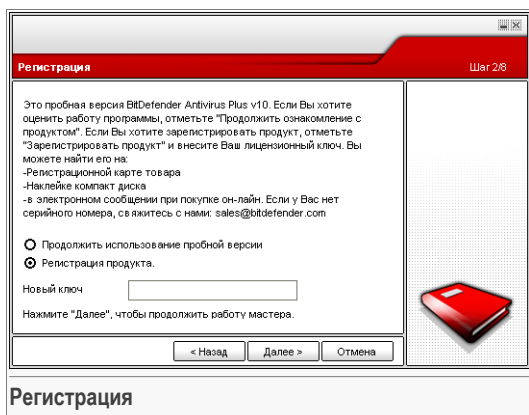


2.3.1. Шаг 1/8 - Мастер настройки BitDefender.



Нажмите **Далее**.

2.3.2. Шаг 2/8 - Регистрация BitDefender Internet Security v10



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

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

Нажмите **Далее**.

2.3.3. Шаг 3/8 - Создать учетную запись BitDefender

Зарегистрировать сейчас Шаг 3/8

Вам необходимо создать учетную запись, чтобы получить доступ к технической поддержке и другим персонализированным услугам BitDefender. Если у Вас уже есть учетная запись BitDefender, пожалуйста, введите необходимые данные. Если у Вас нет учетной записи BitDefender, пожалуйста, введите адрес Вашей электронной почты и пароль.

Имя:

Пароль:

[Забыли пароль?](#)

Пропустить этот шаг

Нажмите "Далее", чтобы продолжить, или "Отмена", чтобы закончить работу

Создание учетной записи

У меня нет учетной записи BitDefender

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

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



Замечание

Пароль должен состоять минимум из четырех символов.

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



Важно

Активируйте свою учетную запись прежде чем переходить к следующему шагу.

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



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

У меня уже есть учетная запись BitDefender .

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

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

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

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

Настроить мою учетную запись Шаг 4/8

Введите информацию для учетной записи. Предоставляемые Вами данные не будут разглашены. Если у Вас уже есть учетная запись, мастер отобразит предоставленную Вами при создании информацию.

Имя:

Фамилия:

Страна:

Нажмите "Далее", чтобы продолжить, или "Отмена", чтобы оканчить работу

Реквизиты учетной записи



Замечание

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

Введите имя и фамилию, выберите страну проживания.

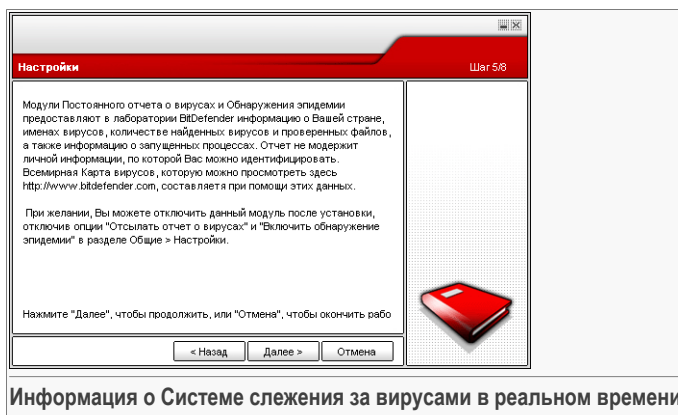
Если у Вас уже есть учетная запись, мастер отобразит информацию, предоставленную Вами ранее, если таковая имеется. По желанию, здесь можно скорректировать данную информацию.

**Важно**

Предоставленные Вами данные конфиденциальны.

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

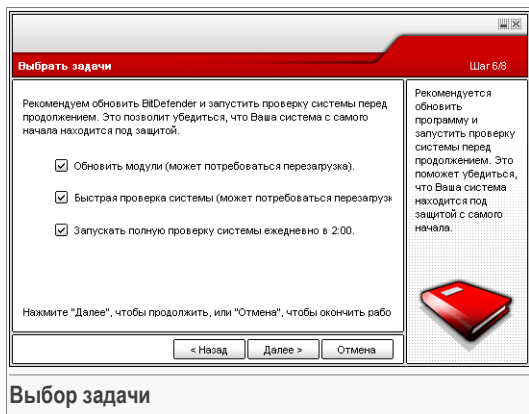
2.3.5. Шаг 5/8 - Информация о системе слежения за вирусами в реальном времени



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



2.3.6. Шаг 6/8 - Выбор задач для запуска



Настройте BitDefender Internet Security v10 выполнять важные задачи для обеспечения безопасности Вашей системы.

Доступны следующие варианты:

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



Важно

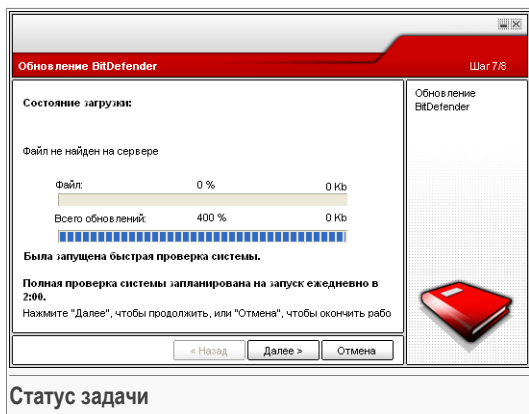
Рекомендуем Вам включить данные опции перед тем, как перейти к следующему шагу, чтобы обеспечить полную безопасность Вашей системы.

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

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

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

2.3.7. Шаг 7/8 - Ожидание завершения задач

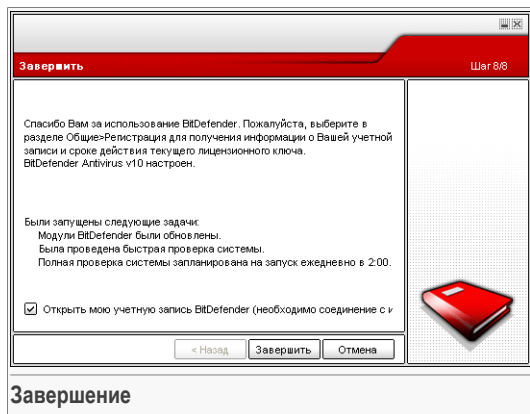


Подождите, пока задачи завершатся. Вы можете наблюдать статус выполнения задачи, выбранной на прошлом шаге.

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



2.3.8. Шаг 8/8 – Итоговый отчет



Это последний шаг мастера установки.

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

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

2.4. Обновление

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

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

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



Важно

Если Вы обновляете ранее установленный BitDefender версии v8 или выше, рекомендуем сохранить **Настройки BitDefender**, **Список друзей** и **Список спаммеров**. После окончания установки новой версии, вы сможете их загрузить.

2.5. Удаление, восстановление или изменение BitDefender.

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

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

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

Замечание



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

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



Важно

Перед восстановлением программы мы рекомендуем Вам сохранить [Список друзей](#), [Список спамеров](#). Вы можете также сохранить [Настройки BitDefender](#) и [Базу данных Байесова фильтра](#). После восстановления Вы снова сможете их загрузить.

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

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

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

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



Описание и особенности



3. BitDefender Internet Security v10

Полная защита от угроз Интернет!

BitDefender Internet Security v10 удовлетворяет всем требованиям безопасности для семьи, подключенной к Интернет. Он предоставляет полноценную защиту от вирусов, программ-шпионов, спама, попыток фишинга, взлома и прочих вредоносных компонентов.

BitDefender v10 разработан таким образом, чтобы пользователю и системе понадобилось как можно меньше усилий и ресурсов для обеспечения самой современной защиты от угроз из Интернета.

3.1. Антивирус

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

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

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

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

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

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

Полная защита электронной почты. BitDefender работает на уровне протоколов POP3/SMTP, фильтруя входящие и исходящие электронные сообщения, независимо от типа используемого почтового клиента (Outlook™, Outlook Express™, The Bat!™, Netscape® и т.д.) без дополнительной настройки.

3.2. Брандмауэр

Модуль брандмауэра отфильтровывает сетевой трафик и контролирует права доступа приложений, пытающихся присоединиться к Интернет. В Невидимом Режиме, Ваш компьютер "скрыт" от вредоносных программ и хакеров. Модуль брандмауэра может автоматически выявлять и отражать попытки сканирования портов (потоки пакетов, присылаемых на машину, чтобы выявить "точки доступа", эта операция часто предшествует атаке).

Контроль Интернет-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.

Контроль приложений. BitDefender имеют базу данных проверенных приложений, и информирует пользователей, можно ли доверять приложениям, запрашивающим доступ по сети, чтобы те могли принять решение. В других случаях, BitDefender может разрешать доступ проверенным приложениям автоматически.

Контроль подключений. BitDefender позволяет в реальном времени просматривать, какие программы имеют открытые соединения к Интернет. Одним нажатием Вы можете выбрать разрешать или запрещать их, временно или постоянно.

Невидимый режим. 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 **Невидимый режим** будет блокировать ответ Вашего компьютера на все запросы о том, какие порты являются открытыми, или о местоположении Вашего компьютера.

Выявление сканирования портов. Модуль Брандмауэр BitDefender может автоматически выявлять и блокировать сканирование портов. Сканирование портов - это простой способ узнать, уязвим ли Ваш компьютер или нет; он представляет собой попытки присоединиться к порту, чтобы увидеть, поступит ли какой-нибудь ответ, по аналогии, словно взломщик одну за другой пробует все двери, чтобы найти открытую.



Мастер Брандмауэра. Мастер Брандмауэра помогает пользователям выбрать наиболее соответствующий настройкам уровень безопасности, в зависимости от места расположения - дома, в офисе или в поездке.

3.3. Антиспам

Технология BitDefender борьбы со спамом использует передовые достижения, которые позволяют приспосабливаться к новым технологиям рассылки спама, а также "учитывать" предпочтения пользователя, чтобы заблокировать спам, сохраняя при этом достаточно низкий коэффициент попадания легитимных писем в категорию спам.

Адаптивная фильтрация. BitDefender использует передовые технологии кластеризации и нейросетевого анализа для классификации электронных сообщений по предпочтениям пользователя и накоплению шаблонов в местной подборке электронных сообщений. Пользователь может "обучать" Байесовский антиспам фильтр (классифицируя некоторые сообщения как спам, или как легитимное письмо), он также самообучается, разрабатывая новые критерии фильтрации, основываясь на прошлых решениях.

Антифишинг. Антифишингограждает Ваш компьютер от подозрительных электронных сообщений, в которых пытаются хитростью узнать Ваш банковский счет или другую конфиденциальную информацию.

Эвристический фильтр, Фильтр URL, Список разрешенных/запрещенных адресов, Фильтр символов и Фильтр изображений. Пять фильтров оптимизируют защиту электронных сообщений. Эвристический фильтр проверяет сообщение на характерные особенности спама. Фильтр разрешенных/запрещенных адресов отсеивает письма от неизвестных адресов спаммеров и пропускает письма Ваших друзей. Фильтр URL блокирует письма с подозрительными ссылками, а фильтр символов блокирует сообщения, написанные "странными" символами. Фильтр изображений принимает решение, являются ли прикрепленные к письму изображения спамом или нет.

Совместимость и интеграция с Outlook™. Антиспам BitDefender совместим со всеми почтовыми клиентами. Панель инструментов антиспама BitDefender в Microsoft Outlook™ и Outlook Express™ позволяет пользователям обучать Байесовский фильтр.

3.4. Антишпион

BitDefender отслеживает и предотвращает потенциальную угрозу сетевых атак в реальном времени до того, как они могут нанести ущерб Вашей системе. За

счет использования обширной базы данных образов программ-шпионов, последние не смогут проникнуть в ваш компьютер.

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

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

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

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

3.5. Доступ

Модуль Контроль доступа BitDefender позволяет блокировать доступ к сайтам, содержимое которых Вы считаете недопустимым, блокировать доступ к Интернет в течение некоторых периодов времени (например, в период времени, отведенного для работы), а также блокировать выполнение приложений, таких как игры, чат, файлообменные программы, и др

Веб-контроль. Фильтр URL дает Вам возможность блокировать доступ к сайтам с недопустимым, по вашему мнению, содержанием. BitDefender предоставляет пользователям и регулярно обновляет список сайтов-кандидатов на блокирование.

Эвристический веб фильтр. Эвристический фильтр автоматически классифицирует веб-страницы, основываясь на содержании или прочих предпосылках. Вместо того, чтобы полагаться только на ключевые слова, данный подход исследует принципы отслеживания антиспама при классификации веб-страниц. Существуют предустановленные профили, основывающиеся на возрасте пользователя.

Фильтр ключевых слов для веб. Пользователи BitDefender могут заблокировать все веб-страницы, содержащие определенное слово или фразу.



Фильтр ключевых слов для электронных сообщений. Входящие электронные сообщения, содержащие определенные слова или фразы, могут быть отфильтрованы перед тем, как они попадут в папку Входящие почтового ящика.

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.

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.

3.6. Другие особенности

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

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

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

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

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



4. Модули BitDefender

BitDefender Internet Security v10 содержит следующие модули: **Общий, Антивирус, Брандмауэр, Антиспам, Антишпион, Контроль доступа и Обновления.**

4.1. Общий модуль

Изначальная конфигурация поставляемого программного продукта BitDefender обеспечивает максимальную безопасность.

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

4.2. Модуль Антивирус

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

Настройки защиты BitDefender разделены на две категории:

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

4.3. Модуль 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.

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).

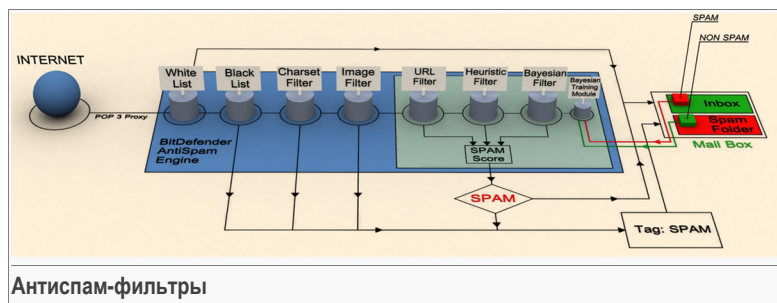
Брандмауэр просто необходим, если Вы пользуетесь широкополосным подключением или подключением по цифровой абонентской линии DSL.

4.4. Модуль Антиспам

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.

4.4.1. Схема работы

На этой схеме показано, как работает BitDefender.





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 Спاما. 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 повторях 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 + эвристическим 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,

отнесенных как Спам в определенный указанный каталог. BitDefender добавляет префикс [СПАМ] в тему сообщения, классифицированного как Спам.

4.4.2. Антиспам-фильтры

Модуль Антиспама BitDefender включает семь различных фильтров, чтобы обеспечить непопадание в Ваш почтовый ящик Спاما: (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 **Параметры 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 BitDefender** или с помощью **Панели инструментов Антиспам BitDefender**.

Замечание



Мы рекомендуем записывать имена и адреса электронной почты друзей в Ваш 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 иероглифами. Установите этот фильтр, если хотите отклонять все письма в этой кодировке.

Фильтр изображений

Поскольку спам-сообщениям становится все сложнее избежать распознавания с помощью 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

Большинство спам-сообщений содержит ссылки на различные ресурсы в Интернете (где размещается еще больше предложений, обычно купить что-нибудь). В базе данных BitDefender содержатся ссылки на эти ресурсы.

Каждая URL ссылка в письме сверяется с базой данных URL. В случае обнаружения спам-оценка будет добавлена, в сообщении.

Нейросетевой (эвристический) фильтр

Нейросетевой (эвристический) фильтр производит ряд проверок компонентов сообщения (не только заголовка, но и тела письма в текстовом или HTML формате) в поисках слов, фраз, ссылок и других характеристик Спاما.

Он также обнаруживает письма с темой **ОТКРОВЕННО СЕКСУАЛЬНОЕ СОДЕРЖАНИЕ** и относит их к СПАМУ.

Замечание



С 19 мая 2004 года спам, содержащий сексуально ориентированную информацию должен содержать предупреждение в поле «тема» или заглавии: **ОТКРОВЕННО СЕКСУАЛЬНОЕ СОДЕРЖАНИЕ**, иначе это будет считаться нарушением федерального закона.

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.

**Важно**

Чтобы защитить Вас от спамеров, Bitdefender может выполнить автоматические обновления. Для этого опция **Автоматическое обновление** должна быть включена.

4.5. Модуль защиты от сетевых атак

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

4.6. Модуль Контроль доступа

Модуль Контроль доступа BitDefender позволяет блокировать доступ к сайтам, содержимое которых Вы считаете недопустимым, блокировать доступ к Интернету в течение некоторых периодов времени (например, в период времени, отведенного для работы), а также блокировать выполнение приложений, таких как игры, чат, файлообменные программы, и др



4.7. Модуль обновлений

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

Существуют следующие варианты обновления:

- **Обновления модуля антивируса** - как только появляется новая угроза, необходимо обновить файл с образцами 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** - образцы новых программ-шпионов будут добавлены в базу данных. Этот тип обновления также известен как **Обновление Антишпиона**.
- **Улучшение программы** - когда выпускается новая версия программы, в новую версию добавляются новые функции и методы проверки, что только улучшает работу программы. Этот тип обновления также известен как **Обновление программы**.

Кроме того, с точки зрения действий пользователя можно выделить:

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



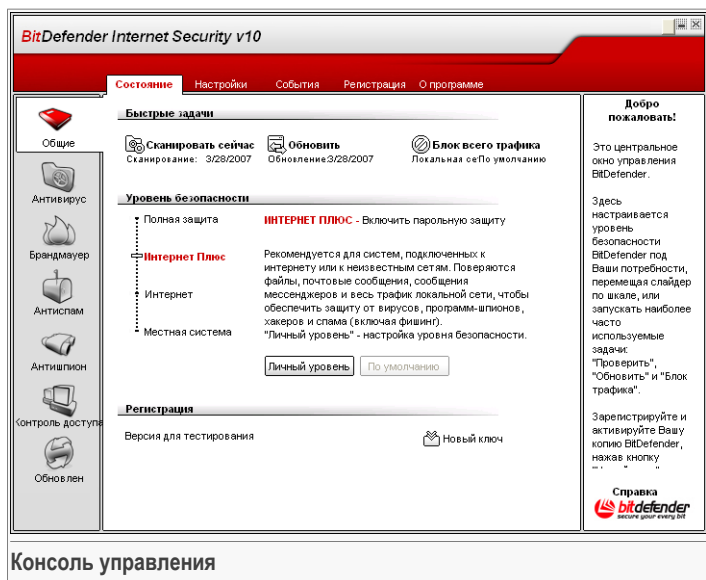
Консоль управления



5. Краткий обзор

BitDefender Internet Security v10 был разработан с централизованной консолью управления, которая позволяет конфигурировать настройки всех модулей BitDefender. Другими словами, достаточно открыть консоль управления, чтобы получить доступ ко всем модулям: **Антивирус**, **Брандмауэр**, **Антиспам**, **Антишпион**, **Контроль доступа** и **Обновления**.

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



В левой части консоли управления расположены ссылки на рабочие модули:

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

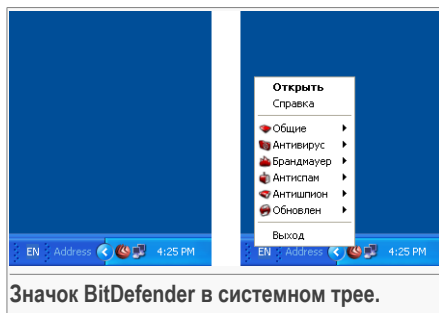
- **Антивирус** - в данном разделе вы можете настроить модуль **Антивирус**.
- **Брандмауэр** - в этой секции вы можете сконфигурировать **Бранмауэр**.
- **Антиспам** - открывает доступ в окно программной **Защиты от спама**.
- **Антишпион** - в этом разделе Вы можете конфигурировать модуль **Антишпион**.
- **Контроль доступа** - в этом разделе Вы можете конфигурировать модуль **Контроль доступа**.
- **Обновление** - открывает доступ в окно **Настройки обновления**.

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

5.1. Системный трей

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




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



Значок BitDefender в системном трее.

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



- **Брандмауэр включен / отключен** - показывает статус **защиты брандмауэром** (включена/отключена). Нажмите здесь, чтобы включить или выключить защиту брандмауэром.
- **Блокировать весь трафик** - блокировка трафика локальной сети / Интернет.
-  **Антиспам** - управление модулем **Антиспам**.
- **Фильтр антиспама включен / отключен** - показывает статус **антиспам защиты** (включена/отключена). Нажмите здесь, чтобы включить или выключить антиспам защиту.
- **Список друзей** - открывает **Список друзей**.
- **Список спаммеров** - открывает **Список спаммеров**.
-  **Антишпион** - администрирование модуля **Защита от сетевых атак**.
- **Поведенческая защита от атак включена / отключена** - показывает статус **поведенческой защиты от сетевых атак** (включена/отключена). Используйте этот пункт, что бы включить или отключить защиту от атак.
- **Дополнительные настройки** - позволяет настроить дополнительные параметры управления защитой от сетевых атак.
-  **Обновления** - управление модулем **Обновления**.
- **Обновить сейчас** - запускает немедленное обновление.
- **Автоматическое обновление включено / отключено** - показывает статус **автоматического обновления** (включено / отключено). Воспользуйтесь этим пунктом для включения или отключения автоматических обновлений.
- **Выход** -закрывает программу. Выбирая этот вариант, значок исчезнет из области уведомлений, и открыть консоль управления можно будет только через меню Пуск Windows.

Замечание



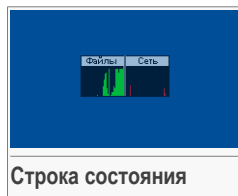
Значок будет затенен, если отключены один или несколько модулей BitDefender. Это позволит Вам знать, что некоторые модули BitDefender отключены, без необходимости открывать консоль управления. Значек начнет мигать, когда появится доступное обновление.

5.2. Строка состояния сканирования

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

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

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

**Замечание**

В окне **График активности** появится обозначение в виде красного креста в соответствующей области (**Файловая зона** или **Сетевая зона**) когда будут заблокированы соответственно Антивирусный монитор или Брандмауэр. Таким образом, даже не открывая консоли управления, Вы будете знать, защищены ли ваша система.

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

**Замечание**

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



6. Общий модуль

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

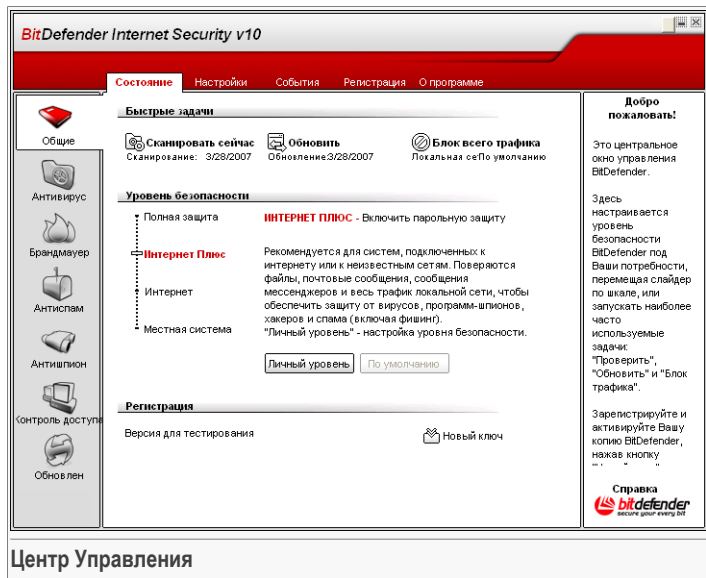
- Центр управления
- Настройки консоли управления
- События
- Регистрация программы
- О программе



Замечание

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


6.1. Центр Управления



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

6.1.1. Быстрые задачи

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


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



Важно

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




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

Замечание



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

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

Чтобы разблокировать трафик нужно нажать кнопку  **Разблокировать трафик**.

Замечание



Чтобы узнать, как эффективно защитить Ваш компьютер внутри локальной сети или ее части, познакомьтесь с разделом **Модуль Брандмауэр** данного руководства пользователя.

6.1.2. Уровни безопасности

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

Существует 4 уровня безопасности:

| Уровень безопасности | Описание |
|--------------------------|--|
| Локальная система | Предлагает стандартную защиту, особенно рекомендуется для компьютеров не подключенных к локальной сети или Интернет. Необходимо малое количество ресурсов. На наличие вирусов и программ-шпионов проверяются все открываемые файлы. |
| Интернет | Предлагает стандартную защиту для компьютеров, непосредственно подключенных к Интернет или локальной сети. Необходимо умеренное количество ресурсов. Проверяются открываемые файлы, электронные сообщения, сообщения мессенджеров и весь трафик |

Уровень безопасности


| | |
|----------------------|---|
| | локальной сети, чтобы обеспечить защиту от вирусов, программ-шпионов и хакеров. |
| Интернет Плюс | Предлагает дополнительную защиту для компьютеров, непосредственно подключенных к Интернет или локальной сети. Необходимо умеренное количество ресурсов. Проверяются открываемые файлы, электронные сообщения, сообщения мессенджеров и весь трафик локальной сети, чтобы обеспечить защиту от вирусов, программ-шпионов, хакеров и спама (включая фишинг). |
| Полная защита | Подразумевает полную защиту Вашей системы. Потребляет значительное количество ресурсов. Проверяются открываемые файлы, электронные сообщения, сообщения мессенджеров и весь трафик локальной сети, чтобы обеспечить защиту от вирусов, программ-шпионов, хакеров и спама (включая фишинг) и неадекватного содержимого веб-страниц. |

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

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

6.1.3. Статус регистрации

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

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



Замечание

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



6.2. Настройки консоли управления



Настройки консоли управления

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

6.2.1. Общие настройки

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

Замечание



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

Если Вы выбираете эту опцию, появится следующее окно:

Подтвердите пароль

Пароль

Подтвердите

Пароль должен быть не менее 8 символов.

Введите пароль

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

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



Важно


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

- **Показывать новости BitDefender (уведомление на тему безопасности)** - время от времени показывает уведомления относительно новых вирусов, рассылаемые сервером BitDefender.
- **Показывать всплывающие окна** - включает функцию всплывающих окон, отображающих статус программы.
- **Запуск BitDefender при загрузке Windows** - BitDefender автоматически запускается при загрузке системы.



Замечание

Мы рекомендуем выбрать эту функцию.

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



6.2.2. Настройки отчета о вирусах

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

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



- **Включить функцию BitDefender обнаружения эпидемий** - отправляет в лаборатории BitDefender Labs отчет о потенциальных вирусных эпидемиях.

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

6.2.3. Настройки фона

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

6.2.4. Управление настройками

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



Важно

Только пользователи с правами администратора могут сохранять и загружать настройки.

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

6.3. События



В этом разделе отображены все события, зафиксированные программой Bitdefender.

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

Примеры событий:

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

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

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

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

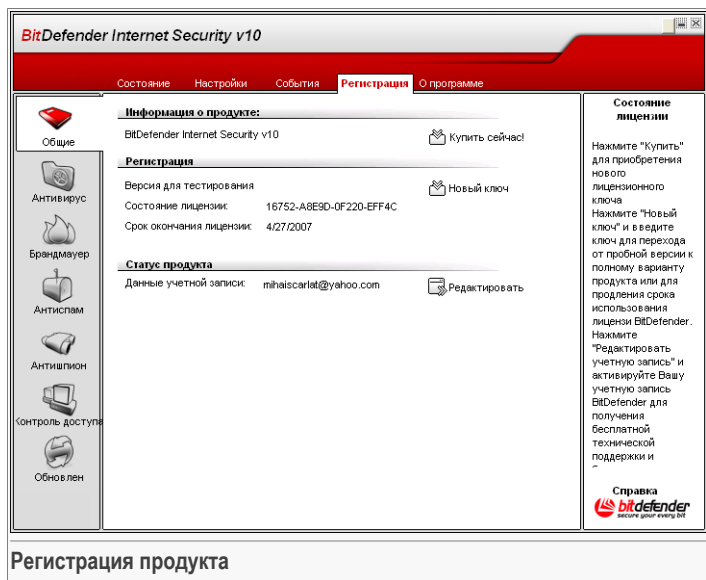


- Выберите источник события в раскрывающемся меню.

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

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


6.4. Регистрация продукта



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

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

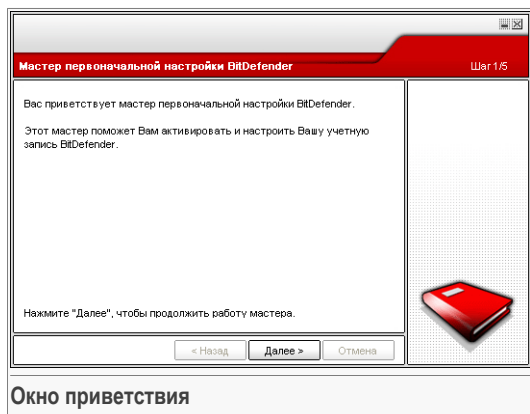
Нажав **Новый ключ**, Вы можете зарегистрировать продукт, изменить ключ регистрации или настройки учетной записи. Чтобы настроить учетную запись

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

6.4.1. Мастер регистрации

Мастер регистрации имеет 5 шагов.

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



Нажмите **Далее**.



Шаг 2/5 - Регистрация BitDefender

Регистрация Шаг 2/5

Это пробная версия BitDefender Internet Security v10. Если Вы хотите оценить работу программы, отметьте "Продолжить ознакомление с продуктом". Если Вы хотите зарегистрировать продукт, отметьте "Зарегистрировать продукт" и внесите Ваш лицензионный ключ. Вы можете найти его на:

- Регистрационной карте товара
- Наклейке компакт диска
- в электронном сообщении при покупке он-лайн. Если у Вас нет серийного номера, свяжитесь с нами: sales@bitdefender.com

Продолжить использование пробной версии

Регистрация продукта.

Новый ключ

Нажмите "Далее", чтобы продолжить работу мастера.

Регистрация

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

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

Нажмите **Далее**.

Шаг 3/5 - Создание учетной записи BitDefender

Зарегистрировать сейчас Шаг 3/5

Вам необходимо создать учетную запись, чтобы получить доступ к технической поддержке и прочим персонализированным услугам BitDefender. Если у Вас уже есть учетная запись BitDefender, пожалуйста, введите необходимые данные. Если у Вас нет учетной записи BitDefender, пожалуйста, введите адрес Вашей электронной почты и пароль.

E-mail:

Пароль:

[Забыли пароль?](#)

Пропустить этот шаг

Нажмите "Далее", чтобы продолжить, или "Отмена", чтобы оканчить работу

Создание учетной записи

У меня нет учетной записи BitDefender

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

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



Замечание

Пароль должен состоять минимум из четырех символов.

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



Важно

Активируйте свою учетную запись прежде чем переходить к следующему шагу.

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

Для продолжения нажмите **Далее**.



У меня уже есть учетная запись BitDefender .

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

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

Для продолжения нажмите **Далее**.

Шаг 4/5 - Введите информацию об учетной записи

Настроить мою учетную запись Шаг 4/5

Введите информацию для учетной записи. Предоставляемые Вами данные не будут разглашены. Если у Вас уже есть учетная запись, мастер отобразит предоставленную Вами при создании информацию.

Имя:

Фамилия:

Страна:

Нажмите "Далее", чтобы продолжить, или "Отмена", чтобы закончить работу

Реквизиты учетной записи



Замечание

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

Введите Ваши имя и фамилию, а также страну проживания.

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

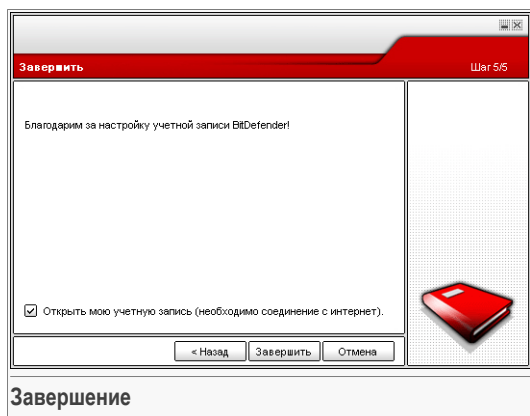


Важно

Предоставленные Вами данные конфиденциальны.

Нажмите **Далее**.

Шаг 5/5 – Итоговый отчет



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

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

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



6.5. О программе

BitDefender Internet Security v10

Состояние Настройки События Регистрация **О программе**

Общие

Антивирус

Брандмауер

Антиспам

Антивижон

Контроль доступа

Обновлен

Информация о продукте:

BitDefender Internet Security v10 - Сборка 247
(c) 2001-2007 SOFTWIN. Все права защищены.

Контактная информация:

WWW: www.bitdefender.com
 Email: sales@bitdefender.com
 Телефон: +7-495-9358276
 Факс: +7-495-9358276

Техподдержка

Техническая поддержка: sales@bitdefender.com
 Чат: <http://www.bitdefender.com/support/faq.htm>
 KB: <http://kb.bitdefender.com/>

О BitDefender

BitDefender(tm) предоставляет решения по информационной защите, удовлетворяющие требованиям защиты современной компьютерной среды, являясь эффективным средством по предотвращению угроз для более 41 млн. пользователей в более 200 странах мира. BitDefender(tm) сертифицирован - ICSA, CheckMark и VB и является единственным ПО защиты,

Справка

 bitdefender.com

Общая информация

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

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

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

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



7. Модуль Антивирус

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

- Входное сканирование
- Сканирование по запросу
- Карантин



Замечание

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

7.1. Входное сканирование

The screenshot shows the BitDefender Internet Security v10 interface. The 'Monitor' tab is active, displaying the status of 'Constant Protection' (Постоянная защита включена). The protection level is set to 'Default' (По умолчанию). A traffic graph shows 0 bytes scanned. The interface includes a sidebar with navigation icons for various security features and a right-hand panel with additional information and a 'Check Now' button.


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

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



Важно

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

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

7.1.1. Уровень защиты

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

Существует 3 уровня защиты:

Уровень защиты. Описание

Разрешающий Охватывает основные нужды в безопасности. Потребляет малое количество ресурсов.

Программы и входящие электронные сообщения проверяются только на наличие вирусов. Кроме классического сканирования при помощи базы образов, также используется эвристический анализ. К зараженным файлам могут применяться следующие действия: вылечить файл/запретить доступ.

Стандартный Предлагает стандартный уровень безопасности. Потребляет малое количество ресурсов.

Все файлы, входящие и исходящие электронные сообщения проверяются на вирусы и программы-шпионы. Кроме классического сканирования при помощи базы образов, также используется эвристический анализ. К зараженным файлам могут применяться следующие действия: вылечить файл/запретить доступ.

Агрессивный Предлагает высокий уровень безопасности. Потребляет среднее количество ресурсов.

Все файлы, входящие и исходящие электронные сообщения, а также веб трафик проверяются на вирусы и



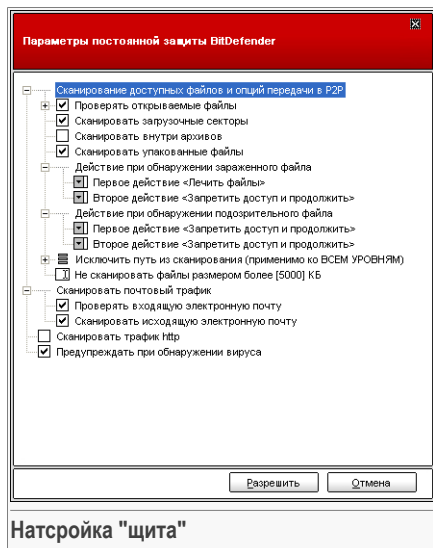
Уровень защиты Описание

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

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

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

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



Настройка "щита"

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

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

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

- Выберите настройку **Проверять открываемые и зачисляемые 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 Проверяются все открываемые файлы, независимо от их формата. |
| Проверить только файлы программ | Проверяются только файлы программ, то есть файлы с расширением: .exe; .bat; .com; .dll; .ocx; .scr; .bin; .dat; .386; .vxd; .sys; .wdm; .cla; .class; .ovl; .ole; .exe; .hlp; .doc; .dot; .xls; .ppt; .wbk; .wiz; .pot; .ppa; .xla; .xlt; .vbs; .vbe; .mdb; .rtf; .htm; .hta; .html; .xml; .xtp; .php; .asp; .js; .shs; .chm; .lnk; .pif; .prc; .url; .smm; .pdf; .msi; .ini; .csc; .cmd; .bas; .eml; .nws. |
| Проверить файлы с заданным расширением | Проверяются только файлы с заданным расширением. Задаваемые расширения разделяются знаком ";". |
| Исключить файлы с расширениями: | Файлы с заданным расширением НЕ проверяются. Задаваемые расширения разделяются знаком ";". |
| Проверка наличия других угроз | Проверка наличия других угроз. Эти файлы будут считаться зараженными. Программное обеспечение, которое включает компоненты adware, может прекратить работу, если выбрана эта настройка. Поставьте значок в поле Пропускать программы дозвона и приложения при сканировании, если Вы хотите пропускать подобные файлы при сканировании. |
| Проверка дисков при обращении | Проверка дисков при первом обращении. |
| Проверять внутри архивов | Проверяются также архивы. Включение данной опции замедлит работу компьютера. |
| Проверить файлы | Проверяются все запакованные файлы. |
| Первоначальное действие | Из выпадающего списка, Вы можете выбрать одно из следующих действий, |



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

| Настройка | Описание |
|-----------|--|
| | уровня защиты (кроме Настроенного уровня). |

- **Сканировать электронную почту** - сканирование электронных сообщений. Доступны следующие варианты:

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

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

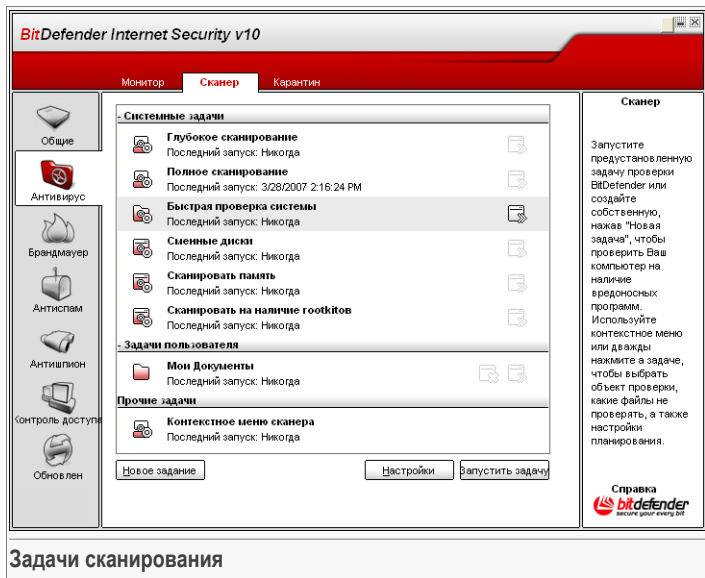
Предупреждение об обнаружении зараженного вирусом файла содержит название вируса, путь к зараженному файлу, действие BitDefender, выполненного с этим файлом, и ссылку на сайт BitDefender, где Вы сможете получить более подробную информацию об этом вирусе. В случае обнаружения вируса в электронной почте,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

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



7.2. Сканирование по требованию



Задачи сканирования

В этом разделе Вы можете конфигурировать проверку Вашего компьютера Bitdefender.

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

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

7.2.1. Задачи сканирования

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



Существует три категории задач сканирования:

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

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

- **Задачи пользователя** - содержит задачи, определенные пользователем. Имеется задача, названная *Мои документы*. Этой задачей можно пользоваться для проверки Ваших документов в папке *Мои документы*.
- **Прочие задачи** - содержит список мелких задач. Эти задачи проверки включают альтернативные типы сканирования, которые не могут быть запущены из данного окна. Вы можете только изменить их настройки или просмотреть отчеты о проверке.

Справа от каждой задачи доступны три кнопки:


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

Замечание



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

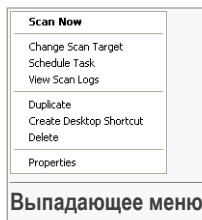


-  **Проверить** - запускает соответствующее задание, запуская **немедленную проверку**.

7.2.2. Выпадающее меню

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

В выпадающем меню имеются следующие команды:



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

Замечание



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

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

Замечание



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

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



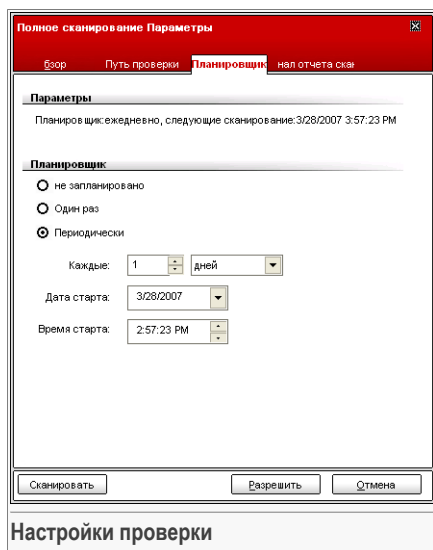
Важно

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

7.2.3. Свойства задач проверки

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

Настройки проверки



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

Уровень проверки

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

Существует 3 уровня проверки:

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

**Уровень защиты** Описание

Программы проверяются только на наличие вирусов. Кроме классической проверки при помощи базы образов, также используется эвристический анализ. К зараженным файлам применяются следующие действия: вылечить файл/поместить в карантин.

Средний

Подразумевает высокую эффективность выявления. Потребляет среднее количество ресурсов.

Все файлы проверяются на наличие вирусов и программ-шпионов. Кроме классической проверки при помощи базы образов, также используется эвристический анализ. К зараженным файлам применяются следующие действия: вылечить файл/поместить в карантин.

Высокий

Подразумевает очень высокую эффективность выявления. Потребляет значительное количество ресурсов.

Все файлы и архивы проверяются на наличие вирусов и программ-шпионов. Кроме классической проверки при помощи базы образов, также используется эвристический анализ. К зараженным файлам применяются следующие действия: вылечить файл/поместить в карантин.

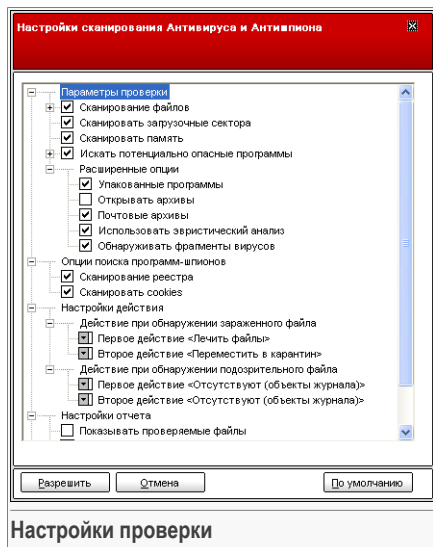
**Важно**

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

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

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

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



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

Опции сканирования сгруппированы в пять категорий:

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

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



Важно

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



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

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

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

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

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

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

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



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

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



Важно

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

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

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

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

Замечание

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

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

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

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

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

Другие настройки

Имеется ряд общих настроек для процесса проверки:

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

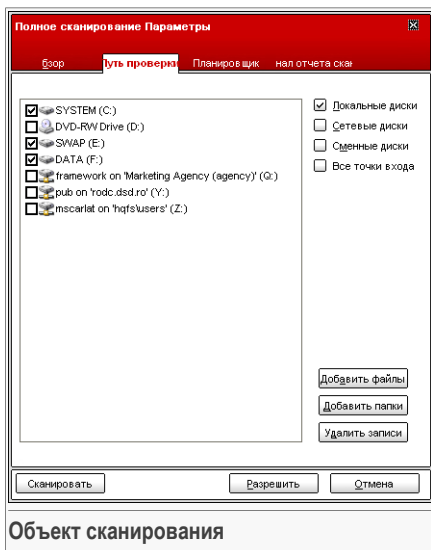


| Настройка | Описание |
|---|---|
| Направить подозрительные файлы в лабораторию BitDefender | Вам будет предложено после завершения процесса проверки переслать все подозрительные файлы в лабораторию BitDefender. |
| Свернуть окно проверки в системный трей при запуске | Окно проверки сворачивается в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

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

Объект сканирования

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



Объект сканирования

Здесь можно задать объект сканирования.

В этом разделе находятся следующие кнопки:

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

**Замечание**

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

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

**Замечание**

Удалить можно только те файлы или папки, которые были добавлены. Объекты, обнаруженные BitDefender автоматически, не могут быть удалены.

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

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

**Замечание**

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

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

Планировщик

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



Быстрая проверка системы Параметры

Взор Путь проверки Планировщик Нал отчета ска

Параметры

Планировщик: ежедневно, следующее сканирование: 3/28/2007 6:21:46 PM

Планировщик

не запланировано

Один раз

Периодически

Каждые: 1 дней

Дата старта: 3/28/2007

Время старта: 5:21:46 PM

Сканировать Разрешить Отмена

Планировщик

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



Важно

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

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

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

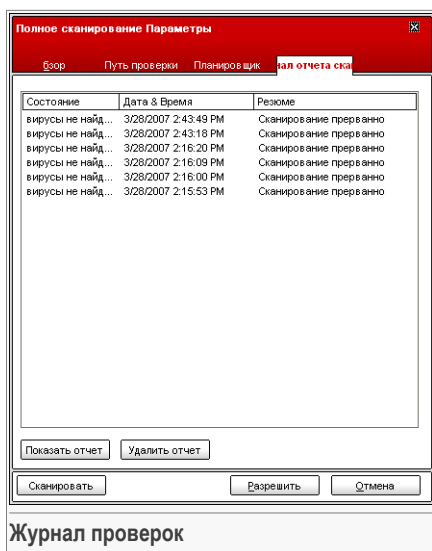
Если Вы хотите повторять процесс проверки через определенные интервалы времени, выберите **Периодически** и в поле **Каждые** введите число минут/часов/дней/недель/месяцев/лет, соответствующих необходимому

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

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

Журнал проверок

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



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

Доступны две кнопки:

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

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



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

7.2.4. Типы проверки по требованию

BitDefender имеет три типа проверок по требованию:

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

Немедленная проверка


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

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

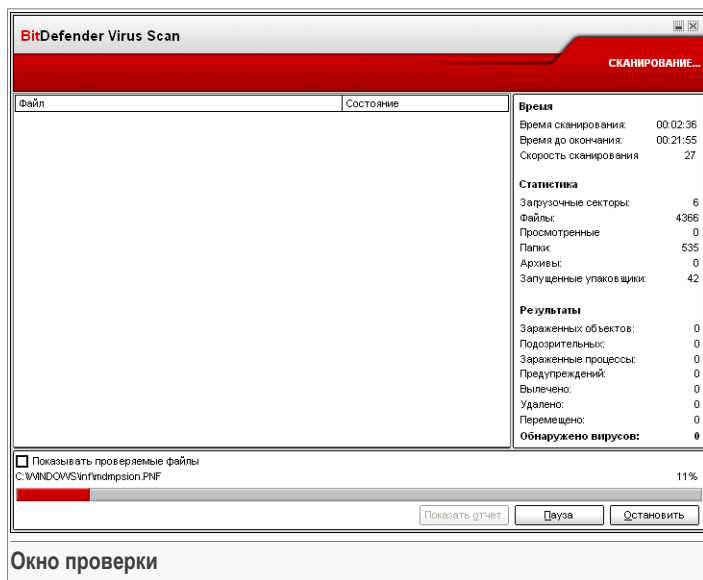
Чтобы BitDefender полностью проверил все Ваши файлы, необходимо закрыть все запущенные приложения, особенно почтовые программы (Outlook, Outlook Express или Eudora).

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

Для запуска проверки, используйте один из способов:

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

Появится окно просмотра.



Окно проверки

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

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

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



Замечание

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

Доступны три кнопки:

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



Замечание

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



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

Замечание



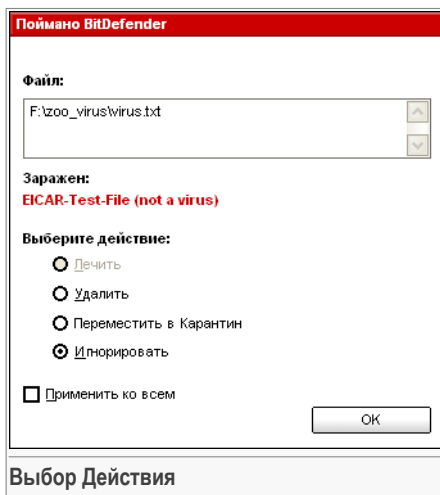
Если нажать правой кнопкой мыши на запущенном процессе, откроется выпадающее (контекстное) меню, которое позволяет управлять окном проверки. Опции (**Пауза / Продолжить**, **Остановить** и **Остановить&Закрыть**) подобны клавишам в окне проверки.

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

В окне Вы увидите название файла и название вируса.

Вы можете выбрать одно из следующих действий над зараженным файлом:

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



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

Замечание



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

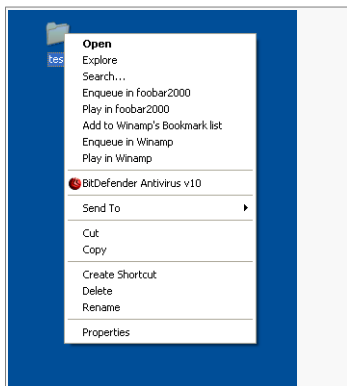
Нажмите **ОК**.



Замечание

Отчеты автоматически сохраняются в разделе [Журнал проверок](#) в окне **Свойства** соответствующей задачи.

Проверка через контекстное меню



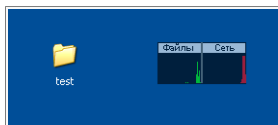
Проверка через контекстное меню

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

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

Проверка перетягиванием.

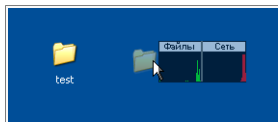
Перетяните файл или папку, которую вы хотите проверить, в **Область состояния проверки**, как показано ниже.



Перетаскивание файла

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

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



Перетаскивание файла



7.2.5. Сканирование на руткиты

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

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



Важно

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

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

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



Внимание

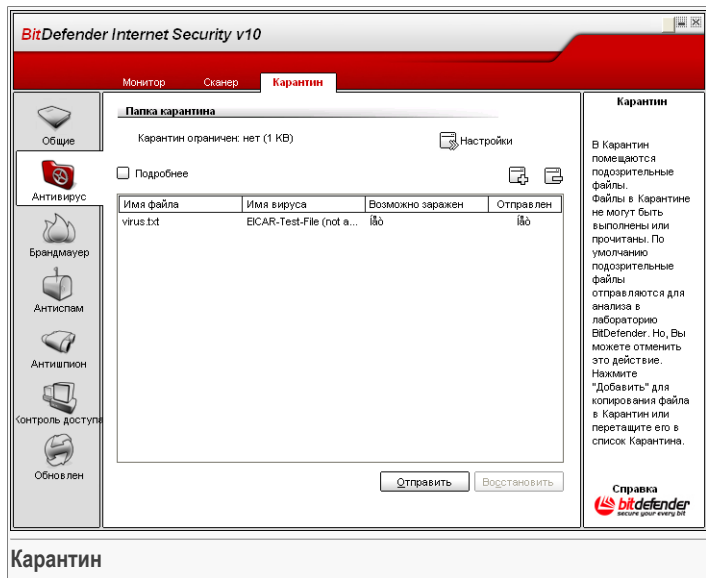
НЕ ВСЕ СКРЫТЫЕ ФАЙЛЫ - ЗЛОВРЕДНЫЕ ПРОГРАММЫ! Перед переименованием скрытых файлов, удостоверьтесь, что они не принадлежат ни к известному приложению, ни к операционной системе. Переименование таких файлов может привести к проблемам в Вашей системе.



Важно

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

7.3. Карантин



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

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

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



Замечание

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



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

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

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



Важно

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

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

Настройки карантина сгруппированы в две категории:

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



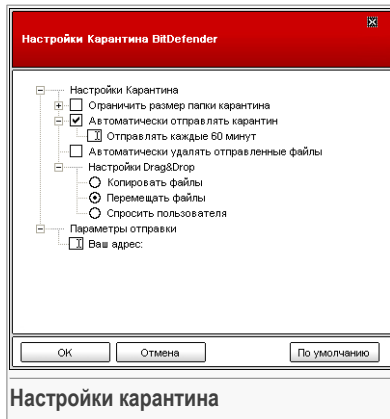
Замечание

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

Настройки карантина

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

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



Замечание

По умолчанию, папка карантина не имеет ограничений по размеру.

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

Настройки электронной почты

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

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



8. Модуль брандмауэр

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

- Мастер Брандмауэра
- Статус Брандмауэра
- Защита трафика
- Дополнительные настройки
- Активность Брандмауэра

Замечание




Для получения более подробной информации относительно модуля **Брандмауэр** выберите описание «*Модуль брандмауэр*» (р. 30).

8.1. Мастер Брандмауэра

При каждом подключении к новой сети, появится мастер, помогающий создать новый профиль брандмауэра BitDefender для данной сети. Мастер также помогает создавать набор базовых правил, необходимых для основных широко используемых приложений. Конечным результатом его работы является защищенная система с функционирующими почтовым клиентом и веб браузером.

Замечание



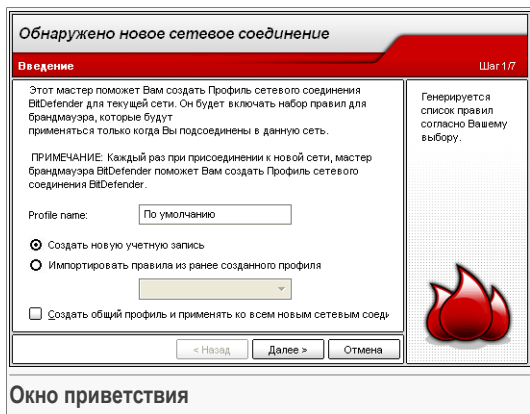
Мастера также можно запустить в любой момент, нажав  **Изменить профиль** в разделе **Трафик**. Пожалуйста помните, что, если Вы сбрасываете профиль, то все правила брандмауэра для текущего профиля будут утеряны.

Важно



Если работа мастера не завершена, то брандмауэр будет отключен. Мастер появится автоматически, когда Вы попытаетесь запустить брандмауэр.

8.1.1. Шаг 1/7 - Экран приветствия



Окно приветствия

Введите название нового профиля сети в поле **Имя профиля**.

Выберите **Создать новый профиль**, чтобы запустить работу мастера и создать набор базовых правил брандмауэра.

Если Вы выберете **Импорт правил из ранее созданного профиля**, то необходимо выбрать сетевой профиль из списка. Новый профиль будет собирать все правила выбранного профиля. Вы будете направлены в последний шаг мастера, без дальнейшей настройки.

Выберите **Сделать профиль общим и применять ко всем новым сетям**, чтобы создать общий профиль или перезаписать уже существующий. Общий профиль будет применяться каждый раз, когда BitDefender выявит новую сеть без необходимости запуска мастера брандмауэра.



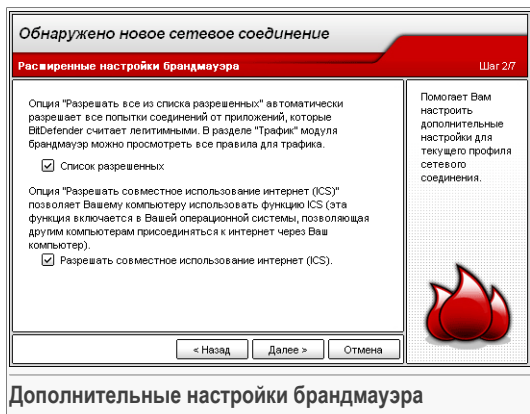
Замечание

Чтобы отключить эту функцию, перейдите в раздел [Дополнительно](#) и уберите галочку в поле **Применять одинаковый (общий) профиль для всех новых сетевых соединений**.

Нажмите **Далее**.



8.1.2. Шаг 2/7 - Дополнительные настройки брандмауэра



Настройка дополнительных настроек брандмауэра для данного профиля сетевого соединения.

Доступны следующие варианты:

| Настройка | Описание |
|--|---|
| Разрешить все из разрешенного списка | Автоматически разрешает все исходящие соединения от программ, известных BitDefender как легитимные. Данная функция позволяет создавать правила для исходящих соединений в разделе Трафик без Вашего вмешательства. Всплывающее окно уведомит о создании подобного правила. Программы 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. |
| Разрешить общий доступ к подключению интернета (ICS) для данного компьютера | Позволяет Вашему компьютеру использовать общий доступ к подключению интернета (ICS). Данная настройке не включает автоматически ICS на Вашей системе, а только разрешает данный тип соединений, |

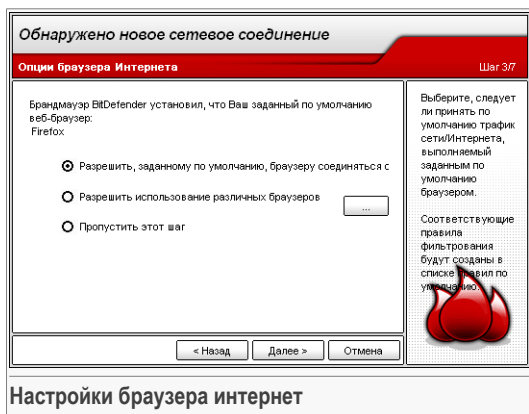
Настройка

Описание

если Вы включите данную функцию в Вашей операционной системе.

Общий доступ к подключению интернета (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.

8.1.3. Шаг 3/7 - Настройки браузера интернет.



BitDefender обнаружит ваш заданный по умолчанию браузер. Выберите, следует ли использовать по умолчанию сетевой/Интернет трафик, генерируемый заданным по умолчанию браузером или выбрать другой браузер.



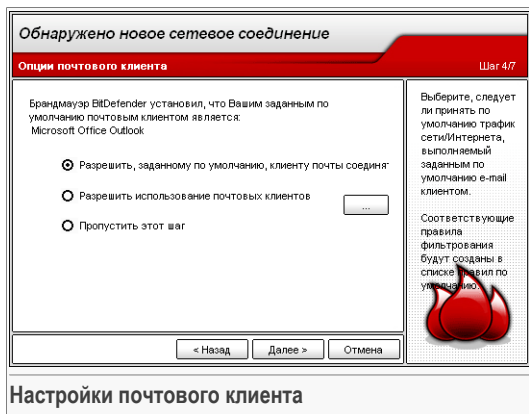
Важно

Если Вы выберете опцию «пропустить этот этап», то правила, связанные с этим выбором, не будут созданы. Вы должны будете создать ваш собственный список правил. Не пропускайте этот этап, если Вы не уверены в том, хотите ли Вы создать соответствующие правила самостоятельно.

Нажмите **Далее**.



8.1.4. Шаг 4/7 - Настройки почтового клиента



BitDefender обнаружит ваш заданный по умолчанию почтовый клиент. Выберите, следует ли использовать по умолчанию сетевой/Интернет трафик, генерируемый заданным по умолчанию почтовым клиентом или выбрать другой почтовый клиент.

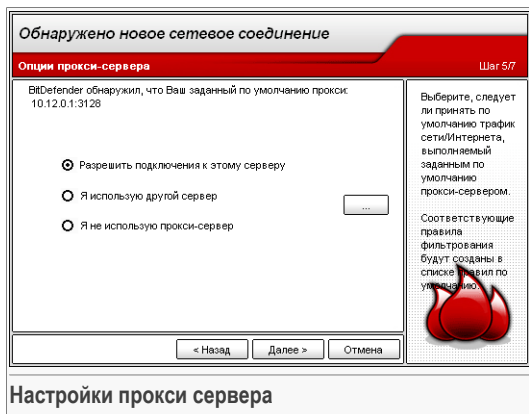


Важно

Если Вы выберете опцию «пропустить этот этап», то правила, связанные с этим выбором, не будут созданы. Вы должны будете создать ваш собственный список правил. Не пропускайте этот этап, если Вы не уверены в том, хотите ли Вы создать соответствующие правила самостоятельно.

Нажмите **Далее**.

8.1.5. Шаг 5/7 - Настройки прокси сервера



Если Вы используете прокси-сервер для подключения к сети Интернет, то BitDefender обнаружит его. Выберите, следует ли использовать по умолчанию сетевой/Интернет трафик через заданный по умолчанию прокси-сервер или нажав **Я использую другой прокси-сервер** и введите IP адрес прокси-сервера и порт.

Нажмите **Далее**.



8.1.6. Шаг 6/7 - Выбор типа сети

Обнаружено новое сетевое соединение

Выбор типа сети Шаг 6/7


Как вы соединяетесь с Интернет?

- Надежное сетевое соединение LAN (офисная сеть)
- ненадежное сетевое соединение LAN
- Прямое подключение (Домашнее/Другое)
- Пропустить этот шаг и установить собственный список правил

Выберите эту установку, если Вы подключаетесь прямо к Интернету, или если Вы не знаете, какого типа подключение Вы используете. Это - настройка по умолчанию, соответствующая повышенному уровню безопасности. Разрешаются только важные входящие подключения, запрещены общие папки и принтеры для этого типа подключения. Вы можете добавить правила вручную для приложений, которые не в состоянии работать или переключать на доверенное подключение, если ваш компьютер находится в локальной сети.

Выберите тип подключения в сетий/Интернете.

Если Вы не уверены, какое подключение к Интернету Вы имеете, пожалуйста выберите "Прямое"



Выбор типа сети

Вы должны выбрать тип вашего сетевого/Интернет подключения. Имеются следующие опции:

| Настройка | Описание |
|---|--|
| Надежная локальная сеть | Вы должны доверять только сетям, которые защищены брандмауэром и антивирусом. Пожалуйста, свяжитесь с вашим сетевым администратором, чтобы проверить это. Если Вы не знаете, какое подключение Вы используете, не выбирайте эту настройку. |
| Ненадежная локальная сеть | Выберите эту настройку, если Вы – пользователь на правах гостя в другой сети кроме своей домашней или офисной сетей. Если Вы не знаете, какое подключение Вы используете, не выбирайте эту настройку. |
| Прямое подключение к сети Интернет | Выберите эту настройку, если Вы соединяетесь напрямую с сетью Интернет или если Вы не знаете, какое подключение Вы используете. Все входящие подключения будут отклонены. Хотя при этом может нарушиться подключение некоторых приложений, это обеспечит более высокий уровень защиты. Для приложений, которые перестали нормально |

| Настройка | Описание |
|-----------|--|
| | функционировать, Вы можете добавить правила вручную. |

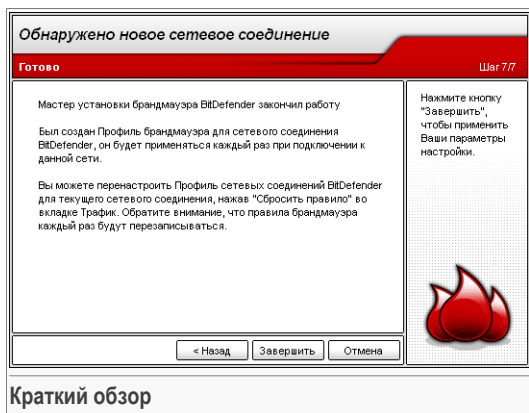


Важно

Если Вы выберете опцию «пропустить этот этап», то правила, связанные с этим выбором, не будут созданы. Вы должны будете создать ваш собственный список правил. Не пропускайте этот этап, если Вы не уверены в том, хотите ли Вы создать соответствующие правила самостоятельно.


Нажмите **Далее**.

8.1.7. Шаг 7/7 – Краткий итоговый отчет



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

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

Мастера настройки Брандмауэра можно запустить в любой момент, нажав  **Сбросить профиль** в разделе **Трафик**.



Замечание

Пожалуйста помните, что если Вы выбрали сброс профиля, то все правила Брандмауэра с текущим профилем будут потеряны.



8.2. Статус Брандмауэра

BitDefender Internet Security v10

Состояние Трафик Расширенные Активность

Брандмауэр активирован

Текущая сеть: По умолчанию **Заблокировать трафик**

IP: 10.10.17.97
Шлюз: 10.10.0.1

Уровень защиты

Справлять **СПИСОК РАЗРЕШЕННЫХ**

Разрешает все попытки соединений от приложений, которые BitDefender считает легитимными. В разделе "Трафик" можно просмотреть все правила для трафика, по мере их добавления.

Разрешить все

Запретить все

Сетевая активность

входящие: 1.10K 120s 60s 0s

исходящие: 0.00K 120s 60s 0s

Брандмауэр

Брандмауэр защищает Ваш компьютер от несанкционированных попыток установли входящих или исходящих соединений.

Здесь содержатся общие настройки брандмауэра. Перетасуйте ползунок вдоль шкалы для установки заданных по умолчанию действий для новых событий.

График показывает трафик за последние две минуты.

Справка **bitdefender** Безопасность. Всегда.

Статус Брандмауэра

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



Важно

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

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

Чтобы разблокировать трафик нужно нажать кнопку **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** заблокирован.

8.2.1. Уровень защиты

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

Существует 4 уровня защиты:

| Уровень защиты | Описание |
|---|---|
| Запретить все | Блокирует без предупреждения весь трафик, который не описан в установленных на данный момент правилах. Используйте этот уровень, если Вы уже установили необходимые Вам правила для программ и подключений. |
| Разрешить все | Разрешает без предупреждения весь трафик, который не описан в установленных на данный момент правилах. Настоятельно не рекомендуем использовать этот уровень, он может быть полезен системным администраторам. |
| Разрешить все из разрешенного списка | <p>Разрешает все исходящие соединения от программ, известных BitDefender как легитимные. В разделе Трафик можно просмотреть все правила для трафика, по мере их добавления.</p> <p>Программы 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.</p> |
| Запрашивать | Запрашивает разрешения при попытках трафика, не совпадающего с текущими правилами. |



Важно

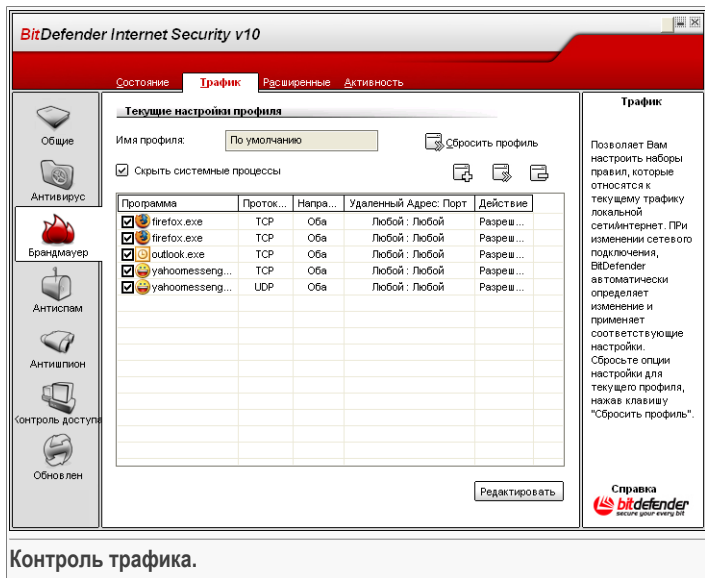
Если консоль управления закрыта, и совпадений в наборе правил не найдено, то выполняется действие **Запретить**.

Нажмите **По умолчанию**, чтобы установить правило по умолчанию (**Разрешать все в списке разрешенных**).

Если Вы хотите просмотреть список программ в разрешенном списке, нажмите **Разрешенные**.



8.3. 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.

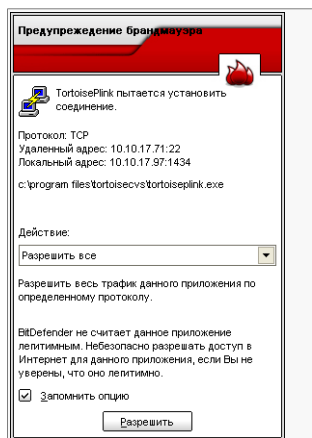
Поставьте отметку в поле **Скрывать системные процессы**, чтобы скрыть правила, касающиеся системных процессов или процессов BitDefender.

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

8.3.1. Автоматическое добавление правил

Правила добавляются в список, когда Вы отвечаете на запросы BitDefender о новой программе, которая пытается получить доступ к сети Интернет.

Со 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, IP адрес и порт через который оно пытается подключиться.

Поставьте галочку в поле **Запомнить ответ** и нажмите **Да** или **Нет**. Будет создано новое правило, которое будет занесено в таблицу правил. Если такая ситуация повторится, Вы не получите больше сообщений.

Вы можете выбрать одно из следующих действий:

| Действие | Описание |
|---|---|
| Разрешить | Разрешить весь трафик для этого приложения по указанному протоколу. |
| Запретить | Блокировать весь трафик для этого приложения по указанному протоколу. |
| Разрешить весь трафик для этого приложения | Разрешить весь трафик для этого приложения по всем IP протоколам. |
| Запретить весь трафик для этого приложения | Блокировать весь трафик для этого приложения по всем IP протоколам. |
| Разрешение только для удаленного хоста | Разрешить трафик для этого приложения по указанному протоколу с указанным удаленным хостом. |
| Разрешение только для этого порта | Разрешить трафик для этого приложения по указанному протоколу на указанном порте для любого адресата. |
| Запрет только для удаленного хоста | Блокировать трафик для этого приложения по указанному протоколу с указанным удаленным хостом. |



Действие

Описание

Запрет только для этого порта Блокировать трафик для этого приложения по указанному протоколу на указанном порте для любого адресата.



Важно

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

К каждому правилу, которое было запомнено, можно обратиться в разделе **Трафик** для дальнейшей подстройки.

8.3.2. Добавление правил вручную

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

Добавить правило

Информация о приложении

Выбрать приложение: Любой | Путь программы: Просмотр

Действие

Действие: Любой | Сетевые процессы: Все

Адреса

Направление: Оба | Протокол: Любой

| Исходный адрес | | Адрес направления | |
|---|----------------------------------|---|----------------------------------|
| IP адрес: | Тип: | IP адрес: | Тип: |
| <input type="text" value="0 . 0 . 0 . 0 . 0 . 0"/> | Любой | <input type="text" value="0 . 0 . 0 . 0 . 0 . 0"/> | Любой |
| Маска: <input type="text" value="0 . 0 . 0 . 0 . 0 . 0"/> | <input type="checkbox"/> Местный | Маска: <input type="text" value="0 . 0 . 0 . 0 . 0 . 0"/> | <input type="checkbox"/> Местный |
| Порт(ы): Любой | | Порт(ы): Любой | |

Постоянство

Создать постоянное правило

Добавить Отмена

Выберите параметры

Вы можете установить следующие параметры:

- **Приложение** - выбор приложения, к которому применяется правило. Можно выбрать только одно приложение (из выпадающего меню **Выбор приложения** выберите **Путь/имя файла**, а затем нажмите **Обзор**, чтобы выбрать приложение) или все приложения (из выпадающего меню **Выбор приложения** выберите **Все**).
- **Действие** - выбрать действие для правила и соответствующего события.

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

- **Адреса** - выбрать направление трафика и протокол для правила.
Направление - выбор направления передачи данных.

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

Тип протокола - выбрать тип протокола - ICMP, TCP, UDP или любой.

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

| Протокол | Описание |
|----------|---|
| ICMP | 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 использует протокол ICMP для тестирования подключения к сети Интернет. |



| Протокол | Описание |
|----------|---|
| 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. |

- **Исходящий адрес** - введите необходимый IP-адрес и маску или поставьте галочку на поле **Локальный** если правило следует применить к локальному компьютеру. Если в качестве протокола Вы выбрали TCP или UDP протоколы, Вы можете указать конкретный номер порт или диапазон его значений в пределах от 0 до 65535. Если Вы хотите распространить действие правила на все порты, выберите опцию **Любой**.
- **Адрес назначения** - введите необходимый IP-адрес и маску или поставьте галочку на поле **Локальный** если правило следует применить к локальному компьютеру. Если в качестве протокола Вы выбрали TCP или UDP протоколы, Вы можете указать конкретный номер порт или диапазон его значений в пределах от 0 до 65535. Если Вы хотите распространить действие правила на все порты, выберите опцию **Любой**.
- **Сохранение правил** - поставьте галочку в поле, соответствующем опции **Сохранить правило на диске** чтобы сохранить правило для последующих "сеансов". Если Вы не выберете эту опцию, правило будет удалено в конце данного сеанса (при перезагрузке компьютера или обновлении BitDefender).

Нажмите **Добавить**.

8.3.3. Управление правилами

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**. Чтобы изменить правило, выберите его и нажмите кнопку **Редактировать правило**

или дважды нажмите на правило. Чтобы временно отключить правило, не удаляя его, ударьте галочку из соответствующего поля.

**Замечание**

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

8.3.4. Модифицирование профилей

Перед включением модуля брандмауэр Вам предложат завершить работу мастера, чтобы создать новый профиль сетевого соединения. Мастер поможет создать набор базовых правил брандмауэра, необходимых для наиболее часто используемых приложений. Нажмите  **Сброс профиля**, чтобы запустить работу мастера еще раз и изменить профиль.

**Важно**

Все правила, которые Вы добавили в данном разделе будут потеряны, если Вы решите изменить профиль сетевого соединения.

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



Детальное представление текущего списка правил

Правила для входящих соединений:

| Приложение | Протокол | Исходный адрес | Исходные порты | Конечный адрес | Конечные порты | Разрешить... | Действие | Путь |
|---|----------|----------------|----------------|----------------|----------------|--------------|----------|------------|
| <input checked="" type="checkbox"/> Любая | UDP | Любой | 53 | Любой | 1024 - 65535 | данные от... | Разр... | |
| <input checked="" type="checkbox"/> bdmscon.exe | TCP | Любой | 80 | Любой | Любой | Да | Разр... | c:\program |
| <input checked="" type="checkbox"/> ysserv.exe | TCP | Любой | 25 | Любой | Любой | Да | Разр... | c:\program |
| <input checked="" type="checkbox"/> ysserv.exe | TCP | Любой | 80 | Любой | Любой | Да | Разр... | c:\program |
| <input checked="" type="checkbox"/> ysserv.exe | TCP | Любой | 110 | Любой | Любой | Да | Разр... | c:\program |
| <input checked="" type="checkbox"/> bdite.exe | TCP | Любой | 80 | Любой | Любой | Да | Разр... | c:\program |
| <input checked="" type="checkbox"/> bdagent.exe | TCP | Любой | 80 | Любой | Любой | Да | Разр... | c:\program |
| <input checked="" type="checkbox"/> bdsuubmit.exe | TCP | Любой | 80 | Любой | Любой | Да | Разр... | c:\program |
| <input checked="" type="checkbox"/> bdsuubmit.exe | TCP | Любой | 80 | Любой | Любой | Да | Разр... | c:\program |
| <input checked="" type="checkbox"/> bdsuubmit.exe | TCP | Любой | 80 | Любой | Любой | Да | Разр... | c:\program |
| <input checked="" type="checkbox"/> livesrv.exe | TCP | Любой | 80 | Любой | Любой | Да | Разр... | c:\program |
| <input checked="" type="checkbox"/> Любая | UDP | 10.12.0.1 | 3128 | Любой | 1024 - 65535 | данные от | Разр... | |

Правила для исходящих подключений:

| Приложение | Протокол | Исходный адрес | Исходные порты | Конечный адрес | Конечные порты | Разрешить... | Действие | Путь |
|---|----------|----------------|----------------|----------------|----------------|--------------|----------|------------|
| <input checked="" type="checkbox"/> Любая | UDP | Любой | 1024 - 65535 | Любой | 53 | данные от... | Разр... | |
| <input checked="" type="checkbox"/> bdmscon.exe | TCP | Любой | Любой | Любой | 80 | Да | Разр... | c:\program |
| <input checked="" type="checkbox"/> ysserv.exe | TCP | Любой | Любой | Любой | 25 | Да | Разр... | c:\program |
| <input checked="" type="checkbox"/> ysserv.exe | TCP | Любой | Любой | Любой | 80 | Да | Разр... | c:\program |
| <input checked="" type="checkbox"/> ysserv.exe | TCP | Любой | Любой | Любой | 110 | Да | Разр... | c:\program |
| <input checked="" type="checkbox"/> bdite.exe | TCP | Любой | Любой | Любой | 80 | Да | Разр... | c:\program |
| <input checked="" type="checkbox"/> bdagent.exe | TCP | Любой | Любой | Любой | 80 | Да | Разр... | c:\program |
| <input checked="" type="checkbox"/> bdsuubmit.exe | TCP | Любой | Любой | Любой | 80 | Да | Разр... | c:\program |
| <input checked="" type="checkbox"/> bdsuubmit.exe | TCP | Любой | Любой | Любой | 80 | Да | Разр... | c:\program |
| <input checked="" type="checkbox"/> bdsuubmit.exe | TCP | Любой | Любой | Любой | 80 | Да | Разр... | c:\program |
| <input checked="" type="checkbox"/> livesrv.exe | TCP | Любой | Любой | Любой | 80 | Да | Разр... | c:\program |
| <input checked="" type="checkbox"/> Любая | UDP | Любой | 1024 - 65535 | 10.12.0.1 | 3128 | данные от | Разр... | |

Разрешить Справка

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.

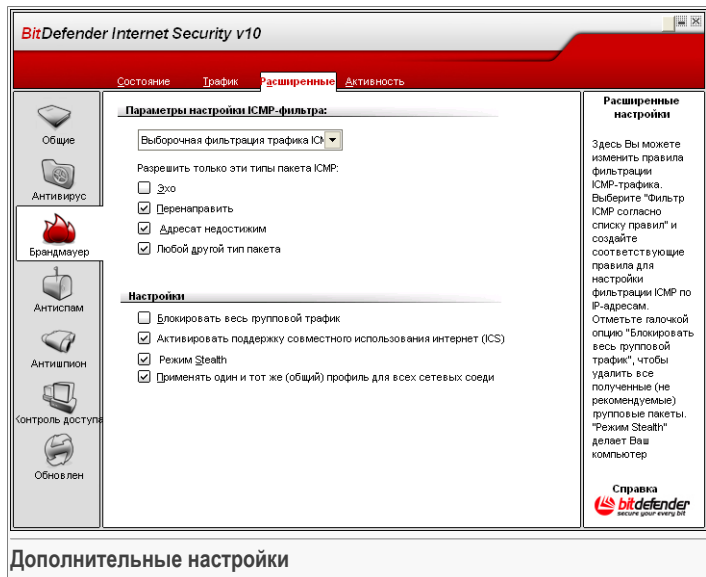


Замечание

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

Нажмите **ОК**, чтобы вернуться к консоли управления.

8.4. Дополнительные настройки



В данном разделе Вы можете изменить дополнительные настройки брандмауэра BitDefender. Дополнительные настройки позволяют проводить фильтрацию ICMP трафика ([Настройки ICMP фильтра](#)) и блокировать групповой трафик, совместное использовать Ваше Интернет соединение или сделать Ваш компьютер невидимым для вредоносных программ или хакеров ([Настройки](#)).

8.4.1. Настройки ICMP фильтра

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

- **Позволять весь ICMP трафик** - позволяет т весь ICMP трафик.
- **Блокировать весь ICMP трафик** - блокировка всего ICMP трафика.
- **Настроить фильтр ICMP** - настройка фильтрации CMP трафика. Вы можете настроить следующие опции:



| 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 недоступим | Это – ICMP сообщение, которое сгенерировано маршрутизатором, чтобы сообщить клиенту, что сервер адресата является недоступным, если дейтаграмма не имеет многоадресного адреса. Появление такого рода сообщений может быть вызвано следующими причинами: отсутствием физического подключения к передающему серверу (бесконечное расстояние), неактивным состоянием |

| Настройка | Описание |
|-----------------------------------|--|
| | 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 недостижим или Переадресовка . |

- **Применить текущий набор ICMP** - применяет текущие настройки к ICMP трафику, указанные в разделе [Статус](#) модуля **Брандмауэр**.

8.4.2. Настройки модуля Антиспам

Доступны следующие дополнительные настройки брандмауэра:

| Настройка | Описание |
|--|---|
| Блокировать весь многоадресный трафик | <p>Блокирует все получаемые многоадресные пакеты.</p> <p>Многоадресный трафик - это трафик, адресуемый конкретной группе в сети. Пакеты отсылаются на специальный адрес, откуда клиенты могут их получать, в случае их согласия.</p> <p>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 отказываться принимать пакеты. Если пакеты принимаются, видео-поток могут просмотреть все "многоадресные" клиенты.</p> <p>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.</p> |



| Настройка | Описание |
|--|--|
| Поддержка разделяемого доступа в Интернет (ICS) | <p>Включение поддержки разделяемого доступа в Интернет (ICS). Данная опция не включает автоматически ICS на Вашей системе, а только позволяет подобный тип соединения, если Вы включите данную функцию в Вашей оперативной системе.</p> <p>Общий доступ к подключению интернета (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.</p> <p>Разделение доступа в Интернет с пользователями локальной сети приводит к повышенному потреблению ресурсов и имеет определенный риск. Он также занимает некоторые Ваши порты (открытые пользователями, использующими Ваше сетевое соединение).</p> |
| Скрытый режим | <p>Делает Ваш компьютер невидимым для вредоносных программ и хакеров.</p> <p>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.</p> <p>Самый простой способ выяснить, подвержен ли Ваш компьютер угрозам, - это подключиться к портам и проверить, приходит ли ответ. Эта процедура называется сканированием портов. BitDefender автоматически проверяет и блокирует попытки сканирования портов.</p> |
| Применить профиль ко всем сетевым подключениям | общий Применяет общий профиль, если такой существует, ко всем сетевым соединениям, обнаруженным BitDefender. Это действие не распространяется |

Настройка

Описание

однако на сетевые соединения, для которых Вы ранее указали профиль. Отключите данную функцию, чтобы запускать мастера брандмауэра каждый раз, когда BitDefender обнаружит новое сетевое соединение.

Общий профиль создается, когда Вы полностью завершаете все шаги **мастера брандмауэра** с включенной опцией **Сделать этот профиль общим для всех новых сетевых соединений** на первом шаге данного мастера.

8.5. Контроль подключений

The screenshot shows the 'Активность' (Activity) tab in BitDefender Internet Security v10. The main window is titled 'Активные подключения и открытые порты:' (Active connections and open ports:). It displays a list of active connections and open ports for various applications. The selected entry is: 10.10.17.97: 1061 к 10.10.0.77: 445 Отправлено <-->: 0 Bytes. Получено: 8 Bytes. The right sidebar contains a 'Активность' (Activity) section with text explaining that the current activity (TCP and UDP) is visible in the Internet settings for applications, and that the 'Блокировка' (Block) button can be used to create rules that limit traffic by application, port, or connection type. The 'Блокировка' button is highlighted in blue. At the bottom of the window, there are buttons for 'Обновить' (Refresh), 'Дог-файл' (Log file), 'Блокировать' (Block), and 'Экспорт снимка' (Export screenshot). The BitDefender logo and 'Справка' (Help) link are visible in the bottom right corner.

Активные подключения и открытые порты:

- c:\windows\system32\svchost.exe <--> Всего отправлено: 0 Bytes. Всего получено: 0 Bytes.
- Открытые порты...
- c:\program files\yahoo!\messenger\yahoo messenger.exe <--> Всего отправлено: 13.4 Bytes. Всего получено: 0 Bytes.
- Подключения...
- Открытые порты...
- system <--> Всего отправлено: 144 Bytes. Всего получено: 9.647 MBytes.
- Подключения...
- 10.10.17.97: 1061 к 10.10.0.77: 445 Отправлено <-->: 0 Bytes. Получено: 8 Bytes.
- 10.10.17.97: 1280 к 10.10.0.6: 445 Отправлено <-->: 0 Bytes. Получено: 13 Bytes.
- Открытые порты...
- 10.10.17.97: 137 <--> [UDP] Режим ожидания...
- 0.0.0.0: 445 <--> [UDP] Режим ожидания...
- 0.0.0.0: 445 <--> [TCP] Режим ожидания...
- 10.10.17.97: 139 <--> [TCP] Режим ожидания...
- 10.10.17.97: 138 <--> [UDP] Режим ожидания...
- c:\windows\system32\lsass.exe <--> Всего отправлено: 8.958 kBytes. Всего получено: 0 Bytes.
- Открытые порты...
- 0.0.0.0: 4500 <--> [UDP] Режим ожидания...
- 0.0.0.0: 500 <--> [UDP] Режим ожидания...

Активность

Текущая активность (TCP и UDP) в сети/Интернете по приложениям.

Используйте кнопку "Блокировка" для создания правил, которые ограничивают трафик по типу приложений, портам или подключениям.

"Блокировка" создает постоянное правило, которое появляется в разделе Трафик, где оно может быть отредактировано/удалено.

Справка bitdefender

Контроль подключений

В данном разделе можно просмотреть текущую сетевую/интернет активность (по TCP и UDP) по каждому приложению. Здесь также можно получить доступ к журналу брандмауэра BitDefender.



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.

Используйте кнопку **Обновить** чтобы повторно открыть раздел **Сетевая активность** (чтобы просмотреть последние действия модуля **Брандмауэр**).

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

Чтобы получить полный список событий, относящихся к модулю брандмауэра (запуск/остановка брандмауэра, блокирование трафика, включение "невидимого режима", изменение настроек, применение профиля) или сгенерированных выявленными им действиями (сканирование портов, блокирование попыток соединения или трафика согласно правилам), проверьте журнал брандмауэра BitDefender, который можно просмотреть, нажав **Показать журнал**. Файл расположен в папке Common Files текущего пользователя Windows по следующему пути `...Softwin\BitDefender Firewall\bdfirewall.txt`.



9. Модуль Антиспам

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

- Статус модуля антиспам
- Настройка модуля антиспам
- Интеграция в Microsoft Outlook / Outlook Express / Windows Mail



Замечание

Для получения более подробной информации относительно модуля **Антиспам** выберите описание «*Модуль Антиспам*» (р. 30).

9.1. Статус модуля Антиспам

BitDefender Internet Security v10

Состояние | Настройки

Антиспам включен

| | | |
|-----------------|-----------|-------------------------|
| Список друзей | 4 записей | Список друзей |
| Список спамеров | 3 записей | Управление списком спам |

Уровень защиты

Агрессивный | **УМЕРЕННО-АГРЕССИВНЫЙ** | Средняя | Разрешенный

Данный уровень рекомендуется, если Вы получаете большое количество спама. Он может приводить к некоторому количеству ложных срабатываний (легитимные сообщения будут помечены как спам). Настройка списков Друзей/Спамеров и обучение Байесова фильтра позволят уменьшить количество ложных срабатываний.

Состояние Антиспама

| | |
|---------------------------------|---|
| Полученные письма (этот сеанс): | 0 |
| Спам (этот сеанс): | 0 |
| Всего получено писем: | 0 |
| Всего писем со спамом: | 0 |

Состояние Антиспама

Используйте ползунок для установки уровня чувствительности. При 'Высок' - некоторое количество спама попадет в Вам в почтовый ящик, при 'Агрессивном' - минимальное количество спама попадет в почтовый ящик, но есть вероятность ложных срабатываний. Список друзей: сообщения с данных адресов всегда будут доставлены в почтовый ящик.

Справка
 bitdefender
 secure your every day

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:

9.1.1. Заполните список адресов



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

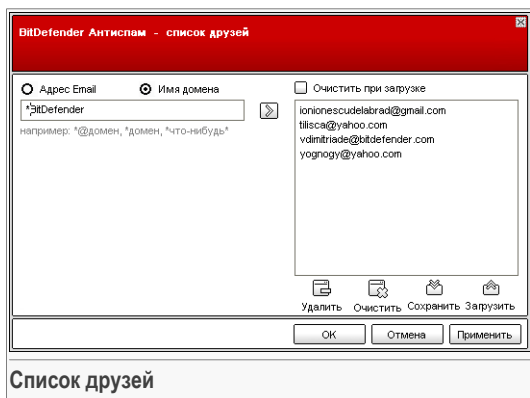
Список друзей

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 Спада.

**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 соответствует **Списку друзей**) или нажмите кнопку  **Друзья** в **Панели инструментов Антиспам**.



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 щелкните мышкой 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 загрузке предварительно сохраненного, нажмите **Очистить текущий список при загрузке**.

Замечание



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

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

Список спамеров

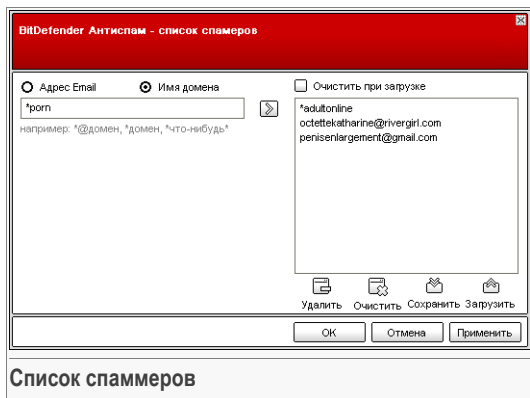
Список спамеров - список адресов электронной почты, с которых Вы не хотите получать письма, независимо от их содержания.

Замечание




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

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



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

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 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** в необходимое место. Файл будет иметь расширение .bwl.

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

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

**Важно**

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

9.1.2. Настройка «уровня толерантности»

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

Существует 5 «уровней толерантности»

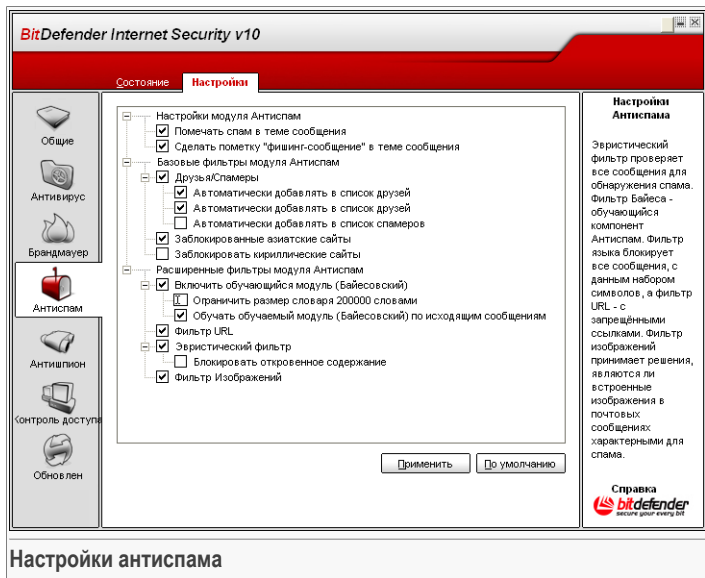
«Уровень толерантности» Описание

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

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



9.2. 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.

9.2.1. 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.

9.2.2. 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 иероглифов** - блокировка сообщений, написанных [иероглифами](#).
- **Блокировка кириллицы** - блокировка сообщений, написанных [кириллицей](#).

9.2.3. 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.

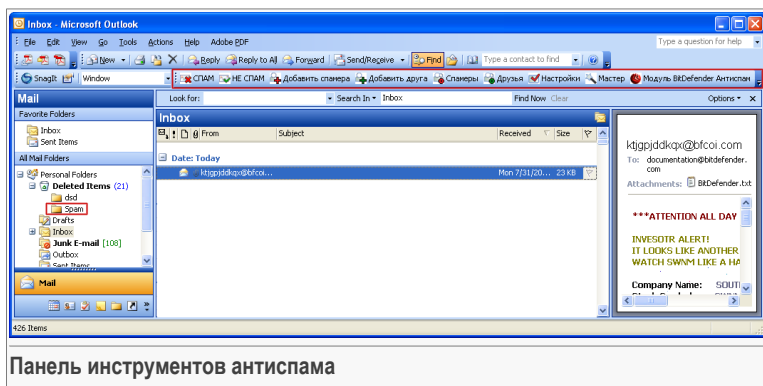
Нажмите **Применить**, чтобы сохранить изменения, или нажмите **По умолчанию**, чтобы загрузить настройки по умолчанию.

9.3. Настройка Антиспама, встроенного в Microsoft Outlook/ Outlook Express / Windows Mail

Программа BitDefender встраивается в интерфейс программ Microsoft Outlook / Outlook Express / Windows Mail с помощью простой и доступной панели инструментов.

9.3.1. Панель инструментов антиспама

В верхней части почтовой программы Microsoft Outlook / Outlook Express / Windows Mail Вы можете увидеть панель инструментов Антиспам.



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




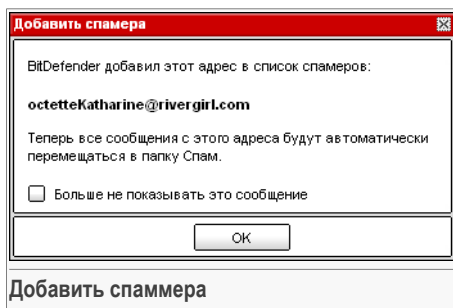
Вы можете выбрать одно письмо или сразу несколько.

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, чтобы добавить отправителя выбранных сообщений в **Список спамеров**.



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


Нажмите **ОК**, чтобы закрыть окно.

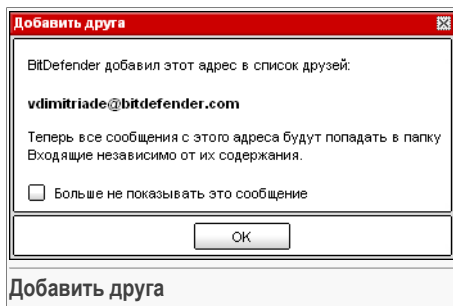
В будущем сообщения от этого адресата будут помечены как СПАМ.

Замечание



Вы можете выбрать одного отправителя или сразу нескольких.

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



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


Нажмите **ОК**, чтобы закрыть окно.

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

Замечание

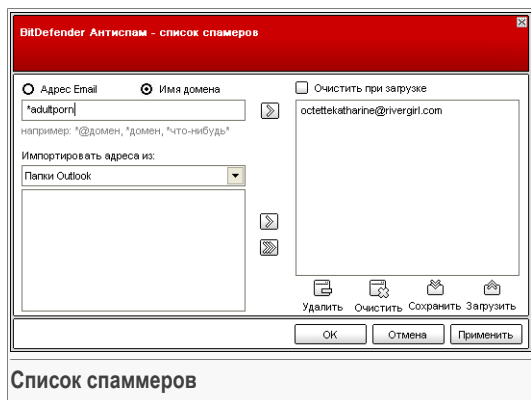


Вы можете выбрать одного отправителя или сразу нескольких.

-  **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.



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



выберите соответствующий 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 спамеров** в необходимое место. Файл будет иметь расширение **.bwl**.

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

Нажмите **Применить** и **ОК** чтобы сохранить и закрыть **Список спамеров**.

- **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.

BitDefender Антиспам - список друзей

Адрес Email Имя домена Очистить при загрузке

*BitDefender

например: *@домен, *домен, *что-нибудь*

Импортировать адреса из:

Адресная книга Outlook


ionionescudelabrad@gmail.com
 tilisca@yahoo.com
 vdimitriade@bitdefender.com
 yognogy@yahoo.com

Удалить Очистить Сохранить Загрузить

ОК Отмена Применить


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** и напишите 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 соответствующий 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 сохраненного, нажмите **Очистить текущий список при загрузке**.




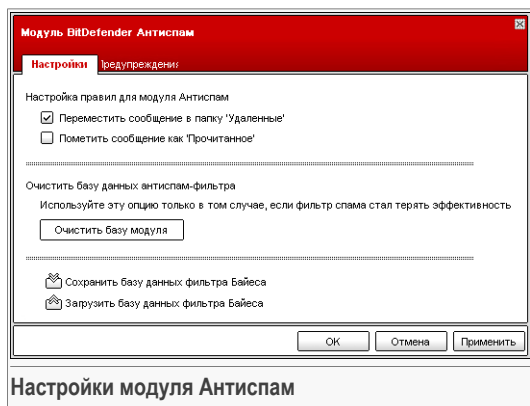
Замечание



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

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



-  **Настройки** - открывает окно **Настройки** в котором Вы можете выбрать различные опции для 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 **Списки друзей и спамеров**.
- **BitDefender Антиспам** - Щелчок мыши на этой кнопке открывает **Консоль управления**.

9.3.2. Мастер настройки Антиспам

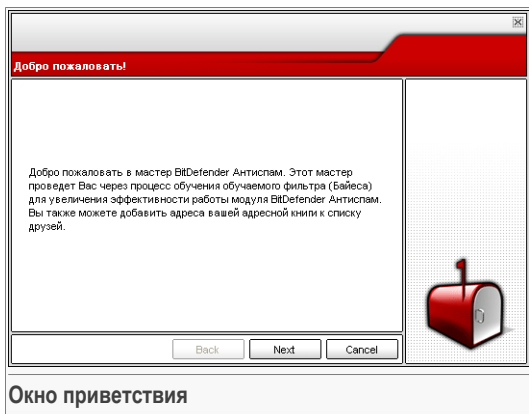
Когда Вы после установки BitDefender впервые запускаете почтовую программу Microsoft Outlook / Outlook Express / Windows Mail, появится программа-мастер, которая поможет Вам настроить **Список друзей**, **Список спамеров** и переобучить **Байесовский фильтр** для того, чтобы повысить эффективность работы фильтров Антиспама.

Замечание

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

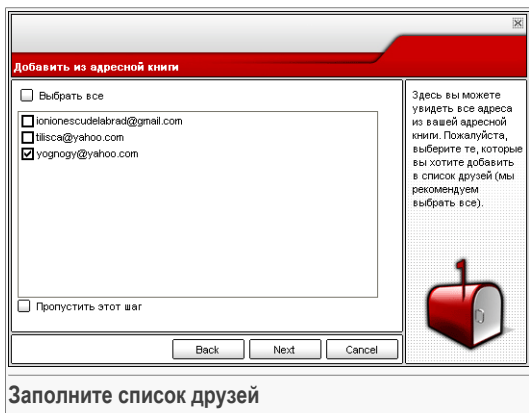


Шаг 1/6 - Экран приветствия



Нажмите **Далее**.

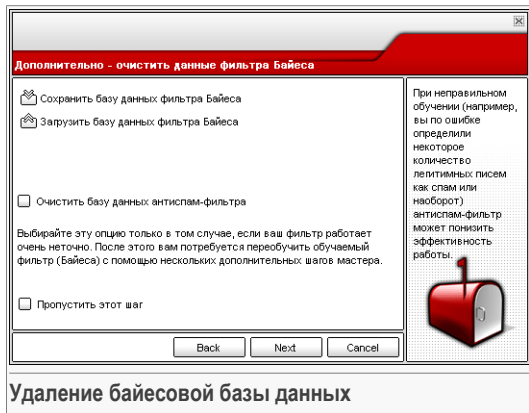
Шаг 2/6 - Заполните список друзей



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.

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



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

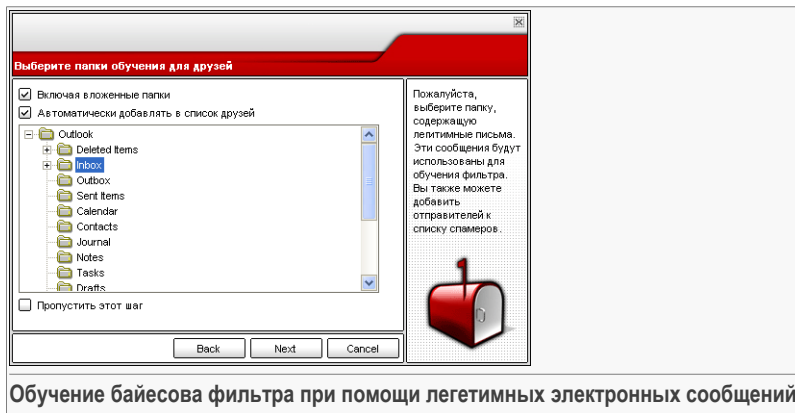
Поставьте значок в поле **Очистить базу данных фильтра Антиспам** если Вы хотите переустановить базу данных Байесовского фильтра.

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 легитимных электронных сообщений



Обучение байесова фильтра при помощи легитимных электронных сообщений

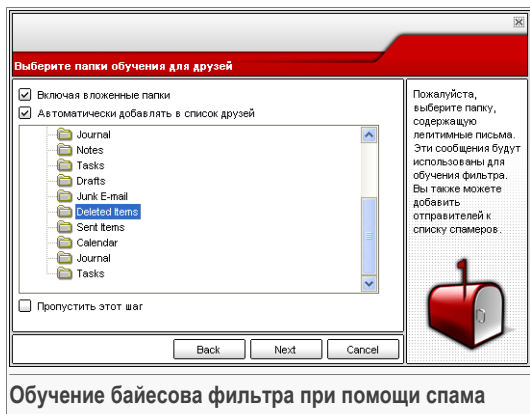
Выберите папку с разрешенными электронными письмами. Они будут использоваться для переобучения Байесовского фильтра.

В верхней части окна можно выбрать две настройки:

- **Включить подкаталоги** - включает в вашу выборку и 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



Выберите папку с электронными письмами, определенными как Спам. Они будут использоваться 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.

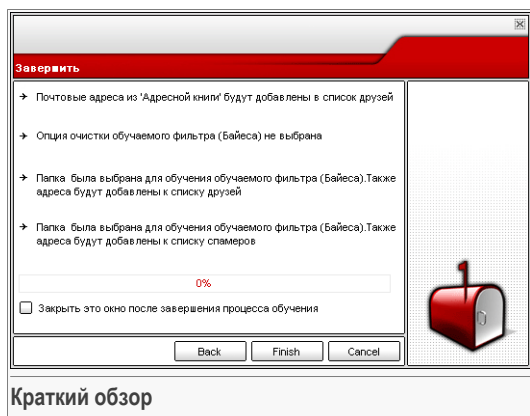
В верхней части окна можно выбрать две настройки:

- **Включить подкаталоги** - включает в вашу выборку и 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



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.



10. Модуль защиты от сетевых атак

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

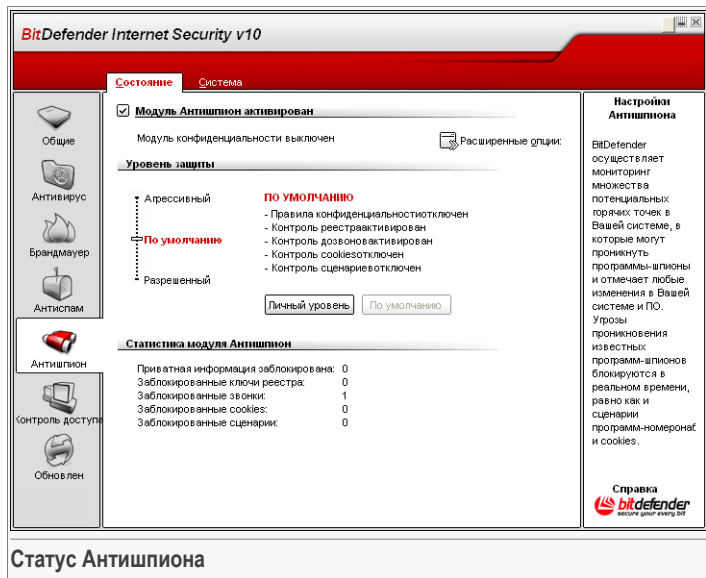
- Статус Антишпиона
- Дополнительные настройки - Контроль конфиденциальности
- Дополнительные настройки - Контроль регистра
- Дополнительные настройки - Контроль дозвона
- Дополнительные настройки - Контроль cookie
- Дополнительные настройки - Контроль скриптов
- Информация о системе

Замечание



Для получения более подробной информации о модуле **Антишпион** прочтите материал, описанный в разделе *«Модуль защиты от сетевых атак»* (р. 34).

10.1. Статус Антишпиона



Статус Антишпиона

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



Важно

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

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

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

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



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

Чтобы установить настройки для этих модулей контроля, нажмите  [Дополнительные настройки](#).

10.1.1. Уровень защиты

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

Существует 3 уровня защиты:

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

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

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

10.2. Дополнительные настройки - Контроль конфиденциальности

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



Шаг 1/3 - Установить тип правила и данных

Мастер BitDefender Шаг 1/3

Название правила

Тип правила

Данные правила

Все вводимые Вами данные зашифрованы. Для дополнительной безопасности не вводите полностью данные, которые Вы хотите защитить.

< Назад **Далее >** Отмена

Установить тип правила и данных

Введите название правила в поле для редактирования.

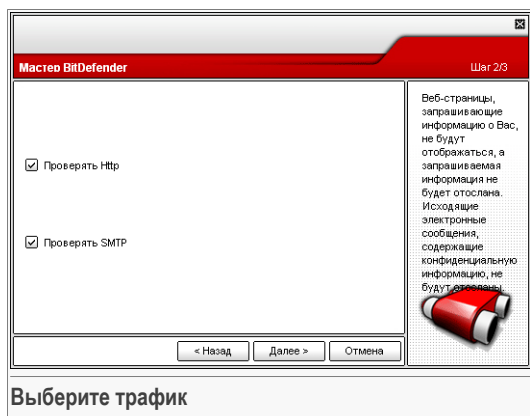
Вы должны установить следующие параметры:

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

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

Нажмите **Далее**.

Шаг 2/3 - Выбор трафика



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

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

Нажмите **Далее**.



Шаг 3/3 - Описание правила

Мастер BitDefender Шаг 3/3

Описание правила

SecurE

Введите описание для данного правила. Описание должно помочь Вам и другим администраторам понять, какая информация блокируется.

< Назад Завершить Отмена


Опишите правило


Введите краткое описание правила в поле редактирования.

Нажмите **Завершить**.

10.2.2. Управление правилами

В этом окне Вы видите список правил в таблице.

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

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

Название правила: secret

Тип правила: SSN (номер социальной страховки)

Данные правил: *****

Сканировать http

Сканировать smtp

Описание правила

Secret


ОК Отмена

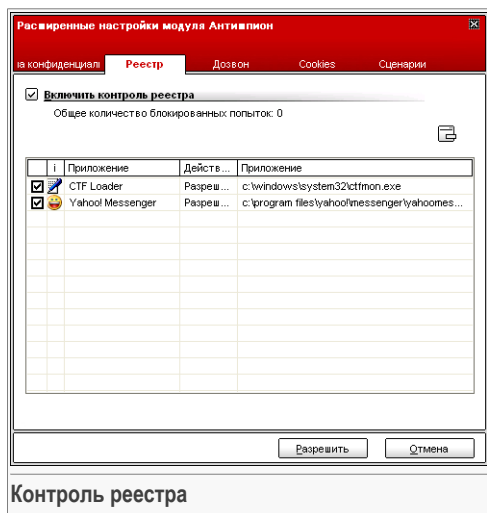
Редактировать правило

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

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

10.3. Дополнительные настройки - Управление реестром

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



Контроль реестра

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

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

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



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

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

Замечание



На основе Ваших ответов будет сформирован список правил.

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

Замечание

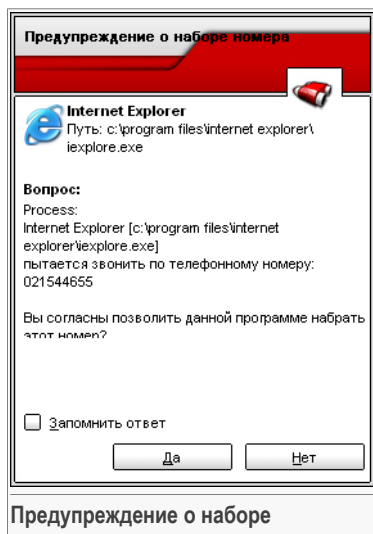


Обычно BitDefender предупреждает Вас, когда Вы устанавливаете программу, запускающуюся после следующей перезагрузки компьютера. В большинстве случаев эти программы официальные и им можно доверять.

Нажмите **ОК**, чтобы закрыть окно.

10.4. Дополнительные настройки - Контроль дозвола

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



В этом окне Вы видите название программы и номер телефона.

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

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



Важно

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

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

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

10.4.1. Мастер конфигурации

Мастер настройки выполняет процедуру из 2 шагов.



Шаг 1/2 - Выбор приложения и действия

Выберите приложение и действие
Шаг 1/2

Выберите приложение

Любой

Выбрать приложение

Выберите действие


Разрешить

Запретить

Выберите 'Любой', если это правило действительно для всех программ.

Для выбора конкретного приложения нажмите [Browse].

Выберите действие для этого правила: Разрешить или Запретить.



Выберите приложение и действие

Вы можете установить следующие параметры:

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

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

Нажмите **Далее**.

Шаг 2/2 - Выбор телефонных номеров

Выбор телефонных номеров Шаг 2/2

Выберите телефонный номер

Любой

Укажите номер телефона

Выберите 'Любой', если это правило действительно для всех телефонных номеров.

Вы также можете создать правило, которое разрешает указанной программе набирать только заданные номера (например, вашего интернет-провайдера).

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

**Замечание**

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

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


**Замечание**

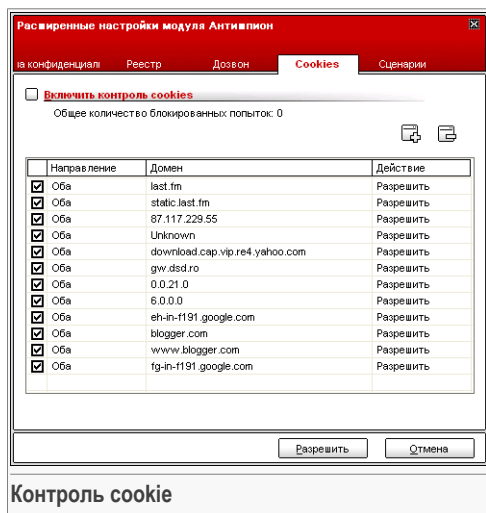
Вы также можете создать правило, разрешающее определенным программам набирать только определенные телефонные номера (например, только номер Вашего Интернет-провайдера или службы новостей по факсу).

Нажмите **Завершить**.

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

10.5. Дополнительные настройки - контроль cookie

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

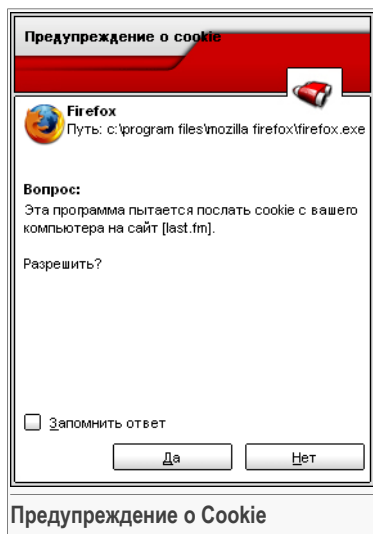


Файлы истории обращений - cookies встречаются в Интернете очень часто. Это небольшие файлы, хранящиеся на Вашем компьютере. Сайты в сети создают такие файлы, чтобы отслеживать некоторую информацию о Вас.

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

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

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



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

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

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



Замечание


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

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




Важно

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

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



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

10.5.1. Мастер конфигурации

Мастер конфигурации запускает процедуру из 1 шага.

Шаг 1/1 - Выбор адреса, действия и направления

Выберите адрес, действие и направление
Шаг 1/1

Укажите домен

Любой

Укажите домен

Выберите действие

Разрешить

Запретить

Выберите направление

Исходящие

Входящие

Оба

Выберите сайты и домены, с которых вы принимаете или отклоняете cookies. Они используются, чтобы отслеживать поведение и другую информацию. Имейте в виду, что некоторые сайты не работают без cookies. Вы можете принимать cookies, но не использовать действие.

Выберите действие

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 исходящие | и Правило применяется и ко входящему, и к исходящему трафику. |

Нажмите **Завершить**.




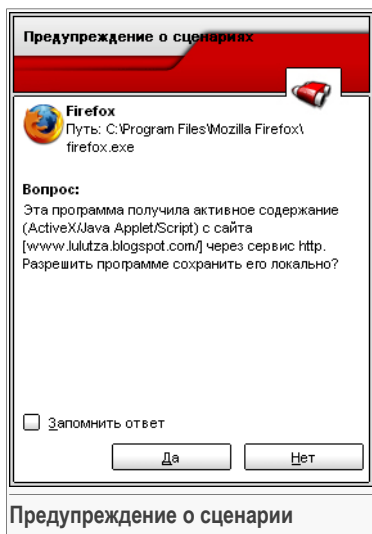
Замечание

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

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

10.6. Дополнительные настройки - Контроль сценариев

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



В этом окне Вы видите название ресурса.

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

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



Важно

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

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

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

10.6.1. Мастер конфигурации

Мастер конфигурации запускает процедуру из 1 шага.



Шаг 1/1 - Выбор адреса и действия

Выберите адрес и действие
Шаг 1/1

Укажите домен

Выберите действие

Разрешить
 Запретить

Выберите домен(ы), для которого вы хотите разрешить или запретить выполнение сценариев. Вообще, этот мастер необходимо использовать, чтобы указать домены, запуск скриптов с которых вы хотите разрешить или запретить.

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.

10.7. Информация о системе



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

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

Доступны три кнопки:

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



11. Модуль Контроль доступа

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

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

Замечание



Для получения более подробной информации относительно модуля **Контроль доступа** выберите описание *«Модуль Контроль доступа»* (р. 34).

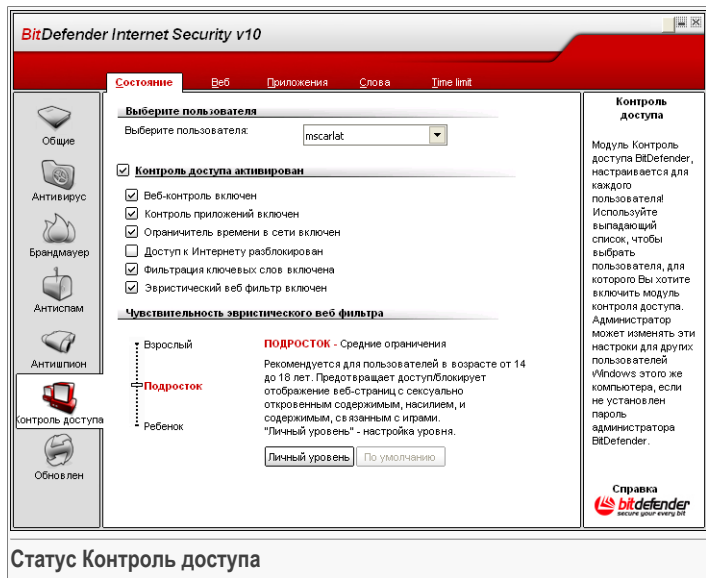
Важно



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.

Если Вы не единственный пользователь компьютера с правами администратора, рекомендуем защитить Ваши настройки BitDefender паролем. Чтобы установить пароль, перейдите в модуль **Общие**, раздел **Настройки** и воспользуйтесь опцией **Включить защиту паролем настроек программы**.

11.1. Статус Контроль доступа



Статус Контроль доступа

В данном разделе можно настроить уровень защиты **Контроль доступа** для выбранного пользователя.



Важно

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

Чтобы настроить 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** - включите **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.

11.1.1. Чувствительность эвристического веб фильтра

Перемещайте ползунок по шкале, чтобы выставить уровень защиты, адекватный на Ваш взгляд для данного пользователя.

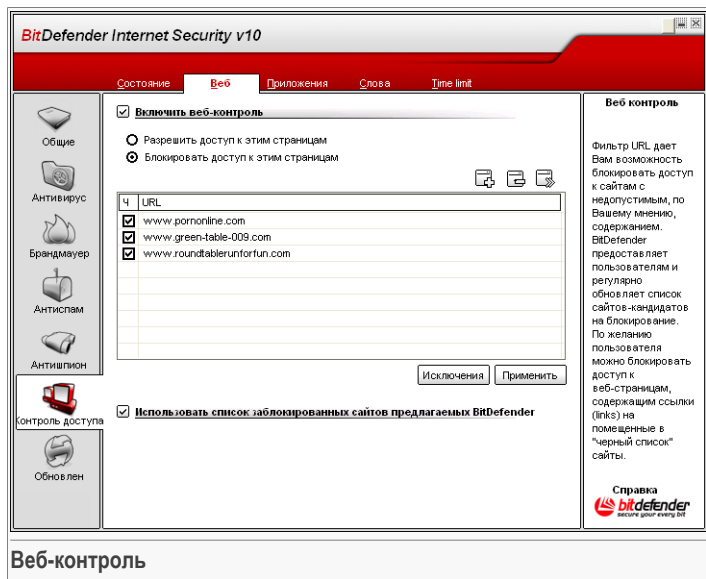
Существует 3 уровня защиты:

| Уровень защиты | 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). |
| 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 **Личный уровень**, чтобы установить Ваши правила фильтрации. В появившемся окне выберите категорию содержимого страниц (азартные игры, хакерство, порнография и т.д.), которая должна блокироваться BitDefender при попытке пользователей доступа на подобные страницы, затем нажмите **ОК**.

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

11.2. 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.

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.



11.2.1. Мастер конфигурации

Мастер конфигурации запускает процедуру из 1 шага.

Шаг 1/1 - Укажите веб-сайты

Укажите URL

Введите URL
www.porn.com

Вы можете ввести адреса конкретной веб-страницы, или универсальные шаблоны адресов.

Например, Вы можете блокировать все адреса, которые содержат слово 'сигары', вводя слово 'сигары' в соответствующее поле.

< Назад Завершить Отмена

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.

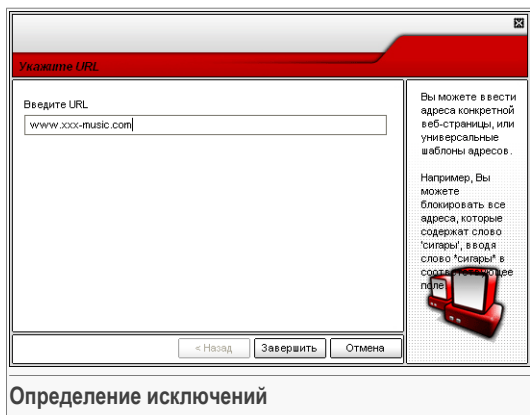
Чтобы удалить правило, выберите его и нажмите кнопку **Удалить**. Чтобы изменить правило, выберите его и нажмите кнопку **Редактировать...** или

дважды нажмите на правило. Чтобы временно отключить правило, не удаляя его, уберите галочку из соответствующего поля.

11.2.2. 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:



Нажмите **Добавить...**, чтобы добавить 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.

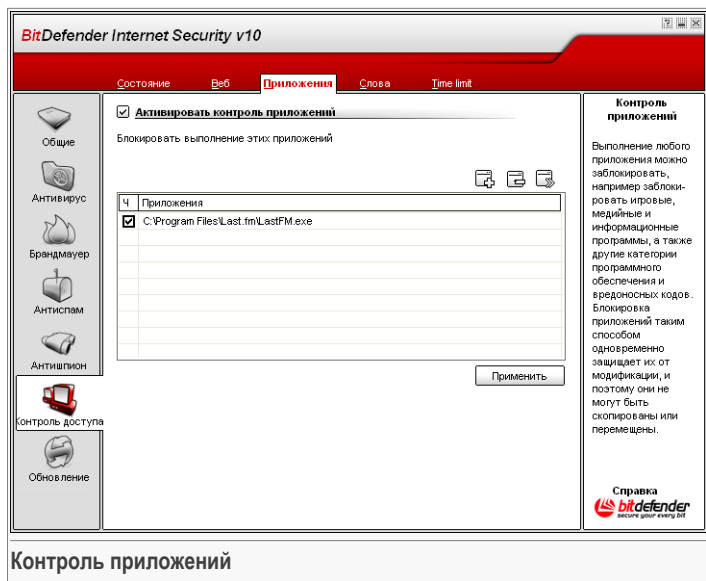
11.2.3. Черный список сайтов BitDefender

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**.

11.3. 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.

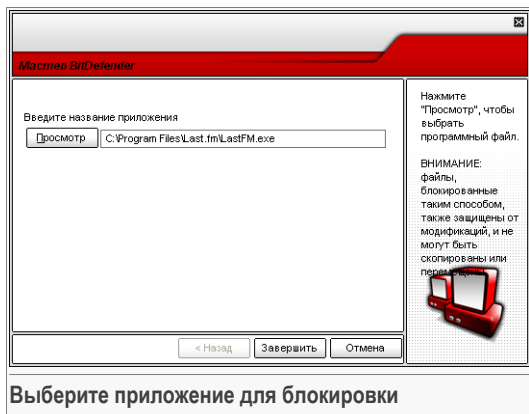
Чтобы включить эту защиту, установите значок на поле, соответствующем опции **Включить контроль приложений**.

Правила необходимо вводить вручную. Нажмите кнопку  **Добавить...**, чтобы запустить мастера настройки.

11.3.1. Мастер конфигурации



Мастер конфигурации запускает процедуру из 1 шага.

Шаг 1/1 - Выбор приложения для блокировки



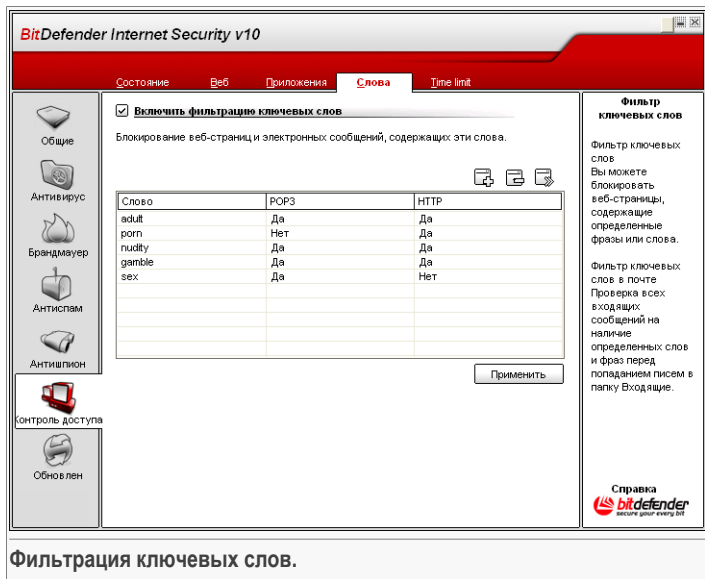
Нажмите **Обзор**, выберите приложение для блокировки и нажмите **Завершить**.

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.



11.4. Фильтрация ключевых слов.



Фильтр ключевых слов помогает блокировать электронные сообщения или веб-страницы, содержащие определенные слова. Таким образом, можно защитить пользователей от просмотра неадекватных слов или фраз.

Чтобы включить эту защиту, установите значок на поле, соответствующем опции **Фильтрация ключевых слов**.

Правила необходимо вводить вручную. Нажмите кнопку **Добавить...**, чтобы запустить мастера настройки.

11.4.1. Мастер конфигурации

Мастер конфигурации запускает процедуру из одного шага.

Шаг 1/1 - Введите ключевое слово

Шаг 1/1 - Введите ключевое слово

Добавить новое слово

sex

Выберите параметр

POP3

HTTP

Оба

Введите новое слово, которое необходимо заблокировать от отображения (электронные письма или веб-страницы будут полностью заблокированы).

< Назад Завершить Отмена

Введите ключевое слово

Вы должны установить следующие параметры:

- **Ключевое слово** - введите в поле редактирования слово или фразу, которую Вы хотите заблокировать.
- **Протокол** - выберите протокол, в котором BitDefender должен искать блокируемое слово.

Доступны следующие варианты:

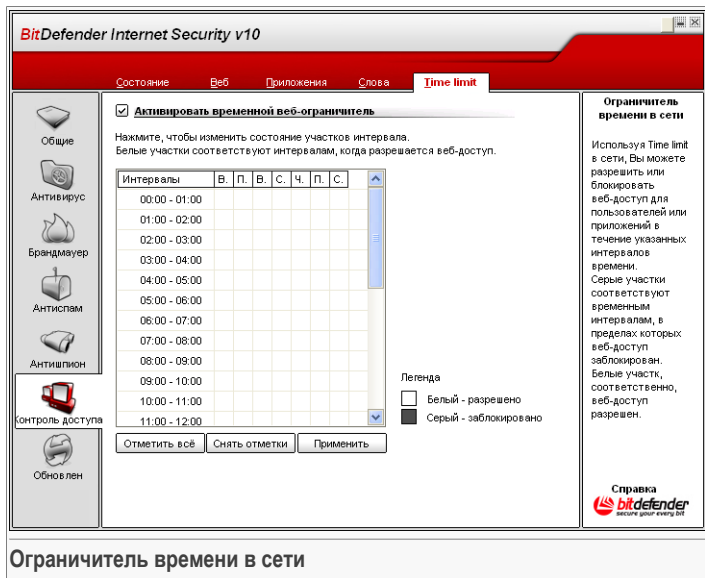
| Настройка | Описание |
|-----------------------------|---|
| POP3 | Блокируются электронные сообщения, содержащие ключевое слово. |
| HTTP | Блокируются веб-страницы, содержащие ключевое слово. |
| Входящие и исходящие | Блокируются и электронные сообщения, и веб-страницы, содержащие ключевое слово. |

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.



11.5. Ограничитель времени в сети



Используя **Ограничитель времени в сети**, Вы можете разрешить или заблокировать веб-доступ для пользователей или приложений в течение указанных интервалов времени.



Замечание

Независимо от настроек **Ограничителя времени в сети** программа BitDefender будет выполнять ежедневное автоматическое обновление продукта.

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, закрасивать 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.



12. Модуль обновлений

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

- Автоматическое обновление
- Ручное обновление
- Настройки обновления



Замечание

Для получения более подробной информации о модуле **Обновления** прочтите материал, описанный в разделе «*Модуль обновлений*» (р. 35).

12.1. Автоматическое обновление

BitDefender Internet Security v10

Обновление | Параметры

Автоматическое обновление активировано

Последний проверенный: 3/28/2007 3:11:33 PM
 Последний обновление: 3/28/2007 2:11:43 PM [Обновить](#)

Вirusов в базе

Вирусные сигнатуры: 444836
 Версия движка: 7.12092 [Список вирусов](#)

Состояние загрузки

Ошибка обновления:
 Обновление отменено. Остановите выполняющийся процесс сканирования и повторите процедуру.

| | | |
|------------------|-----|------|
| Файл: | 0 % | 0 kb |
| Всего обновлений | 0 % | 0 kb |

Обновление BitDefender

Нажмите "Обновить" для поиска более новых версий BitDefender.

Продукты BitDefender имеют возможность самовосстановления и, при необходимости, скачивают нормальные копии поврежденных или потерянных файлов с серверов BitDefender.

Рекомендуется активировать опцию "Автоматическое обновление".

Справка
bitdefender
 secure your every day

Автоматическое обновление


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

**Важно**

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

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

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

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



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

**Важно**

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

**Замечание**

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

Вы можете получить доступ к образам вредоносных программ вашего BitDefender, нажав  **Показать список вирусов**. Будет создан HTML файл, содержащий 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.

12.2. Обновление вручную.

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

**Важно**

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

Обновление вручную можно выполнить двумя способами:

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

12.2.1. Обновление вручную с использованием файла

`weekly.exe`

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

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

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

12.2.2. Обновление вручную при помощи `zip` архивов

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

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

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

- Windows 2000, Windows XP, Windows Vista.

Windows 2000, Windows XP, Windows Vista

Последовательность действий при обновлении:

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

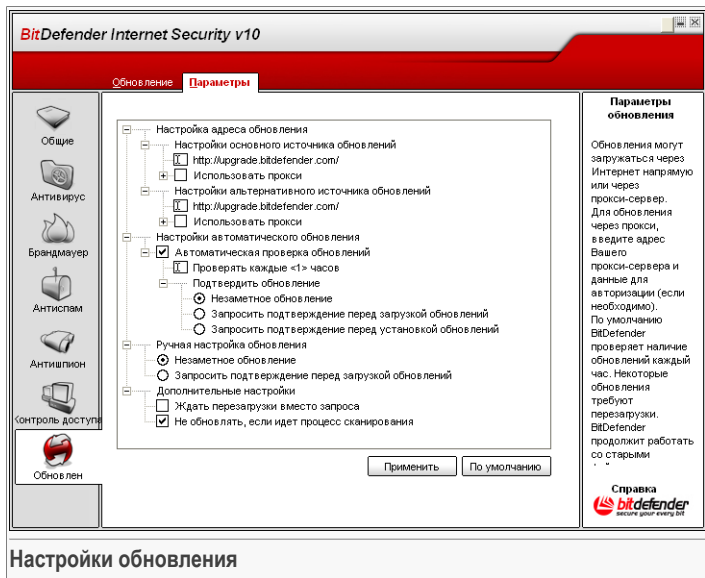
Замечание



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



12.3. Настройки обновления



Настройки обновления

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

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



Замечание

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

12.3.1. Настройки местоположения обновления

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

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

**Важно**

Синтаксис: `name:port` или `ip:port`.

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

**Важно**

Синтаксис: `domain\user`.

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

12.3.2. Опции автоматического обновления

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

**Важно**

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

12.3.3. Настройки обновления вручную

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

**Важно**

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

12.3.4. Дополнительные настройки

- **Ожидать перезагрузки без запроса** - Если для завершения установки обновления необходимо выполнить перезапуск компьютера, программное обеспечение будет при выборе данной опции предложить работу со старыми файлами до перезагрузки системы. При этом не будет появляться сообщение с запросом пользователя о необходимости перезапуска системы, в связи с чем процесс обновления BitDefender не будет мешать работе пользователя.
- **Не выполнять обновление, пока идет проверка** - BitDefender не будет выполнять обновление пока идет проверка. Таким образом, процесс обновления BitDefender не будет мешать задачам проверки.

**Замечание**

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

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



Практические приемы



13. Практические приемы

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

- Как защитить Ваш компьютер, подключенный к Интернет
- Как защитить Ваш компьютер от угроз вредоносных программ
- Как настроить задачу проверки
- Как настроить брандмауэр
- Как оградить Ваш компьютер от спама
- Как защитить Ваших детей от неадекватного контента

13.1. Как защитить Ваш компьютер, подключенный к Интернет



Выполняйте следующие действия, чтобы защитить Ваш компьютер, подключенный к Интернет:

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



Важно

Если у вас есть загрузочный диск BitDefender Internet Security v10 Rescue CD, проверьте Вашу систему перед тем, как устанавливать BitDefender, чтобы убедиться, что на Вашей системе нет никаких вредоносных программ.

2. **Обновите BitDefender.** Если Вы не завершили работу мастера первоначальной установки во время процесса установки, выполните обновление по запросу пользователя (модуль **Обновления**, раздел **Обновления**, и нажмите  **Обновить**).
3. **Выполните полную проверку системы.** Перейдите в модуль **Антивирус**, раздел **Монитор** и нажмите  **Проверить**.

**Замечание**

Вы так же можете запустить полную проверку системы в разделе [Проверка](#). Выберите задачу [Полная проверка системы](#) и нажмите [Запустить задачу](#).

4. **Предотвращение заражения.** В разделе **Монитор**, оставляйте включенной функцию [постоянная защита](#), чтобы обеспечить защиту от вирусов, сетевых атак и других вредоносных программ. Установите наиболее подходящий для Вас [Уровень защиты](#). Вы можете [настроить](#) его, нажав [Настроить Уровень](#).

**Важно**

Настройте Ваш BitDefender на проверку системы хотя бы раз в неделю при помощи [планирования](#) задачи [Полная проверка системы](#) в разделе [Проверка](#).

5. **Постоянно обновляйте BitDefender.** В модуле **Обновления**, разделе [Обновления](#), включите [Автоматическое обновление](#), чтобы быть защищенных от самых последних версий вредоносных программ.
6. **Предотвращение Интернет атак.** Настройте [Брандмауэр BitDefender](#), чтобы защититься от Интернет атак.
7. **Блокирование программ шпионов.** В модуле **Антишпион**, раздел [Статус](#), установить уровень защиты на [рекомендуемый уровень](#) или выше. Таким образом, Вы обеспечите защиту от вредоносных программ, пытающихся внести изменения в записи регистра, и от программ автоматического набора на платные номера. Если Вы хотите обеспечить безопасность конфиденциальных данных, включите [Контроль конфиденциальности](#) и [создайте](#) соответствующие правила.
8. **Защита от спама.** Если у Вас есть адрес электронной почты, который Вы хотите защитить, [настройте](#) модуль [Антиспам](#).
9. **Блокировка доступа к неадекватному контенту.** Если компьютером пользуются Ваши дети, Вы можете защитить их от неадекватного контента, [настроив](#) модуль [Контроль доступа](#).

13.2. Как защитить Ваш компьютер от угроз вредоносных программ

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

1. **Завершите работу мастера первоначальной настройки.** Во время процесса установки будет запущен [мастер](#). Он поможет Вам зарегистрировать



BitDefender и создать учетную запись BitDefender, чтобы Вы могли воспользоваться услугами технической поддержки. Он также поможет настроить BitDefender на выполнение важных задач обеспечения безопасности.

**Важно**

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

2. **Обновите BitDefender.** Если Вы не завершили работу мастера первоначальной установки во время процесса установки, выполните обновление по запросу пользователя (модуль **Обновления**, раздел **Обновления**, и нажмите **Обновить**).
3. **Выполните полную проверку системы.** Перейдите в модуль **Антивирус**, раздел **Монитор** и нажмите **Проверить**.

**Замечание**

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

4. **Предотвращение заражения.** В разделе **Монитор**, оставляйте включенной функцию **постоянная защита**, чтобы обеспечить защиту от вирусов, сетевых атак и других вредоносных программ. Установите наиболее подходящий для Вас **Уровень защиты**. Вы можете **настроить** его, нажав **Настроить Уровень**.

**Важно**

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

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

13.3. Как настроить задачу проверки

Выполните следующие шаги, чтобы создать и настроить задачу проверки:

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

**Замечание**

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

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

13.4. Как настроить модуль брандмауэра

Следуйте следующим инструкциям, чтобы настроить модуль **Бранмауэр**:

1. **Создайте новый профиль сетевого соединения.** Каждый раз при подключении к новой сети, запускается **мастер**. Завершите все шаги мастера брандмауэра, чтобы создать набор базовых правил брандмауэра для профиля сетевого соединения.

**Замечание**


Мастера можно запустить в любой момент, нажав  **Сброс профиля** в разделе **Трафик**

2. **Установите уровень защиты.** Перейдите в раздел **Статус**, чтобы **установить правила брандмауэра** (**Запретить все**, **Разрешить все**, **Разрешить все из разрешенного списка**, **Спросить**).

**Важно**



Рекомендуем поддерживать защиту на уровне **Разрешать все из списка разрешенных**. Таким образом BitDefender создаст правила для наиболее часто используемых приложений, не беспокоя Вас.



3. **Создайте правила.** Перейдите в раздел **Трафик** и нажмите кнопку  **Добавить**, чтобы **создать правила** для наиболее часто используемых приложений. Вы должны указать параметры правил.
4. **Установите дополнительные настройки брандмауэра.** Перейдите в раздел **Дополнительные настройки**, чтобы установить **правила фильтрации** для ICMP трафика и установить **другие настройки брандмауэра**.

13.5. Как оградить Ваш компьютер от спама.


Выполните следующие действия, чтобы предохранить Ваш компьютер от спама:

1. **Настройка «уровня толерантности».** Перейдите в модуль **Антиспам**, раздел **Статус** и установите **уровень толерантности**. Выбрав подходящий уровень толерантности, Вы всегда будете получать в Ваш почтовый ящик только легитимные сообщения, независимо от того, получаете ли Вы обычно много коммерческих сообщений или большие объемы спама.
2. **Завершите все действия мастера настройки Антиспам.** Если Вы используете Microsoft Outlook или Microsoft Outlook Express / Windows Mail, выполните действия **мастера настройки**, который запуститься, когда Вы в первый раз запустите постовый клиент. Вы также можете запустить мастера из **Панели инструментов Антиспам**.
3. **Заполните список друзей.** Перейдите в модуль **Антиспам**, раздел **Статус** и нажмите  или нажмите кнопку  **Друзья** в **Панели инструментов Антиспам**, чтобы открыть **Список друзей**. Добавьте адреса людей, от которых Вы всегда хотите получать электронные сообщения, в **Список друзей**.

Замечание



BitDefender не блокирует письма от людей из этого списка, значит, чем больше друзей занесено в список, тем больше вероятность, что Вы получите ожидаемое сообщение.

4. **Обучение "обучаемого" модуля (Байесового).** Каждый раз, когда Вы получаете электронное сообщение, которое Вы считаете спамом, но BitDefender не обозначил его как спам, выберите это сообщение и нажмите кнопку  **Спам** в **Панели инструментов Антиспам**. В будущем, сообщения, подходящие к **данному шаблону**, будут отмечены как СПАМ.

Замечание



Обучаемый модуль включается только тогда, когда Вы обучили его при помощи минимум 60 легитимных электронных сообщений. Чтобы это сделать, выполните действия **мастера настройки**.

5. **Постоянно обновляйте BitDefender.** В модуле **Обновления**, раздел **Обновления**, включите **автоматическое обновление**, чтобы защитить компьютер от вновь появляющихся угроз.

**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.

6. **Настройка Фильтра символов.** Большинство спама написано **Кириллицей и/или иероглифами**. Перейдите в модуль **Антиспам**, раздел **Настройки** и выберите **Блокировать кириллицу/иероглифы**, если Вы хотите блокировать все электронные сообщения, написанные при помощи этих кодировок.

**Замечание**

Вы можете включить/отключить каждый из фильтров Антиспам в разделе **Настройки** модуля **Антиспам**.

13.6. Как защитить Вашего ребенка от неадекватного контента

Выполняйте следующие действия, чтобы защитить Вашего ребенка от неадекватного контента:

1. **Создайте учетную запись пользователя Windows с ограниченными правами.** Чтобы ограничить ребенка от доступа в модуль **Контроль доступа** или от изменения его настроек, он или она должны иметь ограниченные права в Вашей системе.
2. **Выберите пользователя.** Список людей, которые пользуются компьютером, отображается в разделе **Статус**. Из этого списка выберите пользователя, доступ которого к **Контролю доступа** Вы хотите ограничить.
3. **Установка общей защиты.** Перейдите в раздел **Статус**, чтобы включить **режимы защиты** для Вашего ребенка. Если Вы включили **эвристический веб фильтр**, установите соответствующий **уровень защиты**.
4. **Блокирование сайтов.** Перейдите в **раздел веб**, чтобы **создать** список веб-сайтов, доступ к котором запрещен для Ваших детей. Где необходимо, Вы можете **указать исключения**. Вы также можете закрыть доступ к **списку**



[веб-сайтов](#), предоставленному BitDefender. Эти веб-сайты имеют неадекватное или потенциально опасное содержание.

5. **Блокирование приложений.** Перейдите в раздел **Приложения**, чтобы **заблокировать доступ к приложениям**, которыми не должны пользоваться Ваши дети.

Замечание



Если Вы считаете, что Ваш ребенок проводит слишком много времени за игрой, использованием мультимедийных программ, программ общения или других программ, Вы можете заблокировать ему/ей доступ к этим приложениям.

6. **Блокирование слов.** Чтобы защитить Вашего ребенка от просмотра потенциально опасного содержания веб-страниц или почтовых сообщений, используйте **Фильтрацию ключевых слов**, чтобы искать слова или фразы, свидетельствующие о подобном содержании. Перейдите в раздел **Ключевые слова**, чтобы определить правила, согласно которым будет **блокироваться доступ с веб-сайтам или(и) элеткронным сообщениям**, содержащим определенные фразы.
7. **Контроль доступа в интернет.** Перейдите в раздел **Ограничитель времени**, чтобы **указать расписание**, когда открыт доступ в интернет.
8. **Защите Ваши настройки паролем.** Перейдите в модуль **Общие**, раздел **Настройки** и выберите **Включить защиту паролем настроек программы**. Только пользователи, знающие пароль, смогут изменять настройки, установленные Вами для определенного пользователя.



Реаниматор BitDefender

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

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

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

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



14. Краткий обзор

Ключевые преимущества

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

14.1. Что такое KNOPPIX?

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

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

14.2. Системные требования

Перед загрузкой LinuxDefender, необходимо сначала проверить соответствие вашей системы следующим требованиям.

Тип процессора

x86-совместимый процессор с минимальной тактовой частотой 166 МГц, что, однако, не гарантирует устойчивой работы программы. Предпочтительно выбирать процессор поколения i686, с тактовой частотой 800МГц.

Память

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

CD-ROM

LinuxDefender запускается с компакт-диска, поэтому необходимыми является наличие дисководов CD-ROM и настройка BIOS на загрузку системы с компакт-диска.

Подключение к сети Интернет

Хотя программа LinuxDefender выполняется без подключения к сети Интернет, для процедур обновления необходим доступ к активной ссылке HTTP, хотя бы через прокси-сервер. Поэтому для установки последнего обновления защиты подключение к сети Интернет является ОБЯЗАТЕЛЬНЫМ.

Графическая разрешающая способность

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

14.3. Включенное программное обеспечение

В компакт-диск BitDefender Реаниматор входят следующие пакеты программ.

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

14.4. Антивирусный сканер BitDefender Linux

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



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

14.4.1. BitDefender SMTP прокси-сервер

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

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

14.4.2. Удаленный администратор BitDefender

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

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

14.4.3. Антивирусный сканер BitDefender Linux

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

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



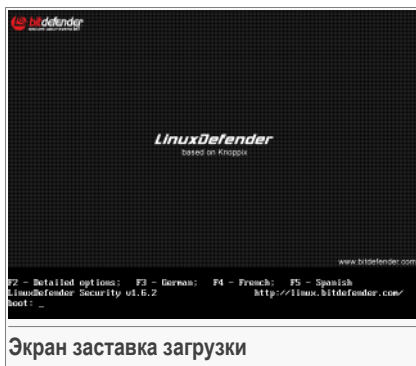
15. Работа с LinuxDefender

15.1. Запуск и остановка

15.1.1. Запуск программы LinuxDefender

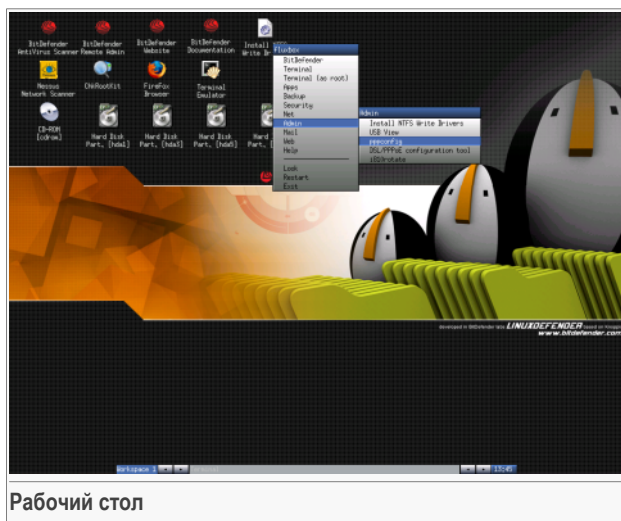
Чтобы запустить компакт-диск с данным программным продуктом, установите настройки BIOS вашего компьютера на загрузку с дисковода компакт-дисков, поместите компакт-диск с продуктом в дисковод и перезагрузите компьютер. Убедитесь в том, что ваш компьютер настроен на загрузку с компакт-диска.

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



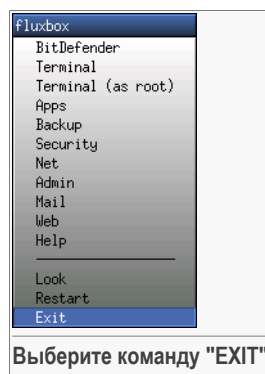
Путем нажатия на клавиатуре клавиши **F2** выберите подробное описание опций. При нажатии **F3** язык описания будет немецкий, при нажатии **F4** – французский, при нажатии **F5** – испанский. Быстрый запуск программы с опциями, заданными по умолчанию, можно осуществить простым нажатием клавиши **ENTER**.

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



15.1.2. Завершение работы LinuxDefender

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



После того, как LinuxDefender благополучно закроет все программы, на экране появится новое изображение, соответствующее показанному на следующем рисунке. Теперь можно извлечь компакт-диск, чтобы последующую загрузку компьютера выполнить уже с жесткого диска. Теперь ваш компьютер можно выключить или перезагрузить.



```
X-Window session terminated without errors.
Shutting down.
INIT: Sending processes the KILL signal
Sent all processes the TERM signal.....
Sent all processes the KILL signal.....
Shutting down network device eth0
Unmounting file systems.
/proc/bus/usb unmounted
/randisk unmounted
could not mount /KNOPPIX - trying /dev/cloop instead
/dev/root unmounted

KNOPPIX halted.
Please remove CD, close cdrom drive and hit return.
```

Ожидайте появления этого сообщения на экране, сигнализирующего о завершении работы программы

15.2. Настройка Интернет соединения

Если Вы находитесь в сети DHCP, и в Вашем компьютере установлена сетевая карта стандарта Ethernet, то в этом случае связь с Internet должна обнаруживаться и устанавливаться автоматически. Для настройки сети вручную, Вам следует выполнить следующие инструкции.

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

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

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

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

15.3. Обновление BitDefender

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

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

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

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

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

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

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



15.4. Проверка на вирусы

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

Поддержка записи файловой системы NTFS

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

Установка NTFS драйверов

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

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

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

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

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

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

15.4.2. Как выполнить вирусную проверку?

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

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

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

Затем нажмите **Сканирование**.

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

15.5. Настройки фильтра почтовых сообщений

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

15.5.1. Требования к системе

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



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

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

15.5.2. Мгновенный почтовый фильтр

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

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

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

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

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

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

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

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

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

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

15.6. Контролер сетевой защиты Nessus

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

15.6.1. Поиск руткитов

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

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

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

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



15.6.2. Сетевой сканер Nessus

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

—www.nessus.org

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

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

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

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

15.7. Проверка работоспособности RAM системы

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

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

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

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

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



Получение справки



16. Тех. поддержка

16.1. Отдел поддержки

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

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

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

16.2. Поддержка в режиме «on-line»

16.2.1. База знаний BitDefender

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

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

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

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

16.3. Контактная информация

Эффективная связь является залогом успешного бизнеса. За последние 10 лет компании SOFTWIN удалось завоевать непререкаемый авторитет среди своих клиентов 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 помощью.

16.3.1. Адреса веб-сайтов

Отдел продаж: <sales@bitdef.ru>

Тех. поддержка: <support@bitdef.ru>

Документация: <documentation@bitdef.ru>

Партнерские программы: <partners@bitdef.ru>

Маркетинг: <marketing@bitdef.ru>

Отдел по связям со СМИ: <pr@bitdef.ru>

Вакансии: <jobs@bitdef.ru>

Лаборатория – для вирусов: <virus_submission@bitdef.ru>

Лаборатория - для спама: <spam_submission@bitdef.ru>

Жалобы: <abuse@bitdef.ru>

Веб-сайт продукта: <http://www.bitdef.ru>

ftp архив продукта: <ftp://ftp.bitdef.ru/pub>

Локальные дистрибьюторы: http://www.bitdef.ru/partner_list

База знаний BitDefender: <http://kb.bitdef.ru>

16.3.2. Офисы филиалов

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

Германия

Softwin GmbH



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

Великобритания и Ирландия

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

Испания

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

США

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

Румыния

SOFTWIN

5th Fabrica de Glucoza St.

PO BOX 52-93

Bucharest

Техническая поддержка: <suport@bitdefender.ro>

Отдел продаж: <sales@bitdefender.ro>

Телефон: +40 21 2330780

Факс: +40 21 2330763

Веб-сайт продукта: <http://www.bitdefender.ro>



Глоссарий

ActiveX

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

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

Программы с рекламной информацией (Adware)

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

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

Архив

Диск или директория, содержащие файлы - резервные копии.

Файл, содержащий один или несколько файлов в сжатом формате.

Брешь в системе (Backdoor)

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

Загрузочный сектор

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

Загрузочный вирус

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

Браузер

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

Командная строка

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

Файлы истории обращений - Cookie

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

Дисковод

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



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

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

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

Загрузка

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

Электронная почта

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

События

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

Ложная тревога

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

Расширение файла

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

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

Эвристический метод

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

IP

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

Прикладная минипрограмма Java апплет

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

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

Макро-вирус

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

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

Почтовый клиент

Приложение, которое позволяет Вам отправлять и получать электронную почту.

Память

Внутренние устройства хранения информации. Термин «Память» относится к запоминающему устройству, например, микросхеме. Термин «Накопитель» относится к таким устройствам, как диски. В каждом компьютере изначально есть физическая память, называемая оперативная память или RAM.

Не-эвристический метод

Этот метод проверки основан на использовании определенных образов вирусов - сигнатур. Основное преимущество этого метода состоит в том, что его нельзя обмануть похожей на вирус программой, а следовательно, не возникает ложная тревога.

Запакованные программы

Файл в сжатом формате. Многие операционные системы и приложения содержат 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 периферийных устройств, если их встроить в соответствующее 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 программы, либо чтобы скрыть присутствие в системе. При совмещении с вредоносными программами, руткиты представляют значительную угрозу для целостности и безопасности системы. Они могут отслеживать трафик, создавать бреши в системе, изменять файлы и журналы, избегая выявления.

Сценарий или скрипт

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

Spam

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

Программа-шпион - Spyware

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



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

Действия программ-шпионов 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 работе 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 ворота, 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.