

bitdefender



INTERNET SECURITY₂₀₀₉

**Руководство
пользователя**

 **bitdefender**



BitDefender Internet Security 2009

Руководство пользователя

Опубликовано 2009.03.03

Copyright© 2009 BitDefender

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 и перезапись), использована в каких-либо информационных системах хранения данных и поисковых системах, без получения письменного разрешения от уполномоченного представителя компании BitDefender. 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 BitDefender, поэтому BitDefender не несет ответственности за содержание какого-либо сайта, на который имеются ссылки в данном документе. Компания Bitdefender приводит эти ссылки только для удобства читателя, но наличие этих ссылок не означает, что BitDefender берет на себя ответственность за содержание какого-либо стороннего веб-сайта.

Торговые марки. В этом документе могут упоминаться различные торговые марки. Все зарегистрированные и незарегистрированные торговые марки, упоминаемые в этом документе, принадлежат только их законным владельцам.



BitDefender Internet Security 2009





Содержание

Лицензионное соглашение для конечного пользователя	x
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
Установка	1
1. Системные требования	2
1.1. Требования к комплектующим компьютера	2
1.2. Требования Программного обеспечения	3
2. Установка BitDefender	4
2.1. Мастер регистрации	6
2.1.1. Шаг 1/2 - Зарегистрируйте BitDefender Internet Security 2009	7
2.1.2. Шаг 2/2 - Создание учетной записи BitDefender	9
2.2. Мастер Конфигурации	11
2.2.1. Этап 1/9 – Окно приветствия	12
2.2.2. Шаг 2/9 - Выберите Режим просмотра	13
2.2.3. Шаг 3/9 - Настройте сеть BitDefender	14
2.2.4. Шаг 4/9 - Настройте Защиту данных	15
2.2.5. Шаг 5/9 - Настройте контроль доступа	19
2.2.6. Шаг 6/9 - Настройте создание отчета о вирусах	21
2.2.7. Шаг 7/9 - Выберите задания для запуска	22
2.2.8. Шаг 8/9 - Ожидайте завершения этих задач	23
2.2.9. Шаг 9/9 - Процедура завершена	24
3. Обновление	25
4. Удаление или восстановление BitDefender.	26
Основные администрирования	28
5. Начало работы	29
5.1. Запуск BitDefender Internet Security 2009	29
5.2. Режим просмотра пользовательского интерфейса	29
5.2.1. Основной вид	29
5.2.2. Расширенный вид	32
5.3. Значок BitDefender в системном трее	34
5.4. Полоса Активности Сканирования	35



5.5. Ручная проверка BitDefender	36
5.6. Игровой режим	37
5.6.1. Использование Игрового режима	37
5.6.2. Изменение Горячих клавиш Режима Игры	37
5.7. Интеграция в почтовые клиенты	38
5.7.1. Панель инструментов антиспама	38
5.7.2. Мастер настройки Антиспам	47
5.8. Интегрирование в браузеры	52
5.9. Интеграция в интернет-пейджер	54
6. Консоль	56
6.1. Обзор	127
6.2. Задачи	58
6.2.1. Сканирование с помощью BitDefender	58
6.2.2. Обновление BitDefender	59
7. Уровень безопасности	61
7.1. Отслеживаемые компоненты	62
7.1.1. Локальная Безопасность	116
7.1.2. Онлайн Безопасность	118
7.1.3. Сканирование на наличие уязвимостей	119
7.2. Задачи	65
7.2.1. Сканирование с помощью BitDefender	66
7.2.2. Обновление BitDefender	67
7.2.3. Поиск уязвимостей	68
8. Родитель	76
8.1. Отслеживаемые компоненты	76
8.1.1. Родительский контроль	77
8.2. Задачи	78
8.2.1. Сканирование с помощью BitDefender	78
8.2.2. Обновление BitDefender	79
9. Хранилище	81
9.1. Отслеживаемые компоненты	82
9.1.1. Хранилище	119
9.2. Задачи	83
9.2.1. Добавление файлов в Хранилище	83
9.2.2. Удаление файлов из хранилища	89
9.2.3. Просмотр файлов в хранилище	94
9.2.4. Блокировка хранилища	98
10. Сеть	102
10.1. Задачи	103
10.1.1. Подключение к сети BitDefender	103
10.1.2. Добавление компьютеров в сеть BitDefender	104
10.1.3. Управление сетью BitDefender	106



10.1.4. Сканирование всех компьютеров	108
10.1.5. Обновление всех компьютеров	109
10.1.6. Регистрация всех компьютеров	110
11. Основные настройки	111
11.1. Локальная Безопасность	112
11.2. Онлайн Безопасность	112
11.3. Настройки модуля Контроль доступа	113
11.4. Настройки сети	113
11.5. Настройки Хранения Файлов	114
11.6. Общие настройки	114
12. Полоса состояния	116
12.1. Локальная Безопасность	116
12.2. Онлайн Безопасность	118
12.3. Хранилище	119
12.4. Сканирование на наличие уязвимостей	119
13. Регистрация	121
13.1. Шаг 1/1 - Зарегистрируйте BitDefender Internet Security 2009	121
14. Журнал	123
<i>Расширенное Администрирование</i>	<i>125</i>
15. Общие	126
15.1. Консоль	126
15.1.1. Статистика	127
15.1.2. Обзор	127
15.2. Настройки	128
15.2.1. Основные настройки	129
15.2.2. Параметры настройки отчета	131
15.3. Системная информация	131
16. Антивирус	133
16.1. Защита в режиме реального времени	133
16.1.1. Конфигурация уровня защиты	134
16.1.2. Настройка уровня защиты	135
16.1.3. Настройка Сканера поведения	139
16.1.4. Отключение постоянной защиты	142
16.1.5. Настройка антифишинговой защиты	142
16.2. Сканирование по требованию	143
16.2.1. Задачи сканирования	145
16.2.2. Использование Выпадающего меню	147
16.2.3. Создание задач сканирования	148
16.2.4. Настройка задач проверки	148
16.2.5. Сканирование объектов	161



16.2.6. Просмотр журнала проверок	168
16.3. Объекты исключены из резидентного сканирования и из сканирования по требованию	170
16.3.1. Исключение путей для сканирования	172
16.3.2. Исключение расширений из сканирования	176
16.4. Область Карантина	180
16.4.1. Управление изолированными файлами	181
16.4.2. Конфигурация настроек Карантина	182
17. Антиспам (защита от спама)	184
17.1. Знакомство с антиспамом	184
17.1.1. Антиспам-фильтры	184
17.1.2. Описание антиспама	187
17.2. Состояние	188
17.2.1. Настройка уровня защиты	189
17.2.2. Настройка списка друзей	191
17.2.3. Настройка списка спамеров	192
17.3. Настройки	194
17.3.1. Настройки Антиспама	196
17.3.2. Базовые фильтры Антиспама	196
17.3.3. Дополнительные фильтры Антиспама	196
18. Родительский контроль	198
18.1. Состояние настройки для каждого пользователя	200
18.1.1. Защита настроек Контроля доступа	201
18.1.2. Конфигурация эвристического веб фильтра	203
18.2. Веб контроль	203
18.2.1. Мастер Конфигурации	205
18.2.2. Установка исключений	206
18.2.3. Черный список сайтов BitDefender	207
18.3. Контроль приложений	207
18.3.1. Мастер Конфигурации	208
18.4. Фильтр ключевых слов	209
18.4.1. Окно конфигурации	210
18.5. Управление мгновенными сообщениями	211
18.5.1. Окно конфигурации	213
18.6. Ограничитель времени в сети	213
19. Анонимность	216
19.1. Настройка Статуса Анонимности	216
19.1.1. Конфигурация уровня защиты	217
19.2. Контроль Идентичности	218
19.2.1. Создание правил конфиденциальности	220
19.2.2. Определение исключений	224
19.2.3. Управление правилами	225
19.3. Управление реестром	226



19.4. Контроль файлов истории обращений (Cookies)	228
19.4.1. Окно конфигурации	231
19.5. Контроль сценариев	232
19.5.1. Окно конфигурации	235
20. Брандмауер	236
20.1. Настройки	236
20.1.1. Установка действия по умолчанию	238
20.1.2. Конфигурация дополнительных настроек брандмауэра	239
20.2. Сеть	241
20.2.1. Изменения уровня доверия	243
20.2.2. Настройка невидимого режима	244
20.2.3. Настройка общих параметров	244
20.2.4. Сетевые зоны	244
20.3. Правила	245
20.3.1. Автоматическое добавление правил	248
20.3.2. Удаление правил	248
20.3.3. Создание и изменение правил	249
20.3.4. Расширенное управление правилами	253
20.4. Контроль соединений	255
21. Уязвимости	257
21.1. Состояние	257
21.1.1. Устранение уязвимостей	258
21.2. Настройки	265
22. Шифрование	267
22.1. Шифрование приложений мгновенного обмена сообщениями	267
22.1.1. Отключение шифрования для отдельных пользователей	269
22.2. Хранилище	269
22.2.1. Создание хранилища	271
22.2.2. Открытие хранилища	272
22.2.3. Блокирование хранилища	273
22.2.4. Смена пароля хранилища	273
22.2.5. Добавление файлов в хранилище	274
22.2.6. Удаление файлов из хранилища	275
23. Игровой режим	276
23.1. Игровой режим	276
23.1.1. Настройка автоматического перехода в Игровой режим	277
23.1.2. Управление списком игр	278
23.1.3. Настройка параметров игрового режима	280
23.1.4. Изменение Горячих клавиш Режима Игры	280
23.2. Laptop	281
23.2.1. Настройка параметров Режима ноутбука	282
24. Сеть	284



24.1. Подключение к сети BitDefender	285
24.2. Добавление компьютеров в сеть BitDefender.....	285
24.3. Управление сетью BitDefender	287
25. Обновление	290
25.1. Автоматическое обновление	291
25.1.1. Требование к обновлению	292
25.1.2. Отключение автоматического обновления	292
25.2. Параметры обновления	293
25.2.1. Настройки местоположения обновления	294
25.2.2. Конфигурирование автоматического обновления	295
25.2.3. Конфигурация обновлений вручную	295
25.2.4. Дополнительные настройки	296
25.2.5. Управление прокси	296
26. Регистрация	299
26.1. Регистрация BitDefender Internet Security 2009	300
26.2. Создание учетной записи BitDefender	301
<i>Получение справки</i>	<i>304</i>
27. Техническая поддержка	305
27.1. База знаний BitDefender	305
27.2. Просьба помощи	306
27.2.1. Перейти к самообслуживанию через веб	306
27.2.2. Откройте тикет техподдержки	306
27.3. Контактная информация:	307
27.3.1. Адреса веб-сайтов	307
27.3.2. Офисы филиалов	307
<i>BitDefender Rescue CD</i>	<i>308</i>
28. Обзор	309
28.1. Системные требования	309
28.2. Включенное программное обеспечение	310
29. Реаниматор BitDefender	313
29.1. Запуск BitDefender Rescue CD	313
29.2. Остановка BitDefender Rescue CD	315
29.3. Как выполнить антивирусную проверку?	316
29.4. Как настроить соединение с интернетом?	317
29.5. Как обновлять BitDefender?	318
29.5.1. Как я делаю обновление BitDefender через прокси?	319
29.6. Как мне сохранить мои данные?	320
Глоссарий	323



Лицензионное соглашение для конечного пользователя

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.

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

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

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

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

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



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

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

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

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

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

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

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



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

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

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

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



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

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

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

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

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

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

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



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

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

BITDEFENDER оставляет за собой право пересмотреть данные Условия в любой момент, и пересмотренные условия автоматически будут применены к 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 BITDEFENDER имеет высшую юридическую силу.

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



Предисловие

Данное пособие предназначено для всех пользователей, которые предпочли **BitDefender Internet Security 2009** в качестве решения обеспечения безопасности для персонального компьютера. Информация, представленная в данном пособии, предназначена не только для опытных пользователей, но и для всех, кто может работать с операционной системой Windows.

Данное пособие расскажет вам о **BitDefender Internet Security 2009**, Компании и команде, создавшей его, а так же поможет провести процесс установки, обучит методам настройки. Вы узнаете, как пользоваться **BitDefender Internet Security 2009**, обновлять, тестировать и настраивать его. Вы узнаете, как извлечь из BitDefender максимум пользы.

Мы желаем Вам увлекательного и поучительного чтения.

1. Соглашения, используемые в данной книге

1.1. Типографские обозначения

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

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



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

1.2. Замечания

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



Замечание

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



Важно

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



Внимание

Это критическая информация, к которой следует 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 нескольких разделов, описывающих основные темы. Кроме того, приводится глоссарий, в котором разъясняются некоторые технические термины.



Установка. Пошаговые инструкции по установке BitDefender на рабочей машине. Это развернутое пособие по установке **BitDefender Internet Security 2009**. Начиная с необходимых требований для успешной установки, вам помогут пройти процесс установки продукта. Наконец, здесь описана процедура удаления в случае, если вам понадобилось удалить BitDefender.

Основны администрирования. Описание основных процедур администрирования и обслуживания BitDefender.

Расширенное Администрирование. Детальное описание всех возможностей обеспечения безопасности при помощи продукта BitDefender. Вас научат настраивать и пользоваться всеми модулями BitDefender для эффективной защиты Вашего компьютера от всевозможных угроз (вредоносных программ, спама, атак хакеров, неадекватного содержимого и т.д.).

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

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

Глоссарий. В глоссарии даются пояснения некоторых 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 в этой книге. Пожалуйста, напишите нам о любых погрешностях и ошибках, найденных Вами в этой книге, а также ваши рекомендации по ее улучшению. Учет ваших замечаний поможет нам обеспечивать Вас максимально улучшенной документацией.

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



Важно

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



Установка



1. Системные требования

Вы можете устанавливать BitDefender Internet Security 2009 только на компьютерах, работающих под следующими операционными системами:

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

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



Замечание

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

1.1. Требования к комплектующим компьютера

Для Windows XP

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

Для Windows Vista

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

Для Домашнего Сервера Windows

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



1.2. Требования Программного обеспечения

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

Антифишинг защита предоставляется только для:

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

Шифрование мгновенных сообщений (IM) осуществляется только для:

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

Функция антиспама предоставляется для всех почтовых клиентов, поддерживающих протоколы POP3/SMTP. Тем не менее, панель антиспама BitDefender интегрируется только в следующие приложения:

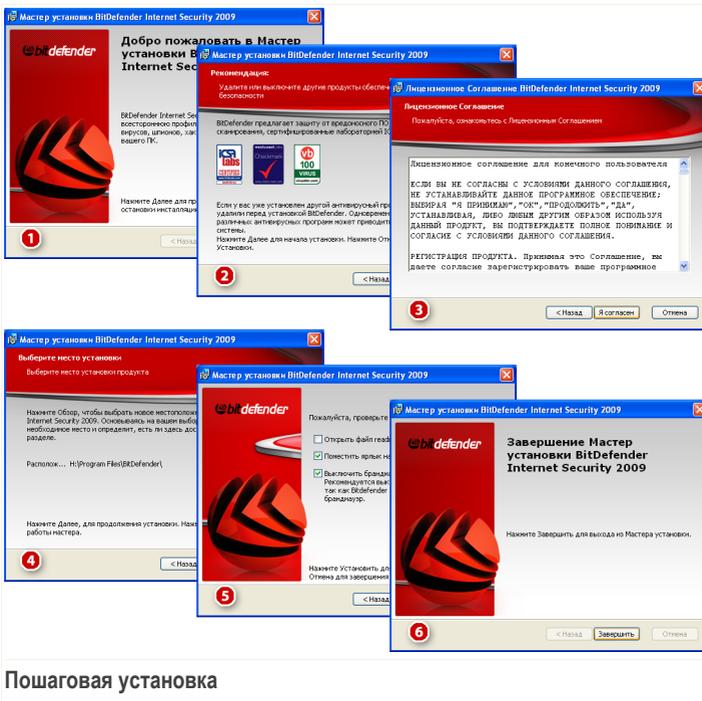
- Microsoft Outlook 2000 / 2002 / 2003 / 2007
- Microsoft Outlook Express
- Microsoft Windows Mail
- Thunderbird 1.5 и 2.0



2. Установка BitDefender

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

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



Пошаговая установка



Следуйте приведенной ниже процедуре для установки BitDefender Internet Security 2009.

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

BitDefender Internet Security 2009 предупредит вас, если на вашем компьютере установлена какая-либо другая антивирусная программа. Нажмите **Удалить**, чтобы деинсталлировать соответствующий продукт. Если Вы хотите продолжить, не удаляя обнаруженные продукты, нажмите **Далее**.



Внимание

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

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



Важно

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

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

Щелкните по кнопке **Далее**.

5. Выберите опции, имеющие отношения к процессу установки. Некоторые из них будут выбраны по умолчанию::

- **Открыть ознакомительный файл** - открывает ознакомительный файл в конце установки.
- **Создать ярлык на рабочем столе** - добавляет ярлык BitDefender Internet Security 2009 на ваш рабочий стол после окончания процесса установки.
- **Извлечь CD из привода после окончания установки** - позволяет извлечь диск из привода после окончания установки; данная опция появляется при установке продукта с CD.



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



Важно

Мы рекомендуем вам выключить Брандмауэр Windows, так как BitDefender Internet Security 2009 уже включает в себя усовершенствованный брандмауэр. Выполнение двух брандмауэров на одном компьютере может вызвать проблемы.

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

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

Подождите, пока завершится процесс установки.

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



Важно

После окончания установки и перезагрузки компьютера, **мастер регистрации** и **мастер настроек** появятся. Выполните работу этих мастеров для регистрации и конфигурации BitDefender Internet Security 2009 и для создания учетной записи BitDefender.

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

2.1. Мастер регистрации

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

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



Замечание

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

2.1.1. Шаг 1/2 - Зарегистрируйте BitDefender Internet Security 2009



Регистрация

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

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

Регистрация BitDefender Internet Security 2009:

1. Выберите **Я хочу зарегистрировать продукт с новым ключем**.



2. Введите лицензионный ключ в поле для редактирования.



Замечание

Вы можете найти ваш лицензионный ключ:

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

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

Для продолжения нажмите **Далее**.



2.1.2. Шаг 2/2 - Создание учетной записи BitDefender

BitDefender Internet Security 2009

Мастер регистрации BitDefender - Шаг 2 из 2

Шаг 1 | Шаг 2

Регистрация Моего Аккаунта

Чтобы Ваш продукт постоянно обновлялся последними антивирусными базами, пожалуйста, зарегистрируйтесь и создайте учетную запись BitDefender. В этом случае, Ваш компьютер будет полностью защищен. Вы также можете выбрать пропустить регистрацию на протяжении 15 дней, если у вас пробная учетная запись, или на протяжении 30 дней, если у вас оплачиваемая учетная запись.

Зайдите в существующую учетную запись BitDefender!

Адрес Email:

Пароль:

[Забыли пароль?](#)

Создать новую учетную запись BitDefender

Адрес Email:

Пароль (6-16 знаков):

Подтвердите пароль:

Имя:

Фамилия:

Страна:

Зарегистрироваться позже

Отправлять мне все сообщения от BitDefender

Отправлять мне только самые важные сообщения

Не отправлять мне никаких сообщений

Поставьте галочку, если вы хотите создать новую учетную запись BitDefender сейчас. Если учетная запись уже была создана, рекомендуется выбрать функцию Войти в уже существующий аккаунт.

Создание учетной записи

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

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



Важно

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



У меня нет учетной записи BitDefender

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

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



Замечание

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

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

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

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

Щелкните мышкой на кнопке **Завершить**.

У меня уже есть учетная запись BitDefender

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

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



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

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

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

Щелкните мышкой на кнопке **Завершить**.

2.2. Мастер Конфигурации

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

Завершение всех шагов мастера необязательно; однако, рекомендуется пройти все шаги, чтобы сэкономить время и убедиться, что ваша система в безопасности еще до установки BitDefender Internet Security 2009.

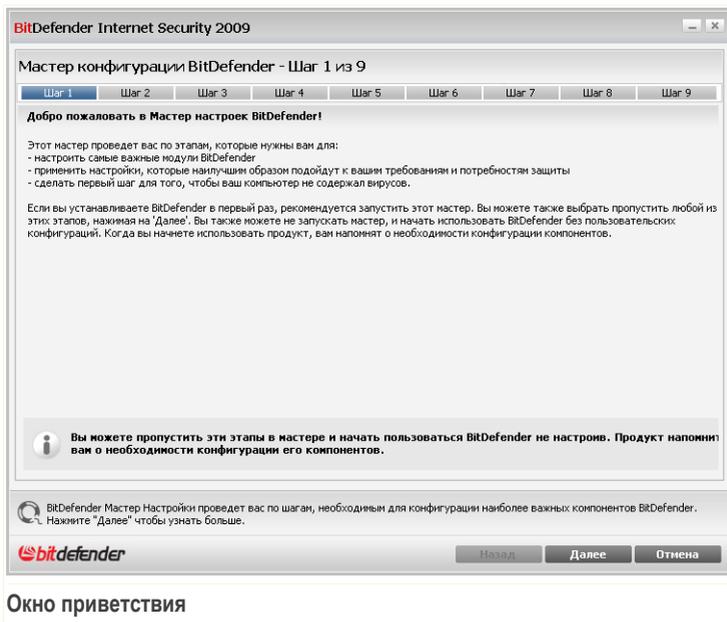


Замечание

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



2.2.1. Этап 1/9 – Окно приветствия



Для продолжения нажмите **Далее**.



2.2.2. Шаг 2/9 - Выберите Режим просмотра

BitDefender Internet Security 2009

Мастер конфигурации BitDefender - Шаг 2 из 9

Шаг 1 | Шаг 2 | Шаг 3 | Шаг 4 | Шаг 5 | Шаг 6 | Шаг 7 | Шаг 8 | Шаг 9

Режим просмотра пользовательского интерфейса

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

Основной вид
Простой интерфейс дает вам доступ ко всем модулям на базовом уровне. Вы можете легко исправлять все неполадки, которые влияют на работу вашей системы.

Расширенный вид
Расширенный интерфейс дает доступ до каждого отдельного компонента BitDefender продукта. Вы сможете настроить все расширенные функции и отслеживать все расширенные свойства.

Вы сможете переключить между этими двумя видами просмотра в любой момент при использовании BitDefender.

Нажмите здесь, чтобы настроить основной вид пользовательского интерфейса BitDefender.

Назад Далее Отмена

Режимы Просмотра

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

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

Для продолжения нажмите **Далее**.



2.2.3. Шаг 3/9 - Настройте сеть BitDefender

BitDefender Internet Security 2009

Мастер конфигурации BitDefender - Шаг 3 из 9

Шаг 1 | Шаг 2 | **Шаг 3** | Шаг 4 | Шаг 5 | Шаг 6 | Шаг 7 | Шаг 8 | Шаг 9

Конфигурация службы Домашнее Управление

BitDefender Internet Security 2009 BitDefender 2009 содержит новый компонент, Домашнее Управление, который дает вам возможность создавать виртуальную сеть между всеми вашими компьютерами дома и управлять всеми продуктами BitDefender, которые были установлены в этой сети. Вы можете действовать от имени администратора сети, которую вы создали, или вы можете быть частью созданной и управляемой с другого компьютера сети.

Поставьте галочку ниже, если вы хотите быть частью BitDefender Домашней Сети. Вам понадобится ввести пароль Домашнего Управления, который позволит администратору вашей сети контролировать настройки BitDefender и процессы на компьютере удаленно.

Я хочу быть частью BitDefender Домашней Сети

Введите пароль:

Введите пароль повторно:

Для того чтобы узнать больше о каждой опции интерфейса BitDefender, проведите мышью поверх окна. Соответствующий текст подсказки будет представлен.

Назад Далее Отмена

Конфигурация сети BitDefender

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

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

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



Важно

Пароль позволяет администратору управлять этим продуктом BitDefender с другого компьютера.



2. Создавайте правила для защиты ваших уязвимых данных. Чтобы узнать больше, обращайтесь «Создание правил Контроля конфиденциальности» (р. 16).
3. При необходимости, определите особые исключения для правил, которые вы создали. Чтобы узнать больше, обращайтесь «Определение исключений в контроле конфиденциальности» (р. 17).

Для продолжения нажмите **Далее**.

Создание правил Контроля конфиденциальности

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

Добавить правило идентификации

Название правила Проверять HTTP
 Проверять SMTP

Тип правила Соответствует цели слован
 С учётом регистра

Данные правила Сканирование IM клиентов

Правило Контроля конфиденциальности

Вам необходимо настроить следующие параметры:

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



Замечание

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

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

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

Чтобы выбрать тип трафика для сканирования, настройте эти функции:

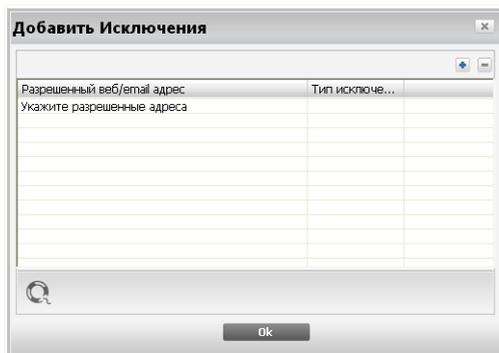
- **Проверять HTTP** - проверяет HTTP (веб) трафик и блокирует исходящие данные, содержащие данные правила.
- **Проверять SMTP** - проверяет SMTP (почта) трафик и блокирует исходящие электронные сообщения, содержащие данные правила.
- **Проверка мгновенных сообщений** - проверяет трафик мгновенных сообщений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

Нажмите **ОК**, чтобы добавить правило.

Определение исключений в контроле конфиденциальности

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

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



Исключения Контроля конфиденциальности

Добавить исключение, следуя по этим шагам:

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

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

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



2.2.5. Шаг 5/9 - Настройте контроль доступа

Мастер конфигурации BitDefender - Шаг 5 из 9

BitDefender Родительский Контроль

BitDefender Родительский контроль доступа позволяет вам контролировать доступ к интернету и определенным приложениям для каждого пользователя, имеющего учетную запись Windows на этой системе. Для пользования этим модулем, вам надо включить и настроить его.

Нажмите правой клавишей на учетную запись Windows, чтобы настроить соответствующие опции Парентального контроля доступа.

Я хочу использовать Родительский контроль доступа

Список пользователей	Состояние
Administrator	Подросток
anirea	Подросток

Для того чтобы узнать больше о каждой опции интерфейса BitDefender, проведите мышью поверх окна. Соответствующий текст подсказки будет представлен.

bitdefender Назад Далее Отмена

Настройка контроля доступа

Родительский контроль доступа BitDefender позволяет контролировать доступ к интернету и определенным приложениям для каждого пользователя, имеющего учетную запись на этой системе.

Если вы хотите воспользоваться контролем доступа, необходимо выполнить следующую процедуру:

1. Выберите **Я хочу использовать Родительский контроль доступа**.
2. Щелкните правой кнопкой мыши на каждой учетной записи Windows и примените соответствующий профиль Контроля доступа.

Профиль	Описание
Ребенок	Предполагает ограниченный доступ в интернет, рекомендуется для пользователей в возрасте до 14 лет. Блокируются



Профиль	Описание
	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.



Замечание

Для полной настройки или отключения контроля доступа для отдельных учетных записей Windows запустите BitDefender, переключитесь в расширенный вид и перейдите в раздел **Родительский контроль**. В модуле контроля доступа можно настроить блокировку:

- неприемлемые веб-страницы.
- Доступа в интернет в определенные промежутки времени (например, когда время уроков).
- Веб-страниц, электронных сообщений и мгновенных сообщений, если они содержат определенные слова.
- приложения, такие как игры, чаты, программы обмена файлами и другие.
- Мгновенных сообщений, отправленных заблокированными контактами интернет-пейджеров.

Для продолжения нажмите **Далее**.



2.2.6. Шаг 6/9 - Настройте создание отчета о вирусах



Настройки отчета

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

Вы можете установить следующие параметры:

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



Замечание

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

Для продолжения нажмите **Далее**.



2.2.7. Шаг 7/9 - Выберите задания для запуска



Выбор задачи

Настройте BitDefender Internet Security 2009 на выполнение важных заданий обеспечения безопасности вашей системы. Доступными являются следующие варианты:

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



Важно

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

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

Для продолжения нажмите **Далее**.

2.2.8. Шаг 8/9 - Ожидайте завершения этих задач

BitDefender Internet Security 2009

Мастер конфигурации BitDefender - Шаг 8 из 9

Шаг 1 | Шаг 2 | Шаг 3 | Шаг 4 | Шаг 5 | Шаг 6 | Шаг 7 | Шаг 8 | Шаг 9

Обновление BitDefender

BitDefender проверяет новые файлы, и автоматически обновляет их. Убедитесь, что подключение к интернету активно перед проведением задачи. Рекомендуется обновлять BitDefender для обеспечения безопасности вашей системы.

Состояние: Обновление завершено

Файл:	100 %	0 КБ
Всего обновлений:	100 %	0 КБ

Назад | Далее | Отмена

Статус задачи

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

Для продолжения нажмите **Далее**.



2.2.9. Шаг 9/9 - Процедура завершена



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

Щелкните мышкой на кнопке **Завершить**.



3. Обновление

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

1. **На выбор!** Если в данную версию BitDefender входит модуль антиспама, вы можете сохранить **Списки друзей и спамеров**, чтобы использовать их после завершения процесса модернизации. Более подробную информацию смотрите в справке или руководстве пользователя к приложению.
2. Удалите старую версию BitDefender со своего компьютера. Более подробную информацию смотрите в справке или руководстве пользователя к приложению.
3. Перезагрузите компьютер.
4. Установите BitDefender Internet Security 2009, как описано в разделе **«Установка BitDefender»** (р. 4) данного руководства пользователя.



4. Удаление или восстановление BitDefender.

Если вы хотите восстановить или удалить **BitDefender Internet Security 2009**, в меню Пуск Windows выберите следующее: **Пуск** → **Программы** → **BitDefender 2009** → **Восстановить или Удалить**.

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

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

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

Перезагрузите компьютер при появлении соответствующего запроса системы и после этого нажмите **Установить**, чтобы переустановить BitDefender Internet Security 2009.

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

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



Замечание

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

Если Вы выбираете удалить BitDefender, появится новое окно.



Важно

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

Нажмите **Удалить**, чтобы начать удаление BitDefender Internet Security 2009 с вашего компьютера.

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

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



Замечание

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

При удалении BitDefender возникла проблема.

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



Основны администрирования



5. Начало работы

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

5.1. Запуск BitDefender Internet Security 2009

Чтобы начать использование функций BitDefender, сначала запустите приложение.

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

5.2. Режим просмотра пользовательского интерфейса

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

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

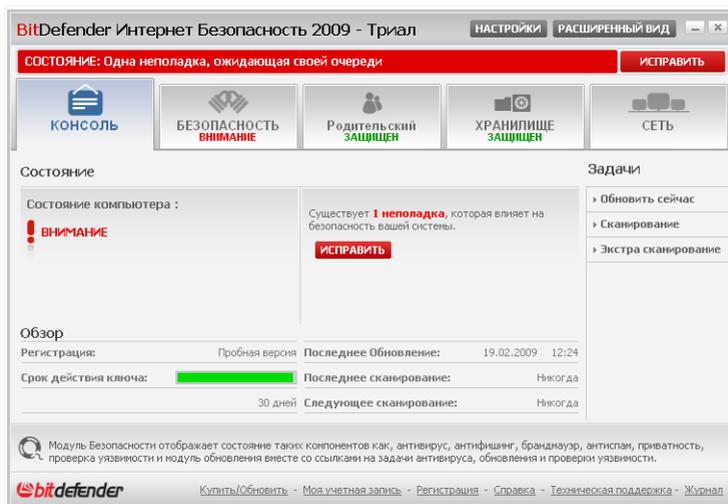


Замечание

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

5.2.1. Основной вид

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



Основной вид

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

Элемент	Описание
Настройки	Открывает окно, где вы можете легко включать или выключать важные модули безопасности (брандмауэр, невидимый режим, автоматические обновления, игровой режим и т.д.).
Переключить в расширенный вид	Открытие окна расширенного вида. В этом окне вы сможете увидеть полный список модулей и подробно настроить каждый компонент. BitDefender использует этот параметр в следующий раз при открытии интерфейса.
Состояние	Отображение информации о приложении и помощь в устранении уязвимостей в компьютере.

- Внутри окна расположены пять вкладок.



Вкладка	Описание
Консоль	Отобразить важную статистику по продукту и ваше состояние регистрации со ссылками на основные задачи, выполняемые по требованию.
Уровень безопасности	Отображает состояние модулей безопасности (антивирус, антифишинг, брандмауэр, антиспам, шифрование мгновенных сообщений, анонимность, сканирование уязвимостей и модули обновления) вместе со ссылками на задания проверки на вирусы, на наличие обновлений и уязвимостей.
Родительский контроль	Отображение статуса модулей, которые дают вам возможность ограничивать доступ ваших детей к интернету и отдельным приложениям.
Менеджер файлов	Отображение состояния хранилища файлов вместе со ссылками на хранилище.
Сеть	Отображение структуры домашней сети BitDefender.

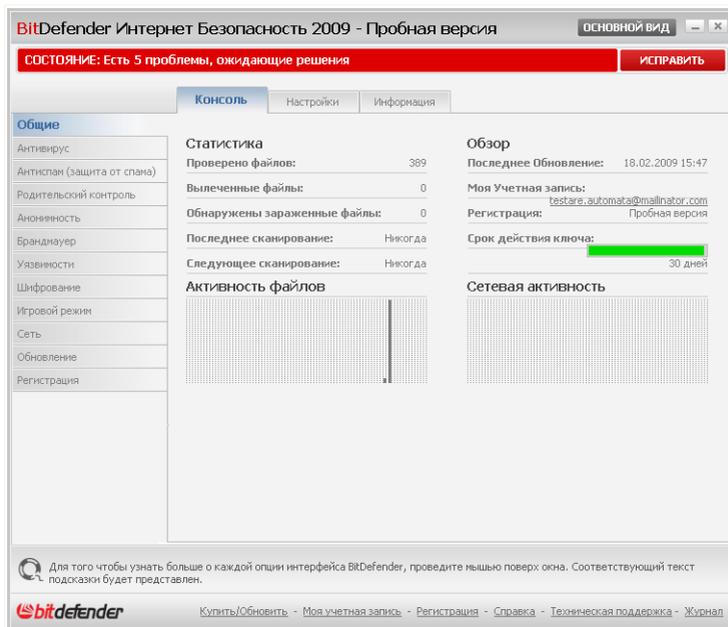
- Кроме того, основной вид окна BitDefender содержит несколько полезных ссылок.

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



5.2.2. Расширенный вид

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



Расширенный вид

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

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



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

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

Модуль	Описание
Общие	Доступ к основным параметрам или просмотр консоли и подробных сведений о системе.
Антивирус	Подробная настройка антивирусных параметров и операций сканирования. Здесь также можно настроить исключения и модуль карантина.
Антиспам	Обеспечивает защиту папки входящих сообщений от спама, а также расширенную настройку параметров антиспама.
Брандмауэр	Защищает ваш компьютер от несанкционированных попыток проникновения и передачи информации. Как страж у ворот, он бдительно следит за вашими подключениями к интернету и определяет, какие данные пропускать в интернет, а какие блокировать.
Анонимность	Предотвращение кражи данных с вашего компьютера и защита вашей конфиденциальности, когда вы находитесь в режиме онлайн.
Родительский контроль	Позволяет защищать ваших детей от неподобающего содержания, используя правила персонализированного доступа к компьютеру.
Шифрование	Позволяет шифровать беседы в приложениях Yahoo и Windows Live (MSN) Messenger, а также локально шифровать важные файлы, папки и разделы.
Уязвимости	Этот параметр позволяет держать важные приложения на вашем ПК в обновленном состоянии.
Режим Игровой/Ноутбук	Позволяет отложить задачи BitDefender по расписанию, пока ноутбук работает от батареи, а также убрать все уведомления и всплывающие окна во время игры.



Модуль	Описание
Сеть	Позволяет настраивать несколько компьютеров у вас дома и управлять ими.
Обновление	Получение сведений о последних обновлениях, собственно обновление и настройка процесса обновления продукта.
Регистрация	Регистрация продукта BitDefender Internet Security 2009, смена лицензионного ключа и создание учетной записи BitDefender.

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

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

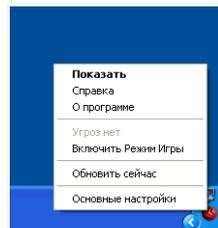
5.3. Значок BitDefender в системном трее.

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



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

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



Значок BitDefender

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

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

5.4. Полоса Активности Сканирования

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

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

Оранжевые полосы в зоне **Сеть** показывают, сколько килобайт информации передается и скачивается из интернета в секунду, по шкале от 0 до 100.



Строка состояния



Замечание

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

Вы можете использовать **Панель активной проверки** для проверки объектов. Для этого перетащите объекты, которые Вы желаете проверить, прямо на нее. Для дополнительной информации, перейдите к *«Проверка перетаскиванием»* (р. 162).

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

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

5.5. Ручная проверка BitDefender

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

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



Ручная проверка BitDefender

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



5.6. Игровой режим

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

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

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

5.6.1. Использование Игрового режима

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

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



Важно

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

5.6.2. Изменение Горячих клавиш Режима Игры

Чтобы изменить Горячие клавиши, необходимо выполнить следующие шаги:

1. Нажмите **Переключить в расширенный вид** (если включен **Основной вид**).
2. Выберите **Режим Игровой / Ноутбук** из бокового меню слева.
3. Щелкните на вкладке **Игровой режим**.
4. Нажмите кнопку **Дополнительно....**



5. Под параметром **Использовать горячие клавиши** выберите горячую клавишу по умолчанию:
- Выберите клавиши, которые Вы хотите изменить, используя следующие: клавиша Control (**Ctrl**), клавиша Shift (**Shift**) или клавиша Alternate (**Alt**).
 - В поле редактирования укажите букву с клавишей, которую Вы хотите использовать.

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



Замечание

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

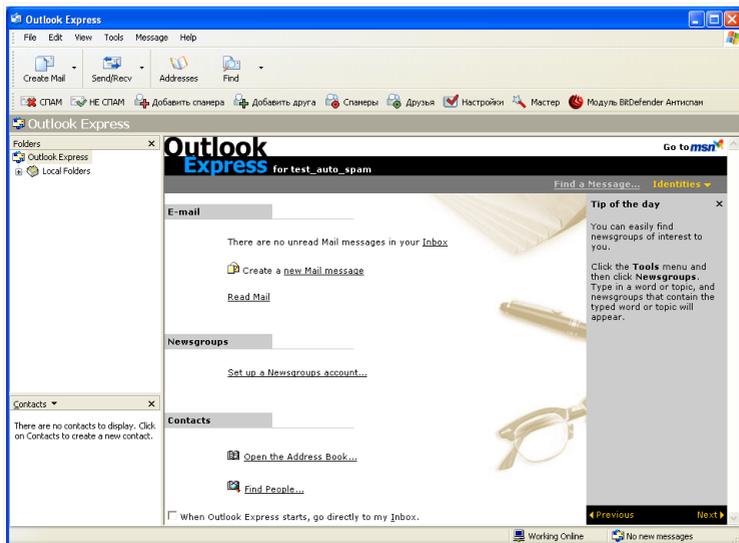
5.7. Интеграция в почтовые клиенты

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

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

5.7.1. Панель инструментов антиспама

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



Панель инструментов антиспама



Важно

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

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

Ниже приводится описание каждой кнопки:

- **Спам** - Отправление сообщения Байесовому модулю о том, что выделенное сообщение является спамом. Это сообщение будет помечено как спам и перемещено 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** - Отправление сообщения Байесовому модулю о том, что выделенное сообщение не является спамом, и программе BitDefender не следует помечать его как спам. Это сообщение будет перемещено из папки **Спам** в папку **Входящие**.

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



Замечание

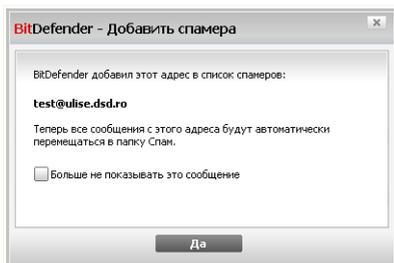
Вы можете выбрать одно письмо или сразу несколько.



Важно

Кнопка **Не Спам** становится активной, когда вы выделяете письмо, помеченное программой BitDefender как СПАМ (обычно эти письма помещаются в папку **Спам**).

- **Добавить спамера** - Добавление отправителя выделенного сообщения в **Список спамеров**.



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

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

Добавить спамера

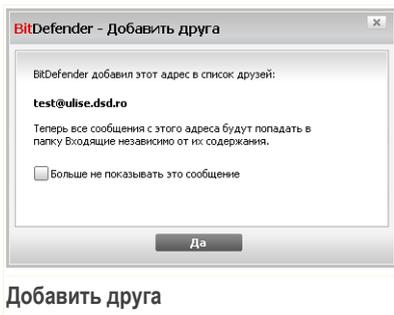
В будущем сообщения от этого адресата будут помечены как СПАМ.



Замечание

Вы можете выбрать одного отправителя или сразу нескольких.

- **Добавить друга** - Добавление отправителя выделенного сообщения в **Список друзей**.



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

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

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



Замечание

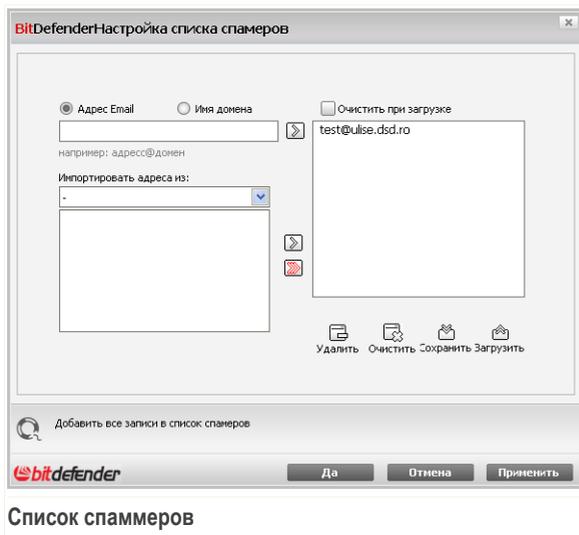
Вы можете выбрать одного отправителя или сразу нескольких.

-  **Спамеры** - Открытие **Списка спамеров**, содержащего адреса, с которых вы не хотите получать сообщения, независимо от их содержания.



Замечание

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



Список спамеров

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 спамеров**.



Важно

Имя домена должно иметь следующий вид:

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

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



выберите 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** внеобходимое место. Файл будет иметь расширение `.bwl`.

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

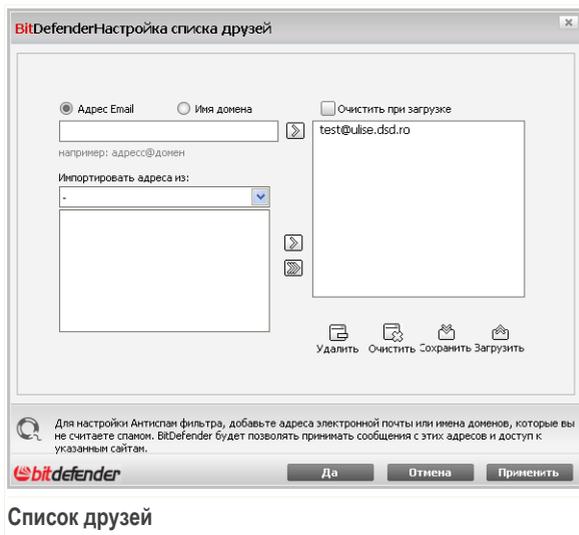
Щелкните мышкой на кнопке **Применить** и **ОК** чтобы сохранить и закрыть **список спамеров**.

-  **Друзья** - Открытие **Списка друзей**, содержащего адреса, с которых вы всегда хотите получать сообщения, независимо от их содержания.



Замечание

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



Список друзей

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

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



Важно

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

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



Важно

Имя домена должно иметь следующий вид:

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



Чтобы импортировать электронные адреса из **Адресной книги Windows / папок Outlook Express в Microsoft Outlook / Outlook Express / Windows Mail**, выберите 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 загрузке предварительно сохраненного, нажмите **Очистить текущий список при загрузке**.



Замечание

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

Щелкните мышкой на кнопке **Применить** и **ОК** чтобы сохранить и закрыть **список друзей**.

- **Настройки** - Открытие окна **Настройки**, где можно указать некоторые параметры модуля **Антиспам**.



Настройки

Доступными являются 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**. Щелкните мышкой на поле **Очистить базу данных антиспама** чтобы переустановить **Байесовский фильтр**.

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

Щелкните мышкой на вкладке **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.



- **Мастер** - Открытие **мастера**, предлагающего пошаговые инструкции в процессе обучения **Байесового фильтра** для дальнейшего повышения эффективности Антиспама BitDefender. Вы также можете добавлять адреса из своей **Адресной книги** в **Список друзей** / **Список спамеров**.
- **Модуль BitDefender Антиспам** - Открытие **пользовательского интерфейса BitDefender**.

5.7.2. Мастер настройки Антиспам

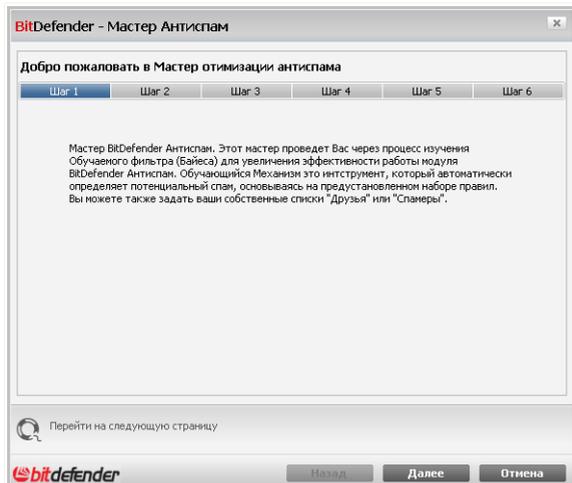
Когда после установки BitDefender вы впервые запускаете почтовый клиент, появится программа-мастер, которая поможет вам настроить **Список друзей**, **Список спамеров** и обучить **Байесовский фильтр** для того, чтобы повысить эффективность работы фильтров Антиспама.



Замечание

Мастер также можно запустить в любой момент, нажав кнопку **Мастер** button from the **Панели инструментов Антиспам**.

Шаг 1/6 - Экран приветствия



Окно приветствия

Щелкните по кнопке **Далее**.



Шаг 2/6 - Заполните список друзей



Заполните список друзей

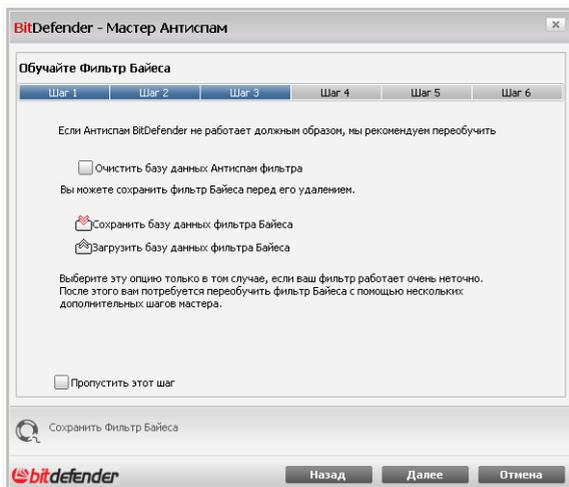
Здесь Вы видите адреса из вашей **Адресной книги**. Выберите из них те, которые хотите занести в **Список друзей**. Мы рекомендуем занести все адреса. Вы будете получать письма от этих отправителей независимо от их содержания.

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

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



Шаг 3/6 - Удаление байесовой базы данных



Удаление байесовой базы данных

Вы можете заметить, что фильтр Защиты от спама стал работать хуже. Причиной этому может быть неверное «обучение». Например, Вы по ошибке 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** / **Загрузить**, чтобы сохранить / загрузить **Список** в необходимое место. Файл будет иметь расширение **.dat**.

Поставьте галочку в поле **Пропустить этот этап** если Вы хотите пропустить этот этап. Щелкните мышкой на кнопке **Назад** чтобы вернуться на предыдущий этап или на кнопке **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.

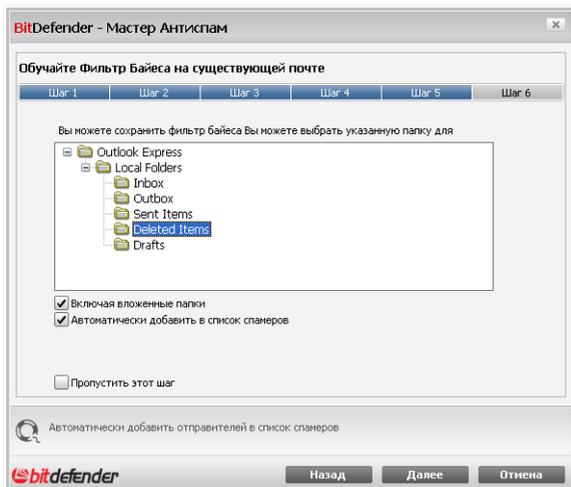
Имеются два дополнительных параметра опции списка поддиректорий:

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

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



Шаг 5/6 - Обучение байесова фильтра при помощи спама



Обучение байесова фильтра при помощи спама

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



Важно

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

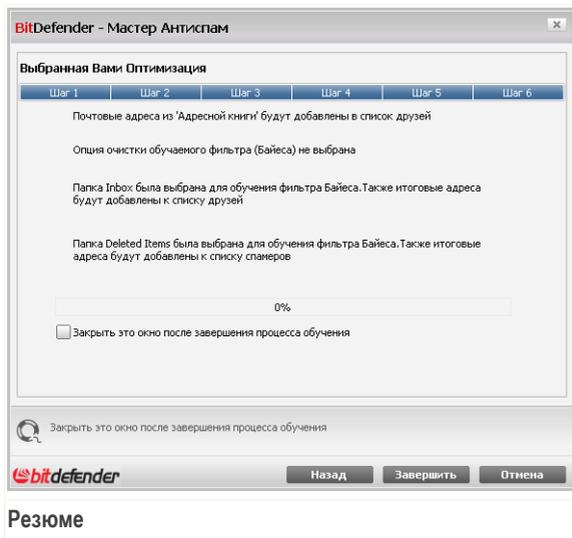
Имеются два дополнительных параметра опции списка поддиректорий:

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

Поставьте галочку в поле **Пропустить этот этап** если Вы хотите пропустить этот этап. Щелкните мышкой на кнопке **Назад** чтобы вернуться на предыдущий этап или на кнопке **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 щелкнув мышкой на кнопке **Назад**).

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

5.8. Интегрирование в браузеры

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

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

- Internet Explorer
- Mozilla Firefox



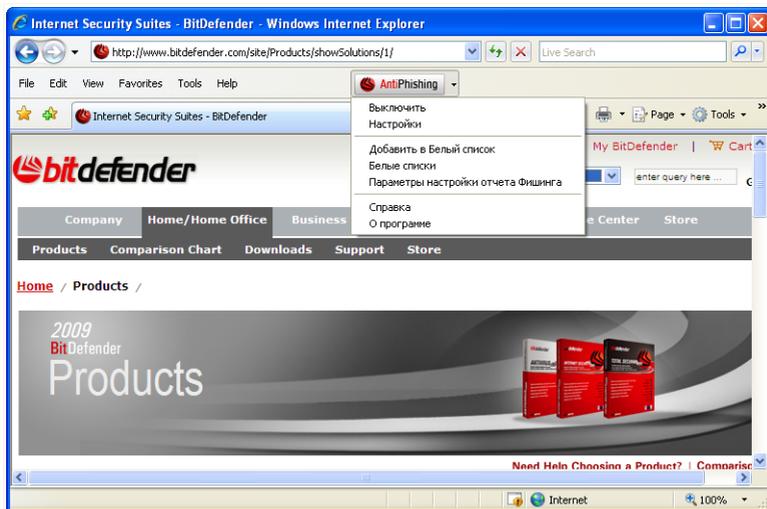
Вы можете легко и эффективно управлять настройками антифишинга и белым списком при помощи панели антифишинга BitDefender, интегрируемой в один из перечисленных браузеров.

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



Замечание

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



Панель инструментов антифишинга

Следующие команды доступны в меню панели инструментов:

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



Замечание

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



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

Доступными являются следующие варианты:

- **Включено сканирование** - включено антифишинговое сканирование.
- **Запрос перед добавлением в белый список** - спрашивает Вас перед добавлением веб сайта в Белый список.
- **Добавить в Белый список** - добавляет нормальные веб сайты в Белый список.



Замечание

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

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

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

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

В Белом списке Вы можете добавлять те сайты, которым полностью доверяете, таким образом, модули антифишинга больше не будут проверять эти страницы. Чтобы добавить сайт в Белый список, введите этот адрес в соответствующее поле и нажмите **Добавить**.

- **Помощь** - открывает документацию к программе в электронном виде.
- **О программе** - открывает окно, где можно просмотреть информацию о BitDefender и о том, где искать помощь в случае непредвиденных обстоятельств.

5.9. Интеграция в интернет-пейджер

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

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



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



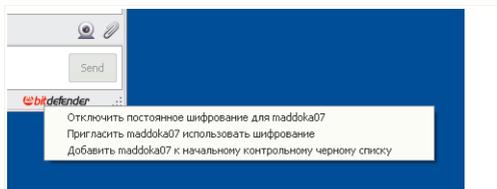
Важно

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

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

Правый щелчок на панели инструментов BitDefender вызывает следующие параметры:

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



Параметры шифрования мгновенных сообщений

Выберите один из вышеперечисленных параметров, чтобы начать их использование.



6. Консоль

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

BitDefender Интернет Безопасность 2009 - Триал

НАСТРОЙКИ РАСШИРЕННЫЙ ВИД

СОСТОЯНИЕ: Одна неполадка, ожидающая своей очереди **ИСПРАВИТЬ**

КОНСОЛЬ БЕЗОПАСНОСТЬ ВНИМАНИЕ Родительский ЗАЩИЩЕН ХРАНИЛИЩЕ ЗАЩИЩЕН СЕТЬ

Состояние Задачи

Состояние компьютера : **ВНИМАНИЕ**

Существует **1 неполадка**, которая влияет на безопасность вашей системы. **ИСПРАВИТЬ**

Обновить сейчас
Сканирование
Экстра сканирование

Обзор

Регистрация: Пробная версия Последнее Обновление: 19.02.2009 12:24

Срок действия ключа: 30 дней Последнее сканирование: Никогда

Следующее сканирование: Никогда

Модуль Безопасности отображает состояние таких компонентов как, антивирус, антифэйк, брандмауэр, антриспи, приватность, проверка уязвимости и модуль обновления вместе со ссылками на задачи антивируса, обновления и проверки уязвимости.

bitdefender Купить/Обновить - Моя учетная запись - Регистрация - Справка - Техническая поддержка - Журнал

Консоль

6.1. Обзор

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

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



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

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

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

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



Замечание

Предоставленные Вами данные конфиденциальны.

Чтобы зарегистрировать BitDefender Internet Security 2009, выполните следующую процедуру.

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

Чтобы приобрести новый лицензионный ключ, выполните следующую процедуру.

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



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

6.2. Задачи

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

Доступны следующие варианты:

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

6.2.1. Сканирование с помощью BitDefender

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

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



Замечание

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



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

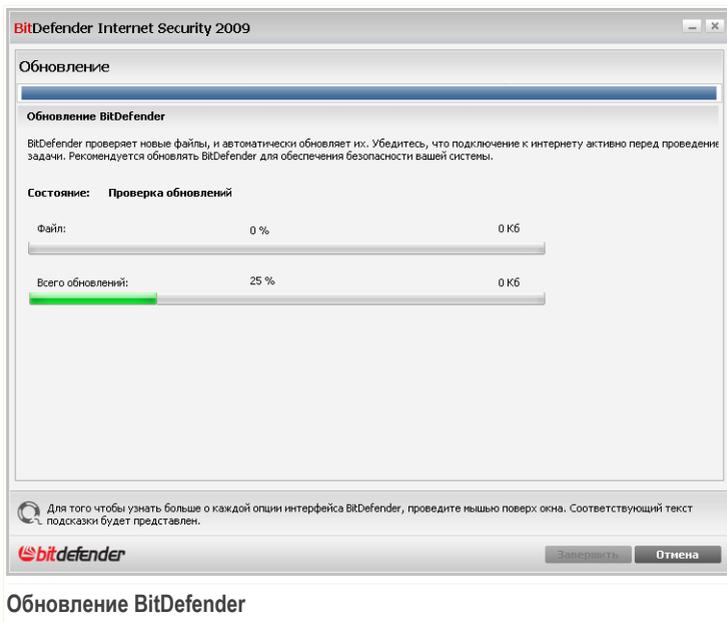
Каждый раз, когда Вы запускаете процесс проверки по требованию или быструю проверку, либо полную проверку, то запускается Сканер BitDefender.

Чтобы завершить процесс проверки выполните последовательность из трех шагов.

6.2.2. Обновление BitDefender

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

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





В этом окне Вы можете видеть статус процесса обновления.

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

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



Замечание

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

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

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

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



7. Уровень безопасности

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

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

The screenshot shows the BitDefender Internet Security 2009 - Trial interface. At the top, there is a status bar indicating "Состояние: Одна неполадка, ожидающая своей очереди" and a button "Исправить". Below this are five main navigation buttons: "Консоль", "Безопасность ВНИМАНИЕ", "Родительский ЗАЩИЩЕН", "Хранилище ЗАЩИЩЕН", and "Сеть". The "Безопасность" button is highlighted in blue.

The main content area is titled "Отслеживаемые компоненты" and "Задачи". Under "Отслеживаемые компоненты", there are two sections: "Локальная Безопасность" and "Онлайн Безопасность".

Компонент	Монитор	Состояние
Защита файлов в режиме реального времени включена	<input checked="" type="checkbox"/> Да	Да
Вы никогда не проводили сканирование вашего компьютера на наличие вредоносного программного обеспечения	<input checked="" type="checkbox"/> Да	Устранить
Обновления проведено сегодня	<input checked="" type="checkbox"/> Да	Да
Брандмауэр включен	<input checked="" type="checkbox"/> Да	Да
Сканирование на наличие уязвимостей		Да

Under "Задачи", there are several links: "Обновить сейчас", "Мои Документы", "Сканирование", "Экстра сканирование", and "Поиск уязвимостей".

At the bottom, there is a note about the Parental Control component and a footer with the BitDefender logo and links: "Купить/Обновить", "Моя учетная запись", "Регистрация", "Справка", "Техническая поддержка", "Журнал".

Уровень безопасности

Модуль безопасности состоит из двух разделов:

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



7.1. Отслеживаемые компоненты

Наблюдаемые компоненты сгруппированы в несколько категорий.

Категория	Описание
Локальная безопасность	С помощью этого компонента вы можете следить за состоянием каждого модуля безопасности, который защищает объекты, хранящиеся на вашем компьютере (файлы, реестр, память и т.п.).
Онлайн безопасность	Здесь вы можете следить за состоянием каждого модуля безопасности, который защищает ваши онлайн-транзакции при подключении к Интернету.
Поиск уязвимостей	Здесь вы можете определить, все ли важное программное обеспечение на вашем компьютере обновлено. Пароли к учетным записям Windows проверяются согласно правилам безопасности.

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

7.1.1. Локальная Безопасность

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

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

Угрозы	Описание
Защита файлов в режиме реального времени включена	Обеспечение проверки всех файлов, когда они запускаются вами или приложением, работающим в вашей системе.



Угрозы	Описание
Вы проводили сканирование на наличие вирусносного программного обеспечения сегодня	Настойчиво рекомендуется провести сканирование по требованию как можно быстрее для проверки всех файлов, хранящихся на вашем компьютере, на наличие вирусносного программного обеспечения.
Автоматическое обновление включено	Пожалуйста, оставляйте автоматическое обновление актуальным, для обеспечения всех антивирусных сигнатур BitDefender обновлениями на постоянной базе.
Выполняется обновление	Проводится обновление подписей продуктов и антивирусных программ.
Брандмауэр включен	Защита вашего компьютера от атак хакеров и вредоносных программ.

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

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

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

7.1.2. Онлайн Безопасность

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

Угрозы	Описание
Антиспам включен	Обеспечивает сканирование ваших электронных сообщений на наличие вредоносного ПО и фильтрацию спама.



Угрозы	Описание
Модуль защиты данных включен	Помогает держать конфиденциальные данные в безопасности путем сканирования всего почтового и веб-трафика на наличие определенных строк. Рекомендуется включить Защиту данных, чтобы ваши конфиденциальные данные (адреса электронной почты, списки контактов, пароли, номера кредиток и т.п.) были защищены от кражи.
Антифишинговая защита для Firefox включена	BitDefender защищает Вас от попыток фишинга, когда Вы используете Интернет.
Антифишинговая защита для Internet Explorer включена	BitDefender защищает Вас от попыток фишинга, когда Вы используете Интернет.

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

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

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

7.1.3. Сканирование на наличие уязвимостей

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

Угрозы	Описание
Служба проверки уязвимостей включена	Отслеживание обновлений Windows Updates, обновлений Microsoft Windows Office и паролей к учетным записям Microsoft Windows, чтобы ваша операционная система была



Угрозы	Описание
	обеспечена обновлениями, а защиту паролем невозможно было обойти.
Критичные обновления Microsoft	Установка доступных важных обновлений Microsoft.
Другие обновления Microsoft	Установка доступных второстепенных обновлений Microsoft.
Автоматические обновления Windows включены	Установка новых обновлений безопасности Windows по мере их доступности.
Администратор (Сильный пароль)	Уровень надежности пароля для определенных пользователей.

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

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

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

7.2. Задачи

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

Доступны следующие варианты:

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



- **Сканировать Мои Документы** - запускает быстрое сканирование документов и настроек.
- **Обновить сейчас** - запускает немедленное обновление.
- **Поиск уязвимостей**

7.2.1. Сканирование с помощью BitDefender

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

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



Замечание

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

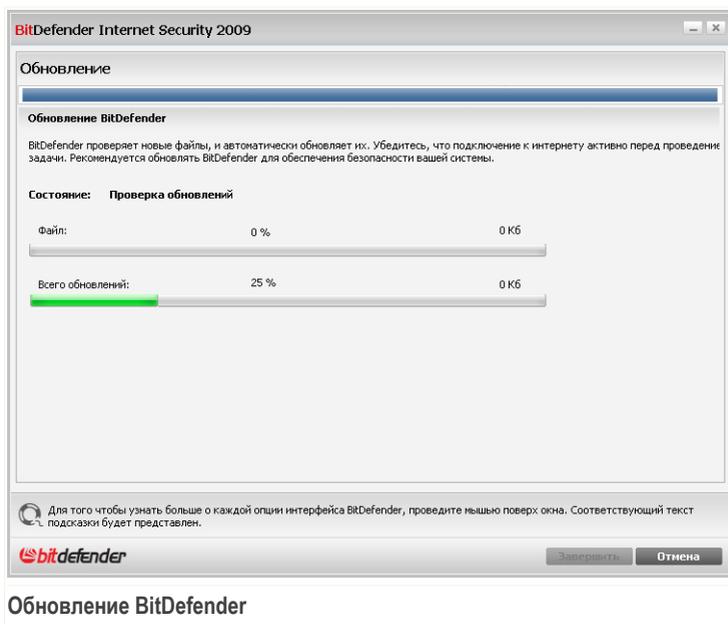
Каждый раз, когда Вы запускаете процесс проверки по требованию или быструю проверку, либо полную проверку, то запускается Сканер BitDefender. Чтобы завершить процесс проверки выполните последовательность из трех шагов.



7.2.2. Обновление BitDefender

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

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



В этом окне Вы можете видеть статус процесса обновления.

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

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



Замечание

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

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

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

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

7.2.3. Поиск уязвимостей

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

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



Шаг 1/6 - Выберите уязвимости для проверки

BitDefender 2009

Мастер сканирования на наличие Уязвимостей

Шаг 1 Шаг 2 Шаг 3 Шаг 4 Шаг 5 Шаг 6

Выбрать задачи

Этот мастер покажет вам действия, которые требуются для определения устаревших приложений и аккаунтов Windows, которые имеют слабый пароль. Пожалуйста, выберите из списка ниже элементы, которые будут проверены на уязвимость.

- Проверить критические обновления Windows
- Проверить случайные обновления Windows
- Проверить обновления приложений
- Проверить пароли учетных записей Windows

Выберите этот блок, чтоб BitDefender проверил получила ли ваша операционная система Windows обновления защиты из Microsoft.

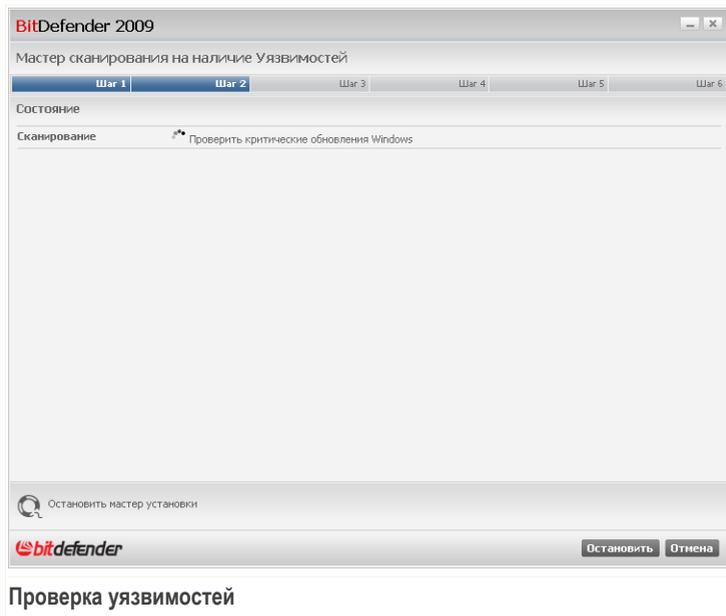
Далее **Отмена**

Уязвимости

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



Шаг 2/6 - Проверка уязвимостей



Подождите, пока BitDefender завершит проверку уязвимостей.



Шаг 3/6 - Смените слабые пароли

BitDefender 2009

Мастер сканирования на наличие Уязвимостей

Шаг 1 Шаг 2 **Шаг 3** Шаг 4 Шаг 5 Шаг 6

Проверить пароли учетных записей Windows

Имя Пользователя	Сила	Состояние
Admin	Слабый	Устранить

Это список Windows множества паролей на ваш компьютер и уровне защиты, которую они обеспечивают. Щелкните кнопку «Местоположение», чтобы изменить слабые пароли.

bitdefender Далее Отмена

Пользовательские пароли

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

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

BitDefender

Choose method to fix:

Force user to change password at next login

Change user password

Type password:

Confirm password:

OK Close

Изменить пароль



Выберите метод устранения проблемы:

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



Замечание

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

Нажмите **ОК**, чтобы сменить пароль.

Щелкните по кнопке **Далее**.



Шаг 4/6 - Обновите приложения

Приложение	Версия установки	Последняя версия	Состояние
Firefox	2.0.0.11 (en-US)	3.0.1 (en-US)	Web-страница

Это список приложений, поддерживаемых BitDefender и обновлений, доступных, если имеется.

Приложения

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

Щелкните по кнопке **Далее**.



Шаг 5/6 - Обновите Windows

BitDefender 2009

Мастер сканирования на наличие Уязвимостей

Шаг 1 | Шаг 2 | Шаг 3 | Шаг 4 | **Шаг 5** | Шаг 6

Обновления Windows

Проверить критические обновления Windows

- Update for Office 2003 (KB907417)
- Office 2003 Service Pack 3 (SP3)
- Microsoft .NET Framework 2.0 Service Pack 1 (KB110906) (x86)
- Security Update for Microsoft XML Core Services 4.0 Service Pack 2 (KB954430)
- Update for Microsoft Office Outlook 2003 Junk Email Filter (KB959614)
- Update Rollup for ActiveX Killbits for Windows XP (KB960715)
- Windows Malicious Software Removal Tool - February 2009 (KB990830)

Проверить случайные обновления Windows

- Update for Windows XP (KB904942)
- Remote Desktop Connection (Terminal Services Client 6.0) for Windows XP (KB925876)
- Update for Microsoft Core XML Services (MSXML) 6.0 Service Pack 1 (KB934268)
- Windows Media Player 11
- Windows Internet Explorer 7 for Windows XP
- Microsoft .NET Framework 3.0: x86 (KB928416)
- Root Certificates Update

Установка обновления

Это список критического или не критических обновлений приложений Windows

bitdefender

Далее Отмена

Обновления Windows

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

Щелкните по кнопке **Далее**.



Шаг 6/6 - Просмотрите результаты

BitDefender 2009

Мастер сканирования на наличие Уязвимостей

Шаг 1 | Шаг 2 | Шаг 3 | Шаг 4 | Шаг 5 | Шаг 6

Сканирование на уязвимости закончено, но обновления не установлены. Настоятельно рекомендуем сделать обновления.

Сканирование на уязвимости закончено, но обновления не установлены. Настоятельно рекомендуем сделать обновления.

bitdefender

Закреть

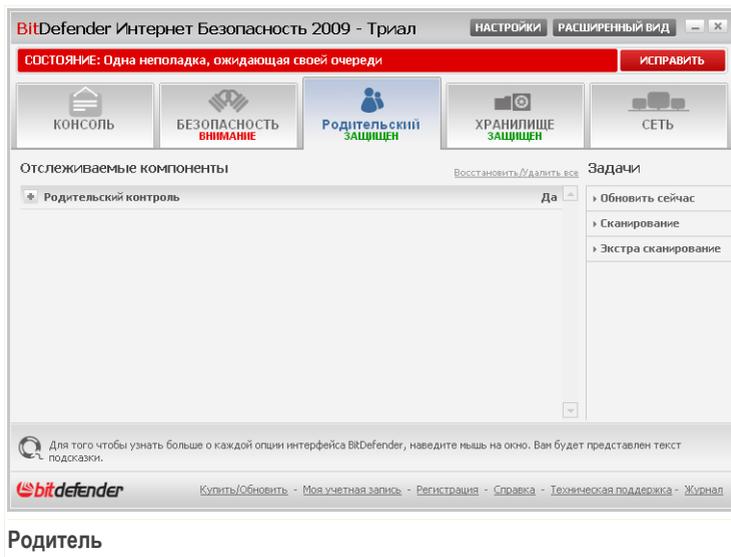
Результаты

Нажмите **Закреть**.



8. Родитель

BitDefender содержит модуль Контроль доступа, которые позволяет держать Чтобы войти в модуль Контроля доступа, нажмите вкладку **Родительский**.



Модуль контроля доступа состоит из двух разделов:

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

8.1. Отслеживаемые компоненты

Отслеживаемый компонент:



Категория	Описание
Родительский контроль	Здесь вы можете проверять состояние модуля Контроля доступа, который позволяет ограничивать доступ ваших детей к интернету и отдельным приложениям.

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

8.1.1. Родительский контроль

Контроль Источника Данных отслеживает статус модулей, которые дают вам возможность ограничивать доступ ваших детей к интернету и отдельным приложениям.

Проблемы, связанные с модулем контроля доступа, описываются развернутыми предложениями. Кроме этого, если что-то может негативно повлиять на ваших детей, вы увидите красную кнопку состояния **Устранить**. В противном случае отображается кнопка **ОК**.

Угрозы	Описание
Контроль доступа не сконфигурирован	Модуль Контроля доступа может блокировать доступ к неразрешенным веб-страницам, доступ в интернет на определенный период времени, а также фильтровать почту, мгновенные сообщения и веб трафик на особенные слова и т.п.

Если кнопки состояния зеленые, ваши дети могут находиться в интернете в безопасности. Чтобы кнопки были зеленые, воспользуйтесь следующей процедурой:

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

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



8.2. Задачи

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

Доступны следующие варианты:

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

8.2.1. Сканирование с помощью BitDefender

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

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



Замечание

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

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

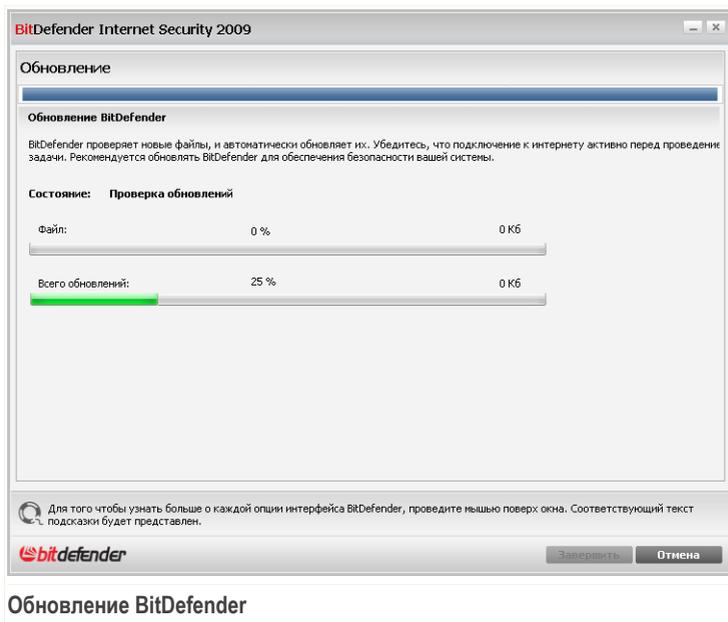


Чтобы завершить процесс проверки выполните последовательность из трех шагов.

8.2.2. Обновление BitDefender

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

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



В этом окне Вы можете видеть статус процесса обновления.

Процесс обновления происходит "на лету", т.е. файлы заменяются по мере обновления. Таким образом, процесс обновления не влияет на работоспособность



продукта, и, в то же время, исключается возможность возникновения уязвимости Вашего компьютера.

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



Замечание

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

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

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

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



9. Хранилище

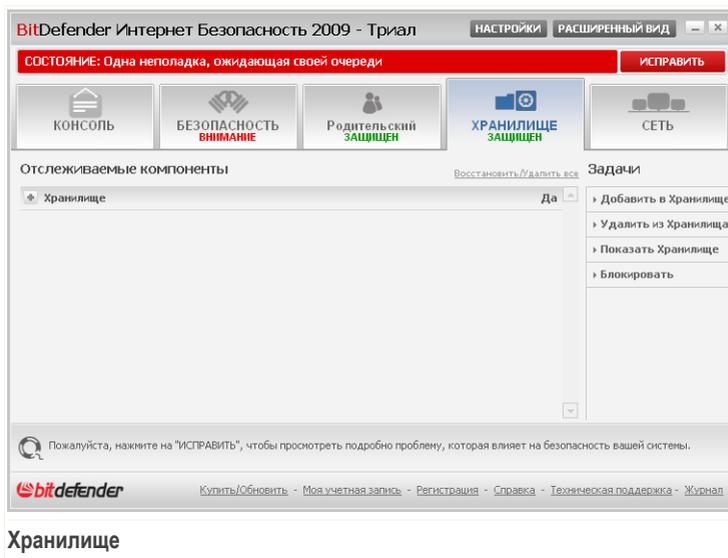
BitDefender содержит модуль Хранилище, который не только обеспечивает сохранность данных, но и их конфиденциальность. Для этого необходимо использовать данный модуль.

Хранилище. Вы безусловно хотите, чтобы ваши важные файлы были скрыты от любопытных глаз. Здесь вам пригодится раздел Хранилище Менеджера файлов.

- Хранилище файлов - это надежное место для хранения вашей конфиденциальной информации или личных файлов.
- Хранилище представляет собой зашифрованный файл на вашем компьютере с расширением `bvd`.
- Так как он зашифрован, данные, находящиеся внутри него, неуязвимы к краже или бреши в системе безопасности.
- Когда вы смонтируете этот файл `bvd`, появится новый логический раздел (новый диск). Вам будет проще понять этот процесс, если вы представите себе монтирование образа ISO в виде виртуального дисковода.

Откройте Мой компьютер, и вы увидите новый диск с содержимым вашего хранилища. Вы сможете выполнять на нем любые операции (копирование, удаление, изменение и т.п.). Файлы остаются защищены, пока они хранятся на этом диске (так как для операции монтирования необходим пароль). Когда вы закончите, заблокируйте (отключите) хранилище, чтобы запустить защиту содержимого.

Чтобы войти в модуль Менеджер файлов, нажмите вкладку **Хранилище**



- **Отслеживаемые компоненты** - Просмотр полного списка отслеживаемых компонентов для каждого модуля. Вы можете выбирать, какие модули следует отслеживать. Рекомендуется включать отслеживание всех компонентов.

9.1. Отслеживаемые компоненты

Отслеживаемый компонент:

Категория	Описание
Хранилище	Это защищенное место для хранения конфиденциальной информации и личных файлов. Так как оно зашифровано, данные, находящиеся внутри него, неуязвимы к краже или бреши в системе безопасности.

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



9.1.1. Хранилище

Проблемы, которые могут повлиять на конфиденциальность ваших данных, описываются развернутыми предложениями. Кроме этого, если что-то может повлиять на конфиденциальность ваших данных, вы увидите красную кнопку состояния **Устранить**. В противном случае отображается кнопка **ОК**.

Угрозы	Описание
Хранилище файлов включено	Хранилище Файлов сохраняет ваши документы приватными, шифруя их в специальные приводы хранилища.

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

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

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

9.2. Задачи

Доступны следующие варианты:

- **Добавить в Хранилище** - Запуск мастера, который позволяет хранить важные файлы / документы, шифруя их на специальных защищенных дисках.
- **Удалить из Хранилища** - Запуск мастера, который поможет вам удалить данные из хранилища.
- **Показать Хранилище** - Запуск мастера, который поможет вам просмотреть содержимое ваших хранилищ.
- **Блокировать** - Запускается мастер, позволяющий блокировать ваше хранилище, тем самым начиная защиту его содержимого.

9.2.1. Добавление файлов в Хранилище

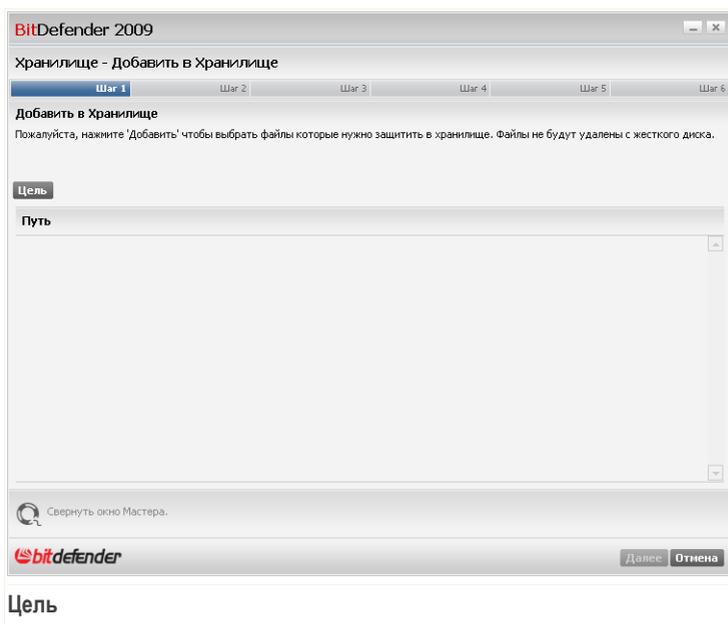
Хранилище - это специальное место для хранения важных данных в безопасных условиях. Документы, извлекающиеся из Хранилища, шифруются.



При щелчке на параметре **Добавить в Хранилище**, появится мастер, который поможет вам в процессе создания хранилища и добавления в него документов.

Шаг 1/6 - Выберите объект

Здесь вы можете определить, какие файлы или папки будут добавляться в хранилище.



Нажмите **Добавить**, выберите файл или папку, которую вы хотите добавить, и нажмите **ОК**. Путь к выбранной папке появится в колонке **Путь**. Если вы передумали насчет пути, нажмите кнопку **Удалить**, которая находится рядом.



Замечание

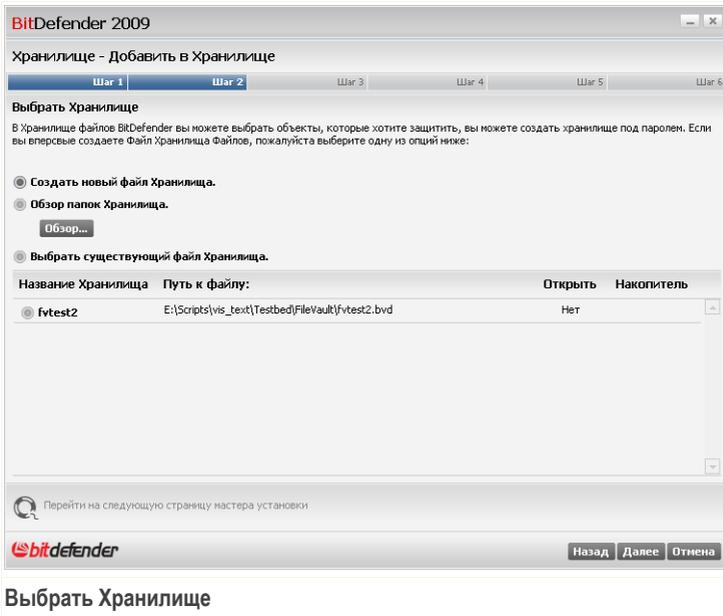
Вы можете выбрать несколько областей.

Щелкните по кнопке **Далее**.



Шаг 2/6 - Выберите хранилище

Здесь вы можете создать новое хранилище или выбрать существующее из списка.



Если вы выбрали **Найти хранилище**, нужно нажать **Обзор** и выбрать хранилище. Вы перейдете к шагу 5, если выбранное хранилище открыто (смонтировано), или к шагу 4, если оно заблокировано (отключено).

Если вы нажали **Выбрать существующее хранилище**, следует щелкнуть на нужном имени хранилища. Вы перейдете к шагу 5, если выбранное хранилище открыто (смонтировано) или к шагу 4, если оно заблокировано (отключено).

Выберите **Создать новое хранилище**, если ни одно из существующих хранилищ не соответствует вашим нуждам. После этого вы перейдете к шагу 3.

Щелкните по кнопке **Далее**.



Шаг 3/6 - Создайте хранилище

Здесь вы можете указать сведения о новом хранилище.

BitDefender 2009

Хранилище - Добавить в Хранилище

Шаг 1 | Шаг 2 | **Шаг 3** | Шаг 4 | Шаг 5 | Шаг 6

Создать Хранилище

Укажите новый пароль хранилища. Укажите место создания хранилища и его размер.

Введите путь к Хранилищу **Обзор**

Файлов:

Буква диска: A: ▾

Изменить пароль к следующему хранилищу файлов Пароль должен быть не менее 8 символов.

Подтвердите пароль Хранилища

Файлов:

Введите размер Хранилища (МВ): 50 Размер должен содержать только цифры.

Установите буквы для открытия Хранилища Файлов.

bitdefender **Назад** **Далее** **Отмена**

Создать Хранилище

Для ввода сведений о хранилище выполните приведенную ниже процедуру:

1. Нажмите **Обзор** и выберите месторасположение для файла `bvd`.



Замечание

Помните, что хранилище представляет собой зашифрованный файл на вашем компьютере с расширением `bvd`.

2. Выберите букву диска для нового хранилища из соответствующего выпадающего меню.



Замечание

Помните, что при монтировании файла `bvd` появляется новый логический раздел (новый диск).



3. Введите пароль для хранилища в соответствующем поле.



Замечание

Пароль должен быть не менее 8 символов.

4. Повторите введение пароля.

5. Установите размер хранилища (в МБ), введя число в соответствующее поле.



Замечание

Размер должен содержать только цифры.

Щелкните по кнопке **Далее**.

После этого вы перейдете к шагу 5.

Шаг 4/6 - Пароль

Здесь вам нужно будет ввести пароль для выбранного хранилища.

BitDefender 2009

Хранилище - Добавить в Хранилище

Шаг 1 | Шаг 2 | Шаг 3 | **Шаг 4** | Шаг 5 | Шаг 6

Запрос пароля для Хранилища

Пожалуйста, введите пароль для выбранного хранилища.

Пароль:

Перейти на следующую страницу мастера установки

bitdefender

Назад | Далее | Отмена

Введите пароль



Введите пароль в соответствующее поле и нажмите **Далее**.

Шаг 5/6 – Итог

Здесь вы можете просмотреть выбранные операции.

BitDefender 2009

Хранилище - Добавить в Хранилище

Шаг 1 | Шаг 2 | Шаг 3 | Шаг 4 | Шаг 5 | Шаг 6

Завершить

Операция добавления	Добавить 1 Файлы/Папки к новому Хранилищу
Имя	fvtest2
Путь	E:\Scripts\vis_text\Testbed\FileVault\fvtest2.bvd
Состояние	Заблокированные сайты

Пожалуйста, проверьте выбранные действия и нажмите **Далее**, если вы хотите продолжить. Вы можете нажать **Назад**, если захотите что-то изменить.

Перейти на следующую страницу мастера установки

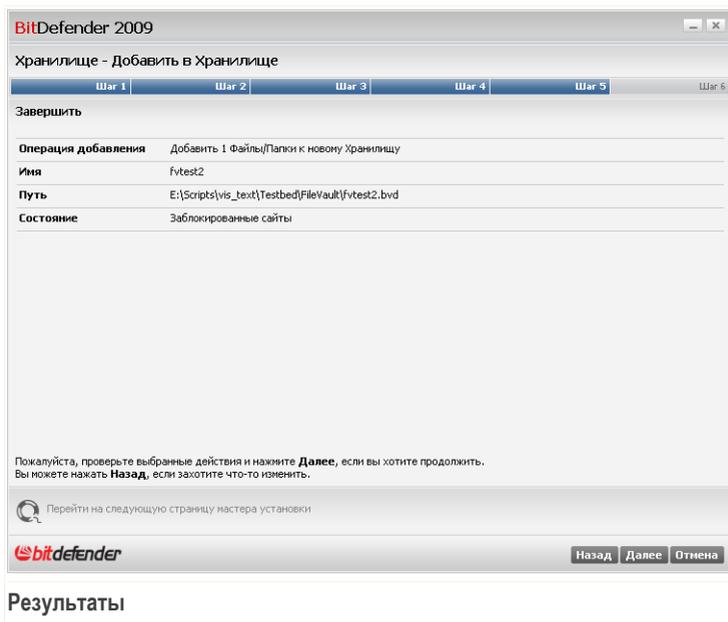
Назад | Далее | Отмена

Резюме

Щелкните по кнопке **Далее**.

Шаг 6/6 - Результаты

Здесь вы можете просмотреть содержимое хранилища.



Результаты

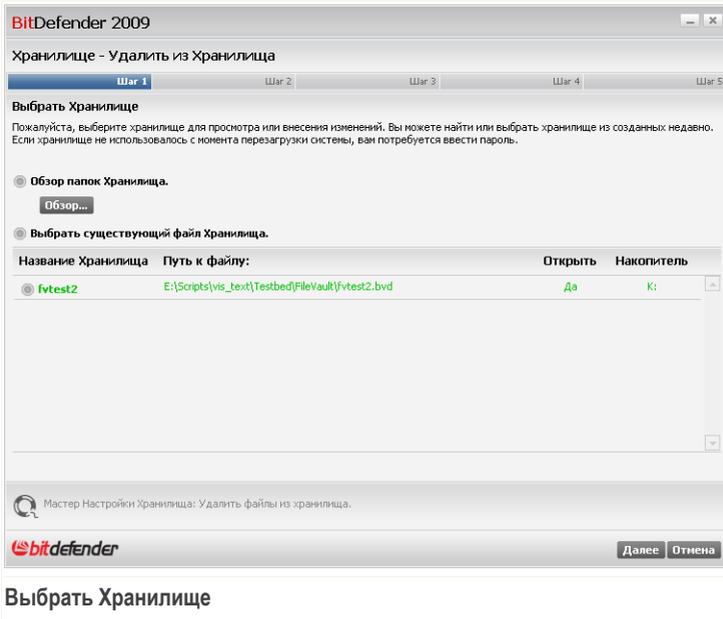
Щелкните мышкой на кнопке **Завершить**.

9.2.2. Удаление файлов из хранилища

При нажатии кнопки **Удалить из хранилища** появится мастер, который поможет вам в процессе удаления файлов из определенного хранилища.

Шаг 1/5 - Выберите хранилище

Здесь вы можете указать, из какого хранилища следует удалить файлы.



Если вы выбрали **Найти хранилище**, нужно нажать **Обзор** и выбрать хранилище. Вы перейдете к шагу 3, если выбранное хранилище открыто (смонтировано), или к шагу 2, если оно заблокировано (отключено).

Если вы нажали **Выбрать существующее хранилище**, следует щелкнуть на нужном имени хранилища. Вы перейдете к шагу 3, если выбранное хранилище открыто (смонтировано) или к шагу 2, если оно заблокировано (отключено).

Щелкните по кнопке **Далее**.

Шаг 2/5 - Пароль

Здесь вам нужно будет ввести пароль для выбранного хранилища.



BitDefender 2009

Хранилище - Удалить из Хранилища

Шаг 1 | Шаг 2 | Шаг 3 | Шаг 4 | Шаг 5

Запрос пароля для Хранилища

Пожалуйста, введите пароль для выбранного хранилища.

Пароль:

Перейти на следующую страницу мастера установки

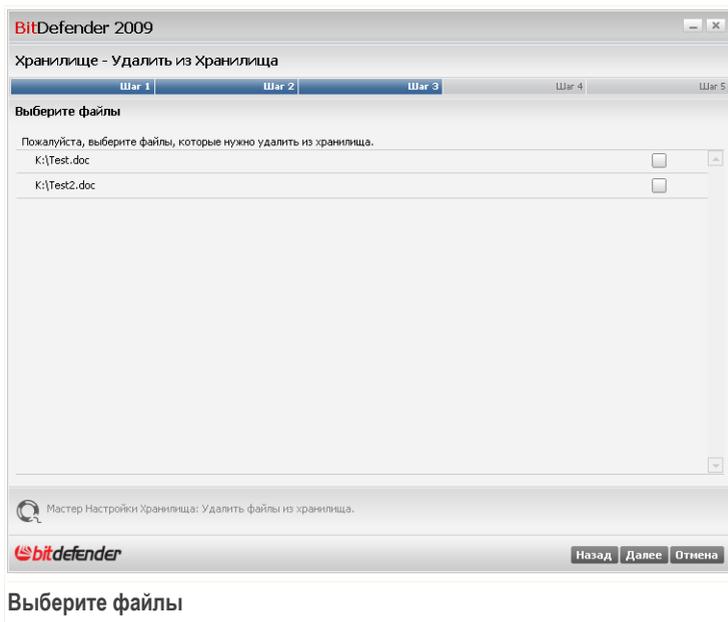
Назад Далее Отмена

Введите пароль

Введите пароль в соответствующее поле и нажмите **Далее**.

Шаг 3/5 - Выберите файлы

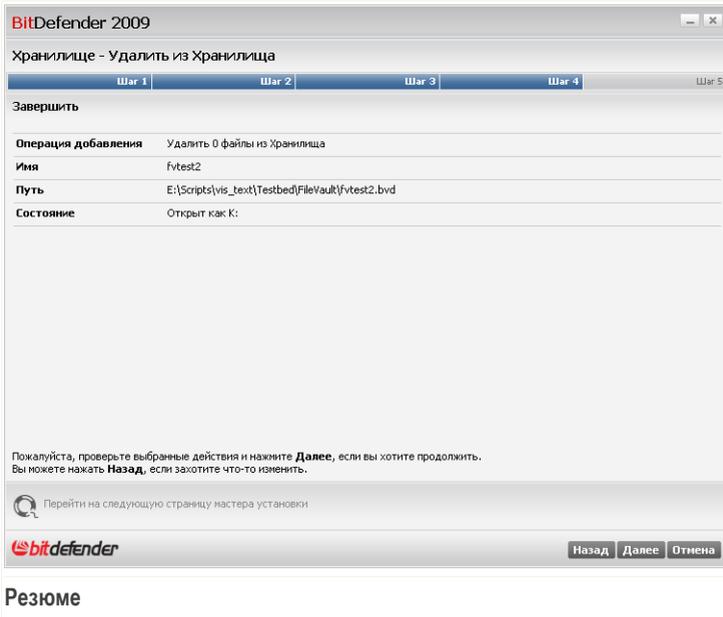
Здесь вы увидите список файлов из выбранного ранее хранилища.



Выберите файлы, которые нужно удалить, и нажмите **Далее**.

Шаг 4/5 - Итоги

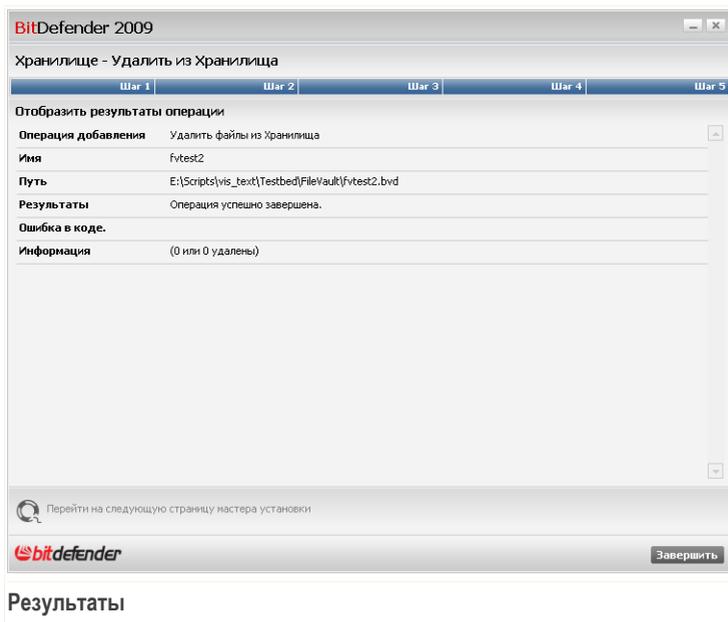
Здесь вы можете просмотреть выбранные операции.



Щелкните по кнопке **Далее**.

Шаг 5/5 - Результаты

Здесь вы можете просмотреть результат операции.



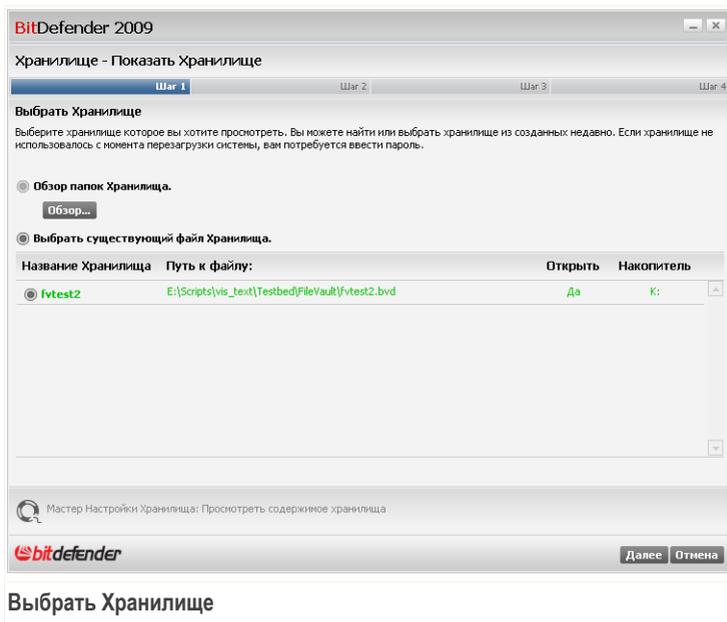
Щелкните мышкой на кнопке **Завершить**.

9.2.3. Просмотр файлов в хранилище

При нажатии кнопки **Показать Хранилище** появится мастер, который поможет вам в просмотре файлов из определенного хранилища.

Шаг 1/4 - Выберите хранилище

Здесь вы можете указать, из какого хранилища следует отобразить файлы.



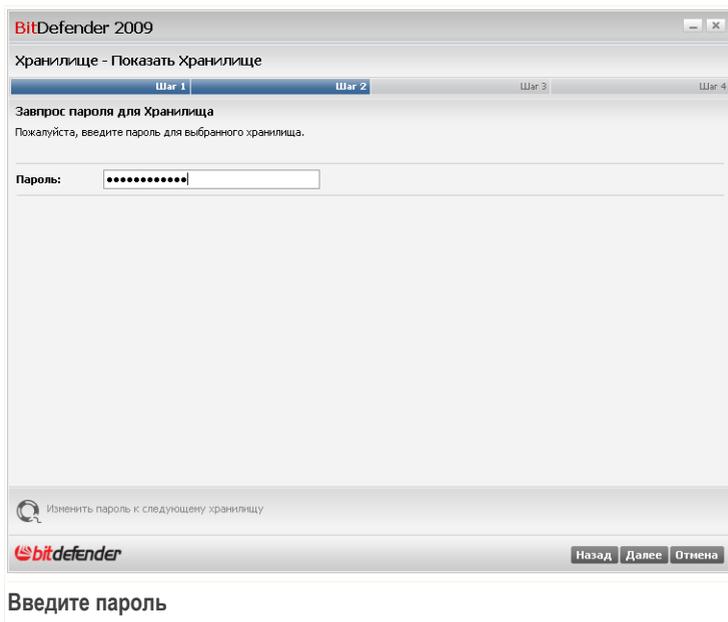
Если вы выбрали **Найти хранилище**, нужно нажать **Обзор** и выбрать хранилище. Вы перейдете к шагу 3, если выбранное хранилище открыто (смонтировано), или к шагу 2, если оно заблокировано (отключено).

Если вы нажали **Выбрать существующее хранилище**, следует щелкнуть на нужном имени хранилища. Вы перейдете к шагу 3, если выбранное хранилище открыто (смонтировано) или к шагу 2, если оно заблокировано (отключено).

Щелкните по кнопке **Далее**.

Шаг 2/4 - Пароль

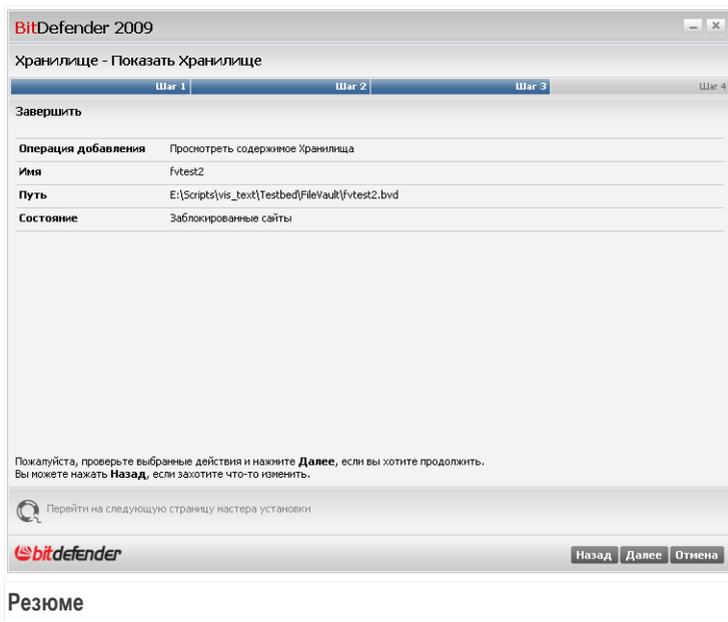
Здесь вам нужно будет ввести пароль для выбранного хранилища.



Введите пароль в соответствующее поле и нажмите **Далее**.

Шаг 3/4 - Итоги

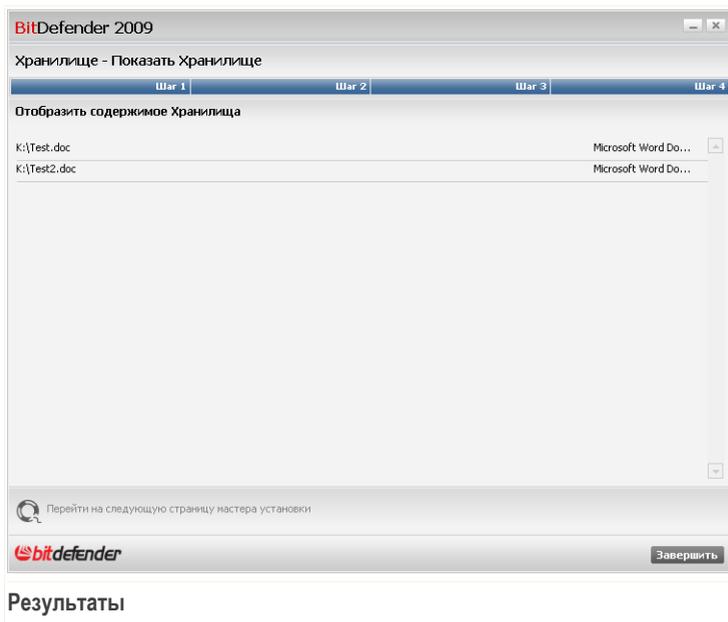
Здесь вы можете просмотреть выбранные операции.



Щелкните по кнопке **Далее**.

Шаг 4/4 - Результаты

Здесь вы можете просмотреть файлы, находящиеся в хранилище.



Щелкните мышкой на кнопке **Завершить**.

9.2.4. Блокировка хранилища

Как вы уже знаете, хранилище файлов представляет из себя зашифрованный файл на вашем компьютере с расширением `bvd`. Хранилище можно открыть (смонтировать) или заблокировать (отключить).

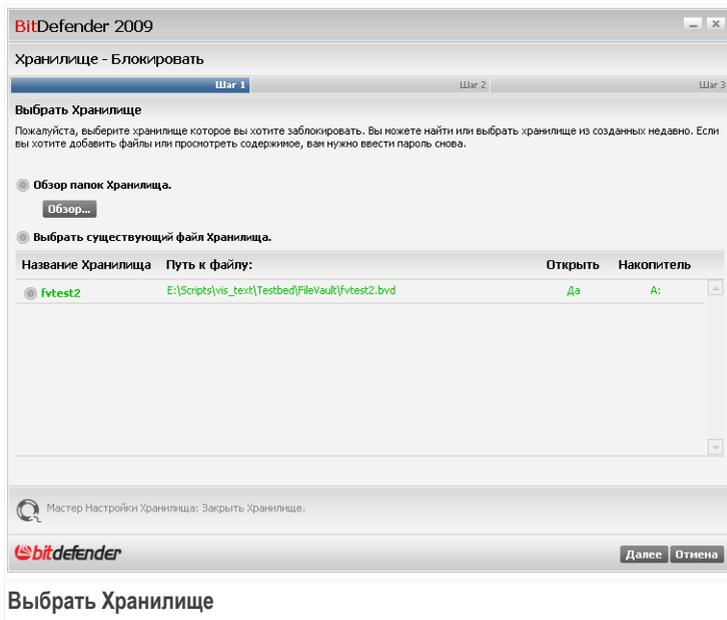
Чтобы лучше понять, как это работает, представьте себе настоящее хранилище в банке - его бронированную дверь можно открыть или заблокировать. Тем не менее, содержимое хранилища может быть в безопасности только тогда, когда дверь закрыта. В то же время, к этому содержимому можно получить доступ только когда дверь открыта.

При нажатии кнопки **Блокировать** появится мастер, который поможет вам в блокировании (отключении) определенного хранилища.



Шаг 1/3 - Выберите хранилище

Здесь вы можете указать, какое хранилище нужно заблокировать.



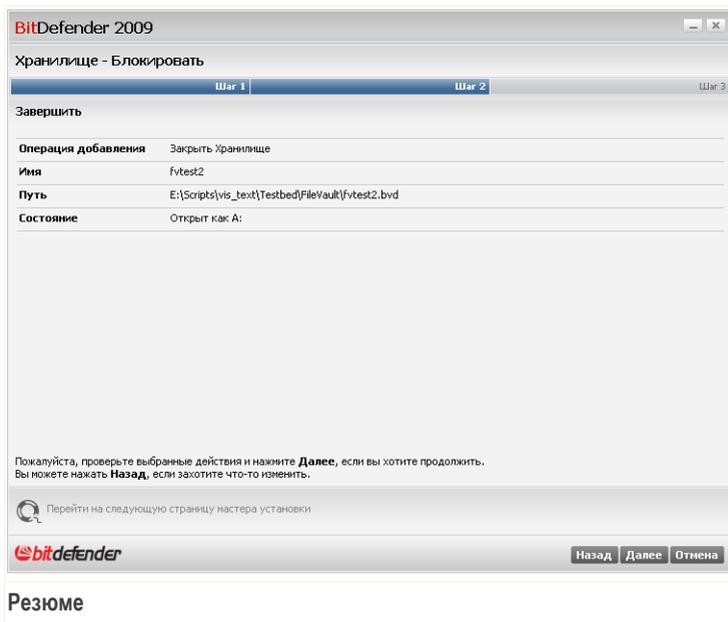
Если вы выбрали **Найти хранилище**, нажмите **Обзор** и выберите хранилище.

Нажав **Выбор существующее хранилище** нужно щелкнуть по имени нужного вам хранилища.

Щелкните по кнопке **Далее**.

Шаг 2/3 - Итог

Здесь вы можете просмотреть выбранные операции.



Щелкните по кнопке **Далее**.

Шаг 3/3 - Результаты

Здесь вы можете просмотреть результат операции.



BitDefender 2009

Хранилище - Блокировать

Шаг 1 | Шаг 2 | Шаг 3

Отобразить результаты операции

Операция добавления	Закреть Хранилище	
Имя	fvtest2	
Путь	E:\Scripts\vis_text\Testbed\FileVault\fvtest2.bvd	
Результаты	Операция успешно завершена.	
Ошибка в коде.		
Информация	Файл заблокирован.	

Перейти на следующую страницу мастера установки

Завершить

Результаты

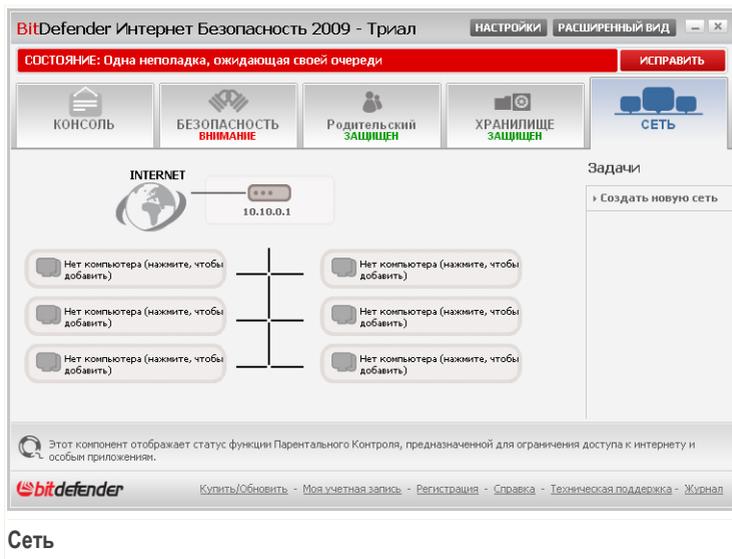
Щелкните мышкой на кнопке **Завершить**.



10. Сеть

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

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



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

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



10.1. Задачи

В самом начале доступна только одна кнопка.

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

После входа в сеть появятся еще несколько кнопок.

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

10.1.1. Подключение к сети BitDefender

Чтобы подключиться к домашней сети BitDefender, выполните следующую процедуру:

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

BitDefender

Введите пароль

Необходим пароль для того, чтобы присоединиться либо создать сеть в целях безопасности (это обеспечит защиту к вашему компьютеру в домашней сети)

Введите пароль:

Подтвердите пароль:

Да Отмена

Настройка пароля

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

На карте сети будет отображаться имя компьютера.

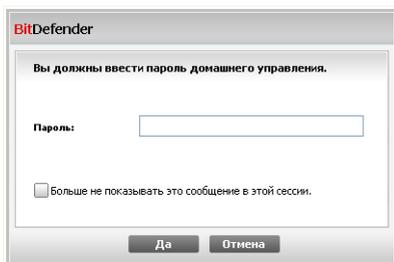


10.1.2. Добавление компьютеров в сеть BitDefender.

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

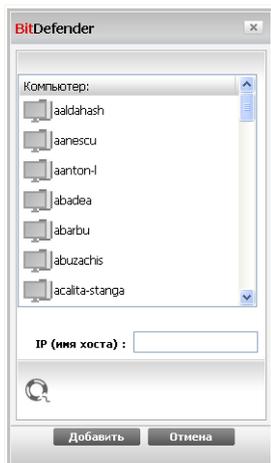
Чтобы добавить компьютер в домашнюю сеть BitDefender, выполните следующую процедуру:

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



Введите пароль

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



Добавить компьютер

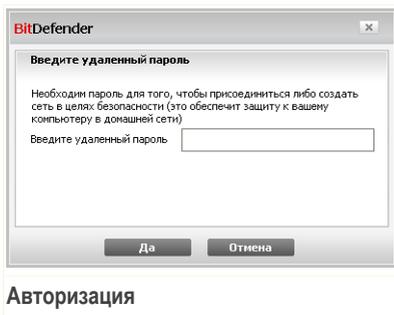
Вы увидите список компьютеров, находящихся в сети. Значки имеют следующие значения:

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

3. Сделайте одно из следующего:

- Выберите из списка имя добавляемого компьютера.
- Введите IP-адрес или имя добавляемого компьютера в соответствующем поле.

4. Нажмите **Добавить**. Появится окно ввода пароля управления домашней сетью для соответствующего компьютера.



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

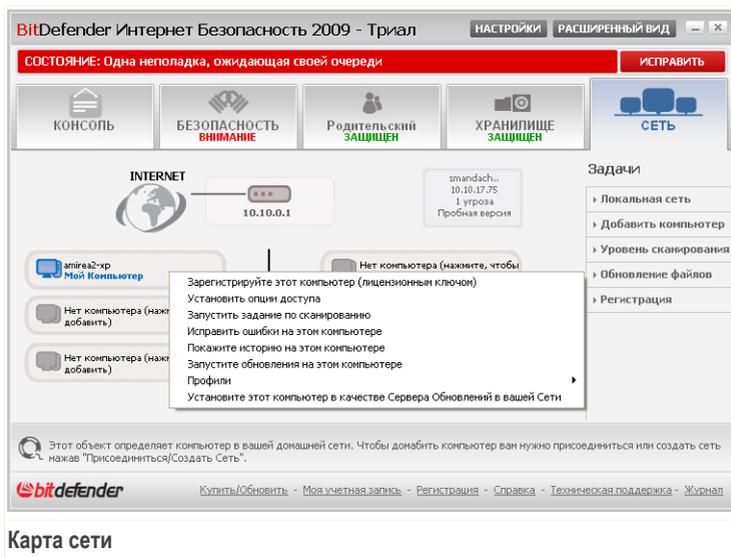


Замечание

На сетевую карту можно добавить до пяти компьютеров.

10.1.3. Управление сетью BitDefender

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



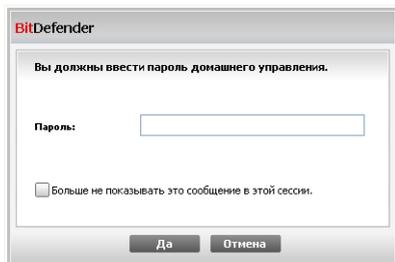
Если передвинуть курсор мыши поверх компьютера на карте сети, вы увидите краткие сведения о нем (имя, IP-адрес, число проблем, влияющих на безопасность системы, состояние регистрации BitDefender).

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

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



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



Введите пароль

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



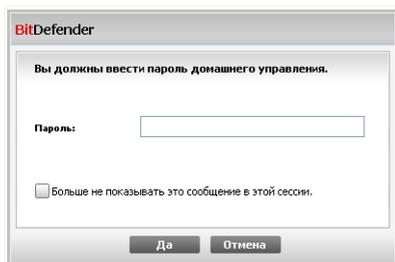
Замечание

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

10.1.4. Сканирование всех компьютеров

Для сканирования всех управляемых компьютеров выполните следующую процедуру:

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

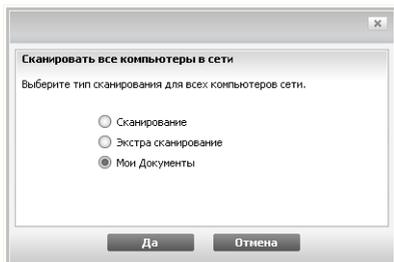


Введите пароль



2. Выберите тип сканирования.

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



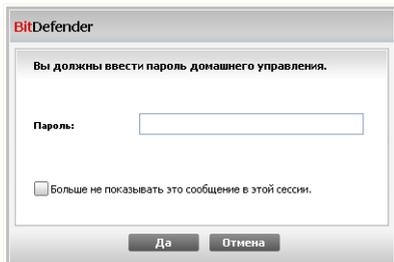
Выберите тип сканирования

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

10.1.5. Обновление всех компьютеров

Для обновления всех управляемых компьютеров выполните следующую процедуру:

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



Введите пароль

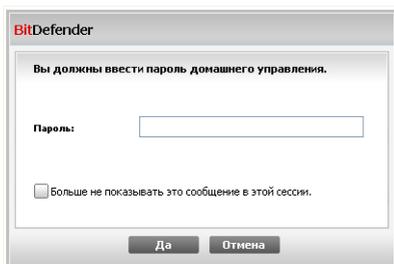


2. В конце щелкните мышкой на кнопке **ОК**.

10.1.6. Регистрация всех компьютеров

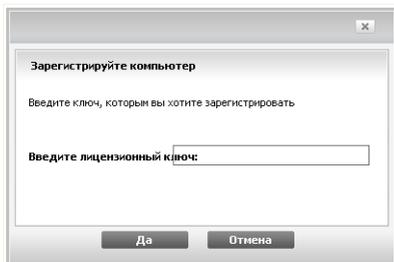
Для регистрации всех управляемых компьютеров выполните следующую процедуру:

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



Введите пароль

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



Регистрация

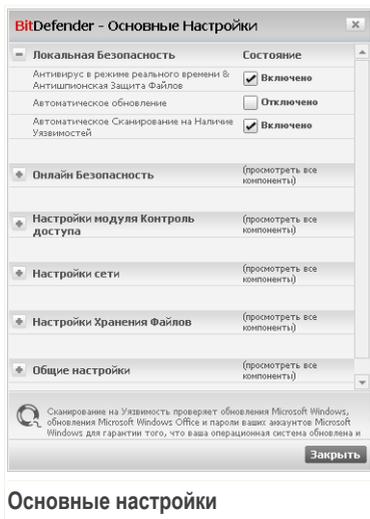
3. В конце щелкните мышкой на кнопке **ОК**.



11. Основные настройки

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

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



Основные настройки

Доступные модули безопасности сгруппированы в несколько категорий.

Категория	Описание
Локальная безопасность	Здесь вы можете включить/выключить защиту файлов в реальном времени или автоматическое обновление.
Онлайн безопасность	Здесь вы можете включить/выключить защиту почты и веба в реальном времени.
Настройки контроля доступа	Тут вы можете включить или выключить контроль доступа.
Безопасность сети	Тут вы можете включить или выключить брандмауэр.



Категория	Описание
Основные настройки	Здесь вы можете включить/выключить игровой режим, режим ноутбука, пароли, полосу активности сканирования и т.п.

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

11.1. Локальная Безопасность

Вы можете включить/выключить модули безопасности одним щелчком.

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

11.2. Онлайн Безопасность

Вы можете включить/выключить модули безопасности одним щелчком.



М о д у л ь безопасности	Описание
Антивирус в режиме реального времени, антиспам и антишпионская защита почты	Модуль защиты почты в реальном времени обеспечивает фильтрацию ваших электронных сообщений от спама и сканирование попыток фишинга.
Антивирус в режиме реального времени и антишпионская защита веб-страниц	Модуль защиты веба в реальном времени обеспечивает сканирование всех файлов, которые загружаются через HTTP на наличие вирусов и шпионящего программного обеспечения.
Антифишинг веб защита в режиме реального времени	Антифишинговая защита веба в реальном времени обеспечивает сканирование всех файлов, загруженных через HTTP, на наличие попыток фишинга.
Защита данных	Служба Контроля Идентичности помогает хранить вашу конфиденциальную информацию, сканируя особенные строки в веб и почтовом трафике.
Шифрование	Если у ваших IM контактов установлен BitDefender 2009, все передачи IM сообщений с помощью Yahoo! Messenger и Windows Live Messenger будут зашифрованы.

11.3. Настройки модуля Контроль доступа

Модуль контроля доступа можно включить/выключить одним щелчком.

Модуль контроля доступа может блокировать доступ к несоответствующим веб-страницам или к интернету на определенный период времени, а также фильтровать почту, мгновенные сообщения и веб-трафик на особенные слова.

11.4. Настройки сети

Брандмауэр можно включить/выключить одним щелчком.



Брандмауэр обеспечивает защиту вашего компьютера от атак хакеров и вредоносных программ.

11.5. Настройки Хранения Файлов

Хранилище файлов можно включить/выключить одним щелчком.

Хранилище Файлов сохраняет ваши документы приватными, шифруя их в специальные приводы хранилища.

11.6. Общие настройки

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

Элемент	Описание
Режим Игры	Режим Игры временно изменяет настройки защиты, чтобы минимизировать их влияние на деятельность системы во время игры.
Режим ноутбука	Режим Ноутбука временно изменяет настройки защиты, чтобы минимизировать их влияние на длительность работы батареи вашего ноутбука.
Пароль настроек	Благодаря этому настройки BitDefender могут быть изменены только теми, кто знает этот пароль.
Пароль контроля источника данных	Установив эту опцию, вы снижаете настройки защиты до модуля родительского контроля. Вы можете убедиться в том что настройки модуля родительского контроля BitDefender могут быть изменены только пользователем, знающим пароль.
Новости BitDefender	Включив этот параметр, вы будете получать важные новости компании, обновления продукта и список новых угроз от BitDefender.
Предупреждение об уведомлении продукта	Включив этот параметр, вы будете получать информационные уведомления.



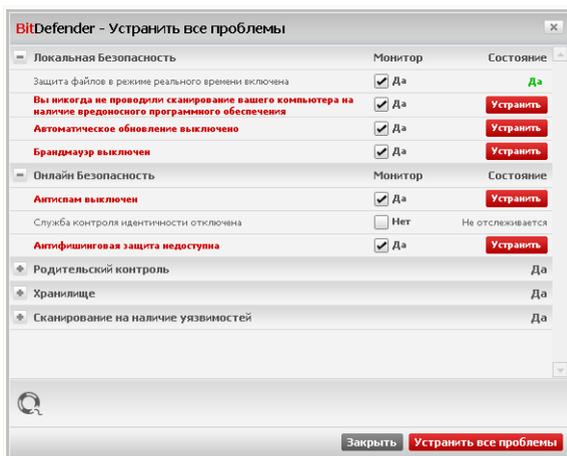
Элемент	Описание
Полоса активности сканирования	Полоса активности сканирования - это небольшая прозрачная панель, отображающая ход сканирования BitDefender. Зеленая полоса отображает активность сканирования на вашей локальной системе. Красная линия отображает активность сканирования вашего интернет-соединения.
Запускать BitDefender при загрузке	Включение этого параметра обеспечивает загрузку пользовательского интерфейса BitDefender при запуске. Этот параметр не повлияет на уровень защиты.
Отправлять отчеты о вирусах	Включение этого параметра обеспечивает отправку отчетов о сканировании на вирусы в лаборатории BitDefender для анализа. Обратите внимание на то, что эти отчеты не будут содержать конфиденциальных данных, таких как, например, ваше имя или IP-адрес, и они не будут использоваться в коммерческих целях.
Определение атак	Включение этого параметра обеспечивает отправку отчетов о потенциальных вирусных атаках в лаборатории BitDefender для анализа. Обратите внимание на то, что эти отчеты не будут содержать конфиденциальных данных, таких как, например, ваше имя или IP-адрес, и они не будут использоваться в коммерческих целях.



12. Полоса состояния

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

Функция состояния безопасности отображает удобный систематизированный список уязвимостей вашего компьютера. BitDefender Internet Security 2009 позволяет сделать вывод, повлияет ли существующая проблема на безопасность вашего компьютера.



Полоса состояния

12.1. Локальная Безопасность

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



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

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

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

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

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



12.2. Онлайн Безопасность

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

Угрозы	Описание
Антиспам включен	Обеспечивает сканирование ваших электронных сообщений на наличие вредоносного ПО и фильтрацию спама.
Модуль защиты данных включен	Помогает держать конфиденциальные данные в безопасности путем сканирования всего почтового и веб-трафика на наличие определенных строк. Рекомендуется включить Защиту данных, чтобы ваши конфиденциальные данные (адреса электронной почты, списки контактов, пароли, номера кредиток и т.п.) были защищены от кражи.
Антифишинговая защита для Firefox включена	BitDefender защищает Вас от попыток фишинга, когда Вы используете Интернет.
Антифишинговая защита для Internet Explorer включена	BitDefender защищает Вас от попыток фишинга, когда Вы используете Интернет.

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

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

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



12.3. Хранилище

Проблемы, которые могут повлиять на конфиденциальность ваших данных, описываются развернутыми предложениями. Кроме этого, если что-то может повлиять на конфиденциальность ваших данных, вы увидите красную кнопку состояния **Устранить**. В противном случае отображается кнопка **ОК**.

Угрозы	Описание
Хранилище файлов включено	Хранилище Файлов сохраняет ваши документы приватными, шифруя их в специальные приводы хранилища.

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

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

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

12.4. Сканирование на наличие уязвимостей

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

Угрозы	Описание
Служба проверки уязвимостей включена	Отслеживание обновлений Windows Updates, обновлений Microsoft Windows Office и паролей к учетным записям Microsoft Windows, чтобы ваша операционная система была обеспечена обновлениями, а защиту паролем невозможно было обойти.
Критичные обновления Microsoft	Установка доступных важных обновлений Microsoft.



Угрозы	Описание
Другие обновления Microsoft	Установка доступных второстепенных обновлений Microsoft.
Автоматические обновления Windows включены	Установка новых обновлений безопасности Windows по мере их доступности.
Администратор (Сильный пароль)	Уровень надежности пароля для определенных пользователей.

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

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

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



13. Регистрация

BitDefender Internet Security 2009 предоставляется с 30-дневным периодом пробного использования. Если вы хотите зарегистрировать BitDefender Internet Security 2009, изменить лицензионный ключ или создать учетную запись BitDefender, нажмите ссылку **Регистрация**, которая находится в нижней части окна BitDefender. Появится Мастер регистрации.

13.1. Шаг 1/1 - Зарегистрируйте BitDefender Internet Security 2009

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

Регистрация BitDefender Internet Security 2009:



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



Замечание

Вы можете найти ваш лицензионный ключ:

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

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

Щелкните мышкой на кнопке **Завершить**.



14. Журнал

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

BitDefender Internet Security 2009

Модуль Истории и Событий BitDefender

Антивирус

Антиспам (защита от спама)
Родительский контроль
Анонимность
Брандмауэр
Уязвимости
Шифрование
Хранилище
Игровой режим
Сеть
Обновление
Регистрация

Постоянная защита

Название действия	Выполненное дей...	Дата и время
Постоянная защита	Включено	18.02.2009 16:31:04
Режимный Сканнер	Включено	18.02.2009 16:31:04
Постоянная защита	Отключено	18.02.2009 16:30:55
Постоянная защита	Включено	18.02.2009 16:17:23
Постоянная защита	Отключено	18.02.2009 16:14:48
Постоянная защита	Включено	18.02.2009 16:07:27
Постоянная защита	Отключено	18.02.2009 16:07:18
Постоянная защита	Включено	18.02.2009 16:06:48
Постоянная защита	Отключено	18.02.2009 16:06:40

События задач по требованию

Название действия	Название задания	Дата и время
Сканирование завершено.	1459	18.02.2009 16:16:35
Сканирование завершено.	1459	18.02.2009 16:16:11
Сканирование завершено.	1459	18.02.2009 16:15:49
Сканирование завершено.	1459	18.02.2009 16:15:23
Сканирование завершено.	Ручное Сканирование	18.02.2009 16:13:09
Сканирование прервано	Мастер Настройки Иск...	18.02.2009 16:11:27
Сканирование прервано	Мои Документы	18.02.2009 16:10:00
Сканирование прервано	Быстрая проверка сис...	18.02.2009 16:09:52
Сканирование прервано	Сканирование	18.02.2009 16:09:43

Для того чтобы узнать больше о каждой опции интерфейса BitDefender, проведите мышью поверх окна. Соответствующий текст подсказки будет представлен.

bitdefender

Очистить Обновить Ok

События

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

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



- **Сеть**
- **Хранилище**

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

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



Расширенное Администрирование



15. Общие

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

15.1. Консоль

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

BitDefender Интернет Безопасность 2009 - Пробная версия [ОСНОВНОЙ ВИД]

СОСТОЯНИЕ: Есть 5 проблемы, ожидающие решения [ИСПРАВИТЬ]

Консоль | Настройки | Информация

Общие

- Антивирус
- Антиспам (защита от спама)
- Родительский контроль
- Анонимность
- Брандмауэр
- Уязвимости
- Шифрование
- Игровой режим
- Сеть
- Обновление
- Регистрация

Статистика

Проверено файлов:	389
Вылеченные файлы:	0
Обнаружены зараженные файлы:	0
Последнее сканирование:	Никогда
Следующее сканирование:	Никогда

Активность файлов

Обзор

Последнее Обновление: 18.02.2009 15:47

Моя Учетная запись: testare.automata@mailinator.com

Регистрация: Пробная версия

Срок действия ключа: 30 дней

Сетевая активность

Для того чтобы узнать больше о каждой опции интерфейса BitDefender, проведите мышью поверх окна. Соответствующий текст подсказки будет представлен.

bitdefender | [Купить/Обновить](#) - [Моя учетная запись](#) - [Регистрация](#) - [Справка](#) - [Техническая поддержка](#) - [Журнал](#)

Консоль

Консоль состоит из нескольких разделов:

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



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

15.1.1. Статистика

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

Элемент	Описание
Проверено файлов	Отображает количество файлов, которые были проверены на наличие вредоносного кода во время последнего сканирования.
Вылеченные файлы	Отображает количество файлов, которые были вылечены BitDefender во время последнего сканирования.
Обнаружено вирусов	Отображает количество вирусов, которые были найдены во время последнего сканирования.
Блокирование сканирования портов	Число попыток сканирования портов, заблокированных брандмауэром BitDefender. Сканирование портов часто предпринимается хакерами для нахождения открытых портов на вашем компьютере с целью несанкционированного доступа. Рекомендуется держать Брандмауэр и Режим «Невидимка» включенными для защиты от сканирования портов.

15.1.2. Обзор

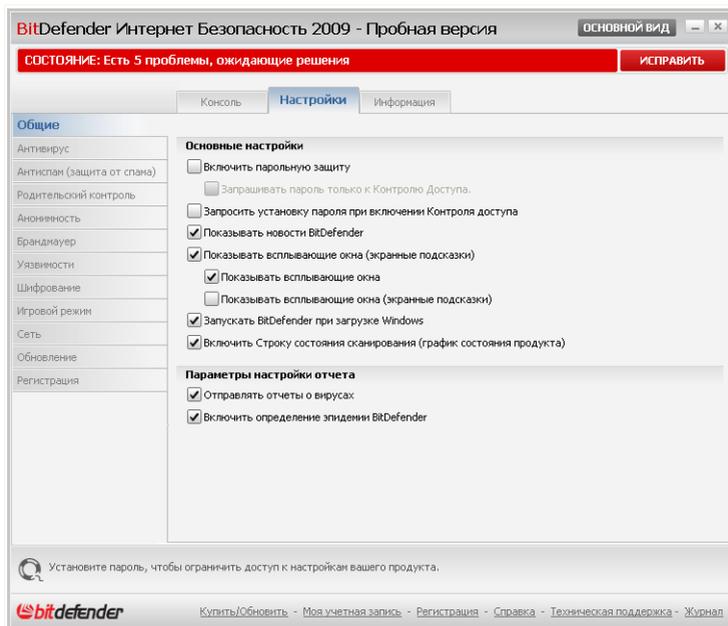
Здесь вы можете видеть краткую статистику о состоянии обновлений, состоянии вашей учетной записи, регистрации и сведениях о лицензии.



Элемент	Описание
Последнее обновление	Отображает дату, когда ваш продукт BitDefender обновлялся в последний раз. Пожалуйста, проводите регулярные обновления, чтобы ваша система была полностью защищенной.
Мой аккаунт	Отображение адреса электронной почты, на который вы можете отправить запрос на получение доступа к вашей оперативной учетной записи для восстановления своего лицензионного ключа BitDefender, а также воспользоваться услугами службы поддержки BitDefender или другими персонализированными услугами.
Регистрация	Отображает тип и состояние вашего лицензионного ключа. Чтобы поддерживать систему в безопасности, настоятельно рекомендуется обновлять BitDefender, если срок действия ключа вышел.
Истечение срока	Число дней до истечения срока действия лицензионного ключа.

15.2. Настройки

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



Основные настройки

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

15.2.1. Основные настройки

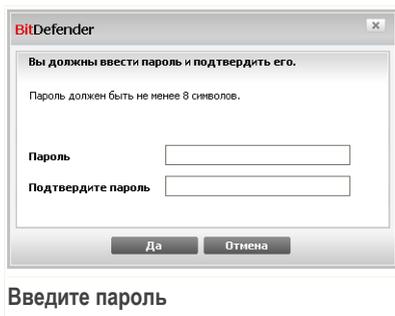
- **Включить защиту паролем настроек программы** - включает защиту паролем конфигурации консоли управления BitDefender.



Замечание

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

Если Вы выбираете эту опцию, появится следующее окно:



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

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

Если вы хотите, чтобы запросы пароля возникали только тогда, когда изменяются настройки модуля Контроль доступа, нужно также выбрать **Запрашивать пароль только к Контролю доступа**. С другой стороны, если пароль был установлен только на Контроль доступа, и Вы не отметили эту опцию, то соответствующий пароль будет запрашиваться при изменении любой опции BitDefender.



Важно

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

- **Запросить установку пароля при включении Контроля доступа** - Запрос на установку пароля при включении Контроля доступа, если пароль не установлен. Установив пароль, вы защитите сконфигурированные вами для определенных пользователей настройки модуля Контроля доступа от изменений другими пользователями, обладающими правами администратора.
- **Показывать новости BitDefender (уведомление на тему безопасности)** - время от времени показывает уведомления относительно новых вирусов, рассылаемые сервером BitDefender.
- **Показывать всплывающие окна** - включает функцию всплывающих окон, отображающих статус программы. Вы можете настроить BitDefender для отображения всплывающих окон только при использовании основного вида или расширенного вида.
- **Запуск BitDefender при загрузке Windows** - BitDefender автоматически запускается при загрузке системы. Мы настоятельно рекомендуем выбрать эту функцию!



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



Замечание

Эта настройка может быть сделана только для текущего пользователя Windows.

15.2.2. Параметры настройки отчета

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

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

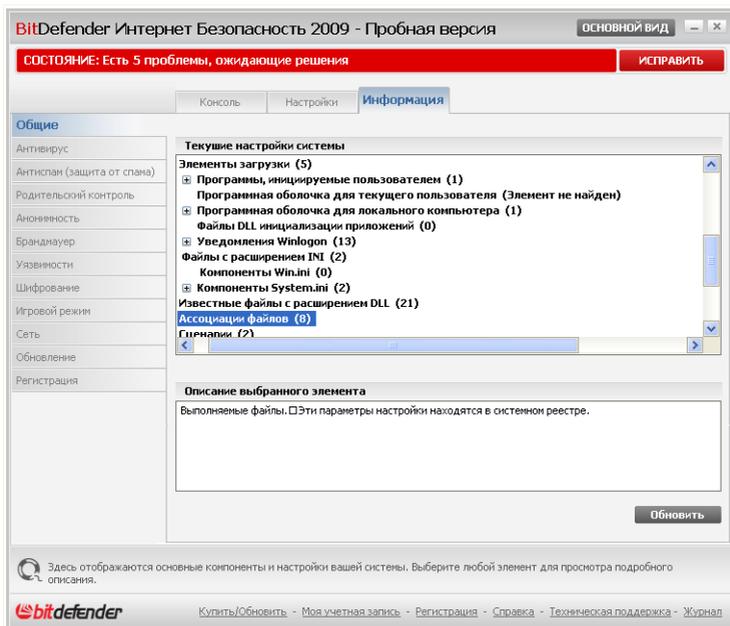
- **Включить функцию BitDefender обнаружения эпидемий** - отправляет в лаборатории BitDefender Labs отчет о потенциальных вирусных эпидемиях.

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

15.3. Системная информация

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

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



Системная информация

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

Три кнопки доступны:

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



Замечание

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

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



16. Антивирус

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

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



Замечание

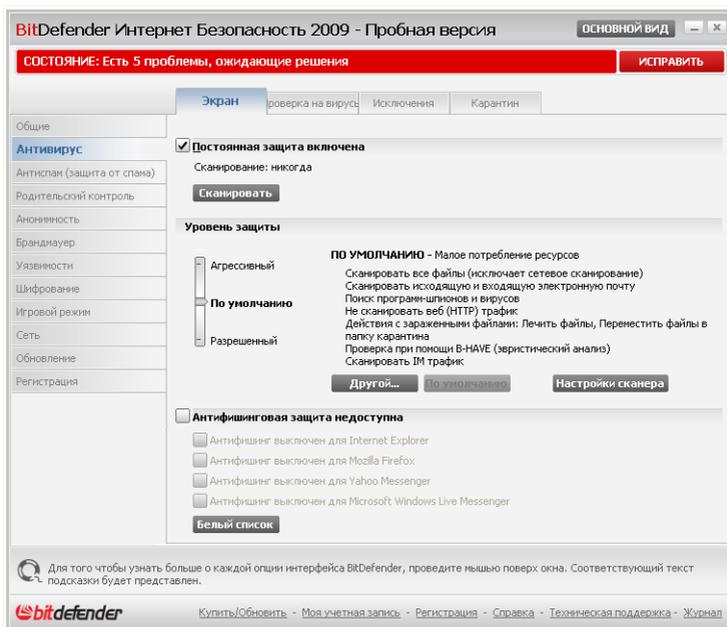
Постоянная защита также называется сканированием на лету - файлы сканируются по мере доступа к ним.

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

16.1. Защита в режиме реального времени

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

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



Защита в режиме реального времени

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



Важно

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

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

16.1.1. Конфигурация уровня защиты

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

Существует 3 уровня защиты:



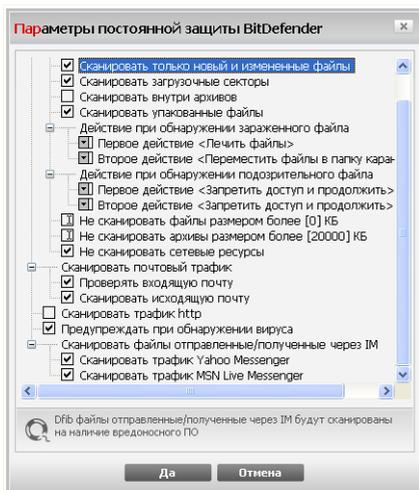
Уровень защиты	Описание
Разрешающий	<p>Выполняет основные процессы безопасности. Потребляет малое количество ресурсов.</p> <p>Программы и входящие электронные сообщения проверяются только на наличие вирусов. Кроме классического сканирования при помощи базы образов, также используется эвристический анализ.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

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

16.1.2. Настройка уровня защиты

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

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



Настройки защиты

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



Замечание

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

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

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



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



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

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



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

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

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

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

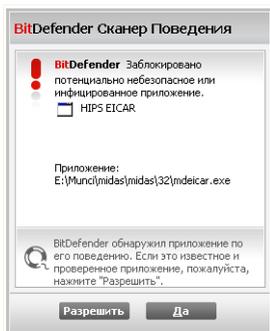
- **Сканирование файлов, полученных через интернет-пейджеры.** Для сканирования файлов, полученных или отправленных программами Yahoo Messenger или Windows Live Messenger, установите соответствующие флажки.

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

16.1.3. Настройка Сканера поведения

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

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

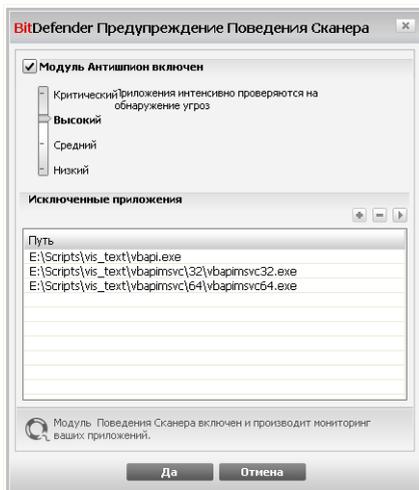


Уведомления Режимного сканера

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

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

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



Настройки Режимного Сканирования

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



Важно

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

Настройка уровня защиты

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



Замечание

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

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

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

Управление исключенными приложениями

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

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

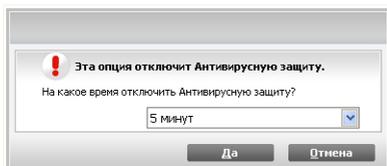
- **Add** - exclude a new application from scanning.
- **Remove** - remove an application from the list.



- Edit - edit an application path.

16.1.4. Отключение постоянной защиты

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



Включенная постоянная защита

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



Внимание

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

16.1.5. Настройка антифишинговой защиты

BitDefender обеспечивает постоянную антифишинговую защиту для следующих приложений:

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

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

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



Белый список антифишинга

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

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



Замечание

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

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

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

16.2. Сканирование по требованию

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



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

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

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

BitDefender Интернет Безопасность 2009 - Пробная версия

основной вид

СОСТОЯНИЕ: Есть 5 проблемы, ожидающие решения

ИСПРАВИТЬ

Экран **Проверка на вирусы** Исключения Карантин

Общие

Антивирус

Антиспам (защита от спама)

Родительский контроль

Анонимность

Брандауэр

Уязвимости

Шифрование

Игровой режим

Сеть

Обновления

Регистрация

Системные задачи

Экстра сканирование
Последний запуск: 18.02.2009 16:07:28

Сканирование
Последний запуск: Никогда

Быстрая проверка системы
Последний запуск: Никогда

Autologon Scan
Последний запуск: 09.05.2008 19:16:42

Задачи пользователя

Мои Документы
Последний запуск: Никогда

Прочие задачи

Контекстное сканирование

Обнаружение устройств

Новое задание Запустить

Нажмите чтобы назначить новое задание, по вашим требованиям.

bitdefender

Купить/Обновить - Моя учетная запись - Регистрация - Справка - Техническая поддержка - Журнал

Задачи сканирования

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



16.2.1. Задачи сканирования

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

У каждого задания есть окно **Свойства**, позволяющее Вам настроить данное задание и просматривать результаты его работы. Более подробную информацию можно найти здесь: *«Настройка задач проверки»* (р. 148).

Существует три категории задач сканирования:

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

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



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



Замечание

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

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

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

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

Справа от каждой задачи доступны три кнопки:

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



Замечание

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

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

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

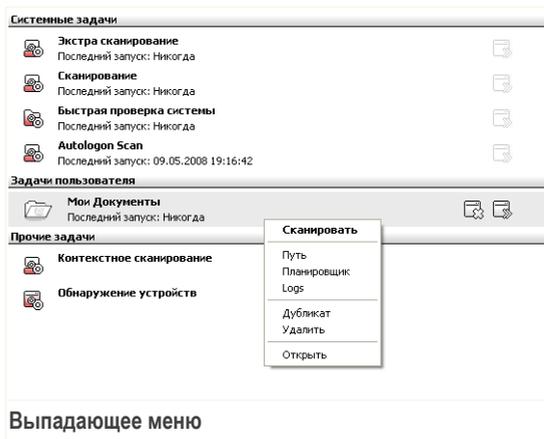


16.2.2. Использование Выпадающего меню

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

В выпадающем меню имеются следующие команды:

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



Замечание

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

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



Замечание

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

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



Замечание

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

16.2.3. Создание задач сканирования

Создать задачу сканирования, используя один из следующих способов:

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

16.2.4. Настройка задач проверки

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

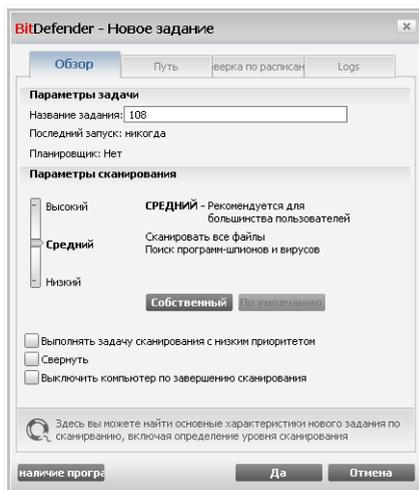


Замечание

Чтобы получить больше информации, просмотрите журналы и таблицу **Журналы**, обратитесь к *«Просмотр журнала проверок»* (р. 168).

Конфигурация настроек сканирования

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



Обзор

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

Выбор уровня проверки

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

Существует 3 уровня проверки:

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



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

Имеется ряд общих настроек для процесса проверки:

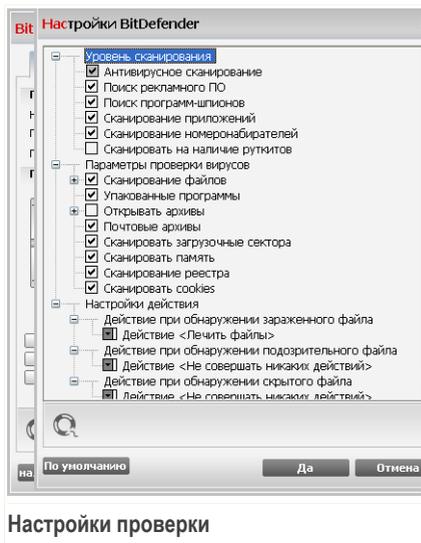
- **Выполнить задачу с низким приоритетом.** Уменьшается приоритет процесса проверки. Таким способом Вы ускоряете работу других программ, но увеличиваете время, необходимое для завершения процесса проверки.
- **Свернуть окно проверки в панель задач при запуске.** Окно проверки свертывается в **системный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

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

Настройка уровня проверки

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

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



Настройки проверки

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

Настройки проверки разделены на 3 категории:

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

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



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

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

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



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

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



Замечание

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

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



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

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

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



Замечание

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

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



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

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

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



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

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

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

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

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



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



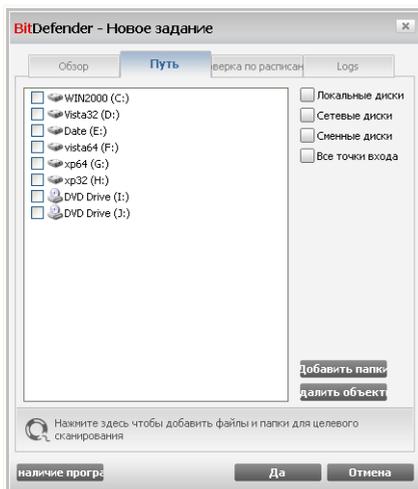
Замечание

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

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

Настройка сканирования

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



Поиск цели



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

В этом разделе находятся следующие кнопки:

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



Замечание

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

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



Замечание

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

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

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



Замечание

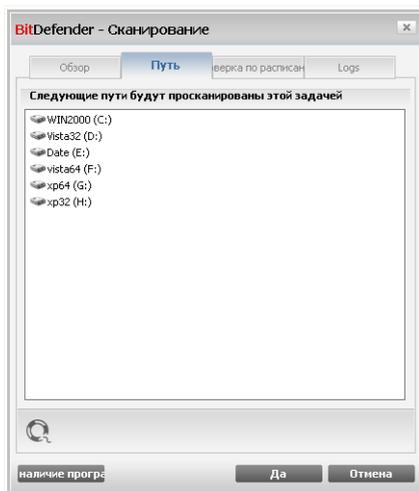
Если Вы хотите проверить на наличие вирусов весь компьютер, поставьте значок в поле **Все объекты**.

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

Просмотр цели сканирования системных задач

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

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



Цель сканирования из задачи "Полное сканирование системы"

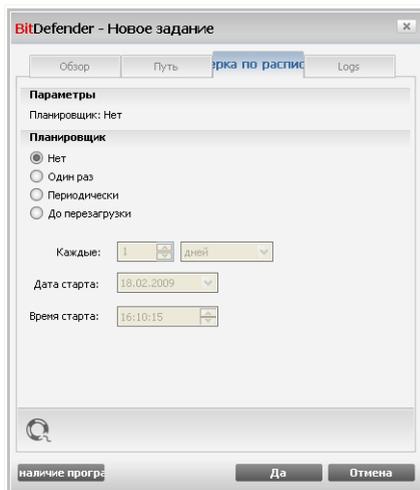
Полное сканирование системы и **Глубокое сканирование системы** просканирует все локальные диски, в то время как **Быстрое сканирование системы** просканирует только папки Windows и Program Files.

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

Планирование задач сканирования

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

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



Проверка по расписанию

Вы можете просмотреть запланированные задачи, если такие есть.

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

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

Если Вы хотите повторять процесс проверки через определенные интервалы времени, выберите **Периодически** и в поле **Каждые** введите число минут/часов/дней/недель/месяцев/лет, соответствующих необходимому интервалу. Также необходимо указать дату и время первого запуска в полях **Дата/Время запуска**.

- **До перезагрузки** - запуск сканирования спустя заданное количество минут после того, как пользователь вошел в систему.



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

16.2.5. Сканирование объектов

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



Замечание

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

Методы сканирования

BitDefender имеет четыре типа сканирования по требованию:

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

Немедленная проверка

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

Чтобы запустить задачу сканирования, используйте один из следующих методов:

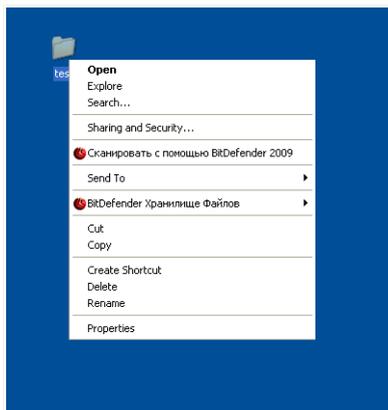
- дважды щелкните на нужной задаче в списке.
- нажмите  **Проверить сейчас** для выполнения задачи.
- выберите задачу и нажмите **Запустить задачу**.



Появится Сканер BitDefender и начнется сканирование. Больше информации найдете «Сканер BitDefender» (р. 164).

Проверка через контекстное меню

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



Контекстное сканирование

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

Появится Сканер BitDefender и начнется сканирование. Больше информации найдете «Сканер BitDefender» (р. 164).

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

Проверка перетаскиванием

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



Тяните Файл



Переместите файл

Появится Сканер BitDefender и начнется сканирование. Больше информации найдете *«Сканер BitDefender»* (р. 164).

Ручное сканирование

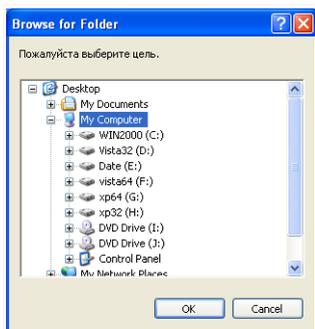
Проверка вручную состоит в том, чтобы непосредственно выбрать объект проверки при помощи опции Ручная проверка BitDefender в группе задач BitDefender в меню Пуск.



Замечание

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

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



Ручное сканирование

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

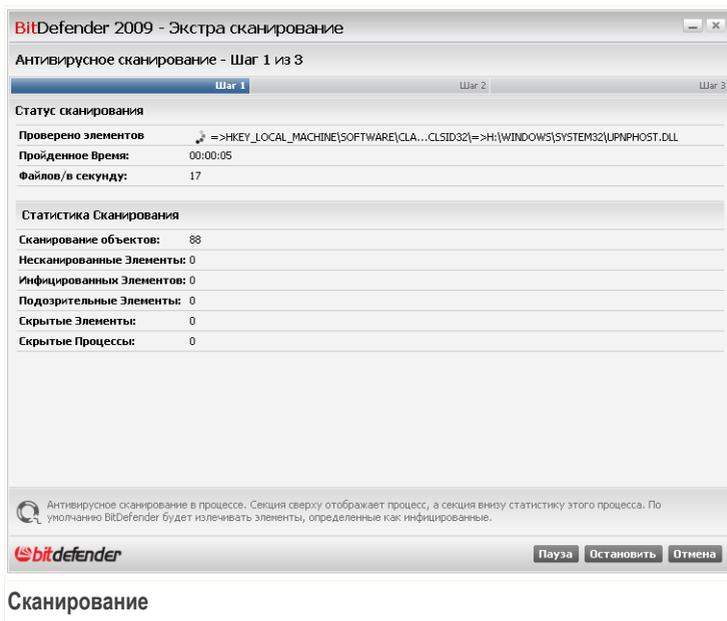
Появится Сканер BitDefender и начнется сканирование. Больше информации найдете «Сканер BitDefender» (р. 164).

Сканер BitDefender

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

Шаг 1/3 - Сканирование

BitDefender начнет проверку выбранных объектов.



The screenshot shows the BitDefender 2009 - Экстра сканирование window. The title bar reads "BitDefender 2009 - Экстра сканирование". The main content area is titled "Антивирусное сканирование - Шаг 1 из 3". Below this, there are three tabs: "Шаг 1", "Шаг 2", and "Шаг 3", with "Шаг 1" selected. The "Статус сканирования" section shows "Проверено элементов" as 88, "Пройденое Время:" as 00:00:05, and "Файлов/в секунду:" as 17. The "Статистика Сканирования" section lists: "Сканирование объектов:" 88, "Несканированные Элементы:" 0, "Инфицированных Элементов:" 0, "Подозрительные Элементы:" 0, "Скрытые Элементы:" 0, and "Скрытые Процессы:" 0. At the bottom, there is a "bitdefender" logo and three buttons: "Пауза", "Остановить", and "Отмена".

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



Замечание

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

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

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

Дождитесь окончания сканирования BitDefender

Шаг 2/3 - Выберите Действия

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



BitDefender 2009 - 1459

Антивирусное сканирование - Шаг 2 из 3

Шаг 1 | **Шаг 2** | Шаг 3

Результаты

1 угроза(ы), которые влияют на 1 объекта(ов), требуют вашего внимания [Не совершать никаких...](#)

EICAR-Test-File (not a virus)	осталась 1 проблема (не удалось вылечить)	Не совершать никаких...
-------------------------------	--	---

Решенные проблемы насчитывают: 1

Путь файла	Имя угрозы	Результат действия
H:\Documents and Setting...\Desktop\av_testbed\3.vir	Win32.Parte.C	Вылечено

Действие, которое было предпринято BitDefender против обнаруженной угрозы

[Продолжить](#)

Действия

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

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

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

Доступны следующие варианты:

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



Действие	Описание
Раскрыть	Сделать скрытые объекты видимыми.

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

Шаг 3/3 - Просмотр результатов

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

BitDefender 2009 - 1459

Антивирусное сканирование - Шаг 3 из 3

	Шаг 1	Шаг 2	Шаг 3
Результаты			
Решенные Объекты:	1		
Нерешенные Объекты:	1		
Объекты, защищенные паролем:	0		
Пропущенные элементы:	0		
Невыполненные элементы:	1		

1 файл не может быть очищен, соответственно, Ваша система остается зараженной. Подробнее: www.bitdefender.com.ua

Количество элементов, сканирование которых не может быть выполнено

Показать файл отчета Заккрыть

Резюме

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



Важно

Если потребуется, перезагрузите Вашу систему для завершения процесса очистки.

Нажмите **Заккрыть**, чтобы закрыть окно.



BitDefender не может исправить некоторые проблемы

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

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

Обнаруженные BitDefender подозрительные файлы

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

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

16.2.6. Просмотр журнала проверок

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



Журнал отчета



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

Доступны две кнопки:

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



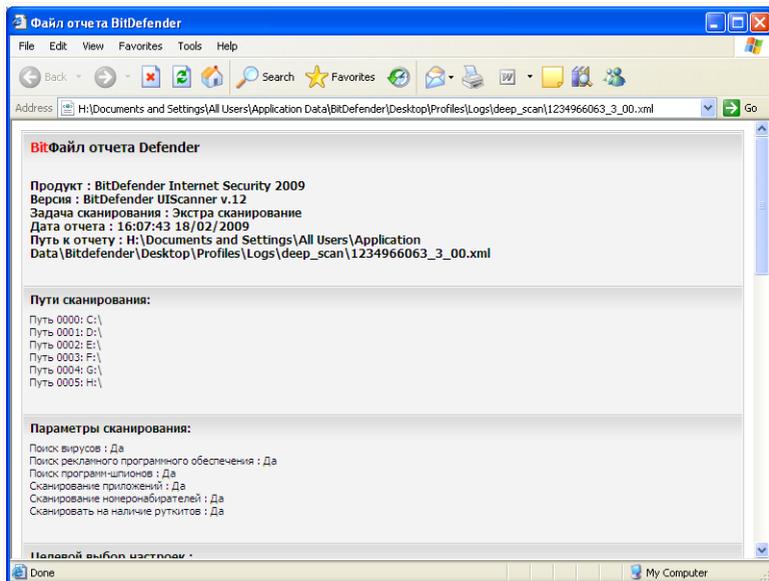
Замечание

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

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

Пример отчета проверок

Следующий рисунок представляет собой пример файла отчета сканирования:



Пример отчета проверки

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

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

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

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

Два типа объектов могут быть исключены из сканирования:



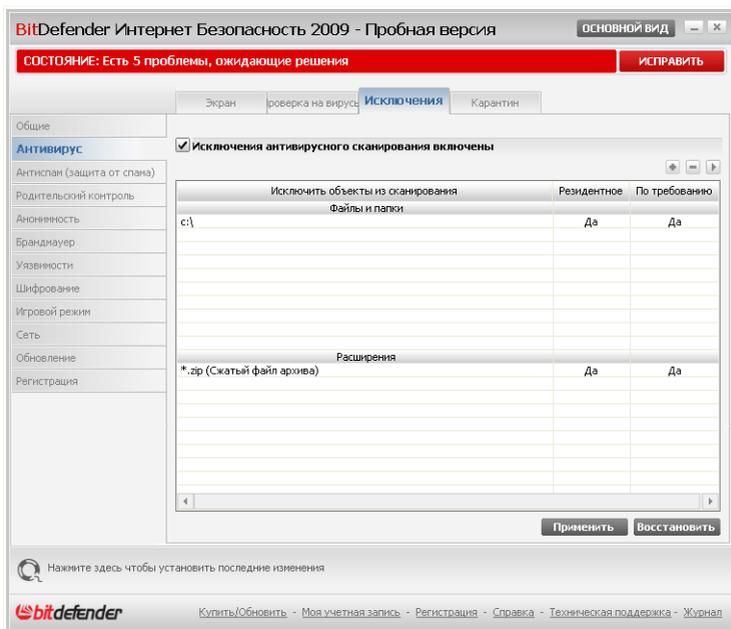
- **Пути** - файл или папка (включая все объекты, которые она содержит), обозначенные путем в системе, которые будут исключены из проверки.
- **Расширения** - все файлы, имеющие определенное расширение будут исключены из просмотра.



Замечание

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

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



Исключения

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



Замечание

Указанные здесь исключения НЕ распространяются на контекстную проверку.

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

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



Замечание

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

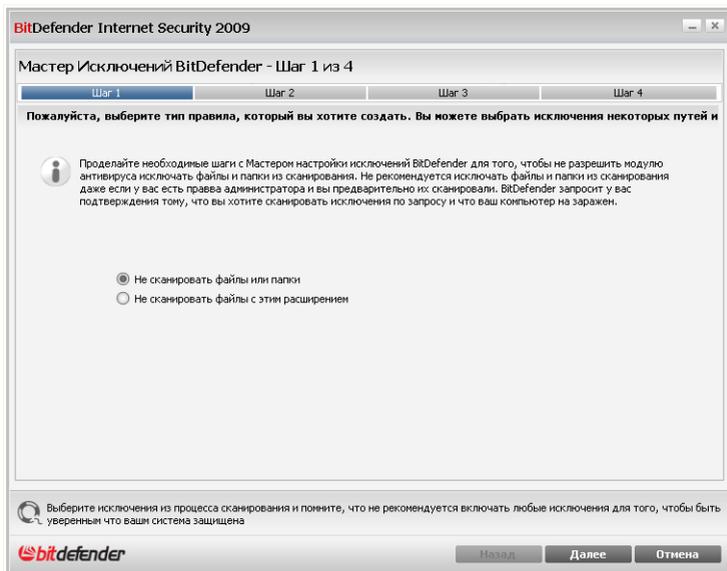
Вы можете нажать на **Сброс** вернув изменения сделанные к правилам, при условии, Вы не сохранили их нажав **Применить**.

16.3.1. Исключение путей для сканирования

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



Шаг 1/4 - Выберите тип объекта



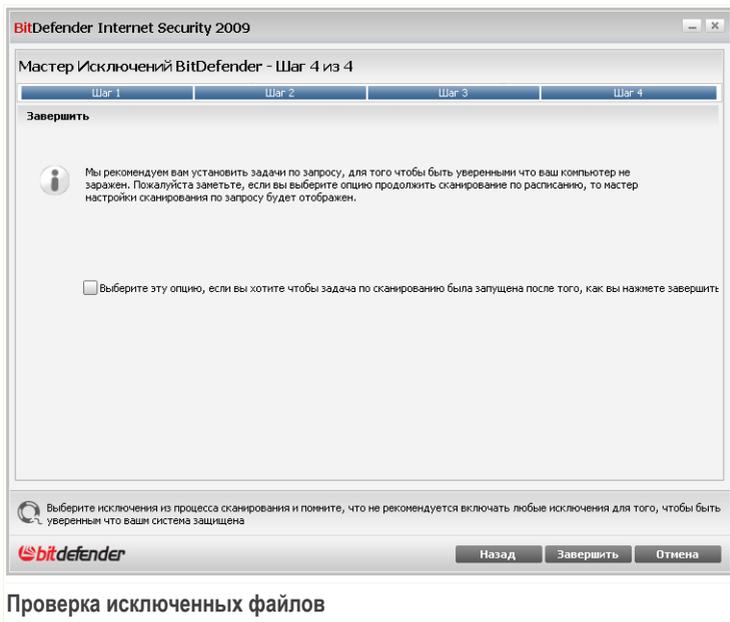
Тип объекта

Выберите опцию для исключения пути из сканирования.

Щелкните по кнопке **Далее**.



Шаг 4/4 - Проверьте исключенные файлы



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

Щелкните мышкой на кнопке **Завершить**.

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

16.3.2. Исключение расширений из сканирования

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



Шаг 1/4 - Выберите тип объекта

BitDefender Internet Security 2009

Мастер Исключений BitDefender - Шаг 1 из 4

Шаг 1 Шаг 2 Шаг 3 Шаг 4

Пожалуйста, выберите тип правила, который вы хотите создать. Вы можете выбрать исключения некоторых путей и

 Проведите необходимые шаги с Мастером настроек исключений BitDefender для того, чтобы не разрешить модулю антивируса исключать файлы и папки из сканирования. Не рекомендуется исключать файлы и папки из сканирования даже если у вас есть права администратора и вы предварительно их сканировали. BitDefender запросит у вас подтверждения тому, что вы хотите сканировать исключения по запросу и что ваш компьютер не заражен.

Не сканировать файлы или папки

Не сканировать файлы с этим расширением

 Выберите исключения из процесса сканирования и помните, что не рекомендуется включать любые исключения для того, чтобы быть уверенным что ваша система защищена



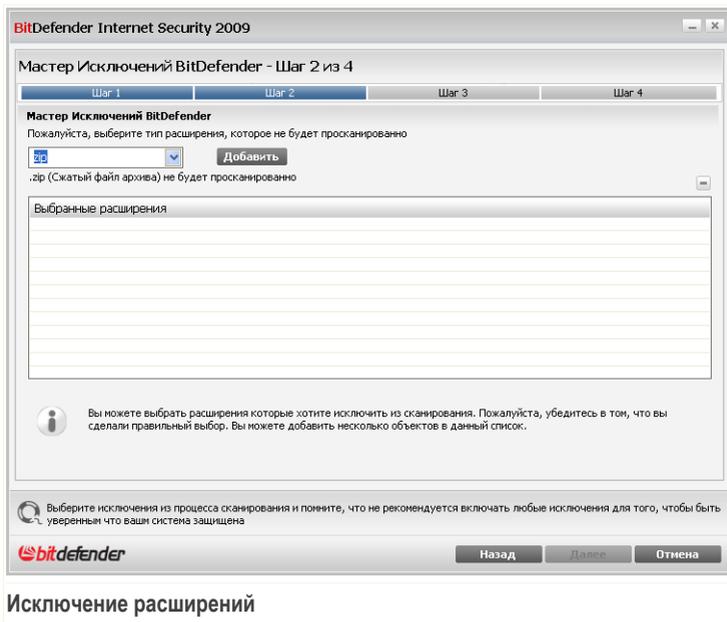
Тип объекта

Выберите опцию, которая исключает расширение из сканирования.

Щелкните по кнопке **Далее**.



Шаг 2/4 - Задайте расширения, которые необходимо исключить



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

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



Замечание

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

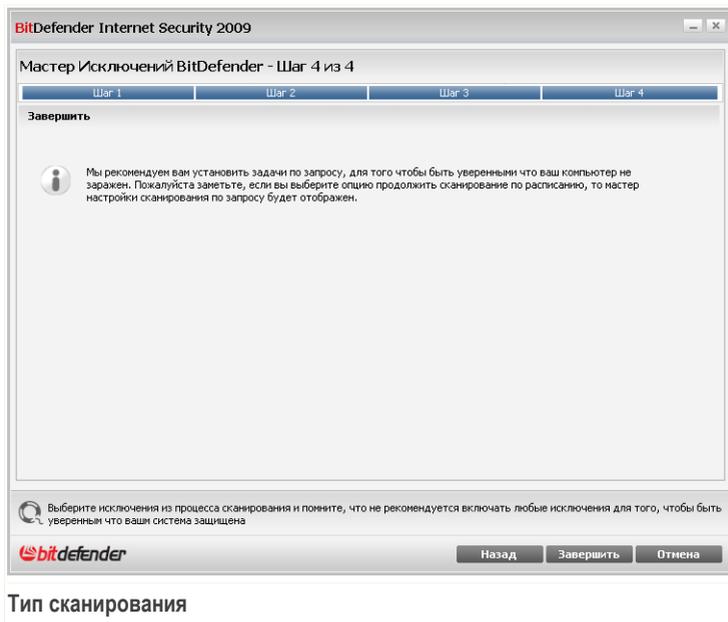
- Тип расширения, которое должно быть исключено из сканирования, в редактирующей области и нажмите **Добавить**.

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

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



Шаг 4/4 - Выберите тип проверки



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

Щелкните мышкой на кнопке **Завершить**.

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

16.4. Область Карантина

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

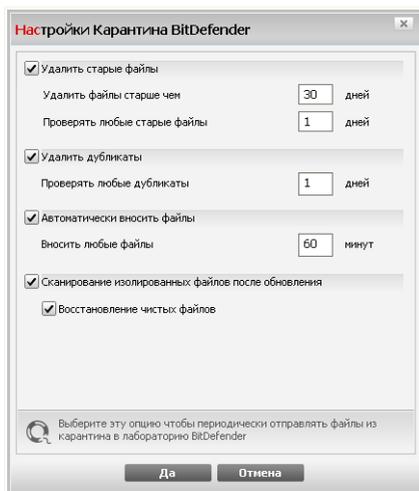
Перейдите к разделу **Антивирус>Карантин** в окне расширенного вида, чтобы просмотреть и выполнить действия над файлами в карантине, а также настроить параметры карантина.



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

16.4.2. Конфигурация настроек Карантина

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



Настройки Карантина

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

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



Замечание

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



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



Замечание

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

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



Замечание

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

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

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



17. Антиспам (защита от спама)

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

17.1. Знакомство с антиспамом

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

17.1.1. Антиспам-фильтры

Механизм BitDefender Антиспам состоит из нескольких различных фильтров, надежно защищающих папку Входящие вашего почтового ящика от спама: [Список друзей](#), [Список спамеров](#), [Фильтр символов](#), [Фильтр изображений](#), [Фильтр URL](#), [NeuNet](#) (эвристический) фильтр и [Байесовский фильтр](#).



Замечание

Вы можете включить/отключить каждый из фильтров Антиспам в разделе [Настройки](#) модуля **Антиспам**.

Список друзей / спамеров

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)."

Списками друзей / спамеров можно управлять из окна [Расширенного вида](#) или с [Панели инструментов Bitdefender Антиспам](#), встроенной в некоторые из наиболее популярных почтовых клиентов.



Замечание

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

Фильтр символов

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

Фильтр изображений

Поскольку спам-сообщениям становится все сложнее избежать распознавания с 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

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

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

NeuNet (эвристический) фильтр

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

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



Замечание

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

Байесовский фильтр

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

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

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



Важно

Модуль Байесовский фильтр можно скорректировать, используя кнопки **Спам** и **Не спам** из **Панели инструментов Антиспама**.



Замечание

Каждый раз, когда Вы выполняете обновление:

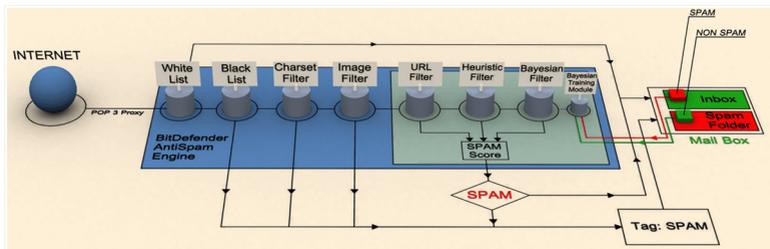
- новые образы изображения будут добавляться в **Фильтр изображения**;
- новые ссылки будут добавляться в **Фильтр URL**;
- новые правила будут добавляться в **Нейросетевой (эвристический) фильтр**;

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



17.1.2. Описание антиспама

На этой схеме показано, как работает BitDefender Антиспам.



Описание антиспама

Представленные на этой схеме антиспам-фильтры (**Список друзей**, **Список спамеров**, **Фильтр символов**, **Фильтр изображения**, **Фильтр URL**, **NeuNet (эвристический) фильтр** и **Байесовский фильтр**) совместно используются модулем Bitdefender Антиспам для того, чтобы определить, следует ли направить часть электронной почты в папку **Входящие**.

Каждое сообщение, получаемое из интернета, сначала проверяется на наличие адресата в **Списке друзей** и **Списке спамеров**. Если адрес отправителя найден в **Списке друзей**, сообщение перемещается непосредственно в папку **Входящие**.

В противном случае сообщение будет проверено с помощью фильтра **Список спамеров** на наличие данного электронного адреса. Если адресат найден в списке, такие письма помечаются как СПАМ и перемещаются в папку **Спам** (в приложении **Microsoft Outlook**).

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

Также, с помощью **Фильтра символов** отсеиваются письма, написанные кириллицей или иероглифами. Такие письма помечаются как СПАМ и перемещаются в папку Спам. Письма, написанные в другой кодировке, 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 Спам. В случае совпадения письмо добавляется к Спаму.



Замечание

Письма категории “ОТКРОВЕННО СЕКСУАЛЬНО” 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 списку.

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.

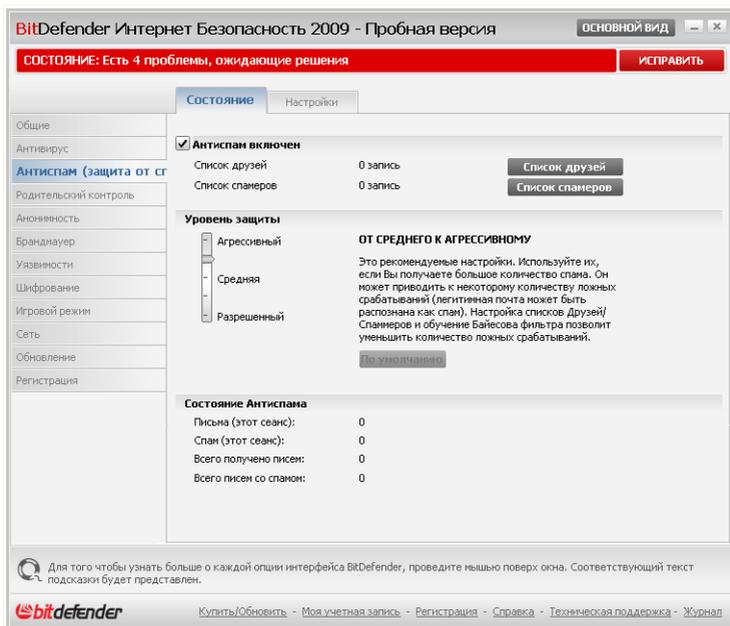


Важно

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.

17.2. Состояние

Чтобы настроить защиту при помощи модуля Антиспам, перейдите в раздел **Антиспам>Состояние** в окне расширенного вида.



Состояние Антиспама

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



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.

17.2.1. Настройка уровня защиты

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

Существует 5 уровней защиты:



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

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



17.2.2. Настройка списка друзей

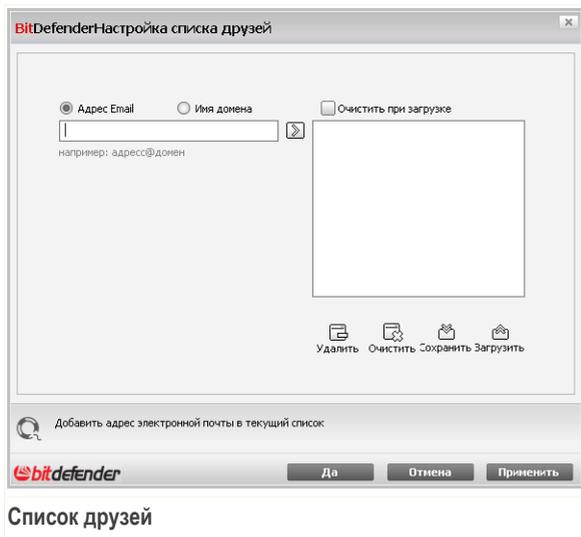
Список друзей список адресов электронной почты, с которых Вы хотите получать письма независимо от их содержания. Сообщения от друзей не помечаются как Спам, даже если их содержание соответствует определению Спاما.



Замечание

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

Для настройки списка друзей нажмите **Список друзей** (или нажмите кнопку **Друзья** на **Панели инструментов Антиспам**).



Список друзей

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

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 .bw1.

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 **Список друзей**. BitDefender пропускает сообщения от адресатов из этого списка. Таким образом, Вы будете уверены, что получите ожидаемые письма.

Щелкните мышкой на кнопке **Применить** и **ОК** чтобы сохранить и закрыть **список друзей**.

17.2.3. Настройка списка спамеров

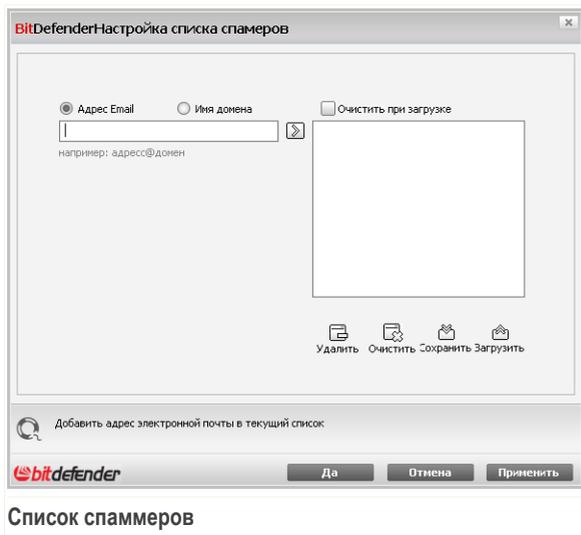
Список спамеров is список адресов электронной почты, с которых Вы не хотите получать письма, независимо от их содержания.



Замечание

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

Для настройки списка спамеров нажмите **Список спамеров** (или нажмите кнопку **Спамеры** на **Панели инструментов Антиспам**).



Список спамеров

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 спамеров**.



Важно

Имя домена должно иметь следующий вид:

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



Чтобы 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**.

Щелкните мышкой на кнопке **Применить** и **ОК** чтобы сохранить и закрыть **список спамеров**.

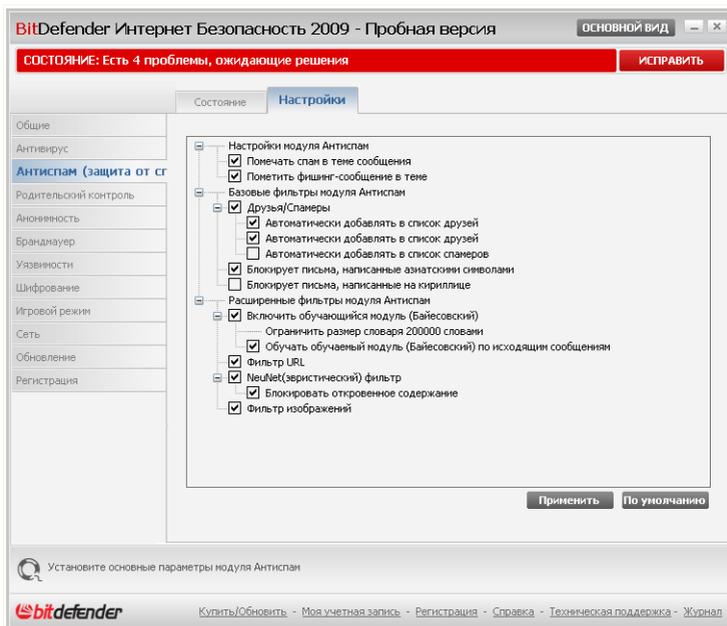


Важно

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

17.3. Настройки

Чтобы настроить параметры и фильтры модуля Антиспам, перейдите в раздел **Антиспам>Настройки** в окне расширенного вида.



Настройки Антиспама

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

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

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

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



17.3.1. Настройки Антиспама

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

17.3.2. Базовые фильтры Антиспама

- **Список друзей/спамеров** - фильтрация электронных сообщений с помощью **Списка друзей/спамеров**.
 - **Автоматически добавлять получателей в список друзей** - добавляет получателей в Список друзей.
 - **Автоматически добавлять в список друзей** - при нажатии кнопки  **Не спам** на **Панели инструментов Антиспам** отправитель выделенного сообщения будет автоматически добавлен в Список друзей.
 - **Автоматически добавлять в список спамеров** - при нажатии кнопки  **Спам** на **Панели инструментов Антиспам** отправитель выделенного сообщения будет автоматически добавлен в Список спамеров.



Замечание

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

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

17.3.3. Дополнительные фильтры Антиспама

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



Замечание

Мы рекомендуем размер словаря в 200 000 слов.

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



18. Родительский контроль

Родительский контроль доступа BitDefender позволяет контролировать доступ к интернету и определенным приложениям для каждого пользователя, имеющего учетную запись на этой системе.

В модуле контроля доступа можно настроить блокировку:

- неприемлемые веб-страницы.
- Доступа в интернет в определенные промежутки времени (например, когда время уроков).
- Веб-страниц, электронных сообщений и мгновенных сообщений, если они содержат определенные слова.
- приложения, такие как игры, чаты, программы обмена файлами и другие.
- Мгновенных сообщений, отправленных заблокированными контактами интернет-пейджеров.



Важно

Только пользователя с правами администратора в системе (системные администраторы) могут получать доступ для настройки Контроля доступа. Чтобы быть уверенным в том, что только вы можете менять настройки Контроля доступа для любого пользователя, мы рекомендуем защитить эти настройки паролем. При включении Контроля доступа для определенного пользователя вам будет предложено установить пароль.

Для успешного использования Контроля с целью для ограничения доступа ваших детей к компьютеру и интернету необходимо выполнить описанную ниже процедуру.

1. Создайте ограниченные (стандартные) учетные записи Windows для своих детей.



Замечание

Чтобы научиться создавать учетные записи Windows, откройте центр справки и поддержки Windows (в меню Пуск нажмите **Справка и поддержка**).

2. Настройте Контроль доступа для учетной записи Windows, которой пользуются ваши дети.



18.1. Состояние настройки для каждого пользователя

Чтобы настроить Контроль доступа для отдельно взятого пользователя, дважды щелкните на имени соответствующего пользователя, затем щелкните на вкладке **Состояние**.

Предупреждение Контроля доступа BitDefender

Состояние WWW Приложения Слова IM Трафик Время в сети

Сохранение настроек для пользователя amigea

Контроль доступа включен

Веб-контроль включен IM-контроль включен

Контроль приложений включен

Ограничитель времени в сети отключен

Доступ к Интернету разблокирован

Фильтр ключевых слов неактивен

Эвристический веб-фильтр включен

Понимание эвристического веб-фильтра

Взрослый Взрослый - Без ограничений
Рекомендуется для взрослых пользователей.
Отображаются все страницы, независимо от их содержания.

Подросток

Ребенок

По умолчанию

Нажмите, чтобы восстановить Эвристический Веб-Фильтр для подростков. Это уровень защиты по умолчанию.

Закрыть

Суммарный статус модуля Контроля доступа

Чтобы настроить Контроль доступа для данной учетной записи, используйте следующую процедуру:

1. Включите Контроль доступа для данной учетной записи, установив флажок рядом с параметром **Родительский доступ**.



Важно

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



2. Установите пароль для защиты параметров Контроля доступа. Более подробные сведения см. в разделе *«Защита настроек Контроля доступа»* (р. 201).
3. Поставьте флажок рядом с элементами управления защитой, которыми вы хотите воспользоваться:
 - **Веб контроль** - фильтрация веб-страниц согласно правил, установленных вами в разделе **Веб**.
 - **Контроль приложений** - блокирование доступа к приложениям, указанным вами в разделе **Приложения**.
 - **Контроль приложений оперативной пересылки сообщений** - позволяет разрешать или блокировать беседы посредством интернет-пейджеров согласно правил, установленных вами в разделе **IM Трафик**.
 - **Ограничитель времени в сети** - обеспечение доступа в веб согласно расписания, установленного вами в разделе **Время в сети**.
 - **Доступ к Интернету** - блокировка доступа ко всем веб-сайтам (не только к тем, которые указаны в разделе **Веб**).
 - **Фильтрация ключевых слов** - фильтрация доступа к веб-страницам, электронной почте и интернет-пейджерам согласно правил, установленных вами в разделе **Слова**.
 - **Эвристический веб фильтр** - блокировка доступа в веб согласно ранее установленным правилам, основанным на возрастных категориях.
4. В полной мере воспользоваться всеми преимуществами модуля Контроль доступа можно только, если Вы настроили следующие опции. Для того, чтобы узнать, как их настроить, обратитесь к следующим темам этой главы.

18.1.1. Защита настроек Контроля доступа

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

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



BitDefender Контроль Доступа - Пароль

Чтобы только Вы могли изменять настройки модуля Контроль доступа, мы рекомендуем защитить его паролем. По умолчанию, только данный модуль будет под паролем, но Вы можете защитить и другие модули, изменив настройки в окне *Дополнительные Настройки*.

Вы хотите установить пароль сейчас?

Пароль

Подтвердите пароль

Пароль должен быть не менее 8 символов длиной.

Не запрашивать пароль, когда включается Контроль Доступа.



Установить парольную защиту

Для того, чтобы установить парольную защиту, сделайте следующее:

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

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



Замечание

Этот пароль не защитит другие настройки BitDefender.

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



18.1.2. Конфигурация эвристического веб фильтра

Эвристический веб фильтр анализирует веб страницы и блокирует те из них, которые соответствуют шаблонам страниц с потенциально неадекватным содержанием.

Для того, чтобы ограничивать доступ к веб-ресурсам с помощью предустановленных установок на основе возраста пользователя, Вы должны выбрать соответствующий уровень толерантности. Перемещайте ползунок по шкале, чтобы выставить уровень толерантности, адекватный на Ваш взгляд для данного пользователя.

Существует 3 «уровня толерантности»

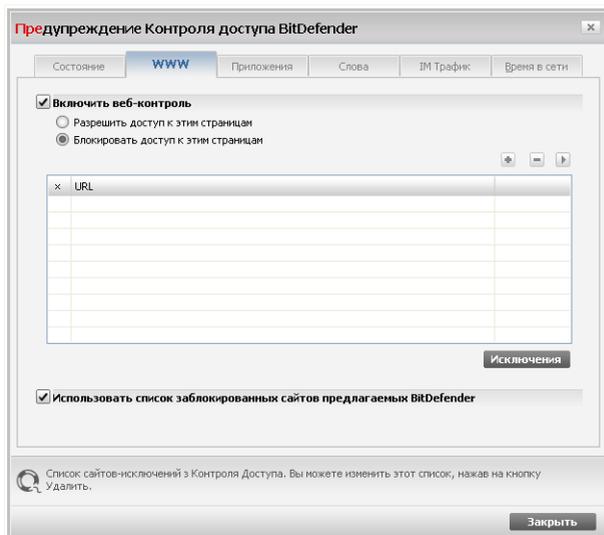
Чувствительность	Описание
Ребенок	Предполагает ограниченный доступ в интернет, рекомендуется для пользователей в возрасте до 14 лет. Блокируются веб-страницы с потенциально вредным для детей содержанием (порнография, сексуальность, наркотики, хакерство и т.п).
Подросток	Предполагает ограниченный доступ 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 **По умолчанию**, чтобы установить слайдер в уровень по умолчанию.

18.2. 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 настроить Веб-контроль для отдельно взятого пользователя, дважды щелкните на имени соответствующего пользователя, затем щелкните на вкладке **Веб**.



Веб контроль

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

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.

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



18.2.1. Мастер Конфигурации

Мастер конфигурации позволяет выполнить одноэтапную процедуру.

Шаг 1/1 - Укажите веб-сайты

BitDefender - Мастер настройки сайтов

Введите URL

Вы можете ввести адреса конкретной веб-страницы, или универсальные шаблоны адресов.
Например, Вы можете блокировать все адреса, которые содержат слово 'cigars', вводя слово *cigars* в соответствующее поле.

Закончить Отмена

Укажите веб-сайты

Введите веб-сайты, для которых будет применяться правило, затем нажмите **Закончить**.



Важно

Имя домена должно иметь следующий вид:

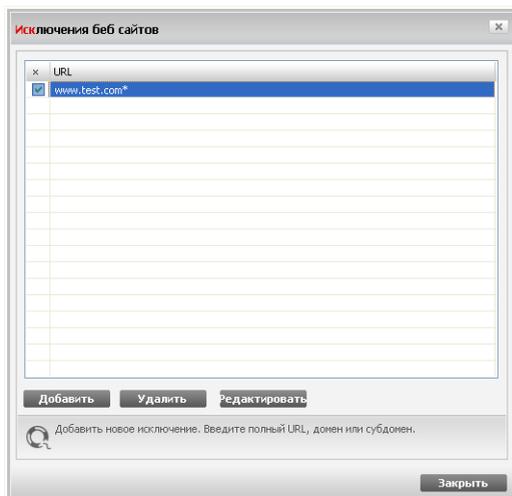
- *.xxx.com - действие правила будет распространяться на все веб-сайты, оканчивающиеся на .xxx.com;
- *porn* - действие правила будет распространяться на все веб-сайты, адрес которых содержит porn;
- www.*.com - действие правила будет распространяться на все веб-сайты с доменным окончанием com;
- www.xxx.* - действие правила будет распространяться на все веб-сайты, адрес которых начинается с www.xxx., независимо от доменного окончания.



18.2.2. 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:



Определение исключений

Нажмите **Добавить...**, чтобы указать исключения. Появится **мастер настройки**. Завершите все шаги мастера, чтобы установить исключения.

Чтобы удалить правило, выберите его и щелкните мышкой на **Удалить**. Чтобы изменить правило, выберите его и щелкните мышкой на **Редактировать** или дважды щелкните на этой опции. Чтобы временно заблокировать действие правила, не удаляя его, уберите галочку в соответствующем поле.

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



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

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

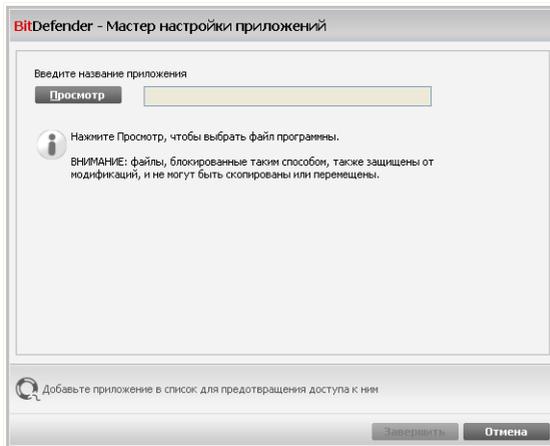
Чтобы удалить правило, выберите его и нажмите кнопку **Удалить**. Чтобы изменить правило, выберите его и нажмите кнопку **Редактировать...** или дважды нажмите на правило. Чтобы временно отключить правило, не удаляя его, уберите галочку из соответствующего поля.

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

18.3.1. Мастер Конфигурации

Мастер конфигурации позволяет выполнить одноэтапную процедуру.

Шаг 1/1 - Выбор приложения для блокировки



Выберите приложение для блокировки

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



18.4. Фильтр ключевых слов

Функция фильтрации ключевых слов позволяет блокировать доступ пользователей к сообщениям электронной почты, веб-страницам и мгновенным сообщениям, которые содержат заданные слова. С помощью фильтрации ключевых слов можно предотвращать просмотр вашими детьми неподобающих слова или фраз, когда они находятся в сети.



Замечание

Фильтрация ключевых слов для мгновенных сообщений доступна только для приложений Yahoo Messenger и Windows Live (MSN) Messenger.

Чтобы настроить функцию фильтрации ключевых слов для отдельно взятого пользователя, дважды щелкните на имени соответствующего пользователя, затем щелкните на вкладке **Слова**.

Предупреждение Контроля доступа BitDefender

Состояние WWW Приложения **Слова** IM Трафик Время в сети

Включить фильтрацию ключевых слов
Блокирование веб-страниц и электронных сообщений, содержащих эти слова.

Слово	HTTP	POP3	IM	Соответствует цел...
test	Да	Нет	Нет	Да

Список ключевых слов по которым блокируются веб-страницы или e-mail.

Заккрыть

Фильтр ключевых слов

Установите флажок рядом с параметром **Включить фильтрацию ключевых слов**, если вы хотите использовать эту функцию.



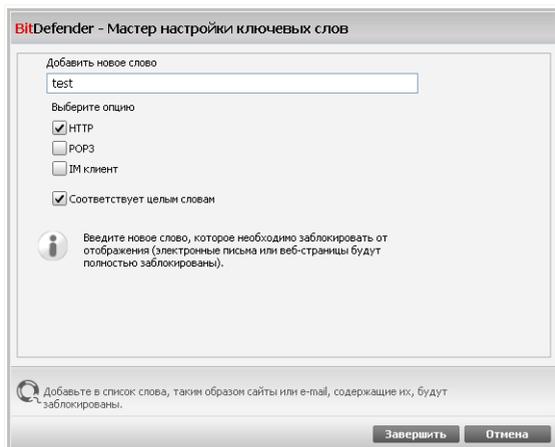
Вы должны добавить правила, чтобы определить, какие ключевые слова нужно блокировать. Чтобы добавить новое правило, нажмите кнопку **+** **Добавить** и настройте параметры правила в окне конфигурации.

Чтобы удалить правило, выберите его и нажмите кнопку **-** **Удалить**. Чтобы редактировать существующее правило, щелкните на его имени дважды или нажмите кнопку **✎** **Редактировать** и выполните нужные изменения в окне конфигурации.

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

18.4.1. Окно конфигурации

При добавлении или редактировании правил появляется окно конфигурации.



Введите ключевое слово

Вам необходимо настроить следующие параметры:

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



Настройка	Описание
POP3	Блокируются электронные сообщения, содержащие ключевое слово.
HTTP	Блокируются веб-страницы, содержащие ключевое слово.
IM клиент	Блокируются мгновенные сообщения, содержащие ключевое слово.

Нажмите **Завершить**, чтобы добавить правило.

18.5. Управление мгновенными сообщениями

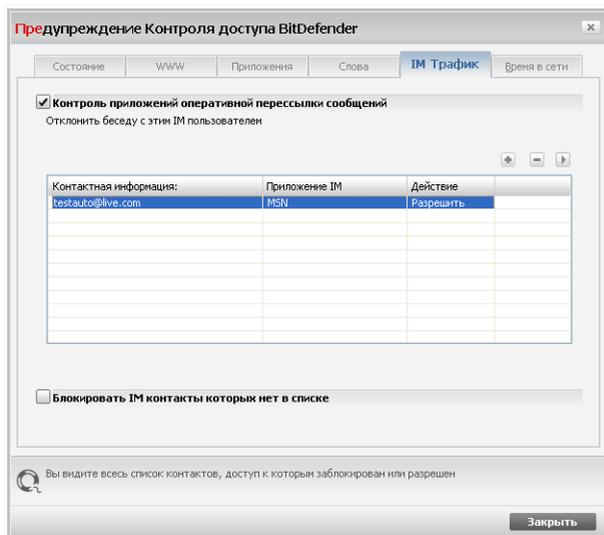
Функция обмена мгновенными сообщениями позволяет указать, с кем могут беседовать ваших дети.



Замечание

Контроль мгновенных сообщений доступен только для приложений Yahoo Messenger и Windows Live (MSN) Messenger.

Чтобы настроить контроль мгновенных сообщений для отдельно взятого пользователя, дважды щелкните на имени соответствующего пользователя, затем щелкните на вкладке **IM Трафик**.



Контроль приложений мгновенной пересылки сообщений

Установите флажок рядом с параметром **Контроль приложений оперативной пересылки сообщений**, если вы хотите использовать эту функцию.

Нужно добавить правила с указанием контактов, с которыми пользователю не разрешается обмениваться сообщениями. Чтобы добавить новое правило, нажмите кнопку **Добавить** и настройте параметры правила в окне конфигурации.

Чтобы удалить правило, выберите его и нажмите кнопку **Удалить**. Чтобы редактировать существующее правило, щелкните на его имени дважды или нажмите кнопку **Редактировать** и выполните нужные изменения в окне конфигурации.

Если вы определили все контакты, с которыми пользователю не разрешается обмениваться мгновенными сообщениями, выберите **Блокировать IM контакты которых нет в списке**. Теперь отправлять мгновенные сообщения пользователю смогут только те контакты, которым это явно разрешено.

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



18.5.1. Окно конфигурации

При добавлении или редактировании правил появляется окно конфигурации.

BitDefender - Мастер настройки IM клиента

Напишите здесь имя контакта, который вы хотели бы добавить в список органичений
testauto@live.com

Выберите тип IM клиента
MSN Live Messenger

Действие

Отклонить беседу с этим пользователем

Разрешить беседу с этим пользователем

Добавьте IM контакт, чтобы разрешить или отклонить пересылку сообщений

Нажмите сюда, чтобы разрешить добавление IM контакта

Завершить Отмена

Добавьте IM контакт

Выполните следующие действия:

1. Введите имя пользователя (идентификатор) контакта.
2. Выберите интернет-пейджер, с которым ассоциирован контакт.
3. Выберите действие для правила:
 - Отклонить беседу с этим пользователем
 - Разрешить беседу с этим пользователем
4. Нажмите **Завершить**, чтобы добавить правило.

18.6. Ограничитель времени в сети

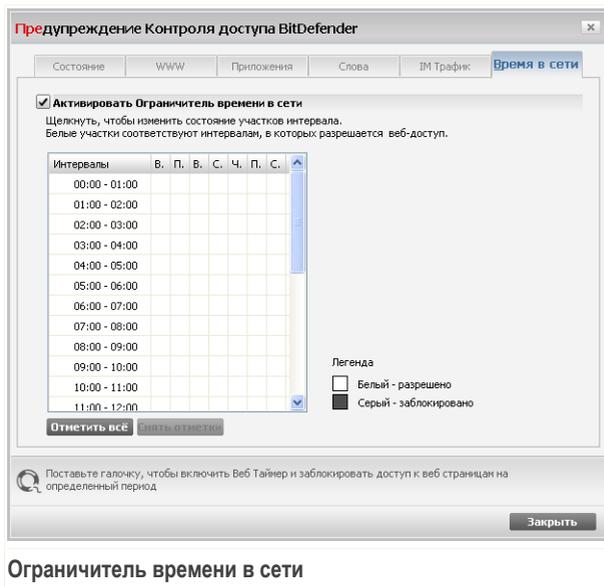
Используя **Ограничитель времени в сети** Вы можете разрешить или заблокировать веб-доступ для пользователей или приложений в течение указанных интервалов времени.



Замечание

Независимо от настроек **Временного веб-ограничителя** программа BitDefender будет выполнять ежечасное автоматическое обновление продукта.

Чтобы настроить Ограничитель времени в сети для отдельно взятого пользователя, дважды щелкните на имени соответствующего пользователя, затем щелкните на вкладке **Время в сети**.



Чтобы включить эту защиту, установите значок на поле, соответствующем опции **Включить Ограничитель времени в сети**.

Выберите временные интервалы, в пределах которых будут заблокированы все соединения с сетью Интернет. Вы можете выбрать короткие интервалы, щелкая мышкой на соответствующих ячейках, а более продолжительные интервалы – наведя курсор, нажав левую кнопку мышки и, не отпуская ее, 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.

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



19. Анонимность

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

19.1. Настройка Статуса Анонимности

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

The screenshot shows the BitDefender Internet Security 2009 - Пробная версия interface. At the top, there is a red status bar indicating "СОСТОЯНИЕ: Есть 4 проблемы, ожидающие решения" and a button "ИСПРАВИТЬ". Below this, the "Состояние" tab is selected, showing various settings for "Защита данных", "Регистр", "Истории обращений", and "Сценарий (скрыт)".

The "Анонимность" section is expanded, showing the "Уровень защиты" slider set to "Разрешенный". The "РАЗРЕШЕННЫЙ" level is detailed with the following settings:

- Защита данных контроль отключен
- Регистр контроль отключен
- Файлы истории обращений (Cookie) контроль отключен
- Сценарий (скрыт) контроль отключен

Buttons "Другой..." and "По умолчанию" are visible below the settings. A "Статистика Контроля Приватности" section shows the following statistics:

Заблокировано информации:	0
Блокировано ключей реестра:	0
Заблокированные cookies:	0
Заблокированные сценарии:	0

At the bottom, there is a note: "Модуль защиты приватности сейчас включен. Для безопасности ваших данных, мы рекомендуем держать защиту модуля приватности включенной все время." and the BitDefender logo with navigation links: "Купить/Обновить", "Моя учетная запись", "Регистрация", "Справка", "Техническая поддержка", "Журнал".

Настройка Статуса Анонимности



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



Важно

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

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

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

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

19.1.1. Конфигурация уровня защиты

Вы можете выбрать уровень защиты согласно Вашим потребностям 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 конфиденциальности .
Агрессивный	Включены только Контроль регистра , Контроль сценариев и Контроль конфиденциальности .



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

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

19.2. Контроль Идентичности

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

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

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

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

Зачем нужна защита данных?

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



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

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

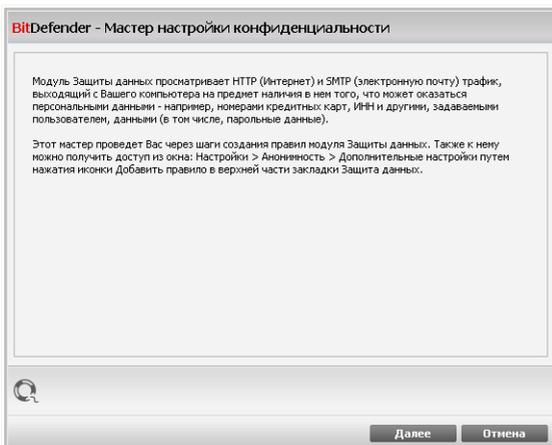
Например, вы можете получить электронное сообщение якобы от вашего банка с просьбой срочно обновить вашу банковскую информацию. В этом сообщении будет находиться ссылка на веб-страницу, где вы должны будете ввести свою личную информацию. Хотя все будет выглядеть вполне правдоподобно, и электронное сообщение,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

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

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



Шаг 1/4 - Окно приветствия



Окно приветствия

Щелкните по кнопке **Далее**.



Шаг 2/4 - Задать тип правила и данные

Установить тип правила и данных

Вам необходимо настроить следующие параметры:

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



Замечание

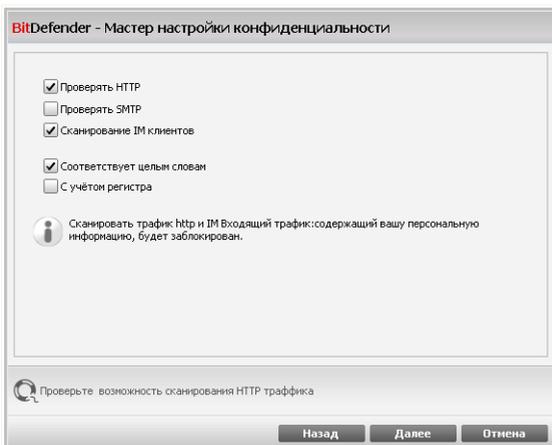
Если Вы введете менее трех символов, Вам будет предложено уточнить данные. Рекомендуем Вам ввести минимум три символа, чтобы избежать блокирования по ошибке сообщений и веб-страниц.

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

Щелкните по кнопке **Далее**.



Шаг 3/4 - Выберите трафик



Выберите трафик

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

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

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

Щелкните по кнопке **Далее**.



Шаг 4/4 - Введите описание правила

BitDefender - Мастер настройки конфиденциальности

Описание правила

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

Введите описание этого правила

Назад Завершить Отмена

Опишите правило

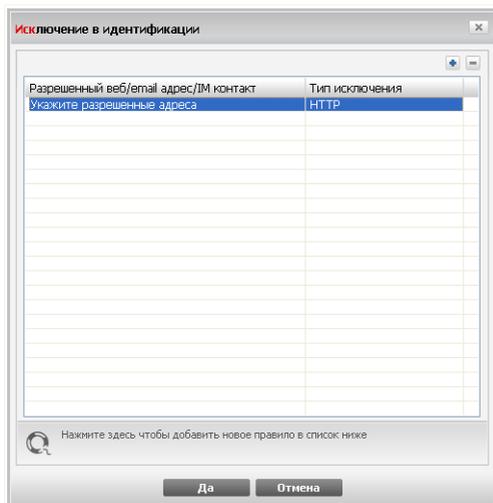
Введите краткое описание правила в поле редактирования. Так как заблокированные данные (символьные строки) не отображаются в виде простого текста при доступе к правилу, описание должно помочь вам легко идентифицировать их.

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

19.2.2. Определение исключений

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

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



Исключения

Добавить исключение, следуя по этим шагам:

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

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

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

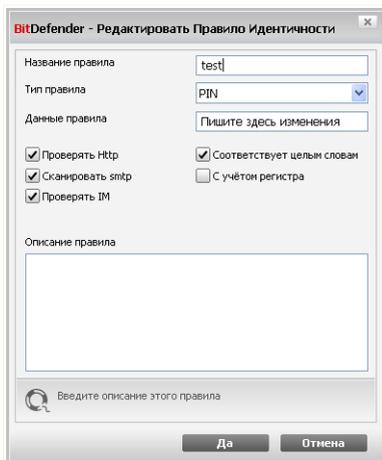
19.2.3. Управление правилами

В этом окне Вы видите список правил в таблице.



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

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



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

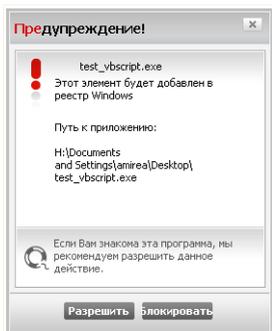
Редактировать правило

19.3. Управление реестром

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

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

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



Предупреждение реестра

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

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

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



Замечание

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

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



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

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



Cookie Предупреждение

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

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

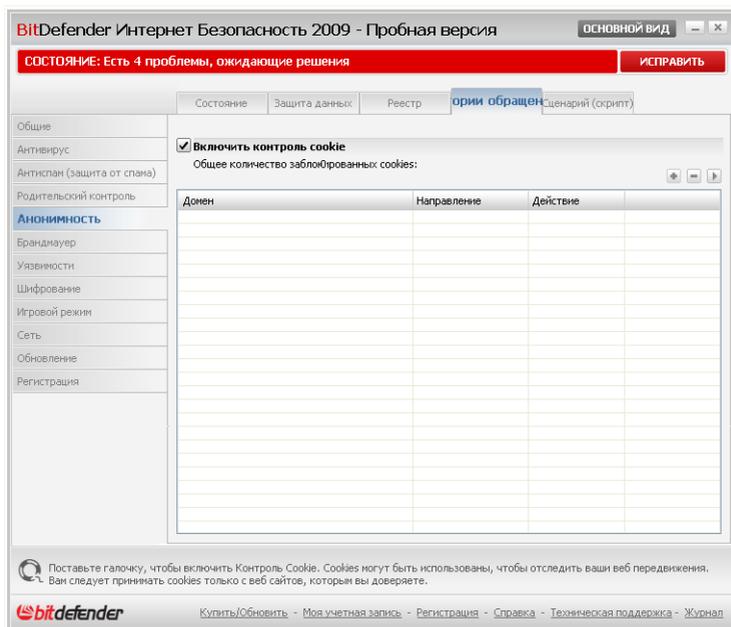
Это поможет Вам решить, каким веб-сайтам стоит доверять, а каким – нет.



Замечание

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

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



Контроль файлов истории обращений (Cookies)

В этом окне Вы видите список правил в таблице.



Важно

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

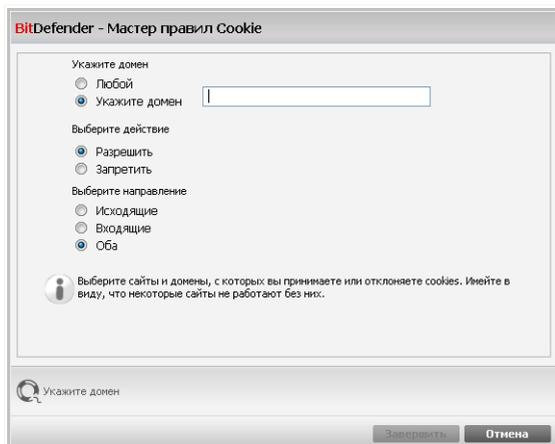
Чтобы удалить правило, выберите его и нажмите кнопку **Удалить**. Для изменения параметров правил дважды щелкните на правиле и выполните желаемые изменения в окне настройки.

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



19.4.1. Окно конфигурации

При редактировании или добавления правила вручную, появится окно конфигурации.



Выберите адрес, действие и направление

Вы можете установить следующие настройки:

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

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

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

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



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



Замечание

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

Щелкните мышкой на кнопке **Завершить**.

19.5. Контроль сценариев

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

BitDefender позволяет Вам разрешить или заблокировать выполнение данных элементов.

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



Предупреждение о сценариях

В этом окне Вы видите название ресурса.

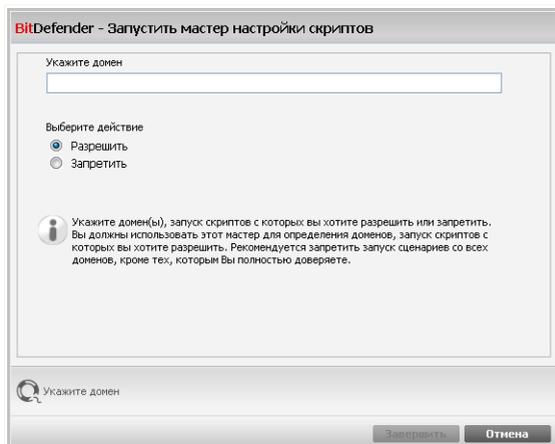
Поставьте галочку в поле **Запомнить этот ответ** и щелкните мышкой на кнопке **Да** или **Нет** Будет создано новое правило, которое будет занесено в таблицу правил. Когда этот же ресурс будет пытаться отправить Вам активный контент, Вы уже не получите предупреждения.

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



19.5.1. Окно конфигурации

При редактировании или добавления правила вручную, появится окно конфигурации.



Выберите адрес и действие

Вы можете установить следующие настройки:

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

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

Щелкните мышкой на кнопке **Завершить**.



20. Брандмауер

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



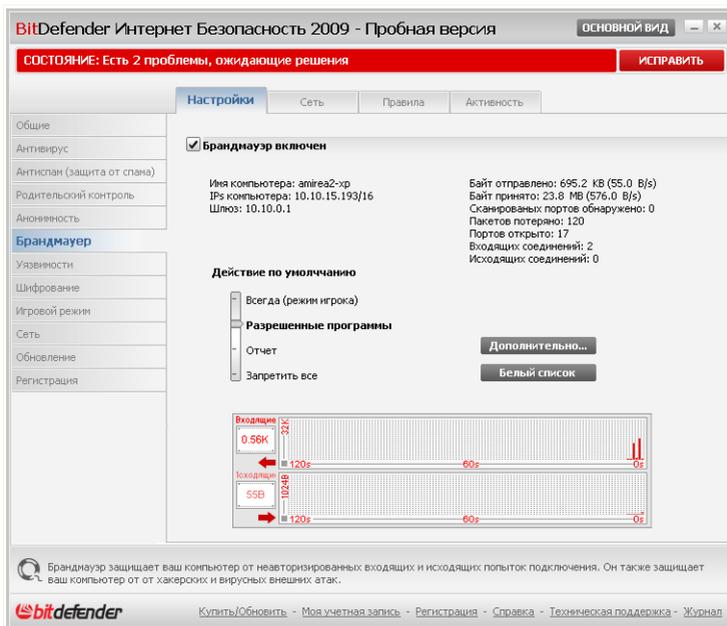
Замечание

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

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

20.1. Настройки

Чтобы настроить защиту при помощи модуля Брандмауэр, перейдите в раздел **Брандмауэр>Настройки** в окне расширенного вида.



Настройки брандмауэра

Здесь вы можете проверить, включен ли брандмауэр BitDefender. Если вы хотите сменить состояние модуля Брандмауэр, уберите или установите соответствующий флажок.



Важно

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

Существует две категории информации:

- **Кратко о настройке сети.** Вы можете найти имя компьютера, его IP-адрес и шлюз по умолчанию. Если у вас несколько сетевых адаптеров (то есть вы подключаетесь к нескольким сетям одновременно), вы увидите IP-адреса и шлюзы, заданные для каждого сетевого адаптера.
- **Статистика.** Вы увидите различную статистику об активности брандмауэра:



- число отправленных байтов;
- число полученных байтов;
- число попыток сканирования портов, обнаруженных и заблокированных программой BitDefender; Сканирование портов часто предпринимается хакерами для нахождения открытых портов на вашем компьютере с целью несанкционированного доступа.
- число отброшенных пакетов;
- число открытых портов;
- число активных входящих соединений;
- число активных исходящих соединений;

Чтобы увидеть активные соединения и открытые порты, перейдите ко вкладке **Активность**.

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



Замечание

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

20.1.1. Установка действия по умолчанию

По умолчанию BitDefender автоматически разрешает доступ всем известным программам из своего белого списка к сетевым службам и интернету. Для всех других программ BitDefender выдает окно с запросом действия. Заданное вами действие применяется каждый раз при запросе доступа к сети/интернету соответствующей программой.

Путем передвижения бегунка вдоль шкалы вы можете задать действие по умолчанию, которое будет применяться при запросе доступа к сети/интернету данным приложением. Доступны следующие действия по умолчанию:

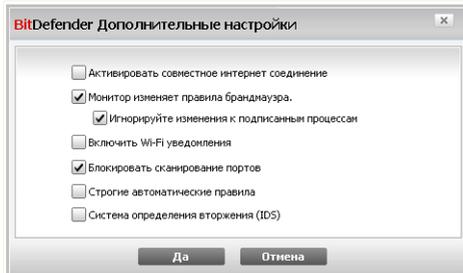
Действие по умолчанию	Описание
Разрешить все	Разрешает без предупреждения весь трафик, который не описан в установленных на данный момент правилах. Настоятельно не рекомендуем



Действие по умолчанию	Описание
	использовать эту политику, но он может быть полезен системным администраторам и геймерам.
Разрешенные программы	<p>Применяет все текущие правила и разрешает все исходящие соединения от программ, известных BitDefender как разрешенные (находящиеся в белом списке). Для всех остальных попыток подключения BitDefender будет запрашивать ваше разрешение.</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>
Отчет	Применяет текущие правила и консультируется с Вами обо всех попытках трафика, который не соответствует ни одному из текущих правил.
Запретить все	Применяет текущие правила и отклоняет любой трафик, который не соответствует ни одному из текущих правил.

20.1.2. Конфигурация дополнительных настроек брандмауэра

Для настройки дополнительных параметров брандмауэра нажмите кнопку **Дополнительно**.



Дополнительные настройки брандмауэра

Доступными являются следующие варианты:

- **Включить общий доступ к подключению интернета (ICS)** - включает поддержку Общего доступа к подключению интернет (ICS).



Замечание

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

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

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

- **Отслеживать изменения в файлах программ, которые соответствуют правилам брандмауэра** - проверка каждого приложения, осуществляющего попытку подключения к Интернет на наличие каких либо изменений в них с момента, когда было добавлено соответствующее правило, регулирующее доступ данного приложения. Если приложение было изменено, Вы будете предупреждены сообщением с просьбой уточнить стоит ли разрешать или запрещать данному приложению выход в Интернет.



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



Замечание

Рекомендуем включать эту опцию и позволять доступ в Интернет только тем приложениям, которые, на Ваш взгляд, действительно могли измениться с момента, когда было создано соответствующее правило доступа данного приложения в Интернет.

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

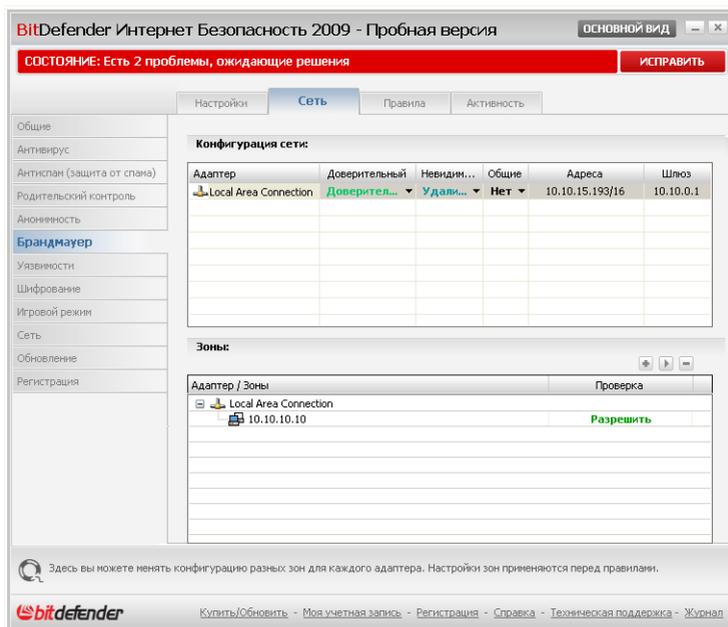
- **Включить Wi-Fi уведомления** - если вы подключены к беспроводной сети, этот параметр будет отображать окна со сведениями о сетевых событиях (например, когда новый компьютер подключается к сети).
- **Блокировать сканирование портов** - обнаружение и блокирование попыток сканирования открытых портов.

Сканирование портов часто используется хакерами для обнаружения открытых портов на вашем компьютере. Они могут проникнуть в ваш компьютер, если найдут уязвимый или менее защищенный порт.

- **Строгие автоматические правила** - создание строгих правил с помощью окна уведомлений брандмауэра. Если этот параметр выбран, BitDefender запросит действие и создаст правила для каждого процесса, который открывает данное приложение с запросом доступа к сети или интернету.
- **Система определения вторжения (IDS)** - включает эвристическое наблюдение за приложениями, пытающимися получить доступ к сетевым службам и интернету.

20.2. Сеть

Чтобы настроить параметры брандмауэра, перейдите в раздел **Брандмауэр>Сеть** в окне расширенного вида.



Сеть

Колонки в таблице **Конфигурация сети** содержат подробные сведения о сети, к которой вы подключены:

- **Адаптер** - сетевой адаптер, который ваш компьютер использует для подключения к сети и интернету.
- **Тип** - уровень доверия, назначенный сетевому адаптеру. В зависимости от параметров сетевого адаптера, BitDefender может автоматически назначить адаптеру уровень доверия или запросить у вас более подробные сведения.
- **Невидимость** - параметр, определяющий возможность быть обнаруженным другими компьютерами.
- **Общие** - параметр, определяющий, применяются ли общие правила к данному соединению.
- **Адреса** - IP-адрес, заданный для адаптера.



- **Шлюз** - IP-адрес, который ваш компьютер использует для подключения к интернету.

20.2.1. Изменения уровня доверия

Каждому сетевому адаптеру BitDefender назначает уровень доверия. Уровень доверия, назначенный адаптеру, указывает, насколько данная сеть заслуживает доверия.

На основе уровня доверия для адаптера создаются особые правила, в зависимости от того, каким образом процессы системы и BitDefender подключаются к сети и интернету.

В таблице **Конфигурация сети** в колонке **Тип** отображается уровень доверия, заданный для каждого адаптера. Чтобы сменить уровень доверия, щелкните на стрелке в колонке **Тип** и выберите нужный уровень.

Доверительный	Описание
Надежный	Отключение брандмауэра для определенного адаптера.
Доверительный	Разрешение всего трафика между вашим компьютером и компьютерами в локальной сети.
Безопасный	Разрешение обмена ресурсами с компьютерами в локальной сети. Этот уровень автоматически устанавливается для локальных (домашних или офисных) сетей.
Не безопасный	Запрет на подключение к вашему компьютеру других компьютеров из интернета или сети. Этот уровень автоматически устанавливается для сетей общего пользования (если IP-адрес вам назначен поставщиком услуг интернета).
Блокирование	Блокирование всего трафика между вашим компьютером и компьютерами в локальной сети, в то же время обеспечивая доступ к интернету. Этот уровень доверия автоматически устанавливается для небезопасных (открытых) беспроводных сетей.
Блокирование	Полное блокирование трафика сети и интернета через соответствующий адаптер.



20.2.2. Настройка невидимого режима

Невидимый режим позволяет прятать компьютер от вредоносного ПО и хакеров в сети или в интернете. Для настройки невидимого режима нажмите стрелку ▼ в колонке **Stealth** и выберите нужный вариант.

Режим «Невидимка»	Описание
Вкл.	Невидимый режим включен. Ваш компьютер невидим из локальной сети и из интернета.
Выкл.	Невидимый режим выключен. Любой пользователь из локальной сети может обнаружить ваш компьютер.
Удаленный	Ваш компьютер не может быть обнаружен из интернета. Пользователи в локальной сети могут обнаружить ваш компьютер.

20.2.3. Настройка общих параметров

Если сменить IP-адрес сетевого адаптера, BitDefender изменит уровень доверия соответствующим образом. Если вы хотите сохранить тот же уровень доверия, нажмите стрелку ▼ в колонке **Невидимость** и выберите **Да**.

20.2.4. Сетевые зоны

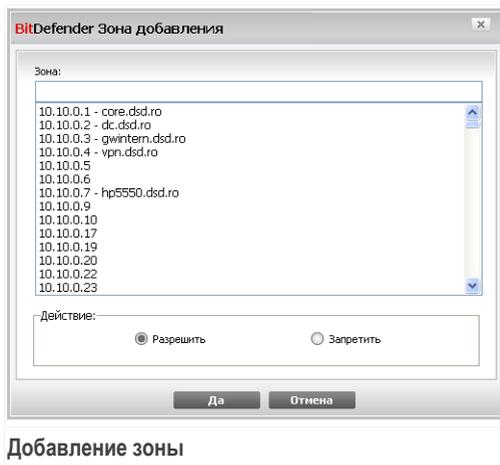
Для определенного адаптера можно добавлять разрешенные или заблокированные компьютеры.

Доверенная зона - это компьютер, которому вы полностью доверяете. Весь трафик между вашим компьютером и доверенным компьютером разрешается. Чтобы открыть доступ к ресурсам для определенных компьютеров в небезопасной беспроводной сети, добавьте их в список разрешенных компьютеров.

Заблокированная зона - это компьютер, с которым вы не хотите обмениваться информацией.

В таблице **Зоны** отображаются текущие сетевые зоны для каждого адаптера.

Чтобы добавить новую зону, нажмите кнопку  **Добавить**.

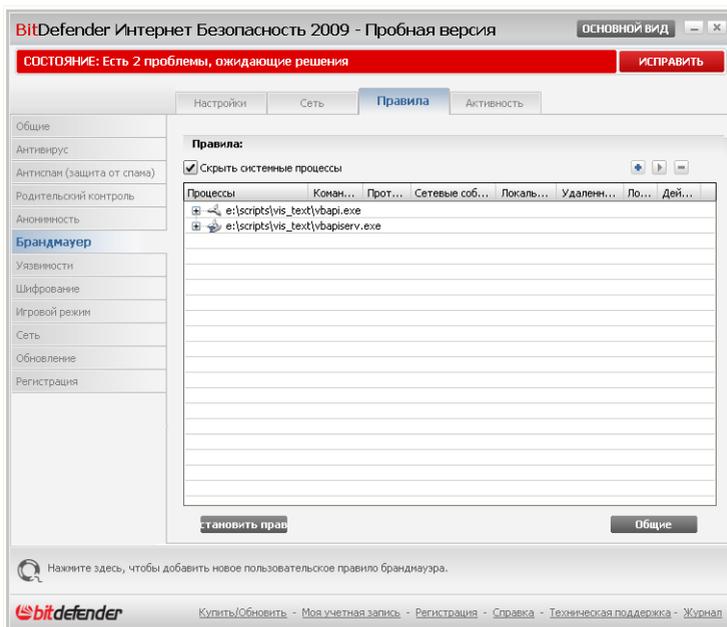


Выполните следующие действия:

1. Выберите IP-адрес компьютера, который вы хотите добавить.
2. Выберите действие:
 - **Разрешить** - разрешить весь трафик между вашим компьютером и выбранным компьютером.
 - **Запретить** - блокировать весь трафик между вашим компьютером и выбранным компьютером.
3. В конце щелкните мышкой на кнопке **ОК**.

20.3. Правила

Для управления правилами брандмауэра, контролирующими доступ приложений к сетевым ресурсам и интернету, перейдите к разделу **Брандмауэр>Правила** в окне расширенного вида.



Правила настройки брандмауэра

Вы можете просмотреть приложения (процессы), для которых были созданы правила брандмауэра. Снимите флажок **Скрыть системные процессы**, если вы также хотите видеть правила, касающиеся системы или процессов BitDefender.

Чтобы видеть правила, созданные для определенного приложения, щелкните на кнопке "+" около соответствующего приложения. Вы можете узнать подробные сведения о каждом правиле, как указано в колонках таблицы:

- **Процессы** - типы процессов и сетевых адаптеров, к которым применяется правило. Правила автоматически создаются для фильтрации доступа к сети и интернету через любой адаптер. Вы можете вручную создавать правила или изменять существующие правила для фильтрации доступа приложения к сети и интернету через определенный адаптер (например, беспроводной сетевой адаптер).
- **Командная строка** - команда, используемая для запуска процессов через интерфейс командной строки Windows (**cmd**).



- **Протокол** - IP-протокол, к которому применяется правило. Вы можете увидеть следующее:

Протокол	Описание
Любой	Включает все IP-протоколы.
TCP	TCP (Transmission Control Protocol) - 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.
Число	Означает определенный IP-протокол (отличный от TCP и UDP). Полный список назначенных номеров IP-протокола можно увидеть на странице www.iana.org/assignments/protocol-numbers .

- **Сетевые события** - сетевые события, к которым применяется правило. Вы можете обратить внимание на следующие события:

Событие	Описание
Подключение	Предварительный обмен стандартными сообщениями, используемыми протоколами на основе соединений (такими как TCP) для установки подключения. Благодаря протоколам на основе соединений данные между двумя компьютерами передаются только после установки подключения.
Трафик	Поток данных между двумя компьютерами.
Список	Состояние, в котором приложение наблюдает за сетью, ожидая установки соединения или получения информации от другого приложения.

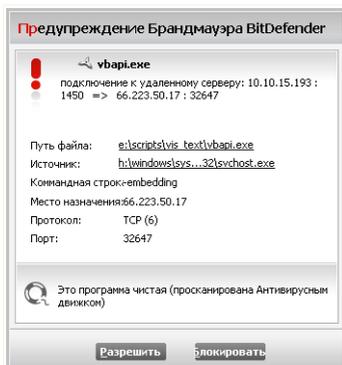
- **Локальные порты** - порты на вашем компьютере, к которым применяется правило.



- **Удаленные порты** - порты на удаленных компьютерах, к которым применяется правило.
- **Локальный** - определяет, применяется ли правило только к компьютерам в локальной сети.
- **Действие** - определяет, разрешен или запрещен доступ данному приложению к сети или интернету при определенных обстоятельствах.

20.3.1. Автоматическое добавление правил

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



Предупреждение брандмауэра

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

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

В зависимости от Вашего ответа будет создано правило, которое тут же применится и запишется в таблицу. При следующей попытке

соединения данного приложения по умолчанию будет использоваться это правило.



Важно

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

20.3.2. Удаление правил

Чтобы удалить правило, выберите его и нажмите кнопку **Удалить правило**. Вы можете выбрать и удалить одновременно несколько правил.



Если вы хотите удалить все правила, созданные для определенного приложения, выберите это приложение из списка и нажмите кнопку **Удалить правило**.

20.3.3. Создание и изменение правил

Создание новых правил и изменение существующих состоит в настройке параметров правил в окне конфигурации.

Создание правил. Чтобы создать правило вручную, выполните следующую процедуру:

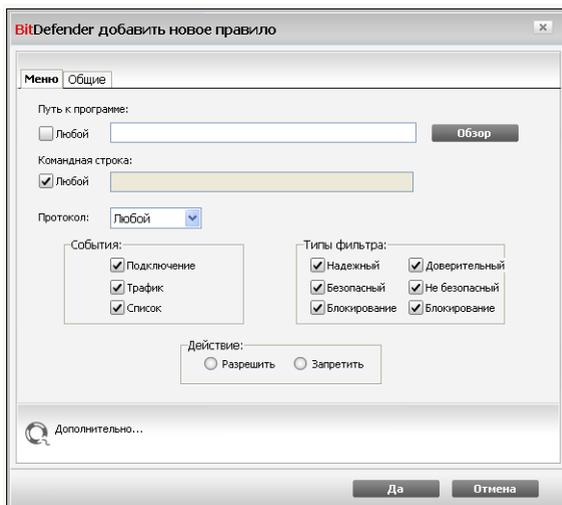
1. Нажмите кнопку **Добавить правило**. Появится окно настроек.
2. Настройте главные и расширенные параметры надлежащим образом.
3. Нажмите **ОК**, чтобы добавить новое правило.

Изменение правил. Чтобы изменить существующее правило, выполните следующую процедуру:

1. Нажмите кнопку **Редактировать правило** или дважды щелкните на правиле. Появится окно настроек.
2. Настройте главные и расширенные параметры надлежащим образом.
3. Щелкните мышкой на **Применить** чтобы сохранить сделанные изменения.

Настройка основных параметров

Вкладка **Общие** окна конфигурации позволяет настраивать основные параметры правил.



Основные параметры

Вы можете установить следующие параметры:

- **Путь к программе.** Нажмите **Обзор** и выберите приложение, к которому вы хотите применить правила. Если вы хотите, чтобы правило применялось ко всем приложениям, выберите **Любой**.
- **Командная строка.** Если вы хотите, чтобы правило применялось только когда выбранное приложение запущено с определенной командой через интерфейс командной строки Windows, снимите флажок **Любой** и введите соответствующую команду в поле ввода.
- **Протокол.** Выберите из меню IP-протокол, к которому будет применяться правило.
 - Если вы хотите, чтобы правило применялось ко всем протоколам, выберите **Любой**.
 - Если вы хотите, чтобы правило применялось к определенному протоколу, выберите **Другое**. Появится поле ввода. Введите номер, назначенный протоколу, который вы хотите отфильтровать, в поле ввода.



Замечание

Номер IP-протокола, назначенный Комитетом по цифровым адресам в интернете (IANA). Полный список назначенных номеров IP-протокола можно увидеть на странице www.iana.org/assignments/protocol-numbers.

- **События.** В зависимости от выбранного протокола, выберите сетевые события, которым будет назначено правило. Вы можете обратить внимание на следующие события:

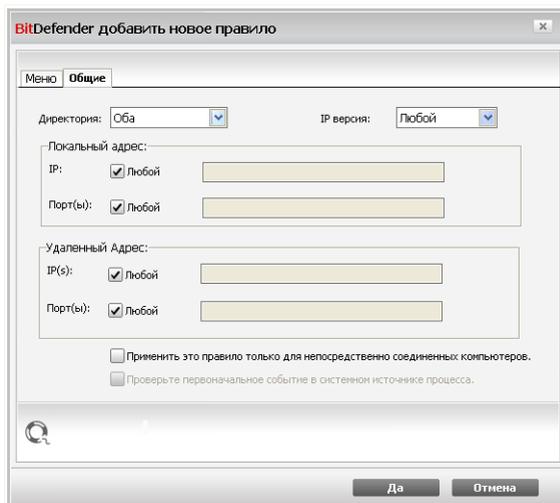
Событие	Описание
Подключение	Предварительный обмен стандартными сообщениями, используемыми протоколами на основе соединений (такими как TCP) для установки подключения. Благодаря протоколам на основе соединений данные между двумя компьютерами передаются только после установки подключения.
Трафик	Поток данных между двумя компьютерами.
Список	Состояние, в котором приложение наблюдает за сетью, ожидая установки соединения или получения информации от другого приложения.

- **Доверительный.** Выберите уровни доверия, которым будет назначено правило.
- **Действие.** Выберите одно из доступных действий:

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

Настройка дополнительных параметров

Вкладка **Общие** окна конфигурации позволяет настраивать расширенные параметры правил.



Расширенные параметры

Вы можете установить следующие расширенные параметры:

- **Направление.** Выберите из меню направление трафика, к которому будет применяться правило.

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

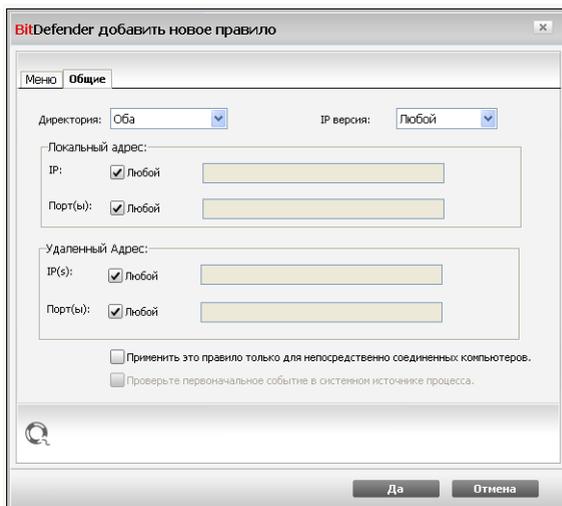
- **Версия IP.** Выберите из меню версию IP-протокола (напр., IPv4 или IPv6), к которой будет применяться правило.
- **Адрес источника.** Укажите локальный IP-адрес и порт, к которому будет применяться правило:
 - Если у вас несколько сетевых адаптеров, вы можете снять флажок **Любой** и ввести определенный IP-адрес.



- Если ранее был выбран протокол TCP или UDP, вы можете указать определенный порт или диапазон портов между 0 и 65535. Если Вы хотите применить правило ко всем портам - выберите **Любой**.
- **Удаленный Адрес.** Укажите удаленный IP-адрес и порт, к которому будет применяться правило:
 - Для фильтрации трафика между вашим компьютером и каким-то другим конкретным компьютером снимите флажок **Любой** и введите его IP-адрес.
 - Если ранее был выбран протокол TCP или UDP, вы можете указать определенный порт или диапазон портов между 0 и 65535. Если Вы хотите применить правило ко всем портам - выберите **Любой**.
- **Применить это правило только для непосредственно соединенных компьютеров.** Выберите этот параметр, если захотите, чтобы правило применялось только к локальному трафику.
- **Проверьте первоначальное событие в системном источнике процесса.** Вы можете изменять этот параметр только если вы выбрали **Строгие автоматические правила** (перейдите ко вкладке **Настройки** и нажмите **Дополнительно**). Строгие правила означают, что BitDefender запросит действие, когда приложение будет спрашивать доступ в сеть/интернет всякий раз, когда старший процесс в иерархии будет отличаться.

20.3.4. Расширенное управление правилами

Если вам нужен расширенный контроль над правилами брандмауэра, нажмите **Общие**. Появится новое окно.



Расширенное управление правилами

Вы увидите правила брандмауэра в том порядке, в котором они были отмечены. В колонках таблицы содержатся подробные сведения о каждом правиле.



Замечание

При попытке соединения (входящего или исходящего) BitDefender применяет действие первого правила, которое соответствует данному соединению. Таким образом, порядок, в которых отмечаются правила, очень важен.

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

Чтобы отредактировать существующее правило, достаточно выбрать его и нажать кнопку **Редактировать правило** или дважды щелкнуть на нем мышью.

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

Нажмите **Заккрыть**, чтобы закрыть окно.



20.4. Контроль соединений

Для наблюдения за текущей активностью сети/интернета (по TCP и UDP) по каждому приложению, а также для открытия журнала брандмауэра BitDefender, перейдите в раздел **Брандмауэр>Активность** в окне расширенного вида.

Название процесса	РИД/П...	Исходя...	Выход...	Входя...	вход	Возраст
10.10.15.193:1900	UDP	0.0 B	0.0 B/s	232.4 KB	88.7 B/s	1h 4m 21s
yserv.exe /service	3620	2.2 KB	0.0 B/s	1.6 KB	0.0 B/s	37m 57s
0.0.0.0:10000	UDP	0.0 B	0.0 B/s	0.0 B	0.0 B/s	37m 56s
multserv32.exe	584	1.0 KB	0.7 B/s	9.2 KB	3.3 B/s	1h 4m 34s
0.0.0.0:30564	TCP	112.0 B	0.7 B/s	560.0 B	3.3 B/s	1h 4m 34s
10.10.15.193:305...	TCP	112.0 B	0.7 B/s	560.0 B	3.3 B/s	10m 37s
10.10.15.193:305...	TCP	112.0 B	0.7 B/s	560.0 B	3.3 B/s	10m 37s
vbapiserv.exe	796	0.0 B	0.0 B/s	0.0 B	0.0 B/s	1h 4m 34s
0.0.0.0:33333	TCP	0.0 B	0.0 B/s	0.0 B	0.0 B/s	1h 4m 32s
lsess.exe	1012	8.9 KB	0.0 B/s	38.8 KB	0.0 B/s	1h 4m 40s
0.0.0.0:IKE	UDP	0.0 B	0.0 B/s	0.0 B	0.0 B/s	1h 4m 34s
0.0.0.0:4500	UDP	0.0 B	0.0 B/s	0.0 B	0.0 B/s	1h 4m 34s
svchost.exe -k rpcss	1264	0.0 B	0.0 B/s	0.0 B	0.0 B/s	1h 4m 39s
0.0.0.0:RPC	TCP	0.0 B	0.0 B/s	0.0 B	0.0 B/s	1h 4m 39s
svchost.exe -k netsvcs	1388	3.0 KB	0.0 B/s	1.9 KB	0.0 B/s	1h 4m 39s
10.10.15.193:NTP	UDP	0.0 B	0.0 B/s	0.0 B	0.0 B/s	1h 4m 25s
svchost.exe -k networ...	1508	23.7 KB	0.0 B/s	46.7 KB	0.0 B/s	1h 4m 39s
0.0.0.0:1025	UDP	2.2 KB	0.0 B/s	4.3 KB	0.0 B/s	1h 4m 36s
0.0.0.0:1333	UDP	3.1 KB	0.0 B/s	6.6 KB	0.0 B/s	16m 59s
0.0.0.0:1312	UDP	3.1 KB	0.0 B/s	6.1 KB	0.0 B/s	17m 0s
0.0.0.0:1026	UDP	15.3 KB	0.0 B/s	29.6 KB	0.0 B/s	1h 4m 36s

Контроль соединений

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

Если вы хотите также просмотреть и неактивные процессы, снимите флажок **Скрыть процессы**.

Описания пиктограмм следующие:

- На вашем компьютере открыто соединение.



-  На вашем компьютере открыт порт.

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

Подробный список событий относительно использования модуля Брандмауэр (включение/выключение брандмауэра, блокирование трафика, изменение параметров) или созданный другими действиями, обнаруженными данным модулем (сканирование портов, блокировка попыток подключения или трафика согласно правил) смотрите в журнале брандмауэра BitDefender, нажав кнопку **Показать Лог**. Этот файл находится в папке Common Files текущего пользователя Windows по адресу: `...BitDefender\BitDefender Firewall\bdfirewall.txt`.

Если вы хотите, чтобы в журнале содержалось больше информации, выберите **Расширенное словесное наполнение лога**.



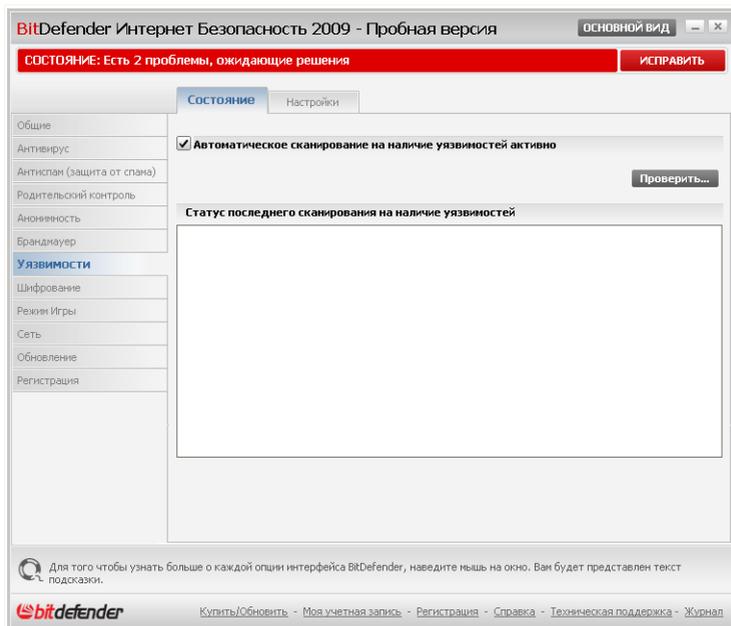
21. Уязвимости

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

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

21.1. Состояние

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



Сканирование на наличие уязвимостей

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



Важно

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

21.1.1. Устранение уязвимостей

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



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

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

Шаг 1/6 - Выберите уязвимости для проверки

BitDefender 2009

Мастер сканирования на наличие Уязвимостей

Шаг 1 | Шаг 2 | Шаг 3 | Шаг 4 | Шаг 5 | Шаг 6

Выбрать задачи

Этот мастер покажет вам действия, которые требуются для определения устаревших приложений и аккаунтов Windows, которые имеют слабый пароль. Пожалуйста, выберите из списка ниже элементы, которые будут проверены на уязвимость.

- Проверить критические обновления Windows
- Проверить случайные обновления Windows
- Проверить обновления приложений
- Проверить пароли учетных записей Windows

Выберите этот блок, чтобы BitDefender проверил получила ли ваша операционная система Windows обновления защиты из Microsoft.

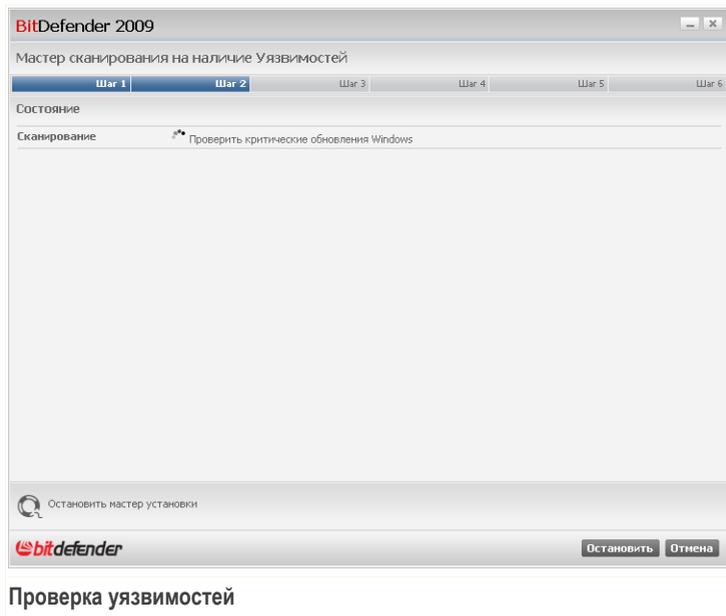
bitdefender Далее Отмена

Уязвимости

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



Шаг 2/6 - Проверка уязвимостей



Подождите, пока BitDefender завершит проверку уязвимостей.



Шаг 3/6 - Смените слабые пароли

BitDefender 2009

Мастер сканирования на наличие Уязвимостей

Шаг 1 Шаг 2 **Шаг 3** Шаг 4 Шаг 5 Шаг 6

Проверить пароли учетных записей Windows

Имя Пользователя	Сила	Состояние
Admin	Слабый	Устранить

Это список Windows множества паролей на ваш компьютер и уровне защиты, которую они обеспечивают. Щелкните кнопку «Местоположение», чтобы изменить слабые пароли.

bitdefender **Далее** **Отмена**

Пользовательские пароли

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

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

BitDefender

Choose method to fix:

Force user to change password at next login

Change user password

Type password:

Confirm password:

OK **Close**

Изменить пароль



Выберите метод устранения проблемы:

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



Замечание

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

Нажмите **ОК**, чтобы сменить пароль.

Щелкните по кнопке **Далее**.



Шаг 4/6 - Обновите приложения

BitDefender 2009

Мастер сканирования на наличие Уязвимостей

Шаг 1 Шаг 2 Шаг 3 Шаг 4 Шаг 5 Шаг 6

Проверить обновления приложений

Приложение	Версия установки	Последняя версия	Состояние
Firefox	2.0.0.11 (en-US)	3.0.1 (en-US)	Web-страница

Это список приложений, поддерживаемых BitDefender и обновлений, доступных, если имеется.

bitdefender **Далее** **Отмена**

Приложения

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

Щелкните по кнопке **Далее**.



Шаг 5/6 - Обновите Windows

BitDefender 2009

Мастер сканирования на наличие Уязвимостей

Шаг 1 | Шаг 2 | Шаг 3 | Шаг 4 | **Шаг 5** | Шаг 6

Обновления Windows

Проверить критические обновления Windows

- Update for Office 2003 (KB907417)
- Office 2003 Service Pack 3 (SP3)
- Microsoft .NET Framework 2.0 Service Pack 1 (KB110906) (x86)
- Security Update for Microsoft XML Core Services 4.0 Service Pack 2 (KB954430)
- Update for Microsoft Office Outlook 2003 Junk Email Filter (KB959614)
- Update Rollup for ActiveX Killbits for Windows XP (KB960715)
- Windows Malicious Software Removal Tool - February 2009 (KB990830)

Проверить случайные обновления Windows

- Update for Windows XP (KB904942)
- Remote Desktop Connection (Terminal Services Client 6.0) for Windows XP (KB925876)
- Update for Microsoft Core XML Services (MSXML) 6.0 Service Pack 1 (KB934268)
- Windows Media Player 11
- Windows Internet Explorer 7 for Windows XP
- Microsoft .NET Framework 3.0: x86 (KB928416)
- Root Certificates Update

Установка обновления

Это список критического или не критических обновлений приложений Windows

Далее **Отмена**

Обновления Windows

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

Щелкните по кнопке **Далее**.



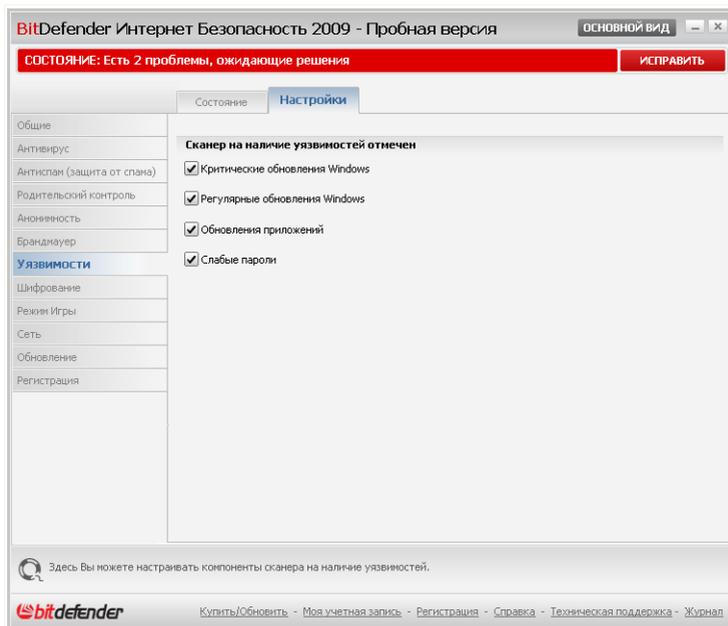
Шаг 6/6 - Просмотрите результаты



Нажмите **Закреть**.

21.2. Настройки

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



Автоматическое сканирование на наличие уязвимостей

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

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



Замечание

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



22. Шифрование

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

22.1. Шифрование приложений мгновенного обмена сообщениями

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

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



Важно

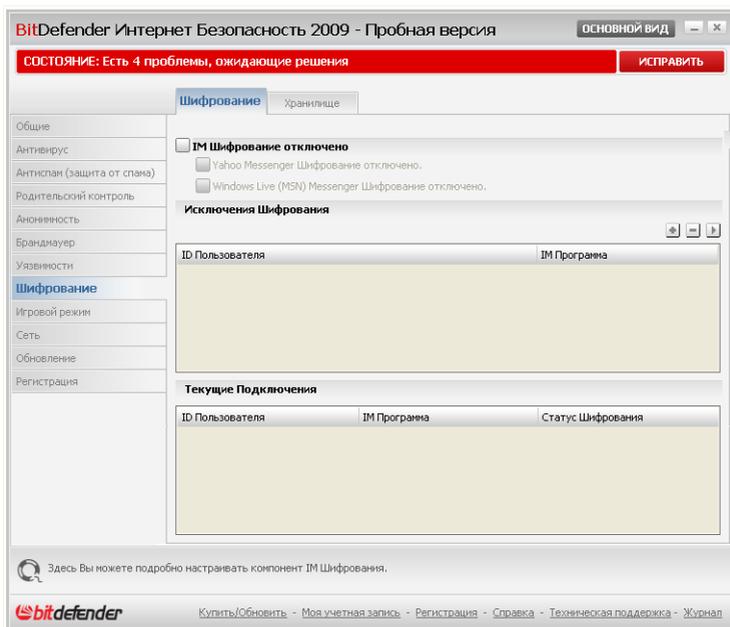
BitDefender не будет шифровать обмен сообщениями, если собеседник использует какой-либо веб-клиент, например Meebo, или другое приложения для чата, поддерживающее Yahoo Messenger или MSN.

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



Замечание

Вы можете легко настроить шифрование мгновенного обмена сообщениями с помощью панели инструментов BitDefender из окна чата. Для получения дополнительной информации перейдите к *«Интеграция в интернет-пейджер»* (р. 54).



Шифрование приложений мгновенной пересылки сообщений

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

Отобразятся две таблицы:

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

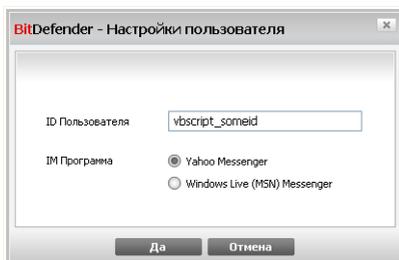


- У вашего контакта не установлена версия BitDefender, которая поддерживает шифрование мгновенных сообщений.

22.1.1. Отключение шифрования для отдельных пользователей

Для отключения шифрования для отдельного пользователя выполните следующую процедуру:

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



Добавление контактов

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

22.2. Хранилище

Хранилище BitDefender позволяет создавать на вашем компьютере зашифрованные и защищенные паролем логические диски (или хранилища), где вы можете безопасно хранить свои конфиденциальные и важные документы. Доступ к данным, хранящимся в этих хранилищах, могут получать пользователи, которые знают пароль.

Пароль позволяет открывать и хранить данные, а также закрывать хранилище, обеспечивая их безопасность. Пока хранилище открыто, вы можете добавлять новые файлы, получать доступ к текущим файлам или изменять их.



Физически хранилище представляет собой расположенный на локальном жестком диске файл с расширением `.bvd`. Хотя физические файлы, которые представляют собой диски хранилища, можно открывать из различных операционных систем (таких как Linux), информация, хранящаяся на них, не может быть прочитана, так как она зашифрована.

Для управления хранилищами на вашем компьютере перейдите к разделу **Шифрование**>**Хранилище** в окне расширенного вида.

The screenshot shows the BitDefender Internet Security 2009 interface. At the top, there is a status bar indicating a problem: "СОСТОЯНИЕ: Одна неполадка, ожидающая своей очереди" (Status: One problem, waiting for its turn) with an "ИСПРАВИТЬ" (Fix) button. The main window has a sidebar with various security modules, and the "Хранилище" (Storage) tab is selected. The "Хранилище" section has a checkbox "Хранилище файлов включено" (File storage is enabled) which is checked. Below it, there is a table titled "Хранить на этом компьютере" (Store on this computer) with columns: "По умолчанию..." (By default...), "Состояние" (Status), "Буква диска" (Disk letter), and "Путь к файлу:" (File path:). The table is currently empty. Below the table is a section titled "Содержимое ..." (Content ...) with a table with columns "Путь к файлу:" (File path:) and "Тип фильтра" (Filter type). This table is also empty. At the bottom of the window, there is a search icon and text: "Список хранилищ найден на этом компьютере. Для поиска других хранилищ нажмите на кнопку справа." (List of storage found on this computer. To search for other storage, click the button on the right). The BitDefender logo and navigation links are at the bottom.

Хранилище

Чтобы отключить хранилище, снимите флажок **Хранилище файлов включено** и нажмите **Да** для подтверждения. Если вы отключите функцию хранилища, все хранилища будут заблокированы, и вы больше не сможете обращаться к файлам, которые в них содержатся.

В таблице, расположенной вверху, отображаются хранилища, расположенные на вашем компьютере. Здесь отображается имя, состояние (открыто /



заблокировано), буква диска и полный путь к хранилищу. В таблице внизу отображается содержимое выбранного хранилища.

22.2.1. Создание хранилища

Чтобы создать новое хранилище, воспользуйтесь любым из следующих способов:

- Нажмите кнопку **Создать Хранилище**.
- Щелкните правой кнопкой внутри таблицы хранилищ и нажмите **Создать**.
- Щелкните правой кнопкой на вашем рабочем столе или в папке на вашем компьютере, укажите на **BitDefender Хранилище Файлов** и выберите **Создать**.

Появится новое окно.

Создать хранилище файлов

Выполните следующие действия:

1. Укажите расположение и имя файла хранилища.
 - Нажмите **Обзор**, выберите расположение хранилища и сохраните файл хранилища под желаемым именем.
 - Введите полный путь к файлу хранилища на диске.
2. Выберите букву диска из меню. Когда вы откроете хранилище, в Моем компьютере появится виртуальный диск, которому будет назначена выбранная буква.
3. Введите пароль к хранилищу в поле **Пароль**. Каждый, кто будет пытаться открыть хранилище и обратиться к файлам, должен будет ввести пароль.



4. Выберите **Форматировать диск**, чтобы отформатировать виртуальный диск, соответствующий хранилищу.
5. Если вы хотите сменить стандартный размер (50 МБ) хранилища, введите нужное значение в поле **Размер хранилища**.
6. Нажмите **Создать**, если вы просто хотите создать хранилище в выбранном месте. Чтобы создать и отобразить хранилище в виде виртуального диска в Моем компьютере, нажмите **Создать&Открыть**.

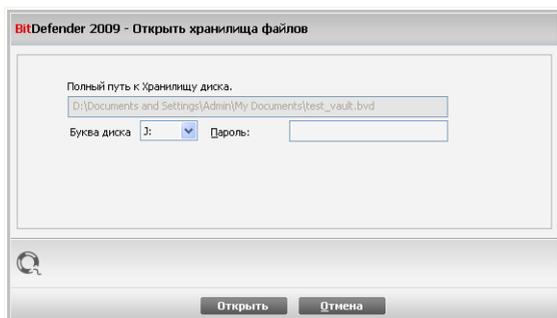
22.2.2. Открытие хранилища

Для работы с файлами, расположенными в хранилище, необходимо открыть хранилище. При открытии хранилища в Моем компьютере появится виртуальный диск. Этот диск будет снабжен буквой, назначенной хранилищу.

Чтобы открыть хранилище, воспользуйтесь любым из следующих способов:

- Выберите хранилище из таблицы и нажмите  **Открыть Хранилище**.
- Щелкните правой кнопкой на хранилище в таблице и выберите **Открыть**.
- Щелкните правой кнопкой на файле хранилища на вашем компьютере, укажите на **BitDefender Хранилище Файлов** и выберите **Открыть**.

Появится новое окно.



Открытие файла хранилища

Выполните следующие действия:

1. Выберите букву диска из меню.



2. Введите пароль к хранилищу в поле **Пароль**.
3. Нажмите **Открыть**.

22.2.3. Блокирование хранилища

Когда вы закончите работать с хранилищем файлов, вам нужно будет заблокировать его, чтобы защитить свои данные.

Для блокирования хранилища воспользуйтесь любым из следующих способов:

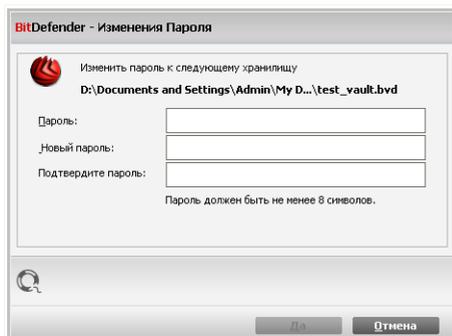
- Выберите хранилище из таблицы и нажмите **Блокировать**.
- Щелкните правой кнопкой на хранилище в таблице и выберите **Заккрыть**.
- Щелкните правой кнопкой на файле хранилища на вашем компьютере, укажите на **BitDefender Хранилище Файлов** и выберите **Заккрыть**.
- Щелкните правой кнопкой на соответствующем виртуальном диске в Моем компьютере, укажите на **BitDefender Хранилище Файлов** и выберите **Заккрыть**.

22.2.4. Смена пароля хранилища

Чтобы сменить пароль хранилища, воспользуйтесь любым их следующих способов:

- Выберите хранилище из таблицы и нажмите **Изменить пароль**.
- Щелкните правой кнопкой на хранилище в таблице и выберите **Изменить пароль**.
- Щелкните правой кнопкой на файле хранилища на вашем компьютере, укажите на **BitDefender Хранилище Файлов** и выберите **Изменить пароль**.

Появится новое окно.



Изменить пароль

Выполните следующие действия:

1. Введите текущий пароль к хранилищу в поле **Старый пароль**.
2. Введите новый пароль в полях **Новый пароль** и **Подтвердите пароль** fields.



Замечание

Пароль должен быть не менее 8 символов. Чтобы получить сильный пароль, используйте комбинации символов в верхнем и нижнем регистре, числа и специальные символы (такие как, например, #, \$ или @).

3. Нажмите **ОК**, чтобы сменить пароль.

22.2.5. Добавление файлов в хранилище

Чтобы добавить файлы в хранилище, воспользуйтесь следующей процедурой:

1. Нажмите кнопку **Добавить файлы**. Появится новое окно.
2. Выберите файлы/папки, которые вы хотите добавить в хранилище.
3. Нажмите **ОК**, чтобы скопировать выделенные объекты в хранилище.



Замечание

Нельзя добавлять в хранилище системные файлы или файлы приложений.



22.2.6. Удаление файлов из хранилища

Чтобы удалить файлы из хранилища, воспользуйтесь следующей процедурой:

1. В таблице хранилищ выберите хранилище, содержащее файл, который вы хотите удалить.
2. Выберите файл, который нужно удалить, из таблицы, где отображается содержание хранилища.
3. Нажмите кнопку **✕ Удалить файл**.



Замечание

Если хранилище открыто, вы можете непосредственно удалять файлы с виртуального диска, связанного с хранилищем.



23. Игровой режим

Модуль игрового режима позволяет настраивать специальные режимы работы BitDefender:

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

23.1. Игровой режим

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

- Все предупреждения и всплывающие окна BitDefender будут отключены.
- Режим защиты BitDefender в реальном времени будет установлен, как **Разрешен**.
- Брандмауэр BitDefender установлен в режим **Всегда**. Это означает, что все новые соединения (входящие и исходящие) автоматически разрешаются, независимо от используемого порта и протокола.
- По умолчанию обновления не выполняются.



Замечание

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

- Запланированные задания проверки отключены по умолчанию

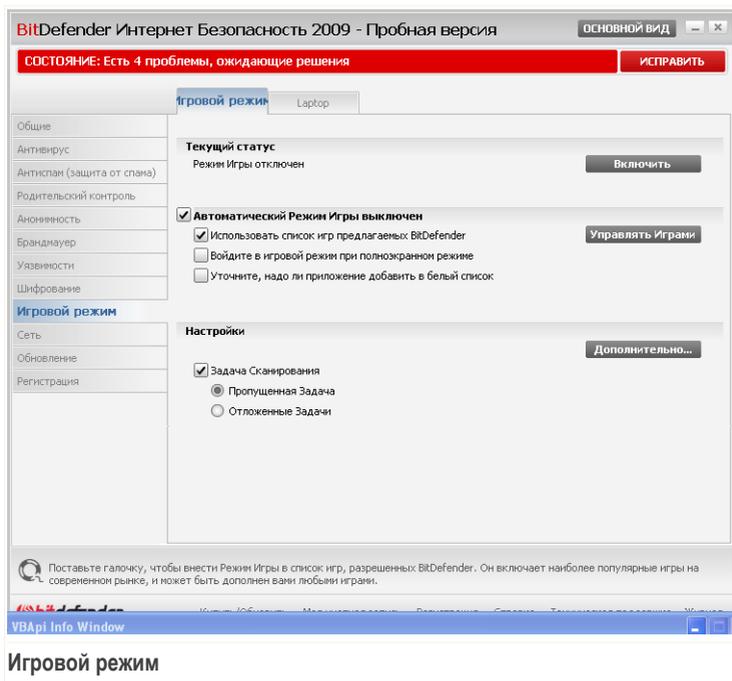
По умолчанию BitDefender автоматически входит в Игровой режим при запуске игры, находящейся в списке известных игр BitDefender, или когда приложение разворачивается на полный экран. Вы можете войти в Игровой режим вручную с помощью горячей клавиши по умолчанию **Ctrl+Alt+Shift+G**. Настоятельно рекомендуется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



Замечание

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

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



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

23.1.1. Настройка автоматического перехода в Игровой режим

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



- **Использовать список игр предлагаемых BitDefender** - для автоматического входа в игровой режим при запуске игры из списка известных игр BitDefender. Для просмотра этого списка нажмите **Управлять играми**, а затем **Игры**.
- **Войдите в игровой режим при полноэкранном режиме** - для автоматического перехода в игровой режим при разворачивании приложения на полный экран.
- **Добавить приложение в список игр?** - вывод запроса на добавление нового приложения в список игр при выходе из полноэкранного режима. Если добавить новое приложение в список игр, то при следующем его запуске BitDefender автоматически перейдет в Игровой режим.

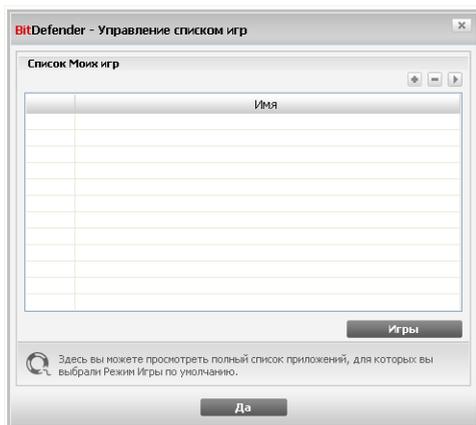


Замечание

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

23.1.2. Управление списком игр

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



Список игр

Новые приложения автоматически добавляются в список при следующих условиях:



- Вы запускаете игру из списка игр, известных программе BitDefender. Для просмотра этого списка нажмите **Игры**.
- Выйдя из полноэкранного режима, вы добавляете приложение в список игр из появившегося окна.

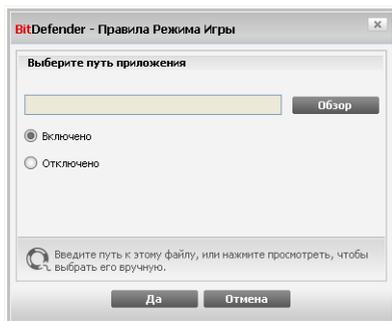
Если вы хотите отключить Автоматический режим игры для отдельного приложения из списка, снимите соответствующий флажок. Следует отключить Автоматический игровой режим для обычных приложений, которые переходят в полноэкранный режим, таких как, например, веб-браузеры и проигрыватели видео.

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

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

Добавление и редактирование игр в списке

При добавлении и редактировании игр в списке появляется следующее окно:



Добавить игру

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

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



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

23.1.3. Настройка параметров игрового режима

Для настройки поведения при запланированных заданиях воспользуйтесь следующими параметрами:

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

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

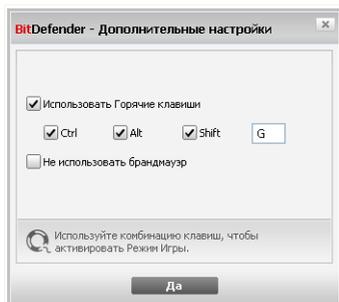
Чтобы автоматически отключать брандмауэр BitDefender, находясь в игровом режиме, воспользуйтесь следующей процедурой:

1. Нажмите **Дополнительно....** Появится новое окно.
2. Установите флажок **Не использовать брандмауэр**.
3. Щелкните мышкой на **Применить** чтобы сохранить сделанные изменения.

23.1.4. Изменение Горячих клавиш Режимы Игры

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

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



Дополнительно...

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

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

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

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



Замечание

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

23.2. Laptop

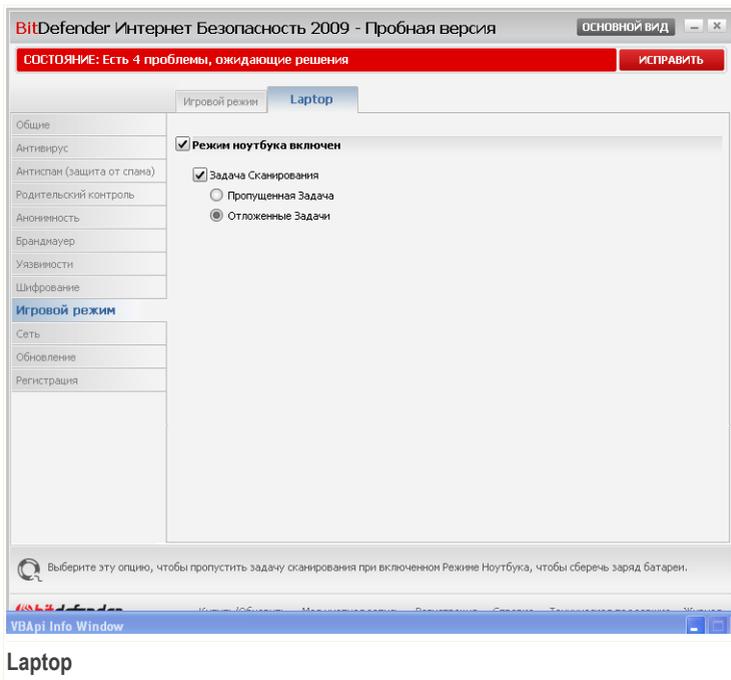
Режим ноутбука специально предназначен для пользователей портативных компьютеров. Его цель - минимизировать влияние работы BitDefender на энергопотребление, когда эти устройства работают от батареи.

В режиме ноутбука запланированные задания не выполняются по умолчанию.

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



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



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

23.2.1. Настройка параметров Режима ноутбука

Для настройки поведения при запланированных заданиях воспользуйтесь следующими параметрами:

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



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



24. Сеть

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

BitDefender Интернет Безопасность 2009 - Пробная версия

основной вид

СОСТОЯНИЕ: Есть 4 проблемы, ожидающие решения

ИСПРАВИТЬ

Сеть

INTERNET 10.10.0.1

Нет компьютера (нажмите, чтобы добавить)

Создать новую сеть

Для того чтобы узнать больше о каждой опции интерфейса BitDefender, проведите мышью поверх окна. Соответствующий текст подсказки будет представлен.

bitdefender

Купить/Обновить - Моя учетная запись - Регистрация - Справка - Техническая поддержка - Журнал

Карта сети

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

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

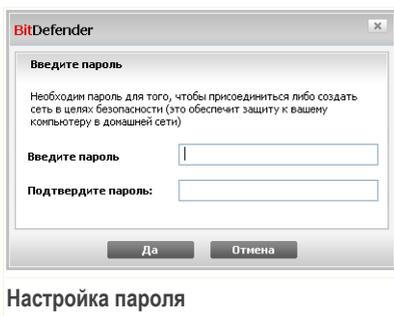


3. Вернитесь к своему компьютеру и добавьте те компьютеры, которыми вы хотите управлять.

24.1. Подключение к сети BitDefender

Чтобы подключиться к домашней сети BitDefender, выполните следующую процедуру:

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



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

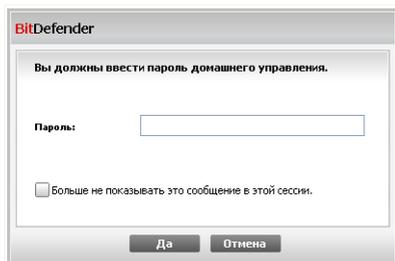
На карте сети будет отображаться имя компьютера.

24.2. Добавление компьютеров в сеть BitDefender.

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

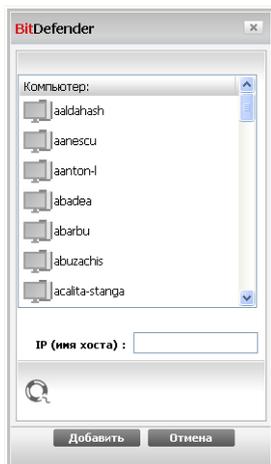
Чтобы добавить компьютер в домашнюю сеть BitDefender, выполните следующую процедуру:

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



Введите пароль

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



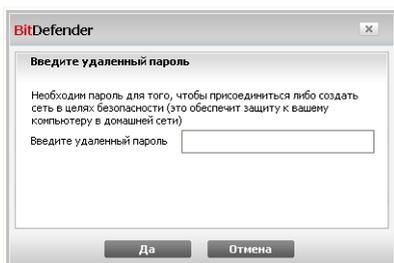
Добавить компьютер

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

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



-  Указывает на находящийся в сети компьютер, на котором установлен BitDefender.
 -  Указывает на автономный компьютер, на котором установлен BitDefender.
3. Сделайте одно из следующего:
- Выберите из списка имя добавляемого компьютера.
 - Введите IP-адрес или имя добавляемого компьютера в соответствующем поле.
4. Нажмите **Добавить**. Появится окно ввода пароля управления домашней сетью для соответствующего компьютера.



Авторизация

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

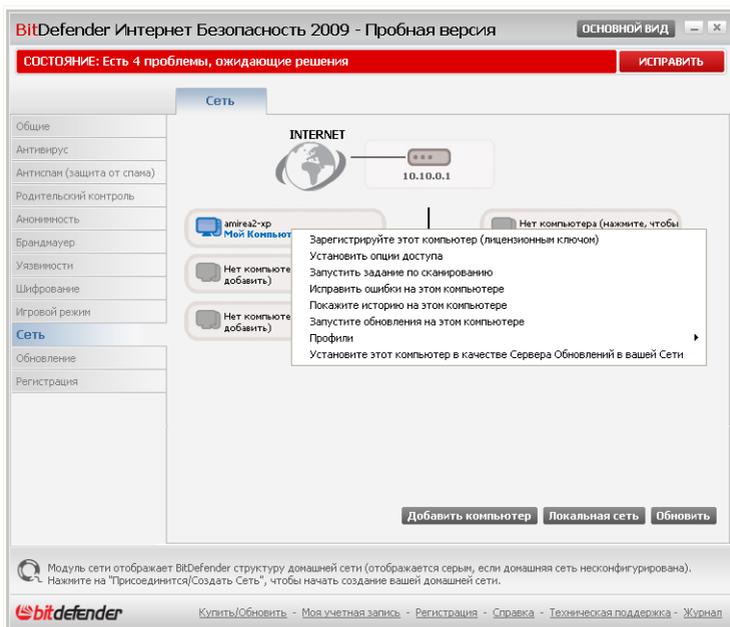


Замечание

На сетевую карту можно добавить до пяти компьютеров.

24.3. Управление сетью BitDefender

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



Карта сети

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

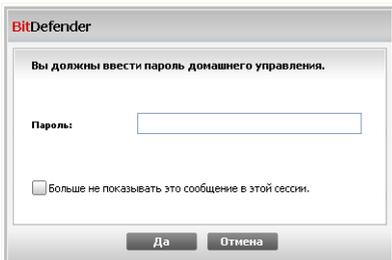
Если щелкнуть правой кнопкой мыши на имени компьютера на карте сети, вы увидите список управляющих заданий, которые можно выполнять с удаленным компьютером.

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



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

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



Введите пароль

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



Замечание

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



25. Обновление

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

Если Вы подключаетесь к Интернет через широкополосное соединения или DSL, BitDefender возьмет на себя решение вопросов безопасности: проверит появление новых образов вирусов сразу же при подключении, и затем будет проверять каждый час.

Если будет обнаружено обновление, вы, возможно, увидите сообщение с просьбой подтвердить обновление, или же обновление начнется автоматически, в зависимости от **настроек автоматического обновления**.

Процесс обновления происходит "на лету", т.е. файлы заменяются по мере обновления. Таким образом, процесс обновления не влияет на работоспособность продукта, и, в то же время, исключается возможность возникновения уязвимости Вашего компьютера.

Имеются следующие варианты обновления:

- **Обновления защиты от вирусов** - как только появляется новая угроза, необходимо обновить файл с образами вирусов, чтобы гарантировать постоянную современную защиту от них. Этот тип обновления также известен как **Обновление образов вирусов**.
- **Обновление защиты от 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 защиты от программ-шпионов** - образы новых программ-шпионов будут добавлены в базу данных. Этот тип обновления также известен как **Обновление Антишпиона**.
- **Обновление программного продукта** - когда выпускается новая версия программы, в новую версию добавляются новые функции и методы проверки, что только улучшает работу программы. Этот тип обновления также известен как **Обновление программы**.



25.1. Автоматическое обновление

Для просмотра сведений, связанных с обновлением, и выполнения автоматических обновлений перейдите в раздел **Обновление**>**Обновление** в окне расширенного вида.

Автоматическое обновление

Здесь Вы можете просмотреть, когда была последняя проверка на наличие обновлений и информацию о последнем обновлении (было ли оно успешным, возникли ли какие-либо ошибки в процессе). Здесь также отображается информация о текущей версии программы и количество образов вредоносных программ.

Если Вы откроете это окно в течение обновления, то увидите статус загрузки.



Важно

Чтобы обезопасить компьютер от атак через Интернет, **Автоматическое обновление** должно быть включено.

Вы можете получить сигнатуры вредоносного ПО для вашего продукта BitDefender, нажав кнопку **Список вирусов**. При этом будет создан и открыт в браузере файл HTML, который будет содержать все доступные сигнатуры. После этого вы сможете выполнять поиск сигнатуры определенного вредоносного ПО по базе или нажатием кнопки **BitDefender Virus List** переходить к онлайн-версии базы сигнатур BitDefender.

25.1.1. Требование к обновлению

Кроме того, вы можете выполнять автоматическое обновление в любое время, нажав кнопку **Обновить сейчас**. Этот тип обновления также именуется **Обновление по требованию**.

Модуль **Обновления** подключится к серверу обновления BitDefender и проверит наличие обновлений. Если программа обнаруживает новое обновление, то, в зависимости от настроек, установленных в разделе **Опции обновления вручную**. Вам будет предложено подтвердить загрузку обновления или обновление будет производиться автоматически.



Важно

Вам может потребоваться перезагрузить компьютер, чтобы завершить обновление. Мы рекомендуем сделать это как можно раньше.

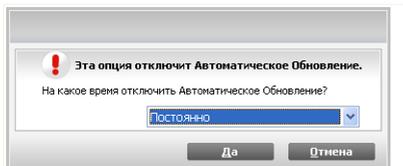


Замечание

Если Вы подключаетесь к Интернету по телефонной линии, лучше всего регулярно обновлять BitDefender по требованию пользователя.

25.1.2. Отключение автоматического обновления

Если Вы выберите эту опцию, то появится окно с предупреждением:



Отключить автоматическое обновление



Вы должны подтвердить свое намерение, выбрав промежуток времени, на который Вы хотите отключить автоматическое обновление. Вы можете отключить на 5, 15 или 30 минут, на час, навсегда или до следующей перезагрузки системы.



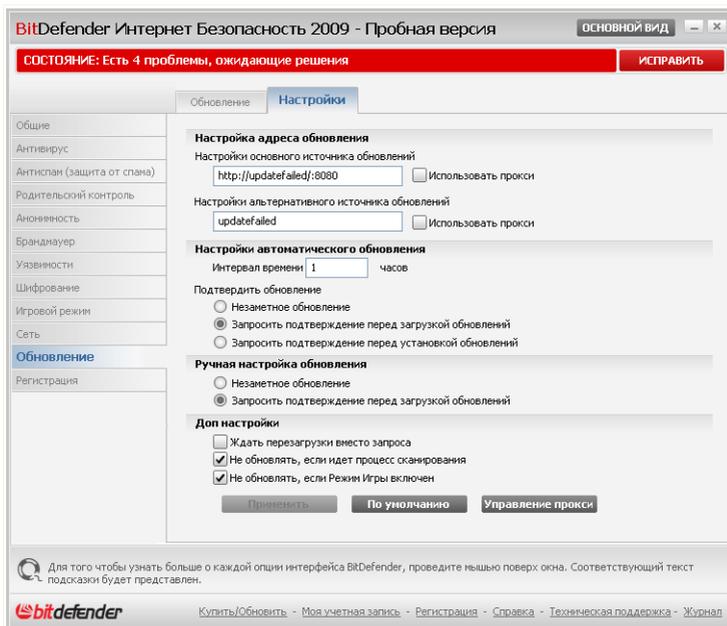
Внимание

Этот аспект является критическим с точки зрения безопасности. Рекомендуем Вам отключать автоматическое обновление на как можно меньший промежуток времени. Если автоматическое обновление отключено, Вы не защищены от самых последних угроз.

25.2. Параметры обновления

Обновление может быть выполнено через локальную сеть, через Интернет напрямую или через прокси-сервер. По умолчанию BitDefender проверяет на наличие обновлений ежечасно через Интернет и устанавливает необходимые обновления без уведомления.

Чтобы установить настройки обновлений и настроить прокси, перейдите в раздел **Обновления>Настройки** окне расширенного вида.



Параметры обновления

В окне Настройки обновления Вы можете увидеть четыре типа настроек: (Настройки местоположения обновления, Настройки автоматического обновления, Обновления вручную и Настройки интерфейса).

25.2.1. Настройки местоположения обновления

Чтобы настроить местоположение обновлений, используйте опции для категории Настройки местоположения обновления.



Замечание

Изменять данные настройки нужно лишь в том случае, если Вы подключены к локальной сети, в которой хранятся обновления BitDefender, или если Вы осуществляете соединение с Интернет через прокси сервер.

Для более надежных и быстрых обновлений, Вы можете настроить 2 места обновления: **Основное местоположение обновлений** и **Альтернативное**



местоположение обновлений. По умолчанию, это: <http://upgrade.bitdefender.com>.

Чтобы изменить адрес источника, откуда берутся обновления, введите URL адрес локального зеркала в поле **URL**, соответствующем месту, которое Вы хотите изменить.



Замечание

Рекомендуем установить местное зеркало в качестве первоначального источника обновления и оставить альтернативный источник без изменений, в качестве запасного на случай, если местное зеркало станет недоступным.

Если компания использует прокси сервер для выхода в Интернет, поставьте отметку в поле **использовать прокси**, а затем нажмите **Настроить прокси**. Больше информации Вы найдете здесь [«Управление прокси»](#) (р. 296)

25.2.2. Конфигурирование автоматического обновления

Чтобы настроить автоматическое обновление, используйте опции в разделе **Настройки автоматического обновления**.

Вы можете указать количество часов между запросами на наличие обновлений в поле **Интервал времени**. По умолчанию интервал составляет 1 час.

Чтобы указать, как необходимо проводить процесс автоматического обновления, выберите одну из следующих опций:

- **Обновление без предупреждения** - BitDefender автоматически скачивает и устанавливает обновления.
- **Запрос перед загрузкой обновлений** - каждый раз, когда появится новое обновление, BitDefender будет запрашивать ваше подтверждение перед загрузкой.
- **Запрос перед установкой обновлений** - каждый раз, когда будет загружено обновление, Вам будет запрос об их загрузке.

25.2.3. Конфигурация обновлений вручную

Чтобы указать, как необходимо проводить процесс ручного обновления (обновления по запросу пользователя), выберите одну из следующих опций в категории **Настройки ручного обновления**:

- **Обновление без предупреждения** - обновление вручную будет выполняться автоматически в фоновом режиме.



- **Запрос перед загрузкой обновлений** - каждый раз, когда появится новое обновление, BitDefender будет запрашивать ваше подтверждение перед загрузкой.

25.2.4. Дополнительные настройки

Чтобы избежать того, когда процесс обновления BitDefender мешает Вашей работе на компьютере, настройте опции в категории **Дополнительные настройки**:

- **Ожидать перезагрузки без запроса** - Если для завершения установки обновления необходимо выполнить 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, BitDefender процесс обновления не будет мешать задачам сканирования.



Замечание

Если BitDefender обновлен, во время сканирования, этот процесс будет прерван.

- **Не выполнять обновление, когда включен режим игры** - BitDefender не обновится, пока включен режим игры. Таким образом, Вы можете минимизировать влияние продукта на работу системы в течение игр.

25.2.5. Управление прокси

Если Ваша компания использует прокси сервер для подключения к Интернет, Вам необходимо указать настройки прокси сервера, чтобы BitDefender имел возможность обновляться. В противном случае, он будет использовать настройки прокси администратора, установившего программу или настройки прокси текущего браузера, если таковые имеются.



Замечание

Настройки прокси сервера могут изменяться только пользователями с правами администратора компьютера или же пользователями, знающими пароль к настройкам программы.



Чтобы настроить прокси сервер, нажмите **Настроить прокси**. Откроется окно **Прокси менеджера**.

Настройки прокси

Администраторские настройки прокси (обнаруженные во время установки)

Адрес : Порт : Имя пользователя:
Пароль :

Текущие настройки прокси (из браузера)

Адрес : Порт : Имя пользователя:
Пароль :

Укажите Ваши настройки прокси

Адрес : Порт : Имя пользователя:
Пароль :

Здесь вы можете поменять прокси настройки администратора.

Да **Отмена**

Управление прокси

Есть три параметра настройки для прокси:

- **Настройки прокси администратора (определены в процессе установки)**
- настройки прокси сервера, определенные в процессе установки программы в учетной записи администратора, эти настройки могут быть изменены, только если Вы работаете под данной учетной записью. Если прокси сервер требует указания имени пользователя и пароля, укажите их в соответствующих полях.
- **Текущие настройки прокси (из браузера, используемого по умолчанию)**
- настройки прокси сервера для текущего пользователя, полученные из браузера, используемого по умолчанию. Если прокси сервер требует указания имени пользователя и пароля, укажите их в соответствующих полях.



Замечание

Поддерживаемыми браузерами являются Internet Explorer, Mozilla Firefox и Opera. Если по умолчанию Вы используете другой браузер, BitDefender не сможет получить настройки прокси сервера для текущего пользователя.



- **Ваши собственные настройки прокси** - вы можете изменять настройки прокси, если зашли как администратор.

Следующие настройки должны быть определены:

- **Адрес** - введите IP-адрес к прокси серверу.
- **Порт** - введите порт использующий BitDefender для подсоединения к прокси серверу.
- **Пользователь** - введите имя пользователя, опознаваемого прокси-сервером.
- **Пароль** - введите пароль пользователя, указанного ранее.

При попытке соединения к Интернет, будет поочередно пробоваться каждый набор настроек прокси, пока BitDefender не удастся установить соединение.

Прежде всего, для соединения к Интернет будет использованы Ваши собственные настройки прокси. Если это не поможет, следующими будут использованы настройки сервера, обнаруженные при установке продукта. В конце концов, если ни один из вариантов не сработает, будут использованы настройки прокси сервера, который использует браузер по умолчанию для соединения с Интернет.

Нажмите **ОК**, чтобы сохранить изменения и закройте окно.

Щелкните мышкой на кнопке **Применить** чтобы сохранить изменения или щелкните мышкой на кнопке **По умолчанию** чтобы загрузить настройки по умолчанию.



26. Регистрация

Чтобы найти полные сведения по вашему продукту BitDefender и состояние регистрации, перейдите в раздел **Регистрация** в окне расширенного вида.

BitDefender Интернет Безопасность 2009 - Пробная версия основной вид

СОСТОЯНИЕ: Есть 4 проблемы, ожидающие решения ИСПРАВИТЬ

Регистрация

Общие
Антивирус
Антиспам (защита от спама)
Родительский контроль
Анонимность
Брандмауэр
Уязвимости
Шифрование
Игровой режим
Сеть
Обновление
Регистрация

Информация о продукте
BitDefender Internet Security 2009
Версия: 12.0.11.4

Информация о регистрации
Зарегистрировано на testare.automat@mailinator.com
Срок действия ключа: 30 дней
Лицензионный ключ: BE1B409B7E067AD03090

Действия

Здесь вы можете просмотреть подробную информацию о регистрации вашего BitDefender продукта, тип лицензии, срок действия и лицензионный ключ.

bitdefender [Купить/Обновить](#) - [Моя учетная запись](#) - [Регистрация](#) - [Справка](#) - [Техническая поддержка](#) - [Журнал](#)

Регистрация

В данном разделе отображаются:

- **Информация о продукте:** продукт BitDefender и его версия.
- **Информация о регистрации:** адрес электронной почты, который используется для входа в учетную запись BitDefender (если она настроена), текущий лицензионный ключ и количество дней до истечения срока действия лицензии.



26.1. Регистрация BitDefender Internet Security 2009

Нажмите **Зарегистрировать** для открытия окна регистрации продукта.

Мастер регистрации

Пожалуйста, следуйте инструкциям ниже, чтобы зарегистрировать ваш продукт BitDefender.

Ваш текущий статус лицензии BitDefender: **Пробная версия**
Ваш текущий лицензионный ключ BitDefender: **VE1B409B7E067AD03090**
Срок действия ключа истекает через: **30 дней**

Здесь вы можете найти ваш лицензионный ключ:

- 1) Наклейка на CD-Rom
- 2) Карта регистрации продукта
- 3) e-mail для онлайн покупок

Параметры лицензии

Если вы хотите сохранить текущий ключ, выберите первую опцию. Если вы хотите добавить новый ключ, выберите вторую опцию и введите ключ в поле ниже.

Продолжить использование текущего ключа
 Я хочу зарегистрировать продукт с новым ключем

Введите новый лицензионный ключ:

Купить лицензию

Чтобы купить лицензионный ключ, нажмите на ссылку ниже.
[Обновите Ваш ключ на BitDefender](#)

Пожалуйста, посетите эту страницу, чтобы зарегистрировать ваш BitDefender продукт.

Регистрация

Вы можете просмотреть статус регистрации BitDefender, действующий лицензионный ключ, и количество дней, которые остались до окончания срока действия лицензии.

Регистрация BitDefender Internet Security 2009:

1. Выберите **Я хочу зарегистрировать продукт с новым ключем**.
2. Введите лицензионный ключ в поле для редактирования.



Замечание

Вы можете найти ваш лицензионный ключ:

- на обложке CD.



- на регистрационной карточке продукта.
- в электронном письме о покупке.

Если у Вас нет лицензионного ключа BitDefender, нажмите соответствующую ссылку для перехода в онлайн-магазин BitDefender и приобретите лицензионный ключ.

Щелкните мышкой на кнопке **Завершить**.

26.2. Создание учетной записи BitDefender

Создание учетной записи BitDefender является обязательной частью процесса регистрации. Учетная запись BitDefender даст вам доступ к обновлениям, специальным предложениям и поощрениям. Если вы потеряете BitDefender лицензионный ключ, вы сможете зайти в свою учетную запись по ссылке <http://myaccount.bitdefender.com>, чтобы восстановить его.



Важно

Вам необходимо создать учетную запись в течении 15 дней со дня установки BitDefender (если вы его зарегистрировали, в течении 30 дней). В противном случае, BitDefender не будет обновляться.

Если вы еще не создали учетную запись BitDefender, нажмите **Учетная запись**, чтобы открыть окно регистрации учетной записи.



BitDefender Internet Security 2009

Учетная запись

Регистрация Моего Аккаунта
Чтобы Ваш продукт постоянно обновлялся последними антивирусными базами, пожалуйста, зарегистрируйтесь и создайте учетную запись BitDefender. В этом случае, Ваш компьютер будет полностью защищен. Вы также можете отложить регистрацию на 15 дней, если у вас пробная учетная запись, или на 30 дней, если у вас оплаченная лицензия.

Зайдите в существующую учетную запись BitDefender! **Создать новую учетную запись BitDefender**

Email:

Пароль:

[Забыли пароль?](#)

Зарегистрироваться позже

Email:

Пароль (6-16 знаков):

Подтвердите пароль:

Имя:

Фамилия:

Страна:

Отправлять мне все сообщения от BitDefender
 Отправлять мне только самые важные сообщения
 Не отправлять мне никаких сообщений

Создание учетной записи

Если Вы не хотите создавать учетную запись BitDefender, выберите **Пропустить регистрацию** и нажмите **Завершить**. В другом случае, действуйте исходя из вашей ситуации:

- «У меня нет учетной записи BitDefender» (р. 302)
- «У меня уже есть учетная запись BitDefender» (р. 303)

У меня нет учетной записи BitDefender

Для создания учетной записи BitDefender выберите **Создать новую учетную запись BitDefender** и введите требуемую информацию. Предоставленные Вами данные конфиденциальны.

- **Адрес электронной почты** - введите адрес своей электронной почты.
- **Пароль** - введите пароль Вашей учетной записи BitDefender. Длина пароля должна быть не менее шести символов.
- **Повторите пароль** - снова введите набранный ранее пароль.



- **Имя** - введите Ваше имя.
- **Фамилия** - введите Вашу фамилию.
- **Страна** - выберите страну, в которой находитесь.



Замечание

Используйте указанные адрес электронной почты и пароль для доступа к своей учетной записи на <http://myaccount.bitdefender.com>.

Чтобы успешно создать учетную запись, Вы должны прежде всего активировать свой электронный адрес. Проверьте электронную почту и следуйте инструкциям в письме, которое будет выслано Вам службой регистрации BitDefender.

Дополнительно, BitDefender может информировать вас о специальных предложениях и поощрениях, через адрес электронной почты, указанной в вашей учетной записи. Выберите одну из доступных функций:

- **Отправлять мне все сообщения от BitDefender**
- **Отправлять мне наиболее важные сообщения**
- **Не отправлять мне сообщения**

Щелкните мышкой на кнопке **Завершить**.

У меня уже есть учетная запись BitDefender

BitDefender автоматически определит, если вы регистрировали учетную запись BitDefender ранее на этом компьютере. В этом случае, предоставьте пароль вашей учетной записи.

Если у Вас уже есть активная учетная запись, но BitDefender не определяет ее, выберите **Использовать существующую учетную запись BitDefender** и укажите e-mail и пароль Вашей учетной записи.

Если Вы забыли пароль, нажмите **Забыли пароль?** и следуйте инструкциям.

Дополнительно, BitDefender может информировать вас о специальных предложениях и поощрениях, через адрес электронной почты, указанной в вашей учетной записи. Выберите одну из доступных функций:

- **Отправлять мне все сообщения от BitDefender**
- **Отправлять мне наиболее важные сообщения**
- **Не отправлять мне сообщения**

Щелкните мышкой на кнопке **Завершить**.



Получение справки



27. Техническая поддержка

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 приоритетом BitDefender.

Вы можете в любое время обратиться за поддержкой по адресу support@bitdef.ru. Чтобы получить оперативный ответ пожалуйста, укажите в Вашем письме как можно больше подробностей о Вашем BitDefender, системе, опишите проблему, с которой Вы столкнулись как можно подробнее.

27.1. База знаний BitDefender

Так называемая «База знаний» BitDefender - это хранилище информации о продуктах BitDefender с открытым доступом для клиентов в режиме реального времени ("on-line"). В ней накапливаются, в виде отчетов, имеющих легкодоступный формат, результаты всей деятельности по оказанию технической поддержки и устранению ошибок в программе группами технической поддержки и разработчиками компании, а также имеются статьи более общего характера об обезвреживании вирусов, управлению внедрением решений BitDefender и подробными пояснениями различных проблем, равно как и множество других материалов.

База знаний BitDefender открыта для всех и снабжена поисковыми средствами, позволяющими легко найти ответ на интересующую Вас проблему. Этот ценный массив информации является еще одним источником технических знаний и экспертных решений для клиентов BitDefender. Все обоснованные информационные запросы и отзывы о найденных программных ошибках, поступившие от клиентов BitDefender своевременно находят свое место в базе знаний BitDefender: в виде отчетов об устранении программных ошибок, обновлениях для максимального устранения недоделок и информационных материалов/статей, дополняющих файлы справки программного продукта.

База знаний BitDefender открыта круглосуточно по адресу <http://kb.bitdefender.com>.



27.2. Просьба помощи

27.2.1. Перейти к самообслуживанию через веб

Возник вопрос? Наши специалисты готовы круглосуточно оказать Вам помощь по телефону, электронной почте или при помощи чата.

Перейдите по нижеследующим ссылкам:

Английский

<http://www.bitdefender.com/site/KnowledgeBase/>

Немецкий

<http://www.bitdefender.com/de/KnowledgeBase/>

Французский

<http://www.bitdefender.com/fr/KnowledgeBase/>

Румынский

<http://www.bitdefender.com/ro/KnowledgeBase/>

Испанский

<http://www.bitdefender.com/es/KnowledgeBase/>

27.2.2. Откройте тикет техподдержки

Если Вы хотите создать уведомление для службы поддержки или получить помощь по электронной почте, просто перейдите по одной из этих ссылок:

Английский: <http://www.bitdefender.com/site/Main/contact/1/>

Немецкий: <http://www.bitdefender.de/site/Main/contact/1/>

Французский: <http://www.bitdefender.fr/site/Main/contact/1/>

Румынский: <http://www.bitdefender.ro/site/Main/contact/1/>

Испанский: <http://www.bitdefender.es/site/Main/contact/1/>



27.3. Контактная информация:

Эффективная связь является залогом успешного бизнеса. За последние 10 лет компании BITDEFENDER удалось завоевать непререкаемый авторитет среди своих клиентов и партнеров за счет превосходства 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.

27.3.1. Адреса веб-сайтов

Отдел продаж: sales@bitdefender.com
Техническая поддержка: support@bitdefender.com
Документация: documentation@bitdefender.com
Партнерские программы: partners@bitdefender.com
Маркетинг: marketing@bitdefender.com
Отдел по связям со СМИ: pr@bitdefender.com
Вакансии: jobs@bitdefender.com
Лаборатория – для вирусов: virus_submission@bitdefender.com
Лаборатория - для спама: spam_submission@bitdefender.com
Жалобы: abuse@bitdefender.com
Веб-сайт: <http://www.bitdefender.com/ru>
ftp архив продукта: <ftp://ftp.bitdefender.com/pub>
Локальные дистрибьюторы: http://www.bitdefender.com/partner_list
База знаний BitDefender: <http://kb.bitdefender.com>

27.3.2. Офисы филиалов

Офисный персонал компании, ответственный за продукт BitDefende, ответит на ваши запросы коммерческого и общего характера, относящейся к сфере их деятельности и географической привязке. Ниже приведены адреса и контактная информация этих офисов.

Россия и страны СНГ (кроме Украины)

BITDEFENDER

West Gate Park, Building H2, 24 Preciziei Street, sector 6
Bucharest, Romania

Э-мейл: sales@bitdefender.com

Телефон: +40 21 2063470

Веб-сайт: <http://www.bitdefender.com/ru>



BitDefender Rescue CD



28. Обзор

BitDefender Internet Security 2009 поставляется с загрузочным диском (BitDefender Rescue CD), который может проверять и лечить все существующие жесткие диски перед запуском операционной системы.

Вы должны использовать компакт-диск BitDefender Реаниматор в любое время, когда операционная система не работает должным образом из-за заражения вирусом. Это обычно случается, когда не используется антивирусная программа.

Обновление базы данных вирусных образов осуществляется автоматически без вмешательства пользователя каждый раз, когда Вы запускаете компакт-диск BitDefender Реаниматор.

BitDefender Rescue CD (диск-реаниматор BitDefender) - это измененный дистрибутив Knoppix, с интегрированным решением BitDefender для Linux на носителе GNU/Linux Knoppix Live CD, который представляет собой готовое к использованию антивирусное решение, которое можно использовать для проверки и "дезинфекции" жестких дисков (включая и разделы Windows NTFS). В то же время, диск-реаниматор BitDefender можно использовать для восстановления ценных данных в случаях, когда не возможно загрузить ОС Windows.



Замечание

Вы можете скачать BitDefender Rescue CD отсюда:
http://download.bitdefender.com/rescue_cd/

28.1. Системные требования

Перед загрузкой BitDefender Rescue CD, необходимо сначала проверить соответствие вашей системы следующим требованиям.

Тип процессора

x86-совместимый процессор с минимальной тактовой частотой 166 МГц, что, однако, не гарантирует устойчивой работы программы. Предпочтительно выбирать процессор поколения i686, с тактовой частотой 800МГц.

Память

Минимум 512 Мб оперативной памяти (рекомендуется 1 Гб)



CD-ROM

BitDefender Rescue CD запускается с компакт-диска, поэтому необходимыми является наличие дисковода CD-ROM и настройка BIOS на загрузку системы с компакт-диска.

Подключение к сети Интернет

Хотя программа BitDefender Rescue CD выполняется без подключения к сети Интернет, для процедур обновления необходим доступ к активной ссылке HTTP, хотя бы через прокси-сервер. Поэтому для установки последнего обновления, подключение к сети Интернет является **ОБЯЗАТЕЛЬНЫМ**.

Графическая разрешающая способность

Стандартная SVGA-совместимая карта.

28.2. Включенное программное обеспечение

В компакт-диск BitDefender Реаниматор входят следующие пакеты программ.

Xedit

Это текстовый редактор.

Vim

Это мощный текстовый редактор, поддерживающий подсветку синтаксиса, графический интерфейс пользователя (GUI) и многое другое. Для более подробной информации смотрите [Домашнюю страницу Vim](#) .

Xcalc

Это калькулятор.

RoxFiler

RoxFiler - быстрый и мощный пакет для работы с графическими файлами.

Больше информации Вы найдете [домашняя страница RoxFiler](#).

MidnightCommander

GNU Midnight Commander (mc) - файловый менеджер.

Более подробная информация [домашняя страница MC](#).

Pstree

Pstree - показывает запущенные процессы.

Top

Top - показывает Linux задачи.



Xkill

Xkill - убивает клиента его X ресурсами.

Partition Image

Partition Image помогает сохранить разделы системных форматов EXT2, Reiserfs, NTFS, HPFS, FAT16 и FAT32 в файлы образов. Данная программа очень полезна при осуществлении резервного копирования данных.

Более подробная информация [домашняя страница Partimage](#).

GtkRecover

GtkRecover - GTK версия консольной программы восстановления. Она помогает восстановить Ваши файлы.

Более подробная информация [домашняя страница GtkRecover](#).

ChkRootKit

ChkRootKit - инструмент, который помогает Вам просматривать ваш компьютер на наличие руткитов.

Более подробная информация [домашняя страница ChkRootKit](#).

Nessus Network Scanner

Nessus - сканер безопасности для Linux, Solaris, FreeBSD и Mac OS X.

Более подробная информация [домашняя страница Nessus](#).

lprtraf

lprtraf – консольная утилита для сбора сетевой статистики.

Более подробная информация [домашняя страница lprtraf](#).

lftop

lftop - утилита позволяющая мониторить трафик в реальном времени.

Более подробная информация [домашняя страница lftop](#).

MTR

MTR - диагностический инструмент сети.

Более подробная информация [домашняя страница MTR](#).

PPPStatus

PPPStatus отображает статистическую информацию о входящих и исходящих потоках трафика по TCP/IP.

Более подробная информация [домашняя страница PPPStatus](#).

Wavemon

Wavemon - программа мониторинга для беспроводных сетевых устройств.



Более подробная информация [домашняя страница Wavemon](#).

USBView

USBView показывает информацию об устройствах, связанных с USB.

Более подробная информация [домашняя страница USBView](#).

Pppconfig

Pppconfig помогает автоматически настраивать dial-up ppp-соединение.

DSL/PPPoE

DSL/PPPoE настраивает PPPoE (ADSL) соединение.

I810rotate

I810rotate - переключатель видео сигналов на i810 аппаратном оборудовании используя i810switch(1).

Более подробная информация [домашняя страница I810rotate](#).

Mutt

Mutt - мощный почтовый клиент на текстовой основе MIME.

Более подробная информация [домашняя страница Mutt](#).

Mozilla Firefox

Mozilla Firefox - один из лучших веб браузеров.

Более подробная информация [домашняя страница Mozilla Firefox](#).

Elinks

Elinks - текстовый веб браузер.

Более подробная информация [домашняя страница Elinks](#).



29. Реаниматор BitDefender

Данный раздел содержит информацию о том, как запускать и останавливать работу диска-реаниматора BitDefender, проверять Ваш компьютер на наличие вредоносных программ, а также сохранять данные с неработающей системы Windows на сменные носители. Однако, при помощи программ, имеющихся на данном диске, Вы можете выполнять гораздо больше действий, чем описано в данном руководстве.

29.1. Запуск BitDefender Rescue CD

Чтобы запустить компакт-диск с данным программным продуктом, установите настройки BIOS вашего компьютера на загрузку с дискового компакт-дисков, поместите компакт-диск с продуктом в дисковод и перезагрузите компьютер. Убедитесь в том, что ваш компьютер настроен на загрузку с компакт-диска.

Подождите, пока на экране монитора появится информация и выполняйте соответствующие инструкции для запуска BitDefender Rescue CD.



Замечание

Перед использованием Реаниматора выберите язык, который вы хотите использовать, из списка доступных языков.



Экран загрузки

При загрузке обновление базы данных вирусных сигнатур осуществляется автоматически без вмешательства пользователя.

После окончания загрузки на экране появится новый интерфейс - рабочий стол. Теперь можно начинать работу с BitDefender Rescue CD.



Рабочий стол



29.2. Остановка BitDefender Rescue CD

Вы можете выполнить безопасное отключение компьютера, для чего следует выбрать команду **Exit** в контекстном меню BitDefender Rescue CD (открывающееся после щелчка правой кнопкой мыши), либо использовать команду **halt** в терминале.



Выберите команду "EXIT"

Когда BitDefender Rescue благополучно закроет все программы, на экране появится новое изображение, соответствующее показанному на следующем рисунке. Теперь можно извлечь CD, чтобы последующую загрузку компьютера выполнить уже с жесткого диска. Теперь ваш компьютер можно выключить или перезагрузить.

```
X Window session terminated without errors.
Shutting down.
INIT: Sending processes the KILL signal
Killing processes with signal 15: (init) (aufs) (aufs) (aufs) (aufs)
ald) (hald-addon-acpi) (hald-addon-keyb) (ksoftirqd/0) (logsave) (inetd)
s/0) (khelper) (kthread) (ata/0) (ata_aux) (kseriod) (kpsmouse) (ksuspend)
) (aio/0) Done.
Waiting for processes to finish.....
Killing processes with signal 9: (init) (aufs) (aufs) (aufs) (aufs)
(kblockd/0) (kacpid) (knoppix-halt) (events/0) (khelper) (kthread) (ata/0)
d) (khsbpkt) (pdflush) (pdflush) (kswapd0) (aio/0) Done.
Waiting for processes to finish.....
Syncing/Unmounting filesystems: /sys/fs/fuse/connections /UNIONFS/lib/in
Turning off swap... Done.
Unmounting remaining file systems.
rootfs unmounted

KNOPPIX halted.
Please remove CD, close cdrom drive and hit return [auto 2 minutes].
```

Ожидайте появления этого сообщения на экране, сигнализирующего о завершении работы программы



29.3. Как выполнить антивирусную проверку?

Когда процесс загрузки завершен, откроется мастер, позволяющий произвести полную проверку Вашего компьютера. Все, что необходимо сделать для этого, - нажать кнопку **Старт**.



Замечание

Если разрешения вашего экрана недостаточно для корректного отображения, Вам будет предложено запустить проверку в текстовом режиме.

Чтобы завершить процесс проверки выполните последовательность из трех шагов.

1. Вы можете просматривать состояние проверки и статистику (скорость сканирования, время до окончания, количество проверенных / зараженных / подозрительных / скрытых объектов и проч.).



Замечание

В зависимости от сложности задач проверки, процесс сканирования может занять некоторое время.

2. Вы можете просмотреть количество проблем, влияющих на безопасность Вашей системы.

Проблемы отображаются группами. Щелчок мышки на значке "+" разворачивает список, а на значке "-" – закрывает его.

Для каждой группы проблем Вы можете выбрать общее действие, либо есть возможность выбрать отдельное действие для каждой проблемы.

3. Здесь Вы можете просмотреть краткий обзор.

Если Вы хотите просканировать только определенную директорию, тогда необходимо:

Просмотрите ваши папки, щелкните правой кнопкой мышки на названии файла или каталога и выберите команду **Послать**. Затем выберите **BitDefender Scanner**.

Вместо этого, Вы можете запустить командную строку с терминала. **BitDefender Antivirus Scanner** начнет проверку выбранного Вами файла или папки с заданным по умолчанию местоположением.

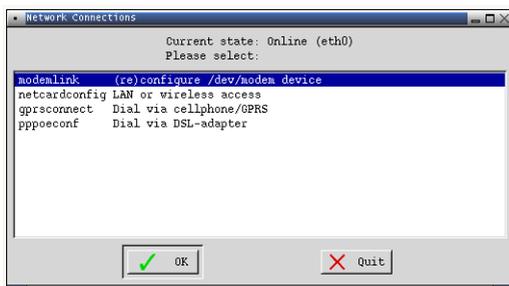
```
# bdsfan /path/to/scan/
```



29.4. Как настроить соединение с интернетом?

Если Вы находитесь в сети DHCP (использующей протокол динамического выбора хост-машины), и в вашем компьютере установлена сетевая карта стандарта Ethernet, то в этом случае связь с Internet должна обнаруживаться и устанавливаться автоматически. Для настройки сети вручную, Вам следует выполнить следующие инструкции.

1. Дважды щелкните на ярлыке Сетевые подключения на рабочем столе. Появится следующее окно.



Сетевые подключения

2. Выберите тип подключения, который вы используете, и нажмите ОК.

Подключение	Описание
modemlink	Выберите этот тип подключения, если для доступа в Интернет вы используете модем и телефонную линию.
netcardconfig	Выберите этот тип подключения, если для доступа в Интернет вы используете локальную сеть (Local Area Network). Она также пригодна для беспроводных соединений.
gprsconnect	Выберите этот тип подключения, если вы выходите в Интернет через мобильную сеть с помощью GPRS (General Packet Radio Service), со своего компьютера.



Подключение	Описание
	Конечно же, вы можете также воспользоваться GPRS-модемом вместо мобильного телефона.
pppoeconf	Выберите этот тип подключения, если для доступа в Интернет вы используете модем DSL (Цифровая абонентская линия).

3. Следуйте указаниям на экране. Если вы не уверены в своем ответе, посоветуйтесь с системным или сетевым администратором.



Важно

Имейте в виду, что только вы активируете модем, выбрав описанные выше параметры. Для настройки сетевого подключения выполните следующие шаги.

1. Щелкните правой кнопкой мыши по рабочей области. Появится контекстное меню BitDefender реаниматор CD.
2. Выберите опцию **Терминал (как root)**.
3. Попробуйте ввести следующие команды:

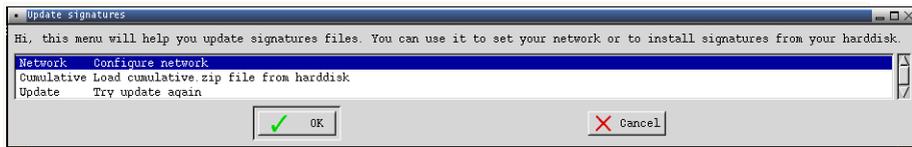
```
# pppoeconf
```

4. Следуйте указаниям на экране. Если вы не уверены в своем ответе, посоветуйтесь с системным или сетевым администратором.

29.5. Как обновлять BitDefender?

Во время загрузки системы обновление вирусных сигнатур происходит автоматически. Однако если вы пропустите этот шаг, здесь описывается процедура обновления BitDefender.

1. Дважды щелкните на ярлыке Обновить сигнатуры на рабочем столе. Появится следующее окно.



Обновление сигнатур

2. Сделайте одно из следующего:
 - Выберите **Кумулятивная** для установки сигнатур, уже сохраненных на жестком диске, найдя и загрузив файл `cumulative.zip` на вашем компьютере.
 - Выберите **Обновить**, чтобы сразу подключиться к интернету и загрузить последние сигнатуры вирусов.
3. В конце щелкните мышкой на кнопке **OK**.

29.5.1. Как я делаю обновление BitDefender через прокси?

Если есть прокси-сервер между вашим компьютером и Интернет, то необходимо сделать некоторые настройки конфигурации, чтобы обновить вирусные сигнатуры. Чтобы выполнить обновление BitDefender через прокси-сервер, необходимо выполнить следующие шаги:

1. Щелкните правой кнопкой мыши по рабочей области. Появится контекстное меню BitDefender реаниматор CD.
2. Выберите опцию **Терминал (как root)**.
3. Тип команды: `cd /ramdisk/BitDefender-scanner/etc`.
4. Тип команды: `mcedit bdscan.conf`, чтобы редактировать этот файл используя GNU Midnight Commander (mc).
5. Раскомментируйте следующую строку: `#HttpProxy =` (просто удалите символ `#`) и задайте домен, имя пользователя, пароль и порт прокси-сервера. Например, эта строка может выглядеть так:
`HttpProxy = myuser:mypassword@proxy.company.com:8080`
6. Нажмите **F2**, чтобы сохранить правильный файл, подтвердите сохранение и тогда нажмите **F10**, чтобы закрыть это.
7. Тип команды: `bdscan update`.



29.6. Как мне сохранить мои данные?

Предположим, Вы не можете запустить Ваш компьютер с ОС Windows из-за неизвестных проблем. В тоже время, Вам очень нужно получить доступ к данным на Вашем компьютере. Именно здесь пригодится диск-реаниматор BitDefender.

Выполните следующие шаги для того, чтобы скопировать данные с Вашего компьютера на сменный носитель, например, на модуль памяти USB:

1. Поместите диск-реаниматор BitDefender в привод, а модуль памяти USB подсоедините к USB порту, и перезагрузите компьютер.



Замечание

Если подключить запоминающее устройство позже, нужно будет смонтировать его с помощью следующей процедуры:

- a. Дважды щелкните на ярлыке Terminal Emulator (Эмулятор консоли) на рабочем столе.
- b. Введите следующую команду:

```
# mount /media/sdb1
```

Примите во внимание, что в зависимости от конфигурации вашего компьютера вместо `sdb1` вам понадобится ввести `sda1`.

2. Ждите, пока BitDefender Rescue CD не загрузится. Появится следующее окно.



Экран рабочего стола

3. Нажмите два раза на раздел, где расположены данные, которые Вы хотите сохранить (например [sda3]).



Замечание

При работе с реаниматором BitDefender Вам придется столкнуться с обозначениями дисков, принятыми в Linux. Таким образом, [sda1] будет скорее всего соответствовать разделу (C:) диска в ОС Windows, [sda3] - (F:), а [sdb1] - модулю памяти.



Важно

Если работа компьютера была неправильно завершена, возможно, причина в том, что некоторые разделы не были смонтированы автоматически. Чтобы смонтировать раздел, выполните следующую процедуру.

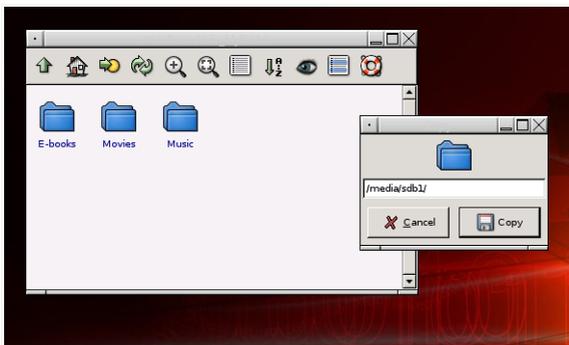
- a. Дважды щелкните на ярлыке Terminal Emulator (Эмулятор консоли) на рабочем столе.
- b. Введите следующую команду:

```
# mount /media/partition_name
```

4. Просмотрите ваши папки и откройте желательную директорию. Например, MyData который содержит поддиректории Видео, Музыка и Книги.



5. Нажмите правой кнопкой мыши на выбранной папки и выберите **Копировать**. Появится следующее окно.



Сохранение данных

6. Введите `/media/sdb1/` в соответствующее текстовое поле и нажмите **Копировать**.

Примите во внимание, что в зависимости от конфигурации вашего компьютера вместо `sdb1` вам понадобится ввести `sda1`.



Глоссарий

ActiveX

ActiveX – это компоненты, которые могут использоваться другими программами и операционными системами вызывающими их. Технология ActiveX используется вместе с программой Microsoft Internet Explorer для создания интерактивных страниц, которые выглядят и работают скорее как компьютерные программы, нежели как простые страницы. С помощью ActiveX пользователь может задавать и отвечать на вопросы, «нажимать» на кнопки и другим способом взаимодействовать с веб-страницей. Элементы ActiveX часто пишутся на языке Visual Basic.

Главный недостаток технологии ActiveX – полное отсутствие какой-либо защиты. Поэтому эксперты по компьютерной безопасности не одобряют их использование в сети Интернет.

Программы сбора рекламной информации о пользователе (Adware)

Программы Adware часто устанавливаются «в качестве нагрузки» к основным приложениям, которые предоставляются бесплатно, при условии что пользователь соглашается установить программу-adware. Поскольку adware-приложения обычно устанавливаются только после того, как пользователь принимает условия, указанные в соответствующем лицензионном соглашении, где указывается функция приложения, то их функционирование не является каким-либо нарушением прав пользователя.

Однако, всплывающие рекламные объявления могут причинять неудобства пользователю, а в некоторых случаях и ухудшать операционные характеристики системы. Кроме того, пользовательская информация, собираемой некоторыми из этих приложений, может показаться недопустимой для разглашения теми пользователями, которые недостаточно полно изучили условия лицензионного соглашения.

Архивировать

Диск или директория, содержащие запасные файлы.

Файл, содержащий один или несколько файлов в сжатом формате.

Брешь в системе (Backdoor)

Брешь в защите системы, специально оставленная разработчиками. Это не всегда делается со злым умыслом: например, в некоторых операционных системах предусмотрены учетные записи, которые могут использоваться персоналом службы технической поддержки или программистами разработчика.



Загрузочный сектор

Сектор в начале каждого диска, в котором хранится информация об архитектуре диска: размер сектора, размер папки и т.д. Загрузочный сектор загрузочного диска содержит еще и программу, загружающую операционную систему.

Загрузочный вирус

Вирус, заражающий загрузочный сектор жесткого или гибкого диска. Попытка загрузиться с зараженной дискеты приводит к тому, что вирус активируется в памяти. Всякий раз, когда Вы загружаете систему с этого места, вирус будет активироваться в памяти.

Браузер

Сокращение от Web browser – приложение, которое ищет и показывает на экране Веб-страницы. Два самых популярных браузера - это Netscape Navigator и Microsoft Internet Explorer. Это графические браузеры, то есть, они показывают и рисунки, и текст. Кроме того, большинство современных браузеров могут отображать мультимедийную информацию, включая звук и видеоизображение, хотя они и требуют установки дополнительных программ и оборудования (plug-ins).

Командная строка

В командной строке пользователь вводит в специальном поле нужные команды на специальном командном языке.

Файлы истории обращений (Cookie)

В сфере Интернет технологий под названием «файлы истории обращений (cookies)» понимаются маленькие файлы, содержащие информацию о компьютере, которую можно проанализировать и использовать для того, чтобы выяснить Ваши интересы и предпочтения. Поэтому технология создания таких файлов процветает, и сейчас Вы можете получить рекламу товаров, основанную на Ваших интересах. Это палка о двух концах. С одной стороны, Вы видите именно то, что Вам может пригодиться. Но с другой – за Вами постоянно следят, и знают, на какой странице Вы находитесь, и на какой кнопке щелкаете мышкой. Понятно, почему сейчас так широко обсуждается конфиденциальность данных пользователей, и многие чувствуют себя ущемленными в своих правах, будучи уверенными, что их «считывают» как кассир в магазине считывает штрих-код на этикетке. Порой эта точка зрения кажется крайностью, но иногда она полностью отражает действительность.



Дисковод

Это оборудование, считывающее данные с диска и записывающее их на диск.

Накопитель на жестких дисках (hard disk drive) считывает данные и записывает их на жесткие диски.

Накопитель на гибких магнитных дисках (floppy drive) работает с гибкими дисками.

Дисковод может быть встроенным, то есть находиться в корпусе компьютера, или же внешним, то есть находиться в отдельном корпусе и подключаться к компьютеру.

Загрузка

Копирование данных (обычно целых файлов) из основного местоположения (источника) на периферийное (внешнее) устройство. Обычно этот термин используется по отношению к копированию файла из источника в сети на свой компьютер. Загрузкой также называют копирование файла с сетевого файлового сервера на компьютер в сети.

Электронная почта

Электронная почта. Отправка сообщений на другие компьютеры через локальную или глобальную сеть.

События

Действие или событие, обнаруженное программой. Событиями могут быть действия пользователя, например щелчок кнопки мыши, или нажатие на клавишу, или системные события, например, переполнение памяти.

Ложная тревога

Событие «ложная тревога» появляется, когда программа считает зараженным файл, который таковым на самом деле не является.

Расширение (имени) файла

Часть названия файла после точки, обозначающая тип данных, хранящихся в нем.

Многие операционные системы, такие как Unix, VMS, и MSDOS, используют расширения имени файла. Обычно они состоят из трех букв, потому что старые ОС не поддерживают более длинные расширения. Например, ".c" текст программы на языке C (C source code), ".ps" – язык PostScript, а ".txt" – любой текстовый файл.



Эвристический (метод)

Способ обнаружения новых вирусов, основанный на правилах. Этот способ проверки не связан напрямую с определенными образами вирусов. Преимущество эвристической проверки состоит в том, что новый вирус не может обмануть фильтр. Однако он может принять подозрительный код в обычных программах за вирус и выдать так называемую «ложную тревогу».

IP

Сокращение от Internet Protocol – Интернет Протокол – маршрутизируемый протокол семейства TCP/IP, отвечающий за адресацию, маршрутизацию, фрагментацию и повторную компоновку IP пакетов.

Прикладная минипрограмма Java апплет

Программа, написанная на языке Java, работающая только на страницах в сети. Чтобы использовать апплет на странице, Вы должны указать его название и размер (длину и ширину в пикселях), которые он может использовать. При открывании страницы браузер загружает эту программу с сервера и запускает ее на компьютере пользователя (который в этом случае называется «клиент»). Апплеты отличаются от приложений, которыми они управляются, более строгим протоколом обеспечения безопасности.

Например, даже если минипрограмма запускается на компьютере-клиенте, она не может считывать или записывать данные на этот компьютер. Кроме того, апплеты могут считывать и записывать данные только с того домена, которым они обслуживаются.

Макро-вирус

Компьютерный вирус, который кодируется как встроенный в документ макрос. Многие приложения, такие как Microsoft Word и Excel поддерживают сложные макроязыки.

Эти приложения позволяют встраивать макросы в документ, и эти макросы выполняются всякий раз, когда Вы открываете документ.

Почтовая программа (клиент)

Приложение, которое позволяет Вам отправлять и получать электронную почту.

Память

Внутренние устройства хранения информации. Термин «Память» относится к запоминающему устройству, например, микросхеме. Термин «Накопитель» относится к таким устройствам, как диски. В каждом компьютере изначально есть физическая память, называемая оперативная (основная) память или RAM.



Не-эвристический (метод)

Этот метод проверки основан на использовании определенных образов вирусов (сигнатур). Основное преимущество этого метода состоит в том, что его нельзя обмануть похожей на вирус программой, а следовательно, не возникает ложная тревога.

Запакованные программы

Файл в сжатом формате. Многие операционные системы и приложения 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, запаковывающая файлы (архиватор), может заменить эти пробелы специальным символом пробелов и количеством замененных пробелов. В этом случае десять пробелов займут всего лишь два байта. И это только один из многих методов архивации файлов.

Путь

Точное местоположение файла на компьютере. Это местоположение обычно описывается средствами иерархической файловой системы сверху вниз, указывая диск, каталог и подкаталоги, сам файл и расширение файла, приблизительно так : c:\jobscompany/resume.txt. Эта подробная информация и есть полный путь.

Маршрут между двумя объектами, например, канал связи между двумя компьютерами.

Фишинг (Phishing)

Действие, сводящееся к отправке пользователю электронного письма якобы от имени реально существующей организации с целью получения обманным путем конфиденциальной информации о пользователе и ее последующего присвоения в корыстных целях. В получаемом пользователем сообщении по электронной почте его с помощью ссылки приглашают посетить якобы официальный веб-сайт реально существующей организации, где его просят подтвердить или обновить личные данные (например, пароли и номера банковского счета, кредитной карточки, карточки социального обеспечения). Однако на самом деле такого рода веб-сайт является поддельным и создается для кражи конфиденциальной информации пользователей.

Полиморфный вирус

Вирус, изменяющий свою форму всякий раз, заражая новый файл. Поскольку у таких вирусов нет бинарной закономерности, их трудно обнаружить.



Порт

Компьютерный интерфейс, с помощью которого подключается внешнее устройство. У персональных компьютеров есть несколько видов портов. Внутри корпуса есть несколько портов для подключения дисководов, монитора и клавиатуры. Снаружи есть порты для подключения модемов, принтеров, мыши и других внешних устройств.

В сетях на базе протоколов TCP/IP и UDP порт – это конечная точка логического подключения. Номер порта указывает на его тип. Например, порт номер 80 используется для HTTP трафика.

Файл отчета

Файл, содержащий список совершенных действий. BitDefender включает в отчеты путь к проверенным файлам, папки, количество проверенных архивов и файлов, а также сколько подозрительных и зараженных файлов обнаружено.

Руткит

Руткиты - это набор программных инструментов, позволяющих получить доступ к системе на уровне администратора. Термин впервые использовался для операционных систем UNIX и относился к инструментам перекомпиляции, которые позволяли получить права администратора, при этом их присутствие оставалось скрытым для системных администраторов.

Основной целью руткитов является скрывать процессы, файлы, логины и журналы. Они также могут перехватывать данные с терминалов, сетевых соединений или 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 (скрипт)

Еще один термин, обозначающий макрос или командный файл. Сценарий – это набор команд, выполняющихся без участия пользователя.



Спам

Рекламное сообщение или новостная рассылка по электронной почте. Обычно под спамом понимают незаконную рассылку электронных писем, часто коммерческого содержания.

Программа-шпион (Spyware)

Любого рода программа-шпион, которая тайно и без ведома пользователя (чаще всего в рекламных целях) собирает информацию о пользователе во время его с соединения с Интернетом. Шпионские программы обычно маскируют как скрытые компоненты бесплатных или условно бесплатных (shareware) приложений, которые можно скачать с Интернета, хотя следует отметить, что большинство бесплатных или условно бесплатных приложений не содержит программ-шпионов. Программа-шпион после своей установки отслеживает адреса в Интернете, к которым обращается пользователь и тайно пересылает эту информацию третьим лицам. Кроме того, программы-шпионы могут собирать информацию об адресах электронной почты, паролях и даже номерах кредитных карточек пользователей.

Программы-шпионы аналогичны вирусам-троянам в том смысле, что и те и другие устанавливаются самими пользователями во время установки других программ. Жертвами программ-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 работы системы и ее сбоям.

Элементы запуска

Все файлы, помещенные в эту папку будут открываться при запуске компьютера. Это могут быть, например, экран запуска, звуковой файл, проигрываемый при первом запуске компьютера, ежедневник с напоминаниями или другие приложения. Обычно в эту папку помещается не сам файл, а его ярлык.

Системный трей (область уведомлений на панели задач)

Область уведомлений впервые появилась в операционной системе Windows 95. Она расположена на панели задач Windows, обычно в нижней части экрана, рядом с часами и содержит маленькие иконки, обеспечивающие быстрый доступ к таким функциям, как факс, принтер, модем, регулировка



громкости и т.д. Чтобы просмотреть подробную информацию о программе и ее настройки, просто дважды щелкните мышкой на иконке.

TCP/IP

Протокол управления передачей/Интернет протокол (Transmission Control Protocol/Internet Protocol) – набор сетевых протоколов, широко используемых в Интернете. Они объединяют в одну большую сеть множество взаимосвязанных сетей, состоящих из компьютеров с различной архитектурой и с различными операционными системами. Протокол TCP/IP включает в себя стандарты связи между компьютерами и общепринятые правила объединения сетей и трафик маршрутизации.

Вирус класса Троян

Вредоносная программа, маскирующаяся под безвредное приложение. В отличие от обычных вирусов, вирус класса Троян не копирует себя, однако, он может быть не менее разрушительным. Вирусы одного из наиболее опасных типов обещают избавить Ваш компьютер от всех вирусов, но на самом деле загружают вирусы на компьютер.

Этот термин взят из поэмы Гомера «Илиада», где в одной из глав описывается, как греки подарили своим врагам, жителям Трои, огромного деревянного коня, якобы в знак мира. Но после того, как троянцы втащили статую в город, греческие солдаты выскочили из полости в теле коня и открыли городские 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.