bitdefender
INTERNET SECURITY 2011

Руководство пользователя

BitDefender Internet Security 2011
Руководство пользователя

Опубликовано 2010.09.08

Правовые положения


bitdefender

Содержание

Установка и удаление

1. Системные требования

Вы можете установить BitDefender Internet Security 2011 только на компьютеры, использующие следующие операционные системы:

- Windows XP Service Pack 3 (32-разрядная версия)/Windows XP Service Pack 2 (64-разрядная версия)
- Windows Vista SP 1 или более поздней версии (32-/64-разрядная)
- Windows 7 (32-/64-разрядная)

Перед установкой убедитесь, что ваш компьютер соответствует минимальным системным требованиям.

Замечание

Чтобы узнать информацию об операционной системе Windows, установленной на вашем компьютере, а также аппаратную информацию, щелкните правой кнопкой мыши **Мой компьютер** на рабочем столе и выберите в меню **Свойства**.

1.1. Минимальные системные требования

- 1 ГБ свободного пространства на жестком диске
- Процессор 800 МГц
- Память RAM:
  - 512 МБ для Windows XP
  - 1 ГБ для Windows Vista и Windows 7
- Internet Explorer 6.0
- .NET Framework 2 (также доступен в пакете инструментов установщика)
- Adobe Flash Player 10.0.45.2

1.2. Рекомендуемые системные требования:

- 1 ГБ свободного пространства на жестком диске
- Intel CORE Duo (1,66 ГГц) или эквивалент
- Память RAM:
  - 1 ГБ для Windows XP и Windows 7
  - 1,5 ГБ для Windows Vista
- Internet Explorer 7
- .NET Framework 2 (также доступен в пакете инструментов установщика)
- Adobe Flash Player 10.0.45.2

1.3. Требования программного обеспечения

Защита от фишинга обеспечивается только для:

- Internet Explorer 6.0 или более новая
- Mozilla Firefox 3.x
- Yahoo! Messenger 8.1

- Microsoft Windows Live Messenger 8

Шифрование мгновенных сообщений (IM) осуществляется только для:

- Yahoo! Messenger 8.1
- Microsoft Windows Live Messenger 8

Защита от спама обеспечивается для всех почтовых клиентов, поддерживающих протоколы POP3/SMTP.Однако панель инструментов антиспама BitDefender интегрируется только в:

- Microsoft Outlook 2003/2007/2010
- Microsoft Outlook Express
- Microsoft Windows Mail
- Mozilla Thunderbird 3.0.4

2. Подготовка к установке

Перед установкой BitDefender Internet Security 2011 завершите эти приготовления для обеспечения беспрепятственной установки:

- Убедитесь, что компьютер, на котором вы собираетесь установить BitDefender, соответствует минимальным системным требованиям.Если компьютер не соответствует минимальным системным требованиям, BitDefender не будет установлен, либо не будет работать должным образом и это приведет к замедлению работы и нестабильности системы.С полным списком системных требований можно ознакомиться в разделе «*Системные требования*» (p. 2).
- Войдите в систему с учетной записью администратора.
- Удалите все другие программы безопасности с компьютера.Одновременный запуск двух программ безопасности может повлиять на их работу и вызвать серьезные проблемы с системой.Защитник Windows будет отключен по умолчанию перед началом установки.
- Отключите или удалите брандмауэр, который может быть запущен на компьютере.Одновременный запуск двух брандмауэров может повлиять на их работу и вызвать серьезные проблемы с системой.Брандмауэр Windows будет отключен по умолчанию перед началом установки.

3. Установка BitDefender

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

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

  Замечание

  Экран приветствия дает возможность скопировать установочный пакет с компакт-диска на USB-устройство хранения данных. Это полезно, если вам необходимо установить BitDefender на компьютер без CD-ROM.Вставьте в USB-порт устройство хранения данных и щелкните **Копировать на USB**.После этого перейдите к компьютеру без устройства CD-ROM, вставьте устройство в USB-порт и дважды щелкните файл `runsetup.exe` из папки, в которую вы сохранили установочный пакет.

  Если экран приветствия не отображается, перейдите в корневой каталог CD и дважды щелкните `autorun.exe`.

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

Сначала программа установки проверит вашу систему для подтверждения установки.Если установка подтверждена, перед открытием мастера установки будет выведен запрос на выбор языка.

Мастер предоставляет инструкции по установке BitDefender на компьютере, а также пошаговое руководство по настройке основных параметров и пользовательского интерфейса.

3.1. Шаг 1. Введение

Ознакомьтесь с лицензионным соглашением и установите флажок **Установите этот флажок, если вы принимаете условия лицензионного соглашения BitDefender**.Для продолжения нажмите **Далее**.

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

3.2. Шаг 2. Подготовка к установке

BitDefender выполнит сканирование системы и проверит ее на наличие другого установленного программного обеспечения безопасности.

Быстрое сканирование

В целях проверки наличия активного вредоносного ПО выполняется быстрое сканирование критических областей системы.

Сканирование должно занимать не более нескольких минут. Сканирование можно в любое время отменить, нажав на соответствующую кнопку.

Важно

Настоятельно рекомендуется дождаться завершения сканирования. Активное вредоносное ПО может нарушить процесс установки или стать причиной его сбоя.

По завершении сканирования отобразятся его результаты. При обнаружении каких-либо угроз перед продолжением установки необходимо выполнить инструкции по их удалению.

Для продолжения нажмите **Далее**.

Удаление существующего программного обеспечения безопасности

BitDefender Internet Security 2011 отобразит оповещение о наличии других установленных на компьютере продуктах безопасности.Нажмите на соответствующую кнопку для запуска процесса удаления и следуйте инструкциям, чтобы удалить все обнаруженные продукты.

Внимание

Настоятельно рекомендуется удалять все другие антивирусные программы перед установкой BitDefender. Одновременный запуск двух или нескольких антивирусных продуктов обычно приводит к неработоспособности системы.

BitDefender также рекомендует действия, которые следует выполнять при включении функций безопасности Windows.

- **Выключить брандмауэр Windows** — выключает брандмауэр Windows.

Важно

Рекомендуется выключить брандмауэр Windows, так как BitDefender Internet Security 2011 уже включает в себя усовершенствованный брандмауэр. Использование двух брандмауэров на одном компьютере может вызвать проблемы.

- **Отключить Защитник Windows** — отключение Защитника Windows.

Для продолжения нажмите **Далее**.

3.3. Шаг 3. Регистрация

Процедура регистрации BitDefender включает регистрацию продукта с использованием лицензионного ключа и активацию онлайн-функций путем создания учетной записи BitDefender.

Регистрация продукта

Выполните действия, соответствующие текущей ситуации:

- **Я приобрел BitDefender Internet Security 2011 на CD или онлайн**

  В этом случае потребуется зарегистрировать продукт:

  1. Введите лицензионный ключ в поле для редактирования.

     Замечание
     Вы можете найти ваш лицензионный ключ:
     - на обложке CD;
     - на регистрационной карточке продукта;
     - в электронном письме о покупке.

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

  2. Нажмите **Зарегистрировать сейчас**.
  3. Нажмите **Далее**.

- **Я загрузил BitDefender Internet Security 2011 для тестирования**

  В этом случае вы сможете использовать все функции продукта в течение 30-дневного периода.Чтобы начать пробное использование, выберите **Я хочу протестировать BitDefender Internet Security 2011 в течение 30 дней** и нажмите **Далее**.

Активировать онлайн-функции

Вам НЕОБХОДИМО создать учетную запись BitDefender, чтобы получать обновления BitDefender.Учетная запись BitDefender также обеспечивает доступ к функции родительского контроля онлайн, бесплатной техподдержке, а также специальным предложениям и скидкам.В случае утраты лицензионного ключа BitDefender вы можете выполнить вход в свою учетную запись в http://myaccount.bitdefender.com для его восстановления.

Если вы не хотите создавать учетную запись BitDefender прямо сейчас, выберите **Создать учетную запись позже** и нажмите **Далее**.

Замечание
Если BitDefender Internet Security 2011 устанавливается на компьютер в целях тестирования, в этом случае необходимо создать учетную запись BitDefender. После приобретения продукта необходимо в течение 30 дней с момента его установки создать учетную запись.

Или действуйте исходя из ситуаций:

- **У меня нет учетной записи BitDefender**

  Для успешного создания учетной записи BitDefender следуйте этим шагам:

  1. Выберите **Создать новую учетную запись**.
  2. Введите необходимую информацию в соответствующих полях.Информация, которую вы предоставите, останется конфиденциальной.
     - **Имя пользователя** — введите свой адрес электронной почты.
     - **Пароль** — введите пароль вашей учетной записи BitDefender.Пароль должен содержать не менее 6 и не более 16 символов.
     - **Введите пароль повторно** — введите ранее заданный пароль повторно.

       Если выбран параметр "не скрывать пароль при вводе", повторный ввод пароля не требуется.

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

  3. Дополнительно BitDefender может информировать вас о специальных предложениях и бонусах по электронной почте, указанной в вашей учетной записи.Нажмите **Просмотр контактной информации** и выберите один из доступных способов связи в открывшемся окне.
     - **Отправлять мне все сообщения**
     - **Отправлять мне важные сообщения**
     - **Не отправлять мне сообщения**
  4. Нажмите **Подтвердить**.
  5. Для продолжения нажмите **Далее**.

     Замечание
     Чтобы использовать учетную запись, вы должны ее активировать. Проверьте почту и следуйте инструкциям в письме, отправленном вам службой регистрации BitDefender.

- **У меня уже есть учетная запись BitDefender**

  BitDefender автоматически определит, если вы уже регистрировали учетную запись BitDefender на этом компьютере.В этом случае введите пароль вашей учетной записи и нажмите **Подтвердить**.Для продолжения нажмите **Далее**.

  Если у вас уже есть активная учетная запись, но BitDefender не может ее обнаружить, следуйте этим шагам, чтобы привязать продукт к этой учетной записи:

  1. Выберите **Вход (предыд. учетная запись)**.
  2. Введите адрес электронной почты и пароль вашей учетной записи в соответствующих полях.

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

  3. Дополнительно BitDefender может информировать вас о специальных предложениях и бонусах по электронной почте, указанной в вашей учетной записи.Нажмите **Просмотр контактной информации** и выберите один из доступных способов связи в открывшемся окне.
     - **Отправлять мне все сообщения**
     - **Отправлять мне важные сообщения**
     - **Не отправлять мне сообщения**
  4. Нажмите **Подтвердить**.
  5. Для продолжения нажмите **Далее**.

3.4. Шаг 4. Выбор режима просмотра

Здесь можно выбрать тип установки и режим пользовательского интерфейса.

Выберите тип установки

Доступны следующие параметры настройки:

- **Быстрая установка** — при выборе этого параметра выполняется быстрая установка BitDefender без его детальной настройки.
- **Настраиваемая установка** — выберите этот параметр, если вы хотите самостоятельно настроить процесс установки и параметры BitDefender.

Для просмотра видеоруководств, содержащих инструкции по установке, нажмите **Помощь**

Замечание

Чтобы выбрать для установки конфигурацию BitDefender по умолчанию и перейти непосредственно к последнему шагу мастера установки, выберите **Не устанавливать**.

Для продолжения нажмите **Далее**.

Выберите путь для установки

Замечание

Этот шаг отображается только при выборе **Настраиваемой установки**.

По умолчанию BitDefender Internet Security 2011 будет установлен в каталог `C:\Program Files\BitDefender\`.Если вы хотите выбрать другую папку для установки, нажмите **Обзор**, а затем в открывшемся окне выберите папку, в которую хотите установить BitDefender.

Пользователи могут обмениваться друг с другом файлами продукта и вирусными сигнатурами BitDefender.Таким образом, доступно более быстрое обновление BitDefender.Если вы не хотите включать эту функцию, установите соответствующий флажок.

Замечание

Если эта функция включена, совместный доступ к личным идентификационным данным предоставляться не будет.

Для продолжения нажмите **Далее**.

Выбор пользовательского интерфейса

Выберите режим просмотра пользовательского интерфейса, оптимально соответствующий вашим требованиям.BitDefender Internet Security 2011 предоставляет на выбор три типа интерфейса, каждый из которых разработан специально в соответствии с потребностями различных типов пользователей.

Интерфейс "Основной"

Подходит для начинающих пользователей и пользователей, которые хотят обеспечить защиту своих компьютеров с помощью BitDefender без значительного участия в этом процессе. Этот интерфейс прост в использовании и предусматривает минимальное взаимодействие с пользователем.

Все, что требуется от вас, — устранить существующие проблемы, обнаруженные BitDefender. Пошаговый мастер поможет вам в их решении.Кроме того, вы можете выполнять общие задачи, такие как обновление сигнатур вирусов BitDefender и файлов продукта или сканирование компьютера.

Интерфейс "Опытный пользователь"

Пользователь может настраивать основные параметры BitDefender, отдельно устранять неисправности, осуществлять управление продуктами BitDefender, установленными на компьютерах в домашней сети, и выбирать неисправности для отслеживания.Кроме того, настроив функцию родительского контроля, можно управлять действиями своих детей на компьютере и в Интернете.

Интерфейс "Эксперт"

Режим подходит для технически подкованных пользователей и позволяет полностью настроить каждую функцию BitDefender.Вы можете также использовать все задачи, предусмотренные для защиты вашего компьютера и данных.

Выберите требуемые элементы и нажмите **Далее** для продолжения.

3.5. Шаг 5. Настройка

Здесь можно выполнить настройку продукта.

Настройка параметров

Замечание

Этот шаг отображается только при выборе для BitDefender режима интерфейса **Эксперт**.

В этом разделе можно включить или отключить функции BitDefender, которые распределены по двум категориям.Чтобы изменить статус настройки, выберите соответствующий параметр.

- **Настройки безопасности**

  В этой области вы можете включить или отключить настройки продуктов, касающиеся различных аспектов компьютерной и информационной безопасности.

Настройки	Описание
Антивирус	Защита файлов в режиме реального времени гарантирует их проверку при запуске вами или приложением, работающим в этой системе.
Автоматическое обновление	Автоматическое обновление гарантирует, что новейшие продукты BitDefender и файлы сигнатур регулярно автоматически загружаются и устанавливаются.

Настройки	Описание
Проверка уязвимостей	Автоматическое сканирование на наличие уязвимостей обеспечивает обновление важного программного обеспечения на вашем компьютере.
Антиспам	Антиспам фильтрует электронную почту, получаемую вами, маркируя нежелательные сообщения как СПАМ.
Антифишинг	Защита от фишинга распознает страницу, созданную для кражи личной информации, и сообщает об этом пользователю.
Контроль личных данных	Контроль личных данных помогает предотвратить отправку ваших личных данных без вашего согласия. Он блокирует любые мгновенные сообщения, сообщения электронной почты или другие формы передачи данных, которые передают данные, определенные как личные.
Шифрование чата	Шифрование чата служит для защиты обмена сообщениями в Yahoo! Messenger и Windows Live Messenger при условии, что ваши IM-контакты используют совместимый продукт BitDefender и IM-приложения.
Родительский контроль	Родительский контроль ограничивает деятельность ваших детей на компьютере и в сети, основываясь на правилах, определенных вами.Ограничения могут включать блокировку неподобающих веб-сайтов, а также ограничение игр и доступа в Интернет в соответствии с установленным расписанием.
Брандмауэр	Брандмауэр обеспечивает защиту вашего компьютера от атак хакеров и вредоносных программ.

- **Общие настройки**

  Здесь вы можете включить или отключить параметры, связанные с характеристиками продукта и опытом пользователя.

Настройки	Описание
Режим игры	Режим игры временно изменяет настройки защиты, чтобы минимизировать их влияние на деятельность системы во время игры.
Обнаружение режима ноутбука	Режим ноутбука временно изменяет настройки защиты, чтобы минимизировать их влияние на длительность работы батареи вашего ноутбука.
Пароль настроек	Благодаря этому настройки BitDefender могут быть изменены только теми, кто знает этот пароль. Когда вы включите этот параметр, вам будет предложено установить пароль настроек.Введите пароль в оба поля и нажмите **OK** для его установки.
Новости BitDefender	Включив этот параметр, вы будете получать важные новости компании, обновления продукта и список новых угроз от BitDefender.
Уведомления	Включив этот параметр, вы будете получать информационные уведомления.
Панель активности сканирования	Панель активности сканирования — это небольшое прозрачное окно, отображающее прогресс сканирования BitDefender.Для получения дополнительной информации перейдите к *«Панель активности сканирования»* (p. 21).
Отправлять отчеты о вирусах	Включение этого параметра обеспечивает отправку отчетов о сканировании на вирусы в лаборатории BitDefender для анализа. Обратите внимание, что эти отчеты не будут содержать конфиденциальных данных, таких как, например, ваше имя или IP-адрес, и они не будут использоваться в коммерческих целях.
Обнаружение атак	Включение этого параметра обеспечивает отправку отчетов о потенциальных вирусных атаках в лаборатории BitDefender для анализа. Обратите внимание на то, что эти отчеты не будут содержать конфиденциальных данных, таких как, например, ваше имя или IP-адрес, и они не будут использоваться в коммерческих целях.

Для продолжения нажмите **Далее**.

Настройка раздела "Мои инструменты"

Замечание

Этот шаг отображается только при выборе для BitDefender режима интерфейса **Основной** или **Опытный пользователь**.

В разделе **Мои инструменты** можно настроить панель управления, добавив ярлыки для часто используемых инструментов.Таким образом можно обеспечить легкий и удобный доступ к ним.

С помощью этого экрана можно добавить ярлыки для любых из следующих инструментов:

- Родительский контроль — отслеживание и управление действиями детей на компьютере.
- Режим игры — установите для BitDefender запрет на вмешательство в процесс игры.
- Режим ноутбука временно изменяет настройки защиты в целях минимизации их влияния на срок работы аккумулятора ноутбука.
- Управление домашней сетью — управление продуктами BitDefender, установленными на компьютерах, которые входят в домашнюю сеть, с одного компьютера.

Выберите инструменты для добавления и нажмите **Далее** для продолжения.

Настройка родительского контроля

Замечание

Этот шаг отображается только при добавлении функции родительского контроля в раздел "Мои инструменты".

Для выбора доступны три параметра:

- **Настройка родительского контроля для учетных записей детей**

  Выберите этот параметр для включения функции родительского контроля для учетных записей Windows, созданных специально для детей, и управления этой функцией из учетной записи администратора.

- **Настройка родительского контроля для текущей учетной записи**

  При выборе этого параметра для текущей учетной записи Windows будет включена функция родительского контроля. При этом необязательно создавать отдельную учетную запись для детей: правила родительского контроля будут применяться ко всем пользователям текущей учетной записи.

В этом случае пароль требуется для защиты настроек родительского контроля.Эту функцию можно настроить сейчас или позднее в окне BitDefender.

- **Не устанавливать сейчас**

  Выберите этот параметр, чтобы настроить данную функцию позднее, в окне BitDefender.

Для продолжения нажмите **Далее**.

Управление домашней сетью

Замечание

Этот шаг отображается только при добавлении функции управления домашней сетью в раздел "Мои инструменты".

Для выбора доступны три параметра:

- **Настроить этот компьютер в качестве сервера**

  Выберите этот параметр, если управление продуктами BitDefender, установленными на других компьютерах в домашней сети, будет осуществляться с этого компьютера.

  Для подключения к сети требуется пароль.Введите пароль в появившихся текстовых полях и нажмите **Подтвердить**.

- **Настройка компьютера в качестве "клиента"**

  Выберите этот параметр, если управление BitDefender планируется осуществлять с другого компьютера в домашней сети, на котором также установлен BitDefender.

  Для подключения к сети требуется пароль.Введите пароль в появившихся текстовых полях и нажмите **Подтвердить**.

- **Не устанавливать сейчас**

  Выберите этот параметр, чтобы настроить данную функцию позднее, в окне BitDefender.

Для продолжения нажмите **Далее**.

3.6. Шаг 6. Параметры технической поддержки

В этом разделе можно настроить параметры справки и поддержки:

- Включить/отключить **Подсказки**.Подсказки представляют собой сообщения, отображаемые на панели управления BitDefender, которые помогут вам оптимизировать производительность системы.

- Подтвердите адрес электронной почты, который будет использоваться при обращении в службу поддержки клиентов BitDefender. Если вы не собираетесь обращаться в службу поддержки клиентов по электронной почте, установите соответствующий флажок.

3.7. Шаг 7. Подтверждение

Здесь можно просмотреть выбранную конфигурацию.

По умолчанию также запланировано выполнение двух заданий:

- Полное сканирование системы будет выполнено непосредственно по завершении установки.

  Рекомендуется выполнить детальное сканирование, которое поможет обнаружить вирусы и вредоносное ПО в компьютере.

- Сканирование системы запланировано на каждое воскресенье в 2:00.

  Настоятельно рекомендуется выполнять сканирование системы не реже одного раза в неделю.Если расписание по умолчанию вам не подходит, можно выбрать другую дату и время. Если ваш компьютер выключен в запланированное время, сканирование запустится, когда вы включите компьютер.

Нажмите **Завершить**.

3.8. Шаг 8. Завершение

Установка близится к завершению. Выполняется окончательная настройка и установка обновлений.

По завершении установки мастер автоматически закроется.При выборе этого параметра в предыдущем шаге выполняется полное сканирование системы.

Мастер установки выполняет обнаружение сети, к которой подключен компьютер, и классифицирует ее как "домашнюю/офисную" или "общедоступную".

Замечание
Возможно, потребуется перезагрузка системы.

4. Обновление предыдущей версии BitDefender

Можно обновить текущую версию до BitDefender Internet Security 2011, если в настоящее время используется BitDefender Internet Security 2011 beta, 2008, 2009 или 2010 версии.

Есть два способа выполнения обновлений:

- Установка BitDefender Internet Security 2011 непосредственно поверх устаревшей версии.При установке текущей версии без удаления версии 2010 списки друзей и спамеров, а также папка карантина будут импортированы автоматически.
- Удалите предыдущую версию, затем перегрузите компьютер и установите новую версию, следуя указаниям раздела «*Установка BitDefender*» (p. 5).Настройки продукта сохранены не будут.Используйте этот метод обновления в случае, если остальные не подошли.

5. Восстановление или удаление BitDefender

Если вы хотите восстановить или удалить BitDefender Internet Security 2011, пройдите по следующему пути из меню Windows "Пуск": **Пуск → Программы → BitDefender 2011 → Восстановить или удалить**.

Откроется мастер, который поможет завершить выполнение требуемого задания.

1. **Восстановить или удалить**

   Выберите действие для выполнения:

   - **Восстановить** — повторная установка всех компонентов программы.
   - **Удалить** — удаление всех установленных компонентов.

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

2. **Подтвердить**

   Обязательно ознакомьтесь с отображаемыми сведениями перед тем, как нажать **Далее** для подтверждения действия.

3. **Ход выполнения**

   Дождитесь, пока BitDefender завершит выполнение выбранного действия.Это займет несколько минут.

4. **Завершить**

   Отобразятся результаты.

   Для завершения процедуры необходимо перезагрузить компьютер. Нажмите **Перезагрузить** для немедленной перезагрузки или **Завершить**, чтобы закрыть окно и перезагрузить компьютер позднее.

Начало работы

6. Обзор

После установки BitDefender Internet Security 2011 компьютер будет защищен от всех типов вредоносных программ (вирусов, шпионских программ и вирусов-троянов) и интернет-угроз (атак хакеров, фишинга и спама).

Настраивать другие параметры BitDefender, помимо настроенных в процессе установки, необязательно.Тем не менее, пользователь может воспользоваться возможностями BitDefender для отладки и повышения эффективности защиты компьютера.

Время от времени необходимо открывать BitDefender и устранять существующие неполадки.Возможно, вам придется настроить отдельные элементы BitDefender или принять превентивные меры для защиты вашего компьютера и данных.При желании вы можете настроить BitDefender так, чтобы не получать уведомления об определенных событиях.

Если вы не зарегистрировали продукт (в том числе не создали учетную запись BitDefender), не забудьте сделать это до конца пробного срока.Вам необходимо создать учетную запись в течение 15 дней со дня установки BitDefender (если вы используете полную версию, то в течение 30 дней).В противном случае BitDefender не будет обновляться.Для получения дополнительной информации о процессе регистрации перейдите к *«Регистрация и моя учетная запись»* (p. 54).

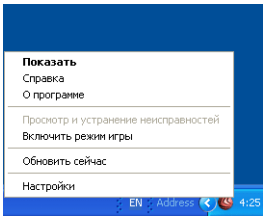
6.1. Открытие BitDefender

Для входа в главный интерфейс BitDefender Internet Security 2011 используйте меню "Пуск" Windows: **Пуск → Программы → BitDefender 2011 → BitDefender Internet Security 2011** или для ускорения процесса дважды щелкните на значке BitDefender на панели задач.

Дополнительные сведения о главном окне приложения см. в *«Окно главного приложения»* (p. 25).

6.2. Значок панели задач

Для более быстрого доступа к управлению продуктом используйте значок BitDefender на панели задач.Двойной щелчок по этому значку открывает приложение BitDefender. Кроме того, щелчок правой кнопкой мыши по значку открывает контекстное меню, которое обеспечивает быстрое управление приложением BitDefender.



Значок панели задач

- **Показать** — открывает основной интерфейс BitDefender.
- **Помощь** — открывает файл помощи, в котором подробно описано, как сконфигурировать и использовать BitDefender Internet Security 2011.
- **О программе** — открывает окно, где можно просмотреть информацию о BitDefender и о том, где искать помощь в случае непредвиденных обстоятельств.
- **Устранить все угрозы** — помогает устранить имеющиеся уязвимости в безопасности компьютера.Если параметр недоступен, значит проблем, требующих решения, нет.Для получения дополнительной информации перейдите к *«Устранение угроз»* (p. 43).
- **Включить/выключить режим игры** — включает/выключает Режим игры.
- **Обновить сейчас** — запускает немедленное обновление.Откроется новое окно, где вы сможете увидеть результаты проверки.
- **Установки** — открывает окно, в котором можно включить или отключить основные настройки продукта, а также изменить настройки профиля пользователя.Для получения дополнительной информации перейдите к *«Настройка основных параметров»* (p. 46).

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

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

Буква G:Продукт работает в Режиме игры.

Если BitDefender не работает, значок на панели задач становится серого цвета.Обычно происходит, когда истекает срок действия лицензионного ключа. Также может произойти, когда BitDefender не отвечает или когда другие ошибки влияют на нормальную работу BitDefender.

6.3. Панель активности сканирования

В окне **График активности** графически показано, как проходит проверка вашей системы на наличие вирусов.По умолчанию это небольшое окно доступно для отображения только в интерфейсе Эксперт.

Серые полоски (**Файловая зона**) показывают число проверенных файлов в секунду, по шкале от 0 до 50.Оранжевые полоски в зоне **Сеть** показывают, сколько килобайт информации передается и загружается из Интернета в секунду, по шкале от 0 до 100.

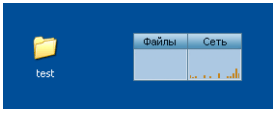
Панель активности сканирования

Замечание

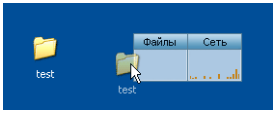
Панель активности сканирования уведомит вас о том, что антивирусная защита или брандмауэр отключены, отображая красный крест поверх соответствующей области (**Файловая зона** или **Зона сети**).

6.3.1. Сканировать файлы и папки

Вы можете использовать панель активности сканирования для быстрого сканирования файлов и папок.Перетащите файл или папку, которую вы хотите проверить, в **Панель активности сканирования**, как показано ниже.



Перетащить файл



Переместить файл

Появится Мастер сканирования и проведет вас по процессу сканирования.

Параметры сканирования. Параметры сканирования предварительно настроены для достижения наилучших результатов обнаружения.При обнаружении инфицированных файлов BitDefender попробует их излечить (удалить вредоносные коды). Если это не удастся, мастер сканирования предоставит вам выбор дальнейших действий с зараженным файлом.Параметры сканирования стандартны, и вы не можете их изменить.

6.3.2. Убрать/восстановить панель активности сканирования

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

1. Откройте BitDefender.
2. Нажмите кнопку **Параметры** в верхнем правом углу окна и выберите **Установки**.
3. В категории "Общие настройки" установите флажок в поле, соответствующем функции **Панель активности сканирования**, для ее включения.
4. Нажмите **OK**, чтобы применить изменения.

6.4. Автоматическое обнаружение устройств

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

Обнаруженные устройства разделяются на следующие категории:

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

При обнаружении такого устройства отображается окно предупреждения.

Для сканирования устройства хранения данных просто нажмите **Да**.Появится Мастер сканирования и проведет вас по процессу сканирования.

Если вы не хотите сканировать устройство, необходимо нажать кнопку **Нет**. В этом случае может оказаться полезной одна из следующих функций:

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

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

1. Откройте BitDefender, нажмите **Параметры** в верхнем правом углу окна и выберите интерфейс **Эксперт**.

2. Перейдите к **Антивирус > Сканировать вирусы**.
3. В списке заданий сканирования найдите задание **Сканирование устройств**.
4. Щелкните на задание правой кнопкой мыши и выберите **Свойства**.Появится новое окно.
5. На вкладке **Обзор** настройте требуемые параметры сканирования.Для получения дополнительной информации перейдите к *«Изменение настроек сканирования»* (p. 79).
6. На вкладке **Обнаружение** выберите типы устройств, которые необходимо обнаружить.
7. Нажмите **OK**, чтобы применить изменения.

7. Окно главного приложения

BitDefender Internet Security 2011 удовлетворяет требованиям как технически подкованных пользователей, так и новичков, так как его графический интерфейс удобен для любой категории пользователей.

Вы можете выбрать один из трех режимов для просмотра пользовательского интерфейса в зависимости от ваших навыков работы на компьютере и своего предыдущего опыта работы с BitDefender.

Интерфейс "Основной"

Подходит для начинающих. Этот режим является простым в использовании и требует минимального взаимодействия с вашей стороны.

Все, что требуется от вас, — устранить существующие проблемы, обнаруженные BitDefender. Пошаговый мастер поможет вам в их решении.Кроме того, вы можете выполнять общие задачи, такие как обновление сигнатур вирусов BitDefender и файлов продукта или сканирование компьютера.

Интерфейс "Опытный пользователь"

Этот интерфейс, предназначенный для пользователей со средними навыками работы на компьютере, предоставляет дополнительные возможности работы в режиме "Основной".

Вы можете устранять проблемы отдельно и решать, какие вопросы контролировать.Более того, вы можете удаленно управлять продуктами BitDefender, установленными на компьютерах в вашем доме.

Интерфейс "Эксперт"

Режим подходит для технически подкованных пользователей и позволяет полностью настроить каждую функцию BitDefender.Вы можете также использовать все задачи, предусмотренные для защиты вашего компьютера и данных.

Выбор режима просмотра осуществляется во время установки.

Изменение режима просмотра:

1. Откройте BitDefender.
2. Нажмите кнопку **Параметры** в верхнем правом углу окна.
3. Выберите в меню желаемый режим просмотра.

7.1. Интерфейс "Основной"

Начинающим неопытным пользователям рекомендуется выбрать интерфейс "Основной".Этот режим прост в использовании и практически не требует вмешательства с вашей стороны.

Это окно включает три основные области:

Область состояния
: Сведения о состоянии отображаются в левой части окна.

Защита компьютера
: Здесь можно выполнить необходимые действия по управлению защитой.

Область справки
: Здесь приведена информация об использовании BitDefender Internet Security 2011 и обращении за поддержкой.

С помощью кнопки **Параметры** в верхнем правом углу окна можно изменить режим пользовательского интерфейса и настроить основные параметры программы.

В правом нижнем углу окна находится несколько полезных ссылок.

Ссылка	Описание
Сведения о лицензии	Откроется окно, в котором отображаются данные о текущем лицензионном ключе. В этом окне также можно зарегистрировать продукт, используя новый лицензионный ключ.
Просмотреть журналы	Просмотр подробного отчета обо всех задачах, выполненных приложением BitDefender в вашей системе.
Справка и поддержка	Для получения помощи по работе с BitDefender перейдите по этой ссылке.
?	Дает доступ к файлу справки об использовании BitDefender.

7.1.1. Область состояния

Сведения о состоянии отображаются в левой части окна.

- **Статус безопасности** информирует вас о проблемах, угрожающих безопасности вашего компьютера, и помогает решить их.При нажатии **Устранить все**, мастер поможет вам легко удалить все угрозы и обеспечить безопасность данных.Для получения дополнительной информации перейдите к «*Устранение угроз*» (p. 43).
- **Статус лицензии** — отображает количество дней, оставшееся до истечения срока действия лицензии.Если вы используете пробную версию или срок действия лицензии вскоре истечет, вы можете нажать **Купить сейчас**, чтобы приобрести лицензионный ключ.Для получения дополнительной информации перейдите к «*Регистрация и моя учетная запись*» (p. 54).

7.1.2. Защита компьютера

Здесь можно выполнить необходимые действия по управлению защитой.

Доступны три кнопки:

- На вкладке **Безопасность** доступны ярлыки для настроек и заданий безопасности.
- С помощью кнопки **Обновить сейчас** можно обновить сигнатуры вирусов и программные файлы BitDefender.Откроется новое окно, где вы сможете увидеть результаты проверки.Если обнаружены обновления, они будут автоматически загружены и установлены на ваш компьютер.
- С помощью раздела **Мои инструменты** можно создавать ярлыки для избранных заданий и настроек.

Для выполнения задания или настройки параметров нажмите на соответствующую кнопку и выберите в меню требуемый инструмент.Чтобы добавить или удалить ярлыки, нажмите на соответствующую кнопку и выберите **Дополнительные параметры**.Для получения дополнительной информации перейдите к *«Мои инструменты»* (p. 33).

7.1.3. Область справки

Здесь приведена информация об использовании BitDefender Internet Security 2011 и обращении за поддержкой.

Подсказки — простой и нескучный способ узнать о принципах компьютерной безопасности и особенностях работы BitDefender Internet Security 2011.

Если вам требуется помощь, введите ключевое слово или вопрос в поле **Справка и поддержка** и нажмите **Поиск**.

7.2. Интерфейс "Опытный пользователь"

Интерфейс "Опытный пользователь", предназначенный для пользователей, обладающих средними навыками работы на компьютере, предоставляет доступ ко всем модулям базового уровня. Позволяет отслеживать предупреждения и критические оповещения, а также устранять нежелательные проблемы.

Окно интерфейса "Опытный пользователь" содержит несколько вкладок.

Панель управления
: Панель управления обеспечивает возможность удобного управления системой защиты и отслеживания ее действий.

Безопасность
: Отображает статус настроек безопасности и позволяет удалить обнаруженные вирусы.Можно запустить задания безопасности или настроить параметры безопасности.

Сеть

Показывает структуру домашней сети BitDefender.Здесь вы можете настраивать и управлять продуктами BitDefender, установленными в вашей домашней сети.Таким образом вы можете управлять безопасностью вашей домашней сети с одного компьютера.

С помощью кнопки **Параметры** в верхнем правом углу окна можно изменить режим пользовательского интерфейса и настроить основные параметры программы.

В правом нижнем углу окна находится несколько полезных ссылок.

Ссылка	Описание
Сведения о лицензии	Откроется окно, в котором отображаются данные о текущем лицензионном ключе. В этом окне также можно зарегистрировать продукт, используя новый лицензионный ключ.
Просмотреть журналы	Просмотр подробного отчета обо всех задачах, выполненных приложением BitDefender в вашей системе.
Купить/продлить	С его помощью вы можете приобрести лицензионный ключ для продукта BitDefender Internet Security 2011.
Справка и поддержка	Для получения помощи по работе с BitDefender перейдите по этой ссылке.
	Дает доступ к файлу справки об использовании BitDefender.

7.2.1. Панель управления

Панель управления обеспечивает возможность удобного управления системой защиты и отслеживания ее действий.

Панель управления состоит из следующих разделов:

- **Подробные сведения о состоянии** — отображает состояние каждого из основных модулей, используя для этого однозначные определения и один из следующих значков:

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

  Красный круг с восклицательным знаком: Существуют проблемы, угрожающие безопсности вашей системы.Критические вопросы требуют вашего немедленного внимания. Не критические вопросы также должны быть решены в кратчайшие сроки.

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

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

- **Статус лицензии** — отображает количество дней, оставшееся до истечения срока действия лицензии.Если вы используете пробную версию или срок действия лицензии вскоре истечет, вы можете нажать **Купить сейчас**, чтобы приобрести лицензионный ключ.Для получения дополнительной информации перейдите к *«Регистрация и моя учетная запись»* (p. 54).
- С помощью раздела **Мои инструменты** можно создавать ярлыки для избранных заданий и настроек.Для получения дополнительной информации перейдите к *«Мои инструменты»* (p. 33).
- **Подсказки** — простой и нескучный способ узнать о принципах компьютерной безопасности и особенностях работы BitDefender Internet Security 2011.

7.2.2. Безопасность

С помощью вкладки "Безопасность" можно осуществлять управление защитой компьютера и данных.

«Область состояния» (p. 29)
«Быстрые задачи» (p. 30)

Область состояния

Область состояния — это полный список контролируемых компонентов безопасности и их текущий статус.Контролируя каждый модуль безопасности, BitDefender информирует вас не только когда вы изменяете настройки, которые могут повлиять на безопасность компьютера, но и когда вы забываете выполнять некоторые важные действия.

Текущее состояние компонента определяется описанием и одним из следующих значков:

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

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

Выбор компонентов для отслеживания:

1. Нажмите **Добавить/редактировать список**.

2. Для включения или отключения отслеживания определенных элементов снимите или установите соответствующий флажок.
3. Нажмите **Закрыть**, чтобы сохранить изменения и закрыть окно.

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

Быстрые задачи

Здесь вы можете найти ссылки на наиважнейшие задачи безопасности:

- **Обновить сейчас** — запускает немедленное обновление.
- **Полное сканирование системы** — эта функция запускает стандартное сканирование системы (за исключением архивов). Для просмотра дополнительных заданий сканирования по запросу нажмите стрелку на этой кнопке и выберите другое задание сканирования.
- **Пользовательское сканирование** — запускает мастера, который поможет вам создать и запустить пользовательскую задачу.
- **Сканирование уязвимостей** — запускает мастер, который проверит вашу систему на наличие уязвимостей и поможет их устранить.
- **Настройка брандмауэра** — отображается окно, в котором можно просмотреть и настроить параметры брандмауэра.Для получения дополнительной информации перейдите к «*Брандмауэр*» (p. 136).

7.2.3. Сеть

Здесь вы можете настраивать и управлять продуктами BitDefender, установленными в вашей домашней сети.Таким образом вы можете управлять безопасностью вашей домашней сети с одного компьютера.

Для получения дополнительной информации перейдите к «*Домашняя сеть*» (p. 161).

7.3. Интерфейс "Эксперт"

В интерфейсе "Эксперт" пользователь получает доступ к каждому отдельному компоненту BitDefender. Здесь можно выполнить детальную настройку BitDefender.

Замечание
Интерфейс "Эксперт" подходит для пользователей, обладающих продвинутыми навыками работы с компьютером, которым известны различные типы угроз безопасности компьютера и принципы работы программного обеспечения безопасности.

В левой части окна расположено меню с перечнем всех модулей безопасности.Каждый модуль имеет несколько закладок, где вы можете настроить соответствующие параметры безопасности или задавать задачи безопасности и административные задачи.В следующем списке приведено краткое описание каждого из модулей.Для получения дополнительной информации перейдите к «Конфигурация и управление» (p. 58) части руководства пользователя.

Общие
: Доступ к основным параметрам или просмотр консоли и подробных сведений о системе.

Антивирус
: Подробная настройка параметров антивируса и операций сканирования, установка исключений и настройка карантина.Здесь также можно настроить антифишинг и оптимизацию поиска.

Антиспам
: Защищает вашу почту от спама, а также позволяет детально настраивать параметры антиспама.

Родительский контроль
: Дает возможность защитить ваших детей от неподобающего содержимого, используя правила персонализированного доступа к компьютеру.

Контроль личных данных
: Предотвращение кражи данных с вашего компьютера и защита вашей конфиденциальности, когда вы находитесь в режиме онлайн.

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.

Уязвимости
: Этот параметр позволяет держать важные приложения на вашем ПК в обновленном состоянии.

Шифрование
: Позволяет шифровать сообщения Yahoo Messenger и Windows Live (MSN) Messenger.

Режим игры/ноутбука
: Позволяет отложить задачи BitDefender по расписанию во время работы ноутбука от батареи, а также убрать все уведомления и всплывающие окна во время игры.

Домашняя сеть
Позволяет настраивать несколько компьютеров у вас дома и управлять ими.

Обновление
Позволяет получать сведения о последних обновлениях, обновления, а также настраивать процесс обновления продукта.

Регистрация
Позволяет регистрировать продукт BitDefender Internet Security 2011, сменять лицензионный ключ и создавать учетную запись BitDefender.

С помощью кнопки **Параметры** в верхнем правом углу окна можно изменить режим пользовательского интерфейса и настроить основные параметры программы.

В правом нижнем углу окна находится несколько полезных ссылок.

Ссылка	Описание
Сведения о лицензии	Откроется окно, в котором отображаются данные о текущем лицензионном ключе. В этом окне также можно зарегистрировать продукт, используя новый лицензионный ключ.
Просмотреть журналы	Просмотр подробного отчета обо всех задачах, выполненных приложением BitDefender в вашей системе.
Купить/продлить	С его помощью вы можете приобрести лицензионный ключ для продукта BitDefender Internet Security 2011.
Справка и поддержка	Для получения помощи по работе с BitDefender перейдите по этой ссылке.
	Дает доступ к файлу справки об использовании BitDefender.

8. Мои инструменты

При работе BitDefender в режиме "Основной" или "Опытный пользователь" можно настроить панель управления по своему выбору, добавив ярлыки часто используемых заданий и настроек.Таким образом, можно быстро получить доступ к регулярно используемым функциям и дополнительным настройкам без необходимости перехода к использованию интерфейса более высокого уровня.

В зависимости от используемого режима пользовательского интерфейса доступны следующие ярлыки, добавленные в раздел "Мои инструменты":

Интерфейс "Основной"
: Выберите "Мои инструменты" в области "Защита компьютера".Отобразится меню.Щелкните ярлык, чтобы запустить соответствующий инструмент.

Интерфейс "Опытный пользователь"
: Ярлыки будут отображаться в разделе "Мои инструменты".Щелкните ярлык, чтобы запустить соответствующий инструмент.

Чтобы открыть окно, в котором можно выбрать ярлыки для отображения в разделе "Мои инструменты", выполните следующие действия:

Интерфейс "Основной"
: В области "Защита компьютера" нажмите "Мои инструменты" и выберите **Дополнительные параметры**.

Интерфейс "Опытный пользователь"
: Нажмите одну из кнопок в разделе "Мои инструменты" или перейдите по ссылке **Настройка раздела "Мои инструменты"**.

С помощью переключателей выберите инструменты для добавления в раздел "Мои инструменты".Можно выбрать любую из следующих категорий инструментов.

- **Задачи сканирования**

  Добавьте задания, регулярно используемые для сканирования системы на наличие угроз безопасности.

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

Задача сканирования	Описание
Сканирование	Проверка всей системы, кроме архивов.При настройках по умолчанию проводится проверка на все типы вирусного ПО, кроме руткитов.
Быстрое сканирование	Функция быстрого сканирования использует технологию "облачного" сканирования для распознавания вредоносных программ, запущенных в системе.Быстрое сканирование занимает, как правило, менее минуты. Быстрое сканирование использует лишь незначительную часть системных ресурсов, которые используются в процессе стандартного вирусного сканирования.
Пользовательское сканирование	Запуск мастера, позволяющего создавать настраиваемые задания сканирования.
Сканировать мои документы	Используйте данное задание для проверки основных папок пользователя: Мои документы, Рабочий стол и Автозагрузка. Это позволит обеспечить безопасность ваших документов, безопасность рабочего пространства и запуск незараженных программ при загрузке.
Настроить расписание сканирования	Переход к окну настройки антивируса, где вы можете настроить сканирование по требованию.

Дополнительные сведения о заданиях сканирования см. в «*Управление существующими заданиями сканирования*» (p. 76).

- **Настройки**

Добавьте ярлыки для тех настроек BitDefender, которые вы хотите отредактировать:

Настройки	Описание
Настройки антивируса	Настройка модуля антивируса. Дополнительные сведения см. в «*Антивирусная защита*» (p. 63).
Настройка брандмауэра	Настройка модуля брандмауэра. Дополнительные сведения см. в «*Брандмауэр*» (p. 136).
Родительский контроль	Настройка модуля родительского контроля. Дополнительные сведения см. в «*Родительский контроль*» (p. 107).

Настройки	Описание
Режим игры	Переключение из режима игры. Дополнительные сведения см. в *«Режим игры»* (p. 155).
Режим ноутбука	Переключение из режима ноутбука. Дополнительные сведения см. в *«Режим ноутбука»* (p. 158).
Обновить сейчас	Запуск обновления BitDefender. Дополнительные сведения см. в *«Обновление»* (p. 165).
Просмотреть и устранить все неполадки	Откройте мастер. С его помощью можно устранить угрозы безопасности, которые отрицательно сказываются на работе системы. Дополнительные сведения см. в *«Устранение угроз»* (p. 43).

- **Помощь и поддержка**

  Перейдите в раздел поддержки. Дополнительные сведения см. в «Свяжитесь с нами непосредственно через интерфейс продукта BitDefender» (p. 214).

9. Оповещения и всплывающие окна

BitDefender использует всплывающие окна и оповещения для информирования о выполняемых операциях или специальных событиях, которые могут заинтересовать пользователя, и при необходимости запрашивает выполнение действий.В этой главе представлено описание всплывающих окон и оповещений BitDefender.

Всплывающие окна представляют собой небольшие окна, которые отображаются на экране в течение определенного времени и содержат сведения о различных событиях BitDefender (например, сканирование сообщений электронной почты, подключение нового компьютера к беспроводной сети, добавление правила брандмауэра и пр.).В отобразившемся всплывающем окне пользователю будет предложено нажать на кнопку **OK** или перейти по соответствующей ссылке.

Оповещения представляют собой окна большего размера, в которых отображается запрос на выполнение действий или сообщения о важных событиях (например, обнаружение вируса).Помимо специальных окон, оповещения могут также отправляться пользователю по электронной почте, через службу мгновенных сообщений или через веб-страницу.

К всплывающим окнам и оповещениям BitDefender относятся:

- Оповещения антивируса
- Оповещения активного вирусного контроля
- Оповещения об обнаружении устройства
- Оповещения и всплывающие окна брандмауэра
- Веб-страницы оповещений антифишинга
- Оповещения родительского контроля
- Оповещения системы защиты данных

9.1. Оповещения антивируса

BitDefender обеспечивает защиту от различных вредоносных программ: вирусов, шпионского ПО и руткитов.При обнаружении вируса или других вредоносных программ BitDefender выполнит определенное действие в отношении зараженного файла и выведет окно оповещения с соответствующим сообщением.

Отображается имя вируса, расположение зараженного файла и действие, выполненное BitDefender.

Нажмите **OK** и закройте окно.

Важно

При обнаружении вируса рекомендуется просканировать всю систему, чтобы убедиться в отсутствии других вирусов.Для получения дополнительной информации перейдите к *«Сканирование файлов и папок»* (p. 171).
Если не удалось заблокировать вирус, см. *«Удаление вредоносного ПО из системы»* (p. 203).

9.2. Оповещения активного вирусного контроля

Активный вирусный контроль может быть настроен на оповещение и напоминание, когда приложение пытается выполнить действие, которое может быть вредоносным.

При выборе интерфейса "Основной" или "Опытный пользователь" при блокировке активным вирусным контролем потенциально опасных приложений будут отображаться всплывающие окна с соответствующими сообщениями.При выборе интерфейса "Эксперт" в окне оповещения выводится запрос на выполнение действия каждый раз, когда какое-либо приложение демонстрирует признаки вредоносного поведения.

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

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

Выберите **Запомнить это действие для этого приложения** перед подтверждением. После этого BitDefender будет впоследствии применять это же действие для обнаруженных приложений.Созданное правило будет отображаться в окне настроек активного вирусного контроля.

9.3. Оповещения об обнаружении устройства

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

Обнаруженные устройства разделяются на следующие категории:

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

При обнаружении такого устройства отображается окно предупреждения.

Для сканирования устройства хранения данных просто нажмите **Да**.Появится мастер сканирования на антивирусы и проведет вас через процесс сканирования.

Если вы не хотите сканировать устройство, необходимо нажать кнопку **Нет**. В этом случае может оказаться полезной одна из следующих функций:

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

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

1. Откройте BitDefender, нажмите **Параметры** в верхнем правом углу окна и выберите интерфейс **Эксперт**.
2. Перейдите к **Антивирус > Сканировать вирусы**.
3. В списке заданий сканирования найдите задание **Сканирование устройств**.
4. Щелкните на задание правой кнопкой мыши и выберите **Свойства**.Появится новое окно.
5. На вкладке **Обзор** настройте требуемые параметры сканирования.Для получения дополнительной информации перейдите к *«Изменение настроек сканирования»* (p. 79).
6. На вкладке **Обнаружение** выберите типы устройств, которые необходимо обнаружить.
7. Нажмите **OK**, чтобы применить изменения.

9.4. Оповещения и всплывающие окна брандмауэра

Брандмауэр использует всплывающие окна для вывода сообщений о различных событиях, связанных с сетевым подключением (например, о подключении нового компьютера к беспроводной сети, о разрешении доступа нового приложения в Интернет или о запрете на сканирование порта).Эти всплывающие окна предоставляют дополнительные возможности для обнаружения попыток вторжения и защиты компьютера от сетевых угроз.

При выборе интерфейса "Эксперт" в окне оповещения выводится запрос на выполнение действия каждый раз, когда неизвестное приложение пытается подключиться к Интернету.

В появившемся окне вы увидите следующее: приложение, пытающееся получить доступ в Интернет, 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.

Важно

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

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.

При использовании интерфейса "Основной" или "Опытный пользователь" попытки подключения будут блокироваться автоматически.

9.5. Оповещения антифишинга

Если включена антифишинговая защита, BitDefender выводит оповещения при попытке доступа к веб-страницам, которые могли быть созданы специально для хищения личных данных.Перед тем как разрешить доступ к такой веб-странице, BitDefender заблокирует страницу и отобразит общее оповещение о веб-странице.

Проверьте адрес веб-страницы в адресной строке браузера.Ищите признаки, которые могут указывать на использование веб-страницы в целях фишинга.Не рекомендуется открывать веб-адреса, если есть сомнения в их надежности.

Вот несколько полезных рекомендаций:

- При вводе адреса легитимного сайта проверьте его правильность. Если адрес введен неверно, повторите ввод и перейдите на веб-страницу еще раз.
- При переходе по ссылке в сообщении электронной почты или в мгновенном сообщении необходимо проверить отправителя такой ссылки. Если отправитель неизвестен, вероятно, вы имеете дело с попыткой фишинговой атаки. Если отправитель вам известен, необходимо проверить, действительно ли этот человек отправил вам данную ссылку.
- При переходе на веб-страницу в Интернете необходимо проверить веб-страницу, на которой обнаружена ссылка (нажмите кнопку "Назад" в веб-браузере).

Если необходимо просмотреть веб-страницу, перейдите по соответствующей ссылке и выполните одно из следующих действий:

- **Просмотреть веб-страницу только в этот раз.** Эта операция не является рискованной, если не отправлять информацию на веб-страницу.Если эта веб-страница является легитимной, вы можете добавить ее в белый список

(перейдите в раздел Панель инструментов антифишинга BitDefender и выберите **Добавить в белый список**).

- **Добавить веб-страницу в белый список.** Веб-страница отобразится сразу, и BitDefender больше не будет выводить это оповещение.

Важно

Добавить в белый список только доверенные веб-страницы (например, веб-страница банка, известные интернет-магазины и пр.).BitDefender не проверяет веб-сайты в белом списке на предмет фишинга.

Управление антифишинговой защитой и белым списком можно осуществлять с помощью панели инструментов BitDefender в веб-браузере.Для получения дополнительной информации перейдите к *«Управление антифишинговой защитой BitDefender в Internet Explorer и Firefox»* (p. 90).

9.6. Оповещения родительского контроля

В модуле родительского контроля можно настроить блокировку:

- неприемлемые веб-страницы.
- Доступ в Интернет в определенные промежутки времени (например, во время уроков).
- веб-страниц, электронных сообщений и мгновенных сообщений, если они содержат определенные слова;
- приложения, такие как игры, чаты, программы обмена файлами и другие.
- Мгновенные сообщения, отправленные заблокированными IM-контактами.

Система информирует пользователя обо всех случаях блокировки активности с помощью определенных типов сообщений оповещения (например, стандартная веб-страница оповещения, сообщение электронной почты или мгновенное сообщение).Предоставляется подробная информация о причинах блокировки действия.

9.7. Оповещения системы защиты данных

Функция контроля личных данных предоставляет опытным пользователям дополнительные возможности защиты личных данных.При включении любого из следующих компонентов в отдельном окне оповещения будет выведен запрос на выполнение действия:

- Контроль реестра — спрашивает разрешения всякий раз, когда какая-либо программа пытается менять запись в реестре для загрузки при запуске системы.
- Контроль cookie — запрашивает разрешение всякий раз, когда новый веб-сайт пытается записать файл cookie.

- Контроль сценариев — запрашивает разрешение всякий раз, когда веб-сайт пытается инициировать выполнение сценария или другого активного контента.

9.7.1. Оповещения реестра

Если включена функция контроля реестра, каждый раз, когда какая-либо программа попытается внести изменения в ключи реестра, исполняемые при загрузке Windows, система будет запрашивать соответствующее разрешение.

Вы можете посмотреть, какая программа пытается внести изменения в системный реестр Windows.

Замечание
BitDefender, как правило, выводит оповещения при установке новых программ, запуск которых требуется при следующей загрузке системы. В большинстве случаев эти программы являются легитимными и могут считаться надежными.

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

На основании вашего ответа создастся правило, которое затем появится в списке правил.То же действие будет применяться, когда эта программа попытается внести изменения в запись реестра.

Для получения дополнительной информации перейдите к *«Контроль реестра»* (p. 132).

9.7.2. Оповещения сценария

Если функция управления сценариями включена, будет выведен запрос на разрешение при каждой попытке запуска веб-сайтом сценариев или другого активного содержимого.

В этом окне вы видите название ресурса.

Нажмите **Да** или **Нет**, и правило будет создано, применено и внесено в список в таблице.Это же действие будет автоматически применяться во всех случаях, когда сайт пытается выполнить запуск активного содержимого.

Замечание
При блокировке активного содержимого некоторые веб-страницы могут отображаться некорректно.

Для получения дополнительной информации перейдите к *«Контроль сценариев»* (p. 134).

9.7.3. Оповещения cookie

Если функция управления cookie включена, система будет запрашивать разрешение каждый раз, когда веб-сайт запрашивает или устанавливает cookie.

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

Нажмите **Да** или **Нет**, и правило будет создано, применено и внесено в список в таблице.Это же действие будет автоматически применяться при каждом подключении к соответствующим веб-сайтам.

Для получения дополнительной информации перейдите к «*Контроль Cookie*» (p. 132).

10. Устранение угроз

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

Уведомления о текущих проблемах:

- Над значком BitDefender на панели задач отображается специальный символ, указывающий на неполадки, ожидающие устранения.Также можно навести курсор на значок, и всплывающее окно подтвердит наличие имеющихся проблем.
- При открытии BitDefender область состояния безопасности покажет количество проблем, влияющих на систему.
  - В интерфейсе "Основной" статус безопасности отображается в левой части окна.
  - Для проверки статуса безопасности в интерфейсе "Эксперт" перейдите в раздел **Общие > Панель управления**.

10.1. Мастер устранения неисправностей

Проще всего устранить существующие проблемы, выполнив пошаговые инструкции **Мастера устранения неисправностей**.Для того чтобы запустить мастер, сделайте следующее:

- Нажмите правой кнопкой мыши значок BitDefender в панели задач и выберите **Устранить все**.
- Откройте BitDefender и в зависимости от используемого режима пользовательского интерфейса выполните следующие действия:
  - В интерфейсе "Основной" нажмите **Просмотреть все проблемы**.
  - В интерфейсе "Эксперт" перейдите в раздел **Общие > Панель управления** и выберите **Просмотреть все проблемы**.

  Замечание
  Также можно добавить ярлык для раздела Мои инструменты.

Отобразится список угроз безопасности, обнаруженных в компьютере.

Все текущие проблемы выбраны для устранения. Если вы не хотите устранять какую-либо из проблем, снимите соответствующий флажок. При этом статус проблемы будет изменен на **Пропустить**.

Замечание
Если вы не хотите получать уведомления об определенных проблемах, необходимо соответствующим образом настроить систему оповещений (как описано в следующем разделе).

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

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

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

  При устранении таких проблем мастер поможет вам успешно завершить задачу.
- **Системные уязвимости.** BitDefender автоматически проверяет вашу систему на наличие уязвимостей и предупреждает вас о них.Системные уязвимости включают следующее:
  - ненадежные пароли учетных записей Windows.
  - устаревшее ПО на вашем компьютере.
  - отсутствующие обновления Windows;
  - Автоматические обновления Windows отключены.

  Когда появляются такие проблемы, запускается мастер сканирования на наличие уязвимостей. Этот мастер поможет вам в устранении обнаруженных системных уязвимостей.Для получения дополнительной информации перейдите к «*Поиск уязвимостей*» (p. 150).

10.2. Настройка отслеживания состояния

Система оповещения о статусе предварительно настроена для отслеживания и оповещения пользователя о наиболее значимых проблемах, которые могут повлиять на безопасность компьютера и данных.Кроме проблем, контролируемых по умолчанию, есть несколько других проблем, о которых вы можете быть проинформированы.

Можно настроить систему оповещений в соответствии с требованиями безопасности и задать конкретные проблемы, о которых система будет

информировать пользователя.Это можно сделать в интерфейсе "Опытный пользователь" или "Эксперт".

- В интерфейсе "Опытный пользователь" систему оповещений можно настраивать из отдельных расположений.Выполните следующие действия:
  1. Перейдите на вкладку **Безопасность**.
  2. Перейдите по ссылке **Добавить/редактировать список** в области состояния.
  3. Для изменения статуса оповещения для элементов используйте соответствующие им флажки.
- В интерфейсе "Эксперт" доступна функция централизованной настройки системы оповещений.Выполните следующие действия:
  1. Перейдите в раздел **Общие > Панель управления**.
  2. Нажмите **Добавить/редактировать оповещения**.
  3. Для изменения статуса оповещения для элементов используйте соответствующие им флажки.

11. Настройка основных параметров

Настроить основные параметры продукта (в том числе перенастроить тип использования) можно в окне "Установки". Чтобы открыть его, выполните следующие действия:

- Откройте BitDefender, нажмите кнопку **Параметры** в верхнем правом углу окна и выберите **Установки**.
- Щелкните правой кнопкой мыши на значок BitDefender на панели задач и выберите **Установки**.

Замечание

Для детальной настройки параметров продукта перейдите в интерфейс "Эксперт".Для получения дополнительной информации перейдите к «Конфигурация и управление» (p. 58) части руководства пользователя.

Настройки организованы в три категории:

- Настройки безопасности
- Настройки оповещений
- Общие настройки

Для отключения настройки выберите соответствующий параметр.

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

Перейдя по ссылке **Перенастроить профиль**, расположенной в правом верхнем углу окна, можно перенастроить тип использования.Для получения дополнительной информации перейдите к *«Перенастройка типа использования»* (p. 50).

11.1. Настройки безопасности

В этой области вы можете включить или отключить настройки продуктов, касающиеся различных аспектов компьютерной и информационной безопасности.Для отключения настройки выберите соответствующий параметр.

Внимание

Используйте уведомление, когда отключаете постоянную защиту или брандмауэр.Выключение этих функций может резко снизить безопасность компьютера. Если их действительно необходимо отключить, не забудьте включить их как можно скорее.

Доступны следующие настройки:

Антивирус

Защита файлов в режиме реального времени гарантирует их проверку при запуске вами или приложением, работающим в этой системе.

Автоматическое обновление

Автоматическое обновление гарантирует, что новейшие продукты BitDefender и файлы сигнатур регулярно автоматически загружаются и устанавливаются.По умолчанию обновления выполняются каждый час.

Поиск уязвимостей

Оповещения модуля автоматического сканирования на наличие уязвимостей сообщают об обнаруженных в системе уязвимостях, которые могут скомпрометировать безопасность компьютера, и предлагают меры по их устранению. К таким уязвимостям относятся: устаревшее программное обеспечение, ненадежные пароли учетных записей пользователей или пропущенные обновления Windows.

Антиспам

Антиспам фильтрует электронную почту, получаемую вами, маркируя нежелательные сообщения как СПАМ.

Антифишинг

Защита от фишинга распознает страницу, созданную для кражи личной информации, и сообщает об этом пользователю.

Оптимизация поиска

Функция оптимизации поиска сканирует ссылки в результатах поиска и сообщает пользователю о том, являются ли эти ссылки надежными и безопасными.

Контроль личных данных

Контроль личных данных помогает предотвратить отправку ваших личных данных без вашего согласия. Он блокирует любые мгновенные сообщения, сообщения электронной почты или другие формы передачи данных, которые передают данные, определенные как личные.

Шифрование чата

Шифрование чата служит для защиты обмена сообщениями в Yahoo! Messenger и Windows Live Messenger при условии, что ваши IM-контакты используют совместимый продукт BitDefender и IM-приложения.

Родительский контроль (текущий пользователь)

Родительский контроль ограничивает деятельность ваших детей на компьютере и в сети, основываясь на правилах, определенных вами.Ограничения могут включать блокировку неподобающих веб-сайтов, а также ограничение игр и доступа в Интернет в соответствии с установленным расписанием.

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

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

Если вы не хотите, чтобы отключенная настройка отображалась как неисправность, необходимо настроить систему слежения соответствующим образом. Это можно сделать в интерфейсе "Опытный пользователь" или "Эксперт".Для получения дополнительной информации перейдите к *«Настройка отслеживания состояния»* (p. 44).

11.2. Настройки оповещений

В этой области можно отключить всплывающие окна и оповещения BitDefender.BitDefender использует оповещения для запроса действий пользователя, а также всплывающие окна для информирования об автоматически выполняемых действиях или других событиях.Для включения или отключения категорий оповещений установите соответствующий флажок.

Важно
Во избежание возникновения проблем большинство таких оповещений и всплывающих окон должны оставаться включенными.

Доступны следующие настройки:

Оповещения антивируса
Оповещения антивируса сообщают пользователю обо всех случаях обнаружения и блокировки BitDefender вирусов.При обнаружении вируса рекомендуется просканировать всю систему, чтобы убедиться в отсутствии других вирусов.

Всплывающие окна активного вирусного контроля.
При выборе интерфейса "Основной" или "Опытный пользователь" при блокировке активным вирусным контролем потенциально опасных приложений будут отображаться всплывающие окна с соответствующими сообщениями.При выборе интерфейса "Эксперт" в окне оповещения выводится запрос на выполнение действия каждый раз, когда какое-либо приложение демонстрирует признаки вредоносного поведения.

Сканирование всплывающих окон электронной почты
В этих всплывающих окнах отображается информация о сканировании BitDefender сообщений электронной почты на наличие вредоносных программ.

Оповещения системы управления домашней сетью

Эти оповещения служат для информирования пользователя о событиях удаленного администрирования.

Всплывающие окна брандмауэра

Брандмауэр использует всплывающие окна для вывода сообщений о различных событиях, связанных с сетевым подключением (например, о подключении нового компьютера к беспроводной сети, о разрешении доступа нового приложения в Интернет или о запрете на сканирование порта).При выборе интерфейса "Эксперт" в окне оповещения выводится запрос на выполнение действия каждый раз, когда неизвестное приложение пытается подключиться к Интернету.

Эти всплывающие окна предоставляют дополнительные возможности для обнаружения попыток вторжения и защиты компьютера от сетевых угроз.

Оповещения карантина

Оповещения карантина сообщают пользователю об удалении старых файлов из папки карантина.

Оповещения системы родительского контроля

При каждом блокировании родительским контролем какой-либо активности выводится соответствующее оповещение (например, вместо заблокированной веб-страницы выводится веб-страница оповещения).

Всплывающие окна регистрации

Всплывающие окна регистрации служат для напоминания о необходимости регистрации BitDefender или для сообщения о том, что срок действия лицензионного ключа истечет в скором времени или уже истек.

11.3. Общие настройки

Здесь вы можете включить или отключить параметры, связанные с характеристиками продукта и опытом пользователя.Для отключения настройки выберите соответствующий параметр.

Доступны следующие настройки:

Режим игры

Режим игры временно изменяет настройки защиты, чтобы минимизировать их влияние на деятельность системы во время игры.

Обнаружение режима ноутбука

Режим ноутбука временно изменяет настройки защиты, чтобы минимизировать их влияние на длительность работы батареи вашего ноутбука.

Пароль настроек

Во избежание несанкционированного изменения настроек BitDefender их можно защитить паролем.Когда вы включите этот параметр, вам будет

предложено установить пароль настроек.Введите пароль в оба поля и нажмите **OK** для его установки.

Новости BitDefender
Включив этот параметр, вы будете получать важные новости компании, обновления продукта и список новых угроз от BitDefender.

Уведомления
Включив этот параметр, вы будете получать информационные уведомления.

Панель активности сканирования
Панель активности сканирования — это небольшое прозрачное окно, отображающее прогресс сканирования BitDefender.

Отправлять отчеты о вирусах
Включение этого параметра обеспечивает отправку отчетов о сканировании на вирусы в лаборатории BitDefender для анализа. Обратите внимание, что эти отчеты не будут содержать конфиденциальных данных, таких как, например, ваше имя или IP-адрес, и они не будут использоваться в коммерческих целях.

Обнаружение атак
Включение этого параметра обеспечивает отправку отчетов о потенциальных вирусных атаках в лаборатории BitDefender для анализа. Обратите внимание на то, что эти отчеты не будут содержать конфиденциальных данных, таких как, например, ваше имя или IP-адрес, и они не будут использоваться в коммерческих целях.

11.4. Перенастройка типа использования

В процессе установки у пользователей была возможность настроить тип использования.Тип использования отражает основные действия, выполняющиеся на компьютере. В зависимости от типа использования интерфейс продукта организуется с целью обеспечения легкого доступа к нужным задачам.

Чтобы перенастроить тип использования, нажмите **Перенастроить профиль** и выполните инструкции мастера конфигурации.Навигация по мастеру осуществляется с помощью кнопок **Далее** и **Назад**.Для выхода из мастера нажмите **Отмена**.

1. **Выберите режим просмотра**

   Выберите предпочтительный режим пользовательского интерфейса.

2. **Настройка раздела "Мои инструменты"**

При выборе интерфейса "Основной" или "Опытный пользователь" выберите также те функции, для которых следует создать ярлыки на панели управления.

3. **Настройка параметров**

   В интерфейсе "Эксперт" пользователь может настроить параметры BitDefender по своему выбору.Для отключения настройки выберите соответствующий параметр.

4. **Настройка родительского контроля**

   Замечание

   Этот шаг отображается только при добавлении функции родительского контроля в раздел "Мои инструменты".

   Для выбора доступны три параметра:

   - **Настройка родительского контроля для учетных записей детей**

     Выберите этот параметр для включения функции родительского контроля для учетных записей Windows, созданных специально для детей, и управления этой функцией из учетной записи администратора.

   - **Настройка родительского контроля для текущей учетной записи**

     При выборе этого параметра для текущей учетной записи Windows будет включена функция родительского контроля. При этом необязательно создавать отдельную учетную запись для детей: правила родительского контроля будут применяться ко всем пользователям текущей учетной записи.

     В этом случае пароль требуется для защиты настроек родительского контроля.Эту функцию можно настроить сейчас или позднее в окне BitDefender.

   - **Не устанавливать сейчас**

     Выберите этот параметр, чтобы настроить данную функцию позднее, в окне BitDefender.

5. **Управление домашней сетью**

   Замечание

   Этот шаг отображается только при добавлении функции управления домашней сетью в раздел "Мои инструменты".

   Для выбора доступны три параметра:

   - **Настроить этот компьютер в качестве "сервера"**

Выберите этот параметр, если управление продуктами BitDefender, установленными на других компьютерах в домашней сети, будет осуществляться с этого компьютера.

Для подключения к сети требуется пароль.Введите пароль в появившихся текстовых полях и нажмите **Подтвердить**.

- **Настройка компьютера в качестве "клиента"**

  Выберите этот параметр, если управление BitDefender планируется осуществлять с другого компьютера в домашней сети, на котором также установлен BitDefender.

  Для подключения к сети требуется пароль.Введите пароль в появившемся текстовом поле и нажмите **Подтвердить**.

- **Не устанавливать сейчас**

  Выберите этот параметр, чтобы настроить данную функцию позднее, в окне BitDefender.

6. **Установка завершена**

   Нажмите **Завершить**.

12. Журнал и события

Ссылка **История** в нижней части главного окна BitDefender открывает другое окно с журналом событий BitDefender. Здесь представлен обзор всех событий, связанных с безопасностью.Например, вы можете проверить, было ли успешным последнее обновление, были ли найдены на вашем компьютере вредоносные программы и т. п.

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

- **Панель управления**
- **Антивирус**
- **Антиспам**
- **Родительский контроль**
- **Контроль личных данных**
- **Брандмауэр**
- **Уязвимости**
- **Шифрование чата**
- **Режим игры/ноутбука**
- **Домашняя сеть**
- **Обновление**
- **Регистрация**

Для каждой категории имеется список событий. Для каждого события отображается следующая информация: краткое описание, действие, выполняемое BitDefender при возникновении события, дата и время события. Для получения дополнительных сведений о конкретном событии дважды щелкните на нем мышью.

Здесь также можно просмотреть подробные сведения и статистику по событиям родительского контроля (веб-сайты, которые посещали дети, или используемые ими приложения).

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

13. Регистрация и моя учетная запись

Регистрация состоит из двух шагов:

1. **Активация (регистрация учетной записи BitDefender).** Вы должны создать учетную запись BitDefender, чтобы получать обновления и доступ к бесплатной техподдержке.Если у вас уже есть учетная запись BitDefender, зарегистрируйте ваш продукт BitDefender в ней.BitDefender сообщит о необходимости активации и поможет решить этот вопрос.

   Важно

   Необходимо создать учетную запись в течение 15 дней с момента установки BitDefender.В противном случае BitDefender не будет обновляться.

2. **Регистрация с лицензионным ключом.** Лицензионный ключ определяет, как долго вы можете использовать продукт.Как только лицензионный ключ истек, BitDefender перестает защищать ваш компьютер.Вам следует приобрести лицензионный ключ или продлить вашу лицензию за несколько дней до истечения срока действия ключа.

При покупке BitDefender Internet Security 2011 на CD, DVD или в Интернете вам предлагалось зарегистрировать продукт во время установки, используя лицензионный ключ.

Если вы загрузили BitDefender Internet Security 2011 для пробного использования и оценки, необходимо зарегистрировать продукт, используя лицензионный ключ, чтобы по истечении 30-дневного пробного периода продолжить пользоваться продуктом.Во время оценочного периода продукт полнофункционален, и вы можете удостовериться в том, что он соответствует вашим ожиданиям.

13.1. Регистрация BitDefender Internet Security 2011

Если вы хотите зарегистрировать продукт с помощью лицензионного ключа или изменить существующий лицензионный ключ, нажмите ссылку **Информация о лицензии**, расположенную в нижней части окна BitDefender.Появится окно регистрации продукта.

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

Регистрация BitDefender Internet Security 2011:

1. Введите лицензионный ключ в поле для редактирования.

Замечание

Вы можете найти ваш лицензионный ключ:

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

Если у вас нет лицензионного ключа BitDefender, нажмите соответствующую ссылку для запуска мастера, с помощью которого вы сможете приобрести ключ.

2. Нажмите **Зарегистрировать сейчас**.
3. Нажмите **Завершить**.

13.2. Активация BitDefender

Для активации BitDefender вы должны войти в учетную запись BitDefender или создать ее.Если вы не зарегистрировали учетную запись BitDefender в процессе запуска мастера установки, можно выполнить следующие действия:

Интерфейс "Основной"

Нажмите **Просмотреть все неполадки**.Этот мастер поможет вам устранить все ожидающие проблемы, включая активацию продукта.

Интерфейс "Опытный пользователь"

Перейдите на вкладку **Безопасность** и нажмите на кнопку **Просмотреть и устранить**, которая соответствует неполадке, возникшей при обновлении продукта.Для активации продукта в окне мастера нажмите **Пуск**.

Интерфейс "Эксперт"

Перейдите в раздел **Регистрация** и нажмите кнопку **Активировать продукт**.

Откроется окно регистрации учетной записи.Здесь вы можете войти в учетную запись BitDefender или создать ее для активации вашего продукта.

Если вы не хотите создавать учетную запись BitDefender прямо сейчас, выберите **Создать учетную запись позже** и нажмите **Завершить**.Или действуйте исходя из ситуаций:

- «У меня нет учетной записи BitDefender» (p. 55).
- «У меня уже есть учетная запись BitDefender» (p. 56).

Важно

Необходимо создать учетную запись в течение 15 дней с момента установки BitDefender.В противном случае BitDefender не будет обновляться.

У меня нет учетной записи BitDefender

Для успешного создания учетной записи BitDefender следуйте этим шагам:

1. Выберите **Создать новую учетную запись**.
2. Введите необходимую информацию в соответствующих полях.Информация, которую вы предоставите, останется конфиденциальной.
   - **Имя пользователя** — введите свой адрес электронной почты.
   - **Пароль** — введите пароль вашей учетной записи BitDefender.Пароль должен содержать не менее 6 и не более 16 символов.
   - **Введите пароль повторно** — введите ранее заданный пароль повторно.

     Если выбран параметр "не скрывать пароль при вводе", повторный ввод пароля не требуется.
   - **Напоминание пароля** — введите слово или фразу, которая поможет вспомнить пароль, если вы его забыли.

   Замечание
   После активации учетной записи вы можете использовать имеющийся адрес электронной почты и пароль, чтобы войти в свою учетную запись на http://myaccount.bitdefender.com.
3. Дополнительно BitDefender может информировать вас о специальных предложениях и бонусах по электронной почте, указанной в вашей учетной записи.Нажмите **Просмотр контактной информации** и выберите один из доступных способов связи в открывшемся окне.
   - **Отправлять мне все сообщения**
   - **Отправлять мне важные сообщения**
   - **Не отправлять мне сообщения**
4. Нажмите **Подтвердить**.
5. Нажмите **Завершить**, чтобы закрыть окно.

Замечание
Чтобы использовать учетную запись, вы должны ее активировать.
Проверьте почту и следуйте инструкциям в письме, отправленном вам службой регистрации BitDefender.

У меня уже есть учетная запись BitDefender

BitDefender автоматически определит, если вы уже регистрировали учетную запись BitDefender на этом компьютере.В этом случае введите пароль вашей учетной записи и нажмите **Подтвердить**.Нажмите **Завершить**, чтобы закрыть окно.

Если у вас уже есть активная учетная запись, но BitDefender не может ее обнаружить, следуйте этим шагам, чтобы привязать продукт к этой учетной записи:

1. Выберите **Вход (предыд. учетная запись)**.
2. Введите адрес электронной почты и пароль вашей учетной записи в соответствующих полях.

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

3. Дополнительно BitDefender может информировать вас о специальных предложениях и бонусах по электронной почте, указанной в вашей учетной записи.Нажмите **Просмотр контактной информации** и выберите один из доступных способов связи в открывшемся окне.
   - **Отправлять мне все сообщения**
   - **Отправлять мне важные сообщения**
   - **Не отправлять мне сообщения**
4. Нажмите **Подтвердить**.
5. Нажмите **Завершить**, чтобы закрыть окно.

13.3. Приобретение или продление лицензионных ключей

Если оценочный период скоро завершается, вам стоит купить лицензионный ключ и зарегистрировать продукт.

Также, если срок действия действующего лицензионного ключа вскоре истекает, необходимо продлить лицензию.Как клиент BitDefender вы имеете право на скидку на продление вашей лицензии. Вы также можете со скидкой или бесплатно обновить продукт до текущей версии.

Чтобы перейти к выполнению простой процедуры, включающей четыре шага, которая позволит приобрести новый ключ или продлить срок действия существующего, откройте BitDefender в интерфейсе "Эксперт" или "Опытный пользователь" и перейдите по ссылке **Купить**/**Продлить** в нижней части окна.

Конфигурация и управление

14. Общие настройки

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

Конфигурация основных настроек:

1. Откройте BitDefender, нажмите **Параметры** в верхнем правом углу окна и выберите интерфейс **Эксперт**.
2. Перейдите в раздел **Общие > Настройки**.

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

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

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

  Если у вас установлен пароль, то он будет запрашиваться всякий раз при изменении настроек BitDefender.Другие администраторы (если такие есть) также должны использовать этот пароль, чтобы изменить настройки BitDefender.

  Если вы хотите, чтобы запрос на ввод пароля выводился только при настройке родительского контроля, необходимо также установить флажок **Применять защиту паролем только для настроек родительского контроля**.В ином случае, если пароль был установлен только на родительский контроль и вы не выбрали этот параметр, соответствующий пароль будет запрашиваться при изменении любого параметра BitDefender.

  Важно
  Если вы забыли пароль, вам придется провести восстановление программы, чтобы изменить настройки BitDefender.

- **Спрашивать о создании пароля при включении родительского контроля** — отображает запрос на установку пароля при включении родительского контроля, если пароль не установлен.Установив пароль, вы защитите установленные вами для определенных пользователей настройки родительского контроля от изменений другими пользователями, обладающими правами администратора.

- **Показывать новости BitDefender (уведомления на тему безопасности)** — время от времени показывает уведомления относительно новых вирусов, рассылаемые сервером BitDefender.
- **Показывать всплывающие окна** — включает функцию всплывающих окон, отображающих статус программы.Можно настроить BitDefender для отображения всплывающих окон только при выборе интерфейса "Основной", "Опытный пользователь" или "Эксперт".
- **Включить панель активности сканирования (экранный график активности программы)** — показывает Активность сканирования всегда при входе в Windows.Снимите галочку в этом поле, если больше не хотите, чтобы отображалась панель активности сканирования.

Замечание

Эта настройка может быть изменена только для текущего пользователя Windows.Панель активности сканирования доступна только при работе в интерфейсе "Эксперт".

Настройки отчета о вирусах

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

  Эти отчеты не содержат никакой конфиденциальной информации, такой как ваше имя, IP-адрес вашего компьютера и пр., и не используются в коммерческих целях. Отправляемая информация содержит только название вируса и используется исключительно для статистики.

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

  Эти отчеты не содержат никакой конфиденциальной информации, такой как ваше имя, IP-адрес вашего компьютера и пр., и не используются в коммерческих целях. Отправляемая информация содержит только возможный вирус и используется исключительно для статистики.

Настройки соединения

Для нескольких компонентов BitDefender (модули брандмауэра, LiveUpdate, отчетности о вирусах в режиме реального времени и отчетности о спаме в режиме реального времени) требуется доступ в Интернет. В комплекте с BitDefender предоставляется модуль управления прокси, с помощью которого можно настроить из одного расположения параметры прокси-сервера, используемые компонентами BitDefender для доступа в Интернет.

Если ваша компания использует прокси-сервер для подсоединения к Интернету, 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.Для получения дополнительной информации перейдите к *«Просмотр сведений о настройках прокси-сервера.»* (p. 222).

Замечание

Настройки прокси-сервера могут изменяться только пользователями с правами администратора компьютера или же пользователями, знающими пароль к настройкам программы.

Для управления настройками прокси-сервера перейдите в раздел **Настройки прокси-сервера**.

Есть три параметра настройки для прокси:

- **Во время установки обнаружен прокси-сервер** — в учетной записи администратора в процессе установки обнаружены настройки прокси-сервера, редактирование которых возможно только из данной учетной записи. Если для прокси-сервера требуется имя пользователя и пароль, необходимо ввести их в соответствующие поля.
- **Прокси браузера по умолчанию** — настройки прокси для текущего пользователя, извлеченные из браузера по умолчанию. Если прокси-сервер требует ввода имени пользователя и пароля, вы должны указать их в соответствующих полях.

  Замечание

  Поддерживаемыми браузерами являются Internet Explorer, Mozilla Firefox и Opera. Если по умолчанию вы используете другой браузер, BitDefender не сможет получить настройки прокси-сервера для текущего пользователя.

- **Пользовательские прокси** — вы можете изменять настройки прокси, если вошли как администратор.

  Должны быть определены следующие настройки:
  - **Адрес** — введите IP-адрес прокси-сервера.
  - **Порт** — введите порт, используемый BitDefender для подсоединения к прокси-серверу.
  - **Пользователь** — введите имя пользователя, опознаваемого прокси-сервером.
  - **Пароль** — введите пароль пользователя, указанного ранее.

BitDefender будет использовать наборы настроек прокси-сервера в следующем порядке до тех пор, пока не удастся установить подключение к Интернету:

1. заданные настройки прокси-сервера.

2. настройки прокси-сервера, обнаруженные во время установки.
3. настройки прокси-сервера для текущего пользователя.

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

Прежде всего, для подключения к Интернету будут использованы ваши собственные настройки прокси. Если это не поможет, следующими будут использованы настройки сервера, обнаруженные при установке продукта. И наконец, если ни один из вариантов не сработает, будут использованы настройки прокси-сервера, который использует браузер по умолчанию для соединения с Интернетом.

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

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

Информация о системе

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

Сбор системной информации:

1. Откройте BitDefender, нажмите **Параметры** в верхнем правом углу окна и выберите интерфейс **Эксперт**.
2. Перейдите в раздел **Общие > Информация о системе**.

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

Доступны три кнопки:

- **Восстановить** — замена текущих связей 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**.

15. Антивирусная защита

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.

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

  Важно
  Чтобы предотвратить попадание вирусов на ваш компьютер, включите **Постоянную защиту**.

- Сканирование по требованию — Обнаружение и удаление вредоносного ПО, которое уже попало в систему.Это классический тип проверки по желанию пользователя: вы выбираете диск, папку или файл для проверки BitDefender, а BitDefender проверяет их по вашему требованию.Задачи проверки позволяют создавать запланированные действия, которые можно регулярно запускать по расписанию.

В случае обнаружения вируса или других вредоносных программ BitDefender попытается автоматически удалить вредоносный код из зараженного файла и воссоздать исходный файл.Эта операция называется "лечение".Файлы, которые не удается вылечить, перемещаются в папку карантина во избежание распространения вируса.Для получения дополнительной информации перейдите к *«Карантин»* (p. 87).

В случае заражения компьютера вирусом см. информацию в *«Удаление вредоносного ПО из системы»* (p. 203).

Если сканирование определенных файлов нежелательно, опытные пользователи могут настроить исключения сканирования самостоятельно.Для получения дополнительной информации перейдите к *«Настройка исключений сканирования»* (p. 83).

15.1. 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 служб мгновенных сообщений (ICQ, NetMeeting, Yahoo Messenger, MSN Messenger).

Настройки по умолчанию защиты в режиме реального времени позволяют обеспечить качественную защиту от вредоносных программ при минимальном влиянии на производительность системыПри необходимости можно легко изменить настройки модуля защиты в режиме реального времени. Для этого необходимо установить один из предварительно определенных уровней защиты.Опытные пользователи могут детально настроить параметры сканирования путем создания настраиваемого уровня защиты.

Дополнительные сведения см. в следующих разделах:

- *«Регулировка уровня защиты в режиме реального времени»* (p. 64)
- *«Создание настраиваемого уровня защиты»* (p. 65)
- *«Изменение действий, выполняемых для обнаруженных файлов»* (p. 67)
- *«Восстановление настроек по умолчанию»* (p. 68)

Для защиты пользователей от неизвестных вредоносных приложений BitDefender использует новейшую технологию эвристического анализа (активный вирусный контроль), а также систему обнаружения вторжений, которая постоянно отслеживает работу вашей системы.Дополнительные сведения см. в следующих разделах:

- *«Настройка активного вирусного контроля (AVC)»* (p. 68)
- *«Настройка системы обнаружения вторжений»* (p. 70)

15.1.1. Регулировка уровня защиты в режиме реального времени

Уровень защиты в режиме реального времени определяет настройки сканирования для защиты в режиме реального времени.При необходимости можно легко изменить настройки модуля защиты в режиме реального времени. Для этого необходимо установить один из предварительно определенных уровней защиты.

Регулировка уровня защиты в режиме реального времени:

1. Откройте BitDefender.
2. В зависимости от режима пользовательского интерфейса выполните следующие действия:

   Интерфейс "Опытный пользователь"
   Перейдите на вкладку **Безопасность** и выберите **Настроить антивирус** в области быстрых задач в левой части окна.

   Перейдите на вкладку **Щит**.

   Интерфейс "Эксперт"
   Перейдите в раздел **Антивирус > Щит**.

Замечание

В интерфейсе "Основной" или "Опытный пользователь" можно создать ярлык для доступа к этим настройкам непосредственно из панели управления.Для получения дополнительной информации перейдите к *«Мои инструменты»* (p. 33).

3. Чтобы установить желаемый уровень защиты, переместите бегунок в требуемое положение.Воспользуйтесь описанием справа от шкалы, чтобы выбрать тот уровень защиты, который оптимально соответствует требованиям к безопасности.

15.1.2. Создание настраиваемого уровня защиты

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

Детальную настройку защиты в режиме реального времени можно выполнить, создав настраиваемый уровень защиты.Создание настраиваемого уровня защиты:

1. Откройте BitDefender, нажмите **Параметры** в верхнем правом углу окна и выберите интерфейс **Эксперт**.
2. Перейдите в раздел **Антивирус > Щит**.
3. Нажмите **Настраиваемый уровень**.
4. Настройте параметры сканирования по своему выбору.Для того чтобы узнать, на что влияет настройка, подержите курсор мыши над ней. Внизу окна появится подсказка.
5. Нажмите **OK**, чтобы сохранить изменения, и закройте окно.

Эти сведения могут быть полезными:

- Значение незнакомых терминов можно посмотреть в глоссарии.Также вы можете найти полезную информацию в Интернете.
- **Проверить открываемые файлы.** Можно настроить BitDefender для сканирования всех открываемых файлов, только приложений (программных файлов) или определенных типов файлов, которые, по вашему мнению, могут быть опасными.Наиболее качественная защита обеспечивается посредством сканирования всех открываемых файлов, однако сканирование только приложений обеспечивает оптимальную производительность системы.

  Приложения (или программные файлы) значительно более уязвимы для вирусных атак, чем другие типы файлов.В эту категорию включены

следующие расширения файлов: .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.

При выборе команды **Сканировать определенные пользователем расширения** рекомендуется включить также все расширения приложения, помимо остальных расширений файла, которые вы считаете опасными.

- **Проверить только новые и измененные файлы.** Сканируя только новые и измененные файлы, можно значительно повысить общее быстродействие системы с минимальными потерями в безопасности.
- **Проверять внутри архивов.** Сканирование архивов — медленный процесс, занимающий большой объем системных ресурсов. Именно поэтому не рекомендуется выполнять такое сканирование в режиме реального времени.Архивы, содержащие зараженные файлы, не представляют собой непосредственной угрозы безопасности системы.Вредоносные программы могут скомпрометировать систему только в том случае, если зараженный файл будет извлечен из архива и исполнен; при этом защита в режиме реального времени должна быть отключена.
- **Настройки действий.** Если требуется изменить действия, выполняемые в отношении обнаруженных файлов, сведения об этой процедуре см. в *«Изменение действий, выполняемых для обнаруженных файлов»* (p. 67).
- **Параметры сканирования трафика электронной почты, Интернета и служб мгновенных сообщений.** В целях предотвращения загрузки вредоносных программ в компьютер BitDefender автоматически сканирует следующие точки входа вредоносных программ:
  - входящие сообщения электронной почты
  - веб-трафик
  - файлы, полученные через Yahoo! Messenger и Windows Live Messenger

  Сканирование веб-трафика может несколько замедлить работу в Интернете, однако такое сканирование позволяет блокировать вредоносные программы, которые проникают в ваш компьютер из Интернета (включая скрытые загрузки).

  В целях повышения производительности системы можно отключить антивирусное сканирование электронной почты, веб-сообщений и мгновенных сообщений (не рекомендуется).Если соответствующие параметры сканирования отключены, сообщения электронной почты и файлы, которые были получены или загружены из Интернета, сканироваться не будут. В результате зараженные файлы могут попасть в компьютер.Это не самая серьезная угроза, поскольку защита в режиме реального времени блокирует вредоносные программы при доступе (открытии, перемещении, копировании или исполнении) к зараженным файлам.

15.1.3. Изменение действий, выполняемых для обнаруженных файлов

Файлы, обнаруженные защитой в режиме реального времени, распределены по двум категориям:

- **Зараженных файлов.** Файлы, распознанные как зараженные вирусом, соответствуют вирусным сигнатурам в базе данных вирусных сигнатур BitDefender.BitDefender, как правило, способен удалить вредоносный код из зараженного файла и воссоздать исходный файл. Эта операция известна как "лечение".

Замечание

Сигнатуры вирусов представляют собой фрагменты кода, извлеченные из образцов настоящих вирусов. Они используются антивирусными программами для поиска по шаблону и распознавания вредоносных программ.
База данных вирусных сигнатур BitDefender представляет собой набор вирусных сигнатур, обновляемый каждый час специалистами BitDefender по анализу вредоносных программ.

- **Подозрительные файлы.** Файлы помечены эвристическим анализом как подозрительные. Лечение подозрительных файлов невозможно, поскольку процедура лечения недоступна.

В зависимости от типа обнаруженного файла автоматически выполняются следующие действия:

- При обнаружении зараженного файла BitDefender автоматически попытается вылечить его.Если файл не удается вылечить, он перемещается в карантин в целях предотвращения распространения вируса.

Важно

В случае определенных типов вредоносных программ лечение невозможно, поскольку вредоносным является весь обнаруженный файл. В таких случаях выполняется удаление зараженного файла с диска.

- При обнаружении подозрительного файла во избежание распространения вируса доступ к такому файлу блокируется.

Без веских причин изменять действия по умолчанию, выполняемые в отношении обнаруженных файлов, не рекомендуется.

Изменение действий по умолчанию, выполняемых в отношении обнаруженных зараженных или подозрительных файлов:

1. Откройте BitDefender, нажмите **Параметры** в верхнем правом углу окна и выберите интерфейс **Эксперт**.
2. Перейдите в раздел **Антивирус > Щит**.

3. Нажмите **Настраиваемый уровень**.
4. Настройка действий, при необходимости выполняемых для каждой категории обнаруженных файлов.Второе действие выполняется в том случае, если не удалось выполнить первое (например, если лечение зараженного файла невозможно, он перемещается в карантин).

15.1.4. Восстановление настроек по умолчанию

Настройки по умолчанию защиты в режиме реального времени позволяют обеспечить качественную защиту от вредоносных программ при минимальном влиянии на производительность системы

Восстановление настроек по умолчанию для защиты в режиме реального времени:

1. Откройте BitDefender, нажмите **Параметры** в верхнем правом углу окна и выберите интерфейс **Эксперт**.
2. Перейдите в раздел **Антивирус > Щит**.
3. Нажмите **По умолчанию**.

15.1.5. Настройка активного вирусного контроля (AVC)

Функция активного вирусного контроля BitDefender распознает потенциально опасные приложения на основе их поведения.

Активный вирусный контроль постоянно отслеживает приложения, запущенные на компьютере, на предмет признаков вредоносного поведения. Для всех вышеперечисленных действий присваивается балл, и для каждого процесса подсчитывается общий рейтинг.Когда суммарный счетчик процесса достигает заданного порогового значения, процесс переходит в категорию вредоносных. В зависимости от настроек программы процесс либо автоматически блокируется, либо система запрашивает выбор действия пользователем.

Активный вирусный контроль может быть настроен на оповещение и напоминание, когда приложение пытается выполнить действие, которое может быть вредоносным.

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

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

Выберите **Запомнить это действие для этого приложения** перед подтверждением. После этого BitDefender будет впоследствии применять это же действие для обнаруженных приложений.Созданное правило будет отображаться в окне настроек активного вирусного контроля.

Настройка активного вирусного контроля:

1. Откройте BitDefender, нажмите **Параметры** в верхнем правом углу окна и выберите интерфейс **Эксперт**.
2. Перейдите в раздел **Антивирус > Щит**.
3. Нажмите **Дополнительные настройки**.
4. Перейдите на вкладку **Активный вирусный контроль (AVC)**.
5. Поставьте соответствующую галочку для активации активного вирусного контроля.
6. Чтобы установить желаемый уровень защиты, переместите бегунок в требуемое положение.Воспользуйтесь описанием справа от шкалы, чтобы выбрать тот уровень защиты, который оптимально соответствует требованиям к безопасности.

Регулировка уровня агрессивности

Настройка уровня защиты активного вирусного контроля:

1. Откройте BitDefender, нажмите **Параметры** в верхнем правом углу окна и выберите интерфейс **Эксперт**.
2. Перейдите в раздел **Антивирус > Щит**.
3. Нажмите **Дополнительные настройки**.
4. Перейдите на вкладку **Активный вирусный контроль (AVC)**.
5. Чтобы установить желаемый уровень защиты, переместите бегунок в требуемое положение.Воспользуйтесь описанием справа от шкалы, чтобы выбрать тот уровень защиты, который оптимально соответствует требованиям к безопасности.

Настройка реагирования на вредоносное поведение

В случае вредоносного поведения приложения пользователю будет предложено разрешить или заблокировать это приложение.

Настройка реагирования на вредоносное поведение:

1. Откройте BitDefender, нажмите **Параметры** в верхнем правом углу окна и выберите интерфейс **Эксперт**.
2. Перейдите в раздел **Антивирус > Щит**.
3. Нажмите **Дополнительные настройки**.
4. Перейдите на вкладку **Активный вирусный контроль (AVC)**.
5. Если вы хотите, чтобы система запрашивала выполнение действия при обнаружении активным вирусным контролем потенциально опасного приложения, установите флажок **Выводить оповещение перед каким-либо действием**.Снимите этот флажок для автоматической

блокировки приложения, демонстрирующего вредоносное поведение (без отображения окна оповещения).

Управление надежными/ненадежными приложениями

Вы можете добавлять приложения, которым доверяете, в список доверенных приложений. Эти приложения не будут проверяться активным вирусным контролем BitDefender, и доступ к ним будет разрешен автоматически.

Управление приложениями, не отслеживаемыми активным вирусным контролем:

1. Откройте BitDefender, нажмите **Параметры** в верхнем правом углу окна и выберите интерфейс **Эксперт**.
2. Перейдите в раздел **Антивирус > Щит**.
3. Нажмите **Дополнительные настройки**.
4. Перейдите на вкладку **Активный вирусный контроль (AVC)**.
5. Перейдите на вкладку **Исключения**.

Приложения, для которых были созданы правила, представлены в таблице **Исключения**.Путь к приложению и действие, установленное для него (доступ разрешен или заблокирован), указаны для каждого правила.

Для изменения действия по отношению к приложению щелкните текущее действие и выберите другое действие из меню.

Для управления списком используйте кнопки, находящиеся над таблицей:

- **Добавить** — добавить новое приложение к списку.
- **Удалить** — удаление нового приложения из списка.
- **Редактировать** — редактировать правило для приложения.

15.1.6. Настройка системы обнаружения вторжений

Система обнаружения вторжений BitDefender отслеживает активность сети и системы на предмет вредоносных действий и нарушений политики.

Настройка системы обнаружения вторжений:

1. Откройте BitDefender, нажмите **Параметры** в верхнем правом углу окна и выберите интерфейс **Эксперт**.
2. Перейдите в раздел **Антивирус > Щит**.
3. Нажмите **Дополнительные настройки**.
4. Перейдите на вкладку **Система обнаружения вторжений (IDS)**.
5. Для включения системы обнаружения вторжений установите соответствующий флажок.

6. Чтобы установить желаемый уровень агрессивности, переместите бегунок в требуемое положение.Воспользуйтесь описанием справа от шкалы, чтобы выбрать тот уровень агрессивности, который оптимально соответствует требованиям к безопасности.

15.2. Сканирование по требованию

Главное назначение программного продукта BitDefender — защищать ваш компьютер от вирусов. В первую очередь он 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.

Проверка по требованию производится согласно установленным задачам. В них указывают параметры проверки, а также объекты, подлежащие проверке.Вы можете сканировать компьютер когда захотите, запуская предустановленные задачи или создавая ваши собственные задачи сканирования. Также вы можете задавать расписание регулярных сканирований или же запускать сканирование, когда система не используется и сканирование не может помешать вашей работе.Для быстрого получения инструкций см. следующие темы:

- «*Сканирование файлов и папок*» (p. 171)
- «*Создание настраиваемого задания сканирования*» (p. 174)
- «*Создание расписания сканирования компьютера*» (p. 176)

15.2.1. Сканирование папок и файлов

Рекомендуется выполнять сканирование файлов и папок каждый раз при подозрении на заражение их вирусом.Щелкните правой кнопкой мыши на файле или папке, которые необходимо проверить, и выберите **Сканировать с BitDefender**.Появится Мастер сканирования и проведет вас по процессу сканирования.

Для сканирования отдельных папок на компьютере можно настроить и запустить настраиваемое задание сканирования.Для получения дополнительной информации перейдите к «*Создание настраиваемого задания сканирования*» (p. 174).

Для проверки вашего компьютера или его части можно воспользоваться заданиями проверки по умолчанию либо создать собственные задания.Для запуска задания сканирования откройте BitDefender и выполните следующие действия (в зависимости от режима пользовательского интерфейса):

Интерфейс "Основной"
Нажмите кнопку **Безопасность** и выберите одно из доступных заданий сканирования.

Интерфейс "Опытный пользователь"
Перейдите на вкладку **Безопасность**.Нажмите **Полное сканирование системы** в области быстрых задач слева и выберите одно из доступных заданий сканирования.

Интерфейс "Эксперт"
Перейдите на вкладку **Антивирус > Сканирование вирусов**.Для запуска задачи сканирования щелкните соответствующую этой задаче кнопку **Запустить**.

Эти задания по умолчанию можно использовать для сканирования компьютера:

Сканирование
Проверка всей системы, кроме архивов.При настройках по умолчанию проводится проверка на все типы вирусного ПО, кроме руткитов.

Быстрое сканирование
Функция быстрого сканирования использует технологию "облачного" сканирования для распознавания вредоносных программ, запущенных в системе.Быстрое сканирование занимает, как правило, менее минуты. Быстрое сканирование использует лишь незначительную часть системных ресурсов, которые используются в процессе стандартного вирусного сканирования.

Глубокое сканирование системы
Проверка всей системы.В конфигурации по умолчанию производится проверка на все виды вредоносных программ, угрожающих безопасности вашей системы, а именно на наличие вирусов, программ-шпионов, рекламного ПО, руткитов и проч.

Перед тем как запустить процесс проверки, вы должны убедиться, что вирусные сигнатуры BitDefender обновлены. 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 BitDefender полностью проверил все ваши файлы, необходимо закрыть все запущенные приложения, особенно почтовые программы, такие как Outlook, Outlook Express или Eudora.

Подсказки сканирования

Вот еще несколько подсказок, которые могут быть весьма полезными:

- В зависимости от объема вашего жесткого диска, полное сканирование системы может занять какое-то время (до часа или даже более).Таким

образом, вам стоит запускать подобные сканирования, когда вы не пользуетесь компьютером на протяжении длительного времени (например, ночью).

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

- Если вы часто загружаете файлы из Интернета в отдельную папку, рекомендуется создать новое задание сканирования и включить папку в задачу по сканированию.Запланируйте ежедневный или более частый запуск задания.
- Существует тип вредоносного ПО, который сам записывает себя в автозагрузку.Чтобы защитить ваш компьютер от подобных вирусов, запланируйте, чтобы задача **Сканиров. объектов, выполняемых при загрузке** выполнялась при запуске системы.Помните, что сканирование при загрузке может влиять на производительность системы некоторое время после загрузки.

15.2.2. Мастер антивирусного сканирования

Каждый раз, когда вы начинаете сканирование по требованию (к примеру, щелкнув правой кнопкой мыши по папке и выбрав **Сканировать с помощью BitDefender**), появляется мастер антивирусного сканирования BitDefender.Чтобы завершить процесс проверки, выполните последовательность из трех шагов.

Замечание

Если мастер сканирования не появился, возможно, сканирование настроено для работы в тихом, фоновом режиме.Найдите значок состояния сканирования на панели задач.Вы можете щелкнуть по этому значку, чтобы открыть окно сканирования и наблюдать прогресс проверки.

Шаг 1/3. Сканирование

BitDefender начнет проверку выбранных объектов.

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

Дождитесь окончания сканирования BitDefender.

Замечание

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

Архивы, защищенные паролем. При обнаружении архива, защищенного паролем, может отобразиться запрос на ввод пароля (в зависимости от настроек сканирования).Защищенные паролем архивы нельзя сканировать, не предоставив пароль.Доступны следующие варианты:

- **Я хочу ввести пароль для этого объекта.** Если вы хотите, чтобы BitDefender проверил архив, выберите этот параметр и введите пароль.Если вы не знаете пароля, выберите любой другой параметр.
- **Я не хочу вводить пароль (пропустить объект).** Выберите этот параметр, чтобы пропустить этот архив.
- **Я не хочу вводить пароль (пропустить все подобные объекты).** Выберите этот параметр, если не хотите, чтобы вас беспокоили по поводу защищенных паролем архивов.BitDefender не будет иметь возможности сканировать их, но запись останется в журнале сканирования.

Для продолжения нажмите **OK**.

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

Шаг 2/3. Выбор действия

Когда проверка завершится, откроется новое окно, где вы сможете просмотреть результаты проверки.

При отсутствии существующих угроз выберите **Продолжить**.В противном случае необходимо настроить дополнительные действия, которые будут выполняться при обнаружении оставшихся угроз в целях обеспечения защиты системы.

Зараженные объекты разделены на группы в зависимости от типа вредоносной программы, которой они были инфицированы.Щелкните 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.Один или несколько следующих параметров могут появиться в меню:

Ничего не делать
Над обнаруженными файлами не будет производиться никаких действий.После завершения сканирования вы можете открыть отчет о проверке, чтобы просмотреть сведения об этих файлах.

Вылечить
Удаляет вредоносный код из инфицированных файлов.

Удалить
Удаляет обнаруженные файлы с диска.

Переместить в карантин
Зараженные файлы перемещаются в карантин.Добавленные в карантин файлы нельзя выполнять или открывать; таким образом, риск заражения сводится к нулю.Для получения дополнительной информации перейдите к «*Карантин*» (p. 87).

Переименовать файлы
Изменяет имена скрытых файлов, добавляя в конце имени `.bd.ren`.В результате у вас будет возможность искать подобные файлы на вашем компьютере.

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

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

Шаг 3/3. Просмотр результатов

Когда BitDefender завершит исправление проблем, результаты проверки будут отображены в новом окне.Если вам требуется полная информация о процессе сканирования, нажмите **Показать журнал**, чтобы просмотреть журнал сканирования.

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

Нажмите **Закрыть**, чтобы закрыть окно.

BitDefender не может исправить некоторые проблемы

В большинстве случаев BitDefender успешно лечит зараженные файлы, которые обнаруживает, или изолирует инфекцию.Тем не менее, существуют проблемы, которые невозможно устранить автоматически.Дополнительные сведения и инструкции по удалению вредоносных программ вручную см. в «*Удаление вредоносного ПО из системы*» (p. 203).

BitDefender обнаружил подозрительные файлы

Подозрительные файлы — это файлы, обнаруженные при эвристическом анализе; 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 **OK**, чтобы отправить эти файлы в лабораторию BitDefender для дальнейшего анализа.

15.2.3. Просмотр журнала проверок

При выполнении каждой процедуры сканирования создается журнал сканирования.Журнал сканирования содержит подробную информацию о записанном процессе сканирования, такую как параметры сканирования, цели сканирования, обнаруженные угрозы и меры, принятые по отношению к этим угрозам.

Открыть журнал сканирования можно непосредственно из мастера сканирования. Для этого по завершении процедуры сканирования нажмите **Показать журнал**.

Проверить журналы сканирования позднее:

1. Откройте BitDefender.
2. Перейдите по ссылке **Просмотреть журналы** в правом нижнем углу окна.
3. Нажмите **Антивирус** в левом меню.
4. В разделе **Задания по запросу** можно просмотреть ранее выполненные задания сканирования.Дважды щелкните события в списке, чтобы просмотреть более подробную информацию.Чтобы открыть журнал сканирования, нажмите **Просмотреть журнал сканирования**.Отчет сканирования откроется в вашем web-браузере по умолчанию.

Чтобы удалить запись из журнала, дважды щелкните на ней и выберите **Удалить**.

15.2.4. Управление существующими заданиями сканирования

BitDefender имеет несколько заданий по умолчанию, которые учитывают основные задачи. Вы также можете создавать свои собственные задания.Для получения дополнительной информации перейдите к *«Создание настраиваемого задания сканирования»* (p. 174).

Управление существующими заданиями сканирования:

1. Откройте BitDefender.
2. В зависимости от режима пользовательского интерфейса выполните следующие действия:

   Интерфейс "Опытный пользователь"

   Перейдите на вкладку **Безопасность** и выберите **Настроить антивирус** в области быстрых задач в левой части окна.

   Перейдите на вкладку **Сканирование вирусов**.

Интерфейс "Эксперт"

Перейдите на вкладку **Антивирус > Сканирование вирусов**.

Замечание

В интерфейсе "Основной" или "Опытный пользователь" можно создать ярлык для доступа к этим настройкам непосредственно из панели управления.Для получения дополнительной информации перейдите к *«Мои инструменты»* (p. 33).

Существует три категории задач сканирования:

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

  Сканирование

  Проверка всей системы, кроме архивов.При настройках по умолчанию проводится проверка на все типы вирусного ПО, кроме руткитов.

  Быстрое сканирование

  Функция быстрого сканирования использует технологию "облачного" сканирования для распознавания вредоносных программ, запущенных в системе.Быстрое сканирование занимает, как правило, менее минуты. Быстрое сканирование использует лишь незначительную часть системных ресурсов, которые используются в процессе стандартного вирусного сканирования.

  Сканирование объектов, выполняемое при загрузке

  Проверка элементов, запускающихся при входе пользователя в систему.По умолчанию проверка элементов автозапуска отключена.

  Если вы хотите воспользоваться этим заданием, щелкните на нем правой кнопкой мыши, выберите **Планировщик** и поставьте задание на выполнение **при запуске системы**.Вы можете указать, сколько времени (в минутах) задание должно выполняться после запуска.

  Глубокое сканирование системы

  Проверка всей системы.В конфигурации по умолчанию производится проверка 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 некоторое время. Поэтому рекомендуется выполнять эти задачи с небольшим приоритетом либо когда ваша система не загружена.

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

Предусмотрена задача Мои документы.Используйте данное задание для проверки основных папок пользователя: Мои документы, Рабочий стол и 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.Доступны следующие задания:

  Сканирование устройства

  BitDefender способен автоматически обнаруживать новые носители, подключенные к компьютеру, и выполнять их сканирование.Используйте это задание для настройки параметров автоматического обнаружения и сканирования носителей данных (CD/DVD, USB-носителей или сопоставленных сетевых устройств).

  Контекстное сканирование

  Это задание используется при сканировании, запущенном с помощью контекстного меню Windows или панели активности сканирования.Можно изменить параметры сканирования в соответствии со своими предпочтениями.

Заданиями сканирования можно управлять с помощью кнопок или контекстного меню.

Для запуска задачи сканирования щелкните соответствующую этой задаче кнопку **Запустить**.Появится Мастер сканирования и проведет вас по процессу сканирования.

Чтобы настроить для задания сканирования автоматический запуск в более поздний срок или на регулярной основе, нажмите соответствующую кнопку **Запланировать** и настройте расписание для задания.

Если вам больше не нужна задача сканирования, которую вы создали (заданная пользователем задача), вы можете ее удалить, щелкнув кнопку **Удалить**, расположенную справа от задачи.Вы не можете удалить системные или смешанные задачи.

Для каждого задания сканирования доступно окно "Свойства", с помощью которого можно настроить параметры задания и просмотреть журналы сканирования.Чтобы открыть это окно, нажмите **Свойства** слева от задачи (или нажмите правой кнопкой мыши на задачу и нажмите **Свойства**).

Дополнительные сведения см. в следующих разделах:

- «*Изменение настроек сканирования*» (p. 79)
- «*Установка объекта сканирования*» (p. 82)

- *«Планирование задач сканирования»* (p. 83)

Использование выпадающего меню

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

Для системных или определенных пользователем задач следующие команды доступны из меню ярлыков:

- **Проверить сейчас** — запуск выбранной задачи, немедленное начало процесса проверки.
- **Путь** — открытие окна **Параметры** и вкладки Путь, где вы можете сменить объект сканирования выбранного задания.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.
- **Просмотреть журнал** — открывает окно **Свойства**, Журнал, где вы можете просмотреть отчеты, созданные после выполнения выбранного задания.
- **Клонировать задачу** — создает дубликат выбранной задачи.Данная функция полезна при создании новых задач, поскольку позволяет изменить настройки дубликата.
- **Удалить** — удаление выбранной задачи.

  Замечание

  Это действие доступно только для заданий, созданных пользователями. Задание по умолчанию удалить нельзя.

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

В связи с особенными свойствами категории **Прочие задачи**, доступны только функции **Просмотреть журнал** и **Свойства**.

Изменение настроек сканирования

Чтобы изменить параметры сканирования для определенной задачи, нажмите правой кнопкой мыши на задачу и выберите**Свойства**.

Можно легко настроить параметры сканирования с помощью регулировки уровня сканирования. Переместите бегунок в требуемое положение, чтобы задать выбранный уровень сканирования.Воспользуйтесь описанием справа от шкалы, чтобы выбрать тот уровень защиты, который оптимально соответствует требованиям к безопасности.

Вы также можете настроить эти основные параметры:

- **Выполнить задачу с низким приоритетом.** Уменьшается приоритет процесса проверки. Таким способом вы ускоряете работу других программ, но увеличиваете время, необходимое для завершения процесса проверки.
- **Свернуть мастер сканирования в область уведомлений.** Окно проверки свертывается на панель задач. Чтобы открыть его, следует дважды щелкнуть на значке BitDefender.
- Задать действие, выполняемое при отсутствии обнаруженных угроз.

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

Детальная настройка параметров сканирования.

1. Нажмите **Настраиваемый**.
2. Настройте параметры сканирования по своему выбору.Для того чтобы узнать, на что влияет настройка, подержите курсор мыши над ней. Внизу окна появится подсказка.
3. Нажмите **OK**, чтобы сохранить изменения, и закройте окно.

Эти сведения могут быть полезными:

- Значение незнакомых терминов можно посмотреть в глоссарии.Также вы можете найти полезную информацию в Интернете.
- **Уровень сканирования.** Укажите тип вредоносных программ, наличие которых необходимо проверить с помощью BitDefender. Для этого выберите соответствующие параметры.
- **Проверка файлов.** Можно настроить BitDefender для сканирования всех типов файлов, только приложений (программных файлов) или определенных типов файлов, которые, по вашему мнению, могут быть опасными.При сканировании всех файлов обеспечивается оптимальная защита. Сканируя только приложения, можно повысить скорость сканирования.

  Приложения (или программные файлы) значительно более уязвимы для вирусных атак, чем другие типы файлов.В эту категорию включены следующие расширения файлов: `.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`.

При выборе команды **Сканировать определенные пользователем расширения** рекомендуется включить также все расширения приложения, помимо остальных расширений файла, которые вы считаете опасными.

- **Проверить только новые и измененные файлы.** Сканируя только новые и измененные файлы, можно значительно повысить общее быстродействие системы с минимальными потерями в безопасности.
- **Проверять внутри архивов.** Архивы, содержащие зараженные файлы, не представляют собой непосредственной угрозы безопасности системы.Вредоносные программы могут скомпрометировать систему только в том случае, если зараженный файл будет извлечен из архива и исполнен; при этом защита в режиме реального времени должна быть отключена.Тем не менее, рекомендуется использовать этот параметр для обнаружения и удаления всех вирусов, даже тех, которые не представляют собой непосредственной угрозы системе.

Замечание

Сканирование файлов, сжатых в архив, увеличивает общее время сканирования и занимает больший объем системных ресурсов.

- **Настройки действий.** Укажите меры, которые должны быть приняты по каждой категории обнаруженных файлов, с помощью ссылок в этой категории.Обнаруженные файлы распределяются по трем категориям:
  - **Зараженных файлов.** Файлы, распознанные как зараженные вирусом, соответствуют вирусным сигнатурам в базе данных вирусных сигнатур BitDefender.BitDefender, как правило, способен удалить вредоносный код из зараженного файла и воссоздать исходный файл. Эта операция известна как "лечение".

Замечание

Сигнатуры вирусов представляют собой фрагменты кода, извлеченные из образцов настоящих вирусов. Они используются антивирусными программами для поиска по шаблону и распознавания вредоносных программ.

База данных вирусных сигнатур BitDefender представляет собой набор вирусных сигнатур, обновляемый каждый час специалистами BitDefender по анализу вредоносных программ.

  - **Подозрительные файлы.** Файлы помечены эвристическим анализом как подозрительные. Лечение подозрительных файлов невозможно, поскольку процедура лечения недоступна.
  - **Скрытые файлы (руткиты).** Обратите внимание, что эти скрытые файлы — не те файлы, которые вы сознательно скрываете от Windows. Это файлы, спрятанные особыми программами — руткитами.Сами по себе руткиты не

вредны. Но они часто используются для того, чтобы сделать вирусы невидимыми для обычных антивирусных программ.

Без веских причин изменять действия по умолчанию, выполняемые в отношении обнаруженных файлов, не рекомендуется.

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

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

Установка объекта сканирования

Вы не можете изменять объект проверки для заданий проверки из категории **Системные задачи**.Вы можете только видеть цель сканирования.Чтобы просмотреть цели сканирования системной задачи, щелкните правой кнопкой мыши на задаче и выберите **Показать пути сканирования**.

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

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.

Доступны следующие кнопки:

- **Добавить объект** — открывает окно, где вы можете выбрать файлы и папки, которые хотите просканировать.

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

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

Помимо этих кнопок есть несколько вариантов, позволяющих быстро выбрать объекты для сканирования.

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

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

Планирование задач сканирования

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

Чтобы увидеть расписание конкретных задач или изменить его, щелкните правой кнопкой мыши задачу и выберите **Расписание**. Если вы уже находитесь в окне "Свойства" задачи, выберите вкладку **Планировщик**.

Вы можете просмотреть запланированные задачи, если такие есть.

При планировании задачи нужно выбрать один из следующих параметров:

- **Нет** — запускает задачу только тогда, когда пользователь требует этого.
- **Однократно** — запуск проверки однократно в определенный момент. Укажите дату и время в полях **Дата/время запуска**.
- **Периодически** — процедура проверки запускается многократно, периодически через определенные промежутки времени (часы, дни, недели, месяцы, годы), начиная с заданных даты и времени.
- **При запуске системы** — запуск сканирования через заданное количество минут после того, как пользователь вошел в систему.

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

15.3. Настройка исключений сканирования

Иногда вам может понадобиться исключить определенные файлы из сканирования. К примеру, вы захотите исключить тестовый файл EICAR из объектов входной проверки или файлы с расширением `.avi` из объектов проверки по требованию.

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

Два типа объектов могут быть исключены из сканирования:

- **Пути** — файл или папка (включая все объекты, которые она содержит), обозначенные путем в системе, будут исключены из проверки.
- **Расширения** — все файлы с определенным расширением будут исключены при сканировании, независимо от их расположения на жестком диске.

Объекты не будут проверяться, если они исключены из списка входного сканирования, независимо от того, используются ли они вами или приложением.

Замечание

Исключения НЕ применяются для контекстного сканирования.Контекстное сканирование — тип сканирования по требованию: вы щелкаете правой кнопкой на нужный файл или папку и выбираете **Сканировать с BitDefender**.

15.3.1. Исключение расширений файла из сканирования

Исключение путей из сканирования:

1. Откройте BitDefender.
2. В зависимости от режима пользовательского интерфейса выполните следующие действия:

   Интерфейс "Опытный пользователь"
   Перейдите на вкладку **Безопасность** и выберите **Настроить антивирус** в области быстрых задач в левой части окна.

   Перейдите на вкладку **Исключения**.

   Интерфейс "Эксперт"
   Перейдите в раздел **Антивирус > Исключения**.

   Замечание

   В интерфейсе "Основной" или "Опытный пользователь" можно создать ярлык для доступа к этим настройкам непосредственно из панели управления.Для получения дополнительной информации перейдите к *«Мои инструменты»* (p. 33).

3. Чтобы включить функцию исключений сканирования, установите соответствующий флажок.
4. Выполните следующие действия, чтобы запустить мастер конфигурации:
   - Щелкните правой кнопкой мыши в таблице "Файлы и папки" и выберите **Добавить новый путь**.
   - Нажмите кнопку **Добавить** в верхней части таблицы исключений.
5. Следуйте инструкциям мастера настройки.Навигация по мастеру осуществляется с помощью кнопок **Далее** и **Назад**.Для выхода из мастера нажмите **Отмена**.
   a. Выберите параметр для исключения пути из сканирования.Этот шаг отображается только при запуске мастера нажатием на кнопку **Добавить**.
   b. Чтобы определить пути, которые будут исключены из сканирования, используйте один из следующих методов:
      - Нажмите **Обзор**, выберите файл или папку для исключения из сканирования и нажмите **Добавить**.

- Введите путь, который вы хотите исключить из проверки, в соответствующее поле и нажмите **Добавить**.

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

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

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

Нажмите **Завершить**, чтобы добавить исключения сканирования.

6. Нажмите **Применить**, чтобы сохранить сделанные изменения.

15.3.2. Исключение расширений файла из сканирования

Исключение расширений файлов из сканирования:

1. Откройте BitDefender.
2. В зависимости от режима пользовательского интерфейса выполните следующие действия:

   Интерфейс "Опытный пользователь"
   Перейдите на вкладку **Безопасность** и выберите **Настроить антивирус** в области быстрых задач в левой части окна.

   Перейдите на вкладку **Исключения**.

   Интерфейс "Эксперт"
   Перейдите в раздел **Антивирус > Исключения**.

   Замечание

   В интерфейсе "Основной" или "Опытный пользователь" можно создать ярлык для доступа к этим настройкам непосредственно из панели управления.Для получения дополнительной информации перейдите к *«Мои инструменты»* (p. 33).

3. Чтобы включить функцию исключений сканирования, установите соответствующий флажок.
4. Выполните следующие действия, чтобы запустить мастер конфигурации:
   - Щелкните правой кнопкой мыши в таблице "Расширения" и выберите **Добавить расширения**.
   - Нажмите кнопку **Добавить** в верхней части таблицы исключений.

5. Следуйте инструкциям мастера настройки.Навигация по мастеру осуществляется с помощью кнопок **Далее** и **Назад**.Для выхода из мастера нажмите **Отмена**.

   a. Выберите параметр исключения расширений из сканирования.Этот шаг отображается только при запуске мастера нажатием на кнопку **Добавить**.

   b. 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 оно имеется.

   - В поле редактирования укажите расширение, которое должно быть исключено из сканирования, и нажмите **Добавить**.

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

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

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

      Нажмите **Завершить**, чтобы добавить исключения сканирования.

6. Нажмите **Применить**, чтобы сохранить сделанные изменения.

15.3.3. Управление исключениями сканирования

Если настроенные исключения сканирования больше не нужны, рекомендуется удалить или отключить их.

Управление исключениями сканирования:

1. Откройте BitDefender, нажмите **Параметры** в верхнем правом углу окна и выберите интерфейс **Эксперт**.
2. Перейдите в раздел **Антивирус > Исключения**.

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

Чтобы редактировать запись в таблице, выберите и нажмите кнопку **Редактировать**.Откроется новое окно, где вы сможете изменить расширение

или путь к исключению и тип сканирования, из которого вы хотите его исключить. Внесите необходимые изменения и нажмите **OK**.

Замечание

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

Чтобы отключить функцию исключений сканирования, снимите соответствующий флажок.

15.4. Карантин

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

Замечание

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

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

Просмотр и управление файлами в папке карантина и настройка параметров карантина:

1. Откройте BitDefender.
2. В зависимости от режима пользовательского интерфейса выполните следующие действия:

   Интерфейс "Опытный пользователь"

   Перейдите на вкладку **Безопасность** и выберите **Настроить антивирус** в области быстрых задач в левой части окна.

   Перейдите на вкладку **Карантин**.

   Интерфейс "Эксперт"

   Перейдите в раздел **Антивирус > Карантин**.

Замечание

В интерфейсе "Основной" или "Опытный пользователь" можно создать ярлык для доступа к этим настройкам непосредственно из панели управления.Для получения дополнительной информации перейдите к *«Мои инструменты»* (p. 33).

Управление файлами в карантине

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

Для удаления файлов, помещенных в карантин, выделите их и нажмите кнопку **Удалить**.

Для восстановления файла из папки карантина в исходную папку необходимо выбрать файл и нажать **Восстановить**.

Изменение настроек карантина

Чтобы изменить настройки карантина, нажмите **Настройки**.Используя настройки карантина, можно настроить BitDefender на автоматическое выполнение следующих действий:

Удаление старых файлов. Чтобы автоматически удалить старые файлы в карантине, включите соответствующий параметр.Вы должны указать количество дней, по истечении которых файлы из карантина будут удалены, и период, в который BitDefender будет проверять старые файлы.

Проверять файлы автоматически. Чтобы автоматически предлагать на рассмотрение изолированные файлы, выберите соответствующий параметр.Вы должны указать частоту, с которой следует предлагать файлы на рассмотрение.

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

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

16. Антифишинговая защита

Антифишинг BitDefender предотвращает разглашение личной информации при просмотре интернет-страниц путем уведомления о потенциально опасных веб-страницах.

BitDefender обеспечивает постоянную антифишинговую защиту для следующих приложений:

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

16.1. Настройка белого списка для антифишинга

Можно настроить и контролировать белый список веб-сайтов, для которых сканирование ядром антифишинга BitDefender выполняться не будет.Белый список должен содержать только те веб-сайты, которым вы полностью доверяете.Например, добавьте туда веб-сайты, где вы совершаете интернет-покупки.

Замечание

В белый список веб-сайты можно добавлять из панели антифишинга BitDefender, встроенного в ваш браузер.Для получения дополнительной информации перейдите к *«Управление антифишинговой защитой BitDefender в Internet Explorer и Firefox»* (p. 90).

Настройка и управление белым списком антифишинга:

- Если используется поддерживаемый веб-браузер, выберите Панель инструментов BitDefender, после чего выберите в меню **Белый список**.
- Также можно выполнить следующие действия:
  1. Откройте BitDefender, нажмите **Параметры** в верхнем правом углу окна и выберите интерфейс **Эксперт**.
  2. Перейдите в раздел **Антивирус > Щит**.
  3. Нажмите **Белый список**.

Чтобы добавить сайт в белый список, введите этот адрес в соответствующее поле и нажмите **Добавить**.

Если вы хотите удалить веб-сайт из белого списка, нажмите соответствующую кнопку **Удалить**.

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

16.2. Управление антифишинговой защитой BitDefender в Internet Explorer и Firefox

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

- Internet Explorer
- Mozilla Firefox

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

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

Замечание

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

Следующие команды доступны в меню панели инструментов:

- **Включить/выключить** — включает/выключает защиту антифишинга BitDefender в текущем браузере.
- **Настройки** — открывает окно, где вы можете определить настройки панели инструментов антифишинга.Доступны следующие варианты:
  - **Защита от фишинга в режиме реального времени** — обнаруживает и сообщает об обнаружении фишинг-сайта (созданного для кражи личной информации).Эта настройка контролирует защиту от фишинга BitDefender только в текущем браузере.
  - **Запрос перед добавлением в белый список** — запрашивает вас перед добавлением веб-сайта в белый список.
- **Добавить в белый список** — добавляет текущий веб-сайт в белый список.

Важно

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.

- **Белый список** — открывает белый список.Для получения дополнительной информации перейдите к *«Настройка белого списка для антифишинга»* (p. 89).
- **Отправить отчет о фишинге** — информирует специалистов BitDefender о подозрении в том, что данный сайт используется для фишинга.Сообщая о

фишинг-сайтах, вы помогаете другим не допустить кражу личной информации.

- **Справка** — открывает файл справки.
- **О программе** — открывает окно, где можно просмотреть информацию о BitDefender и о том, где искать помощь в случае непредвиденных обстоятельств.

17. Оптимизация поиска

Оптимизация поиска позволяет повысить уровень защиты от интернет-угроз, отображая оповещения о попытках фишинга и ненадежных веб-сайтах непосредственно на странице результатов поиска.

Функция оптимизации поиска совместима с любым веб-браузером. Эта функция служит для проверки результатов поиска, отображаемых наиболее распространенными поисковыми системами.

- Google
- Yahoo!
- Звуковое оповещение

Оптимизация поиска показывает, является ли результат поиска надежным. Для этого рядом с каждой из ссылок помещается соответствующий значок.

Зеленый круг с галочкой: Теперь можно безопасно выполнить переход по ссылке.

Красный круг с восклицательным знаком: Этот веб-сайт является фишинговым или ненадежным.Осуществлять переход по ссылке не рекомендуется.При попытке перейти по ссылке в браузерах Internet Explorer или Firefox BitDefender автоматически блокирует веб-страницу и отображает вместо этого страницу оповещения.Чтобы проигнорировать оповещение и перейти на веб-страницу, выполните инструкции, отображаемые на странице оповещения.

17.1. Отключение оптимизации поиска

Отключение оптимизации поиска:

1. Откройте BitDefender, нажмите кнопку **Параметры** в верхнем правом углу окна и выберите **Установки**.
2. Перейдите в раздел **Настройки безопасности**.
3. Для отключения оптимизации поиска воспользуйтесь переключателем.

18. Антиспам

Термином "спам" обозначаются нежелательные сообщения электронной почты.Проблема спама актуальна и для простых пользователей, и для больших компаний. Вам не хотелось бы, чтобы некоторые из этих писем попали на глаза вашим детям, а на работе вас могут даже уволить за трату рабочего времени на спам или за получение на ваш рабочий адрес электронной почты рассылок сексуального содержания. И вы не можете помешать таким рассылкам! 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.

Антиспам BitDefender использует передовые технологические достижения и соответствующие стандарты для отсеивания спама фильтром еще до того, как он попадает в ваш почтовый ящик.Для получения дополнительной информации перейдите к «*Об антиспаме*» (p. 93).

Защита антиспама BitDefender доступна только для клиентов электронной почты, настроенной на прием сообщений электронной почты по протоколу POP3.POP3 является одним из наиболее широко используемых протоколов для загрузки сообщений электронной почты с почтового сервера.

Замечание

BitDefender не предоставляет защиту антиспама для учетных записей электронной почты, доступ к которым осуществляется через веб-интерфейс.

Спам-сообщения, обнаруженные BitDefender, помечаются префиксом [spam] в строке темы.BitDefender автоматически перемещает спам в особую папку, такую как:

- В Microsoft Outlook спам перемещается в папку **Спам**, находящуюся в папке **Удаленные**.Папка **Спам** создается во время установки BitDefender.
- В Outlook Express и Windows Mail спам перемещается в папку **Удаленные**.
- В Mozilla Thunderbird спам перемещается в папку **Спам**, находящуюся в папке **Удаленные**.Папка **Спам** создается во время установки BitDefender.

При использовании других почтовых клиентов необходимо создать правило, позволяющее перемещать сообщения электронной почты, помеченные как [spam] BitDefender в настраиваемую папку карантина.

18.1. Об антиспаме

18.1.1. Антиспам-фильтры

Механизм ядра антиспама BitDefender состоит из нескольких различных фильтров, надежно защищающих папку входящих сообщений от СПАМА:

Список друзей, Список спамеров, Фильтр символов, Фильтр изображений, Фильтр URL, Фильтр NeuNet (эвристический) и Байесовский фильтр.

Список друзей/список спамеров

Большинство людей переписываются с определенной группой людей или получают письма от компаний с одного домена. Используя **списки друзей или спамеров**, вы легко можете выделить людей, от которых вы хотите получать письма независимо от их содержания (друзья), и людей, от которых вы не хотите получать ни строчки (спамеры).

Замечание

Рекомендуется записывать имена и адреса электронной почты друзей в **Список друзей**. BitDefender пропускает сообщения от адресатов из этого списка. Так вы будете уверены, что получите ожидаемые письма.

Фильтр символов

Многие спам-сообщения написаны кириллицей или иероглифами. Фильтр кодировки определяет подобные сообщения и помечает их как СПАМ.

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 ввел **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 СПАМ.

Фильтр URL

Практически все спам-сообщения содержат ссылки на различные ресурсы. Обычно эти ресурсы содержат еще больше рекламы, а также 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 СПАМ.

Фильтр NeuNet (эвристический)

Нейросетевой (эвристический) фильтр производит ряд тестов над всеми компонентами сообщения (т. е. не только над заголовком, но и над текстом сообщения в текстовом или HTML-формате) путем поиска 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 СОДЕРЖАЩИЕ ИНФОРМАЦИЮ СЕКСУАЛЬНОГО ХАРАКТЕРА:, и также помечает их как СПАМ.

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

Байесовский фильтр можно скорректировать, используя кнопки **Это спам** и **Не спам**, размещенные на панели управления антиспамом.

18.1.2. Работа антиспама

Ядро антиспама BitDefender использует все антиспамовые фильтры, чтобы определить, должно ли сообщение попасть во **Входящие** или нет.

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**.

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

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

Фильтр URL-адресов сопоставляет ссылки, найденные в сообщениях электронной почты, со ссылками из базы данных зарегистрированных спам-ссылок BitDefender. При обнаружении совпадений соответствующее сообщение электронной почты будет помечено как СПАМ.

Затем фильтр NeuNet (эвристический) проведет ряд проверок компонентов сообщения поиском слов, фраз, ссылок или других характеристик СПАМА.В зависимости от результатов анализа сообщению электронной почты присваивается рейтинг спама.

Замечание

Письма категории "ОТКРОВЕННО СЕКСУАЛЬНОЕ" BitDefender считает СПАМОМ.

Далее письмо анализируется с помощью Байесовского фильтра на основе статистической информации о повторах определенных слов в сообщениях, помеченных как СПАМ, в сравнении с письмами, помеченными вами или эвристическим фильтром как НЕ СПАМ. В результате письмо добавляется к списку.

Если совокупный рейтинг спама (рейтинг, присвоенный эвристическим анализом, + рейтинг, присвоенный Байесовским ядром) превышает пороговое значение, электронное сообщение расценивается как СПАМ.Пороговый уровень определяется уровнем защиты антиспама.Для получения дополнительной информации перейдите к «*Настройка уровня защиты*» (p. 102).

18.1.3. Обновления антиспама

Каждый раз, когда вы выполняете обновление:

- новые сигнатуры изображений будут добавляться в **Фильтр изображений**;
- новые ссылки будут добавляться в **Фильтр URL**;
- новые правила будут добавляться в **фильтр NeuNet (эвристический)**;

Это поможет повысить эффективность вашего ядра антиспама.

Чтобы защитить вас от спамеров, BitDefender может выполнить автоматические обновления. Для этого параметр **Автоматическое обновление** должен быть включен.

18.2. Мастер оптимизации антиспама

При первом запуске почтового клиента, после установки BitDefender, появится программа-мастер, которая поможет вам настроить Список друзей, Список спамеров и обучить Байесовский фильтр для того, чтобы повысить эффективность работы фильтров Антиспама.

Замечание
Также можно запустить мастер в нужное вам время, нажав **Мастер** на Панели инструментов антиспама.

Навигация по мастеру осуществляется с помощью кнопок **Далее** и **Назад**.Если вы хотите пропустить шаг конфигурации, выберите **Пропустить этот шаг**.Для выхода из мастера нажмите **Отмена**.

1. **Окно приветствия**
2. **Добавить контакты в список друзей**

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

   Чтобы добавить все ваши контакты в список друзей, нажмите **Выбрать все**.
3. **Удаление байесовой базы данных**

   Замечание
   При первом запуске мастера перейдите сразу к следующему шагу.

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

   Поставьте значок в поле **Очистить базу данных фильтра антиспама**, если хотите переустановить базу данных Байесовского фильтра.

   Вы можете сохранить Байесовскую базу данных в файл для использования с другим продуктом BitDefender или после переустановки BitDefender.Для сохранения Байесовской базы данных нажмите кнопку **Сохранить базу**

данных Байесовского фильтра и сохраните ее в желаемое место.Файл будет иметь расширение `.dat`.

Для загрузки ранее сохраненной Байесовской базы данных нажмите кнопку **Загрузить базу данных Байесовского фильтра** и откройте соответствующий файл.

4. **Установка настроек байесовского фильтра для легитимных сообщений электронной почты (не спам)**

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

   Имеются два дополнительных параметра в списке каталогов:
   - **Включать все подкаталоги** — включает в вашу выборку подкаталоги.
   - **Автоматически добавлять в список друзей** — добавление отправителей в список друзей.

5. **Установка настроек Байесовского фильтра для сообщений электронной почты, содержащих спам**

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

   Важно
   Убедитесь в том, что выбранная вами папка не содержит легальных почтовых сообщений (не спам). В противном случае эффективность работы антиспама будет существенно снижена.

   Имеются два дополнительных параметра в списке каталогов:
   - **Включать все подкаталоги** — включает в вашу выборку подкаталоги.
   - **Автоматически добавлять в список спамеров** — для добавления отправителей в список спамеров.Сообщения электронной почты от этих пользователей всегда будут помечаться как СПАМ и обрабатываться соответствующим образом.

6. **Сводка**

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

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

18.3. Использование панели инструментов антиспама в окне почтового клиента

В верхней части вашей почтовой программы вы можете увидеть панель антиспама.Панель антиспама позволяет вам управлять защитой от спама

непосредственно из почтовой программы.Вы можете легко поправить BitDefender, если он принял легальное письмо за СПАМ.

Важно

BitDefender интегрируется в наиболее часто используемые почтовые клиенты с помощью простой в использовании антиспам панели инструментов.С полным списком системных требований можно ознакомиться в разделе *«Требования программного обеспечения»* (p. 2).

Ниже приводится описание каждой кнопки панели инструментов BitDefender:

- **Это спам** — отправление Байесовскому модулю сообщения 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.

- **Не спам** — отправление сообщения Байесовскому модулю о том, что выделенное сообщение не является спамом и программе BitDefender не следует помечать его как спам.Письмо будет перемещено из папки **Спам** в папку **Входящие**.

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

  Важно

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

- **Добавить спамера** — добавляет отправителя выбранного письма в список спамеров.Вам будет необходимо нажать **OK** для подтверждения.Почтовые сообщения, полученные с адресов из списка спамеров, автоматически помечены как [спам].

- **Добавить друга** — добавляет отправителя выбранного письма в список друзей.Вам будет необходимо нажать **OK** для подтверждения.Вы всегда будете получать сообщения от этого адресата, независимо от их содержания.

- **Спамеры** — открытие **Списка спамеров**, содержащего адреса, с которых вы не хотите получать сообщения, независимо от их содержания.Для получения дополнительной информации перейдите к *«Настройка списка спамеров»* (p. 104).

- **Друзья** — открытие **Списка друзей**, содержащего адреса, с которых вы всегда хотите получать сообщения независимо от их содержания.Для получения дополнительной информации перейдите к *«Настройка списка друзей»* (p. 103).

- **Настройки** — открытие окна **Настройки**, где можно указать некоторые параметры **антиспама**.
- **Мастер** — открывает мастер оптимизации антиспама.С помощью этого мастера вы сможете обучить Байесовский фильтр и сделать защиту антиспама еще более эффективной.Вы можете также добавлять адреса из вашей адресной книги в список друзей/спамеров.
- **Антиспам BitDefender** — открывает окно, в котором можно настроить уровень защиты антиспама и фильтры антиспама.

18.3.1. Отображение ошибок обнаружения

Если вы используете поддерживаемый почтовый клиент, вы можете легко корректировать фильтр антиспама (указывая письма, которые не надо помечать как [спам]). Данные действия улучшат эффективность фильтра антиспама.Выполните следующие действия:

1. Откройте ваш почтовый клиент.
2. Перейдите в папку нежелательной почты, куда помещаются спам-сообщения.
3. Выберите легитимные сообщения, ошибочно помеченные BitDefender как [спам].
4. Нажмите кнопку **Добавить друга** на панели управления антиспама BitDefender для добавления отправителя в список друзей.Вам будет необходимо нажать **OK** для подтверждения.Вы всегда будете получать сообщения от этого адресата, независимо от их содержания.
5. Нажмите кнопку **Не спам** на панели антиспама BitDefender (обычно расположенной в верхней части окна почтового клиента). Это укажет обучающему ядру, что выбранные сообщения не являются спамом, и они будут перемещены в папку "Входящие".Следующие сообщения электронной почты, содержащие одинаковые части, больше не будут помечены как [спам].

18.3.2. Обозначение необнаруженных спам-сообщений

Если вы используете поддерживаемый почтовый клиент, вы можете легко определить, какие сообщения должны быть определены как спам. Эти действия значительно улучшат эффективность фильтра антиспама.Выполните следующие действия:

1. Откройте ваш почтовый клиент.
2. Перейти к папке "Входящие".
3. Выберите необнаруженные спам-сообщения.

4. Нажмите кнопку **Это спам** на панели антиспама BitDefender (обычно она расположена в верхней части окна почтового клиента). Это укажет обучающему ядру, что выбранные сообщения являются спамом. Они незамедлительно будут помечены как [спам] и перенесены в папку нежелательной почты.Следующие сообщения электронной почты, содержащие одинаковые части, будут помечены как [спам].

18.3.3. Переподготовка обучающего ядра (Байесовского)

Если работа фильтра антиспама некорректна, возможно, потребуется очистить Байесовскую базу данных и переподготовить Байесовский фильтр.

Перед тренировкой обучающего ядра (Байесовского) приготовьте одну папку, содержащую только СПАМ-сообщения, и другую, содержащую только легальную почту.Обучающее ядро проанализирует их и выучит характеристики, определяющие спам или легальные сообщения, которые вам обычно приходят. Для того чтобы обучение было эффективным, в каждой папке должно быть более 50 сообщений.

Чтобы сбросить Байесовскую базу данных и переобучить обучающее ядро, следуйте этим шагам:

1. Откройте ваш почтовый клиент.
2. На панели инструментов аниспама BitDefender нажмите кнопку **Мастер** для запуска мастера настройки антиспама.
3. Нажмите **Далее**.
4. Выберите **Пропустить этот шаг** и нажмите **Далее**.
5. Выберите **Очистить базу данных фильтра антиспама** и нажмите **Далее**.
6. Выберите папку, содержащую легальную почту, и нажмите **Далее**.
7. Выберите папку, содержащую СПАМ-сообщения, и нажмите **Далее**.
8. Нажмите **Завершить** для запуска процесса тренировки.
9. Когда обучение закончится, нажмите **Закрыть**.

18.3.4. Сохранение и загрузка Байесовской базы данных

Вы можете сохранить Байесовскую базу данных в файл для использования с другим продуктом BitDefender или после переустановки BitDefender.

Нажмите кнопку **Настройка** на панели инструментов модуля антиспама BitDefender.

Для сохранения Байесовской базы данных нажмите кнопку **Сохранить базу данных Байесовского фильтра** и сохраните ее в желаемое место.Файл будет иметь расширение .dat.

Для загрузки ранее сохраненной Байесовской базы данных нажмите кнопку **Загрузить базу данных Байесовского фильтра** и откройте соответствующий файл.

18.3.5. Конфигурация основных настроек

Чтобы задать общие настройки защиты антиспама для почтового клиента, нажмите кнопку **Настройки** на панели инструментов модуля антиспама BitDefender.

Доступны следующие варианты:

- **Перемещать сообщения в папку "Удаленные"** - 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.

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

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

18.4. Настройка уровня защиты

Некоторые фильтры антиспама способны распознавать спам непосредственно в сообщениях электронной почты; другие присваивают сообщению рейтинг спама в зависимости от распознанных характеристик спама.

Уровень защиты антиспама позволяет определить, содержит ли сообщение электронной почты спам, исходя из общего рейтинга спама (этот рейтинг формируется после проверки сообщения всеми фильтрами антиспама).

Уровень защиты для модуля антиспама рекомендуется изменять только в том случае, если защита антиспама не работает должным образом.Тем не менее, вместо того, чтобы изменить отдельно уровень защиты, рекомендуется сначала ознакомиться с *«Антиспам работает некорректно»* (p. 194) и следовать инструкциям по устранению проблемы.

Регулировка уровня защиты антиспама:

1. Откройте BitDefender, нажмите **Параметры** в верхнем правом углу окна и выберите интерфейс **Эксперт**.
2. Перейдите в раздел **Антиспам > Состояние**.

3. Чтобы установить желаемый уровень защиты, перетащите бегунок в требуемое положение.Для выбора уровня по умолчанию (**Умеренно агрессивный**) нажмите **Уровень по умолчанию**.

Воспользуйтесь описанием справа от шкалы, чтобы выбрать тот уровень защиты, который оптимально соответствует требованиям к безопасности.В описании также приведены сведения о дополнительных действиях, которые необходимо выполнить во избежание проблем или в целях повышения эффективности распознавания спама.

18.5. 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 спама.

Замечание

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

Настройка и управление списком друзей:

- Если используется Microsoft Outlook/Outlook Express/Windows Mail/Thunderbird, нажмите кнопку **Друзья** на панели инструментов BitDefender, интегрированной в почтовый клиент.
- Также можно выполнить следующие действия:
  1. Откройте BitDefender, нажмите **Параметры** в верхнем правом углу окна и выберите интерфейс **Эксперт**.
  2. Перейдите в раздел **Антиспам > Состояние**.
  3. Нажмите **Управление друзьями**.

Для добавления адреса электронной почты выберите параметр **Адрес электронной почты**, введите адрес и нажмите на кнопку, расположенную рядом с полем редактирования.Адрес должен иметь следующую структуру: name@domain.com.

Чтобы добавить адреса электронной почты из конкретного домена, выберите параметр **Имя домена**, введите имя домена и нажмите на кнопку рядом с полем редактирования.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;

Рекомендуется избегать добавления целых доменов, хотя в некоторых ситуациях это может оказаться полезным.Например, можно добавить домен электронной почты вашей компании или домены доверенных партнеров.

Чтобы удалить элемент из списка, выберите его и нажмите кнопку **Удалить**.Чтобы удалить все содержимое из списка, нажмите **Очистить список** и **Да** для подтверждения выбора.

Вы можете сохранить список друзей в файл для использования на другом компьютере или после переустановки продукта.Для сохранения списка друзей нажмите кнопку **Сохранить** и сохраните список в желаемое место.Расширение файла будет `.bwl` .

Для загрузки сохраненного ранее списка друзей нажмите кнопку **Загрузка** и откройте соответствующий `.bwl`-файл.Чтобы сбросить содержание текущего списка при загрузке предварительно сохраненного, нажмите **Перезаписать список**.

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

18.6. Настройка списка спамеров

Список спамеров — список адресов электронной почты, с которых вы не хотите получать письма независимо от их содержания.Все электронные письма, приходящие с адресов, указанных в **Списке спамеров**, будут помечены как СПАМ автоматически, без обработки.

Настройка и управление списком спамеров:

- Если используется Microsoft Outlook/Outlook Express/Windows Mail/Thunderbird, нажмите кнопку **Спамеры** на панели инструментов BitDefender, интегрированной в почтовый клиент.
- Также можно выполнить следующие действия:
  1. Откройте BitDefender, нажмите **Параметры** в верхнем правом углу окна и выберите интерфейс **Эксперт**.
  2. Перейдите в раздел **Антиспам > Состояние**.
  3. Нажмите **Управление спамерами**.

Для добавления адреса электронной почты выберите параметр **Адрес электронной почты**, введите адрес и нажмите на кнопку, расположенную рядом с полем редактирования.Адрес должен иметь следующую структуру: name@domain.com.

Чтобы добавить адреса электронной почты из конкретного домена, выберите параметр **Имя домена**, введите имя домена и нажмите на кнопку рядом с полем редактирования.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.

Рекомендуется избегать добавления целых доменов, хотя в некоторых ситуациях это может оказаться полезным.

Внимание

На добавляйте домены легальных онлайн-служб электронной почты (таких как Yahoo, Gmail, Hotmail и другие) в список спамеров, иначе любое сообщение, полученное от пользователя такой службы, будет определено как спам.Например, если вы добавите `yahoo.com` в список спамеров, все сообщения электронной почты, приходящие от адресов `yahoo.com`, будут помечены как `[спам]`.

Чтобы удалить элемент из списка, выберите его и нажмите кнопку **Удалить**.Чтобы удалить все содержимое из списка, нажмите **Очистить список** и **Да** для подтверждения выбора.

Вы можете сохранить список спамеров в файл для использования на другом компьютере или после переустановки продукта.Для сохранения списка спамеров нажмите кнопку **Сохранить** и сохраните список в желаемое место.Расширение файла будет `.bwl` .

Для загрузки сохраненного ранее списка спамеров нажмите кнопку **Загрузка** и откройте соответствующий `.bwl`-файл.Чтобы сбросить содержание текущего списка при загрузке предварительно сохраненного, нажмите **Перезаписать список**.

Нажмите **Применить** и **OK**, чтобы сохранить и закрыть **Список спамеров**.

18.7. Настройка фильтров антиспама и параметров антиспама

Как описано в «*Об антиспаме*» (p. 93), для распознавания спама BitDefender использует комбинацию из нескольких различных фильтров антиспама.Фильтры антиспама предварительно настроены в целях обеспечения эффективной защиты.

Можно отключить любой из этих фильтров или изменить их настройки (не рекомендуется).Здесь представлены некоторые доступные изменения:

- В зависимости от того, получаете ли вы легитимные сообщения электронной почты, созданные с использованием символов кириллицы или иероглифов, следует включить или отключить параметр, автоматически блокирующий прием таких сообщений.

Замечание

В локализованных версиях программы, в которых используются такие шрифты, соответствующая настройка отключена (например, в русской или китайской версии).

- Если вы не хотите автоматически добавлять получателей отправленных сообщений электронной почты в список друзей, можно отключить соответствующую настройку.В этом случае необходимо добавить контакты в список друзей, как описано в *«Настройка списка друзей»* (p. 103).
- Опытные пользователи могут в целях оптимизации работы антиспама самостоятельно отрегулировать размер Байесовского словаря.При использовании меньшего количества слов обработка антиспама выполняется быстрее, но с меньшей точностью.Использование большего количества слов позволяет повысить точность распознавания спама, но при этом увеличивает время открытия сообщений электронной почты.

Замечание

Для достижения желаемого уровня производительности может потребоваться неоднократная регулировка размера Байесовского словаря.Если не удалось достичь желаемого результата, выполните возврат к настройкам по умолчанию и задайте рекомендуемый размер в 200 000 слов.

Настройка параметров и фильтров антиспама:

1. Откройте BitDefender, нажмите **Параметры** в верхнем правом углу окна и выберите интерфейс **Эксперт**.
2. Перейдите в раздел **Антиспам > Настройки**.
3. Установите требуемые настройки.Для того чтобы узнать, на что влияет настройка, подержите курсор мыши над ней. Внизу окна появится подсказка.
4. Нажмите **Применить**, чтобы сохранить сделанные изменения.

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

19. Родительский контроль

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

В модуле родительского контроля можно настроить блокировку:

- неприемлемые веб-страницы.
- Доступ в Интернет в определенные промежутки времени (например, во время уроков).
- веб-страниц, электронных сообщений и мгновенных сообщений, если они содержат определенные слова;
- приложения, такие как игры, чаты, программы обмена файлами и другие.
- Мгновенные сообщения, отправленные заблокированными IM-контактами.

Важно

Только пользователи с правами администратора (системные администраторы) могут получить доступ для настройки родительского контроля.Чтобы быть уверенным в том, что только вы можете менять настройки родительского контроля для любого пользователя, рекомендуется защитить эти настройки паролем.При включении родительского контроля для определенного пользователя вам будет предложено установить пароль.

Настроив родительский контроль, можно легко выяснить, чем занимались дети на компьютере.

Даже находясь не дома, с помощью функции удаленного родительского контроля вы сможете проверять, что делают дети в Интернете и на компьютере, и изменять настройки родительского контроля.

19.1. Настройка Родительского Контроля

Перед тем как приступить к настройке родительского контроля, необходимо создать отдельные учетные записи пользователей Windows, которые будут использоваться детьми. Таким образом вы всегда будете точно знать, чем они занимаются за компьютером. Рекомендуется создать ограниченные (стандартные) учетные записи, параметры которых не позволяют изменять настройки родительского контроля.Для получения дополнительной информации перейдите к *«Создание учетных записей пользователя Windows»* (p. 178).

Если дети имеют доступ к учетной записи администратора на своем компьютере, необходимо задать пароль для защиты настроек родительского

контроля.Для получения дополнительной информации перейдите к *«Защита настроек родительского контроля»* (p. 109).

Настройка родительского контроля:

1. При загрузке системы необходимо выполнить вход в учетную запись администратора.Только пользователи с правами администратора (системные администраторы) могут получить доступ для настройки родительского контроля.
2. Откройте BitDefender.
3. Перейдите в раздел настроек родительского контроля. Для этого выполните следующие действия (в зависимости от режима пользовательского интерфейса):

   Интерфейс "Опытный пользователь"
   Перейдите на вкладку **Безопасность** и выберите **Родительский контроль** в области быстрых задач в левой части окна.

   Интерфейс "Эксперт"
   Выберите **Родительский контроль** в меню с левой стороны.

Замечание

В интерфейсе "Основной" или "Опытный пользователь" можно создать ярлык для доступа к этим настройкам непосредственно из панели управления.Для получения дополнительной информации перейдите к *«Мои инструменты»* (p. 33).

Вы можете увидеть информацию о статусе родительского контроля для каждой учетной записи Windows.Возрастные категории отображаются ниже имени каждого пользователя, если родительский контроль включен.Если родительский контроль отключен, статус будет **Не настроен**.

Настройка родительского контроля для конкретной учетной записи пользователя:

1. Для включения родительского контроля для этой учетной записи пользователя установите соответствующий флажок.
2. Пользователю будет предложено настроить пароль для родительского контроля.Установите пароль для защиты параметров родительского контроля.Для получения дополнительной информации перейдите к *«Защита настроек родительского контроля»* (p. 109).
3. Задайте возрастную категорию, чтобы открыть вашим детям доступ к тем сайтам, которые подходят им по возрасту.Когда пользователь указывает возраст ребенка, автоматически загружаются настройки, соответствующие данной категории возраста (на основе стандартов детского развития).

4. Если требуется детальная настройка параметров родительского контроля, нажмите **Настройки**.Перейдите на вкладку конфигурации соответствующей функции родительского контроля:
   - **Веб** — для фильтрации веб-навигации в соответствии с правилами, установленными вами в разделе Веб.
   - **Приложения** — для блокировки приложений, определенных вами в разделе Приложения.
   - **Ключевые слова** — для фильтрации Интернета, почты и мгновенных сообщений в соответствии с правилами, установленными вами в разделе Ключевые слова.
   - **Обмен сообщениями** — разрешение или блокировка чата с IM-контактами в соответствии с правилами, заданными в разделе Обмен сообщениями.

Замечание
Для того чтобы узнать, как их настроить, обратитесь к следующим темам этой главы.

Настройте параметры отслеживания по своему выбору:

- **Отправить мне отчет об активности по электронной почте.** Уведомление по электронной почте отправляется каждый раз, когда родительский контроль BitDefender блокирует действие.Сначала необходимо настроить параметры уведомления.
- **Сохранять журнал интернет-трафика.** Журналы посещенных сайтов тех пользователей, в отношении которых включен родительский контроль.

Для получения дополнительной информации перейдите к *«Контроль детской активности»* (p. 117).

Если вы хотите отслеживать и контролировать действия детей на компьютере и в Интернете, включите удаленный родительский контроль с помощью соответствующего переключателя.Для получения дополнительной информации перейдите к *«Удаленный родительский контроль»* (p. 120).

19.1.1. Защита настроек родительского контроля

Если вы не единственный, кто имеет права администратора данного компьютера, рекомендуется защитить настройки родительского контроля паролем.Установив пароль, вы защитите установленные вами для определенных пользователей настройки родительского контроля от изменений другими пользователями, обладающими правами администратора.

При включении родительского контроля BitDefender запросит у вас пароль (при настройках по умолчанию).Для того чтобы установить защиту паролем, проделайте следующее:

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

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

Замечание
Этот пароль не защитит другие настройки BitDefender.

Если вы не хотите, чтобы постоянно появлялось это окно, отметьте **Не запрашивать пароль при включении родительского контроля**.

Важно
Если вы забыли пароль, вам придется переустановить программу или обратиться за помощью в службу поддержки клиентов BitDefender.

Удаление защиты паролем:

1. Откройте BitDefender и нажмите кнопку **Параметры** в верхнем правом углу окна.
2. Перейдите в раздел **Общие настройки**.
3. Для отключения параметра **Пароль настроек** снимите соответствующий флажок.
4. Введите пароль.
5. Нажмите **OK**.

19.1.2. Веб-контроль

Веб-контроль дает вам возможность блокировать доступ к сайтам с недопустимым, по вашему мнению, содержимым. 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.

Замечание
При включении функции родительского контроля и вводе возраста ребенка автоматически будет включен веб-контроль, настроенный для блокировки доступа к веб-сайтам, посещение которых детьми этого возраста считается недопустимым.

Настройка веб-контроля для отдельной учетной записи пользователя:

1. Откройте окно настроек родительского контроля BitDefender для этой учетной записи пользователя.
2. Перейдите на вкладку **Интернет**.
3. Для включения веб-контроля установите соответствующий флажок.
4. Вы можете проверить, какие веб-категории блокируются или ограничиваются автоматически для текущих заданных возрастных групп.Если настройки по умолчанию вам не подходят, можно настроить параметры по собственному выбору.

   Для изменения действия, настроенного для определенной категории веб-содержимого, щелкните на текущем статусе и выберите в меню требуемое действие.
5. При необходимости пользователь может создать собственные правила, позволяющие разрешить или запретить доступ к определенным веб-сайтам.Если доступ к веб-сайту автоматически блокируется родительским контролем, можно создать правило, в котором будет явно задано разрешение для доступа к этому сайту.
6. Можно установить ограничения по времени для работы детей в Интернете.Для получения дополнительной информации перейдите к «Ограничение доступа в Интернет по времени» (p. 112).

Создание правил веб-контроля

Что бы разрешить или заблокировать доступ к сайту, следуйте этим шагам:

1. Нажмите **Разрешить веб-сайт** или **Заблокировать веб-сайт**.
2. Введите адреса сайтов в поле **Веб-сайт**.
3. Выберите желаемое действие для этого правила — **Разрешить** или **Блокировать**
4. Нажмите **Завершить**, чтобы добавить правило.

Управление правилами веб-контроля

Назначенные правила контроля сайтов перечислены в таблице в нижней части окна. Адрес сайта и текущий статус отображены для каждого правила.

Чтобы удалить правило, выделите его и нажмите **Удалить**.

Чтобы изменить правило, выберите его и нажмите **Редактировать** или дважды щелкните на нем мышью.Внесите необходимые изменения в окне конфигурации.

Ограничение доступа в Интернет по времени

В разделе "Настройка расписания веб-доступа" можно задать ограничения по времени доступа детей в Интернет.

Чтобы полностью заблокировать доступ в Интернет, выберите **Блокировать веб-доступ**.

Ограничение доступа в Интернет в заданные периоды:

1. Выберите **Ограничить веб-доступ по времени**.
2. Нажмите **Изменить расписание**.
3. Задайте в сетке периоды, в течение которых доступ в Интернет будет заблокирован.Можно щелчком мыши отметить отдельные клетки или нажать на клетку и перетащить, чтобы задать более длительный период.
4. Нажмите **Сохранить**.

Замечание

BitDefender выполняет обновление раз в час, несмотря на блокировку доступа в Интернет.

19.1.3. Контроль приложений

Контроль приложений позволяет вам блокировать выполнение любого приложения. Таким образом можно заблокировать игровые, медийные и информационные программы, а также другие категории программного обеспечения и вредоносных кодов. Блокировка приложений таким способом одновременно защищает их от модификации, и поэтому они не могут быть скопированы или перемещены.Вы можете заблокировать приложение навсегда или на определенные интервалы времени, например на такие, когда вашим детям необходимо делать домашнее задание.

Настройка управления приложениями для конкретной учетной записи пользователя:

1. Откройте окно настроек родительского контроля BitDefender для этой учетной записи пользователя.
2. Перейдите на вкладку **Приложения**.
3. Для включения контроля приложений воспользуйтесь соответствующим переключателем.
4. Создайте правила для приложений, которые необходимо заблокировать или ограничить к ним доступ.

Создание правил контроля приложений

Чтобы заблокировать или ограничить доступ к приложению, следуйте этим шагам:

1. Нажмите **Заблокировать приложение** или **Ограничить приложение**.
2. Нажмите **Обзор** для определения приложения, к которому вы хотите заблокировать/разрешить доступ.Установленные приложения находятся в папке `C:\Program Files`.
3. Выберите действие для правила:
   - **Блокировать навсегда** для полного ограничения доступа к приложению.
   - **Блокирование, основанное на этом расписании** для ограничения доступа в определенные интервалы времени.

   Если вы выбрали ограничение доступа, а не блокирование приложения полностью, вы должны также выбрать из сетки дни и временные интервалы времени, в течение которых будет заблокирован доступ.
4. Нажмите **Сохранить**, чтобы добавить правило.

Управление правилами контроля приложений

Назначенные правила контроля приложений перечислены в таблице в нижней части окна. Имя приложения, путь и текущий статус отображены для каждого правила.

Чтобы удалить правило, выделите его и нажмите **Удалить**.

Чтобы изменить правило, выберите его и нажмите **Редактировать** или дважды щелкните на нем мышью.Внесите необходимые изменения в окне конфигурации.

19.1.4. Модуль контроля ключевых слов

Контроль ключевых слов помогает блокировать доступ пользователя к сообщениям электронной почты и мгновенным сообщениям, содержащим определенные слова.Используя контроль ключевых слов, можно предотвращать просмотр вашими детьми неподобающих слов или фраз, когда они находятся в сети.

Замечание
Контроль ключевых слов мгновенных сообщений доступен только для приложений Yahoo Messenger и Windows Live (MSN) Messenger.

Настройка контроля ключевых слов для отдельной учетной записи пользователя:

1. Откройте окно настроек родительского контроля BitDefender для этой учетной записи пользователя.
2. Перейдите на вкладку **Ключевые слова**.
3. Для включения контроля ключевых слов установите соответствующий флажок.
4. Создайте правила контроля ключевых слов, с помощью которых будут блокироваться нежелательные ключевые слова.
5. Во избежание отправки детьми личных данных (домашнего адреса или номера телефона) людям, с которыми они познакомились в сети, необходимо создать правила контроля личных данных.Для получения дополнительной информации перейдите к «Создание правил контроля конфиденциальности» (p. 115).

Создание правил контроля ключевых слов

Чтобы заблокировать слово или фразу, следуйте этим шагам:

1. Нажмите **Блокировать ключевое слово**.
2. Введите слово или фразу, которую вы хотите заблокировать. Если вы хотите, чтобы определялись только все слова, отметьте флажок **Совпадение всех слов**.
3. Выберите тип трафика, который должен сканировать BitDefender на наличие определенного слова.

Настройка	Описание
HTTP	Блокируются веб-страницы, содержащие ключевое слово.
POP3	Блокируются электронные сообщения, содержащие ключевое слово.
Службы мгновенных сообщений	Блокируются мгновенные сообщения, содержащие ключевое слово.

4. Нажмите **Завершить**, чтобы добавить правило.

Управление правилами контроля ключевых слов

Настроенные правила контроля ключевых слов перечислены в таблице. Для каждого из правил приведено подробное описание.

Чтобы удалить правило, выделите его и нажмите **Удалить**.

Чтобы изменить правило, выберите его и нажмите **Редактировать** или дважды щелкните на нем мышью.Внесите необходимые изменения в окне конфигурации.

Создание правил контроля конфиденциальности

Чтобы создать новое правило контроля личных данных, нажмите соответствующую кнопку **Блокировать ключевое слово** и следуйте инструкциям мастера конфигурации.Навигация по мастеру осуществляется с помощью кнопок **Далее** и **Назад**.Для выхода из мастера нажмите **Отмена**.

1. **Окно приветствия**
2. **Установка типа правила и данных**

   Вам необходимо настроить следующие параметры:

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

     Важно
     Если вы введете менее трех символов, вам будет предложено уточнить данные. Рекомендуется вводить минимум три символа, чтобы избежать ошибочного блокирования сообщений и веб-страниц.

   Все введенные вами данные шифруются. Для дополнительной безопасности не вводите полностью данные, которые вы хотите защитить.

3. **Выбор параметров сканирования**

   Выберите тип трафика, который будет проверяться BitDefender.

   - **Проверять веб-трафик (HTTP-трафик)** — сканирует HTTP-трафик (веб-трафик) и блокирует исходящие данные в соответствии с правилами.
   - **Проверка трафика эл. почты (SMTP-трафика)** — проверяет SMTP-трафик (почтовый трафик) и блокирует исходящие электронные сообщения, содержащие данные правила.
   - **Проверка IM-трафика** — сканирует трафик мгновенных сообщений и блокирует исходящие сообщения в соответствии с правилами.

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

4. **Опишите правило**

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

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

С этого момента любые попытки отправить указанные данные (по электронной почте, через службу мгновенных сообщений или через веб-страницу) будут блокироваться. При этом будет выводиться оповещение о том, что BitDefender заблокировал отправку личных данных.

19.1.5. Контроль службы мгновенных сообщений (IM)

Контроль службы мгновенных сообщений (IM) позволяет указать, с кем из IM-контактов могут беседовать ваши дети.

Замечание

Контроль службы мгновенных сообщений доступен только для приложений Yahoo Messenger и Windows Live (MSN) Messenger.

Настройка IM-контроля для отдельных пользовательских учетных записей:

1. Откройте окно настроек родительского контроля BitDefender для этой учетной записи пользователя.
2. Нажмите **Обмен сообщениями**.
3. Для включения функции контроля мгновенных сообщений установите соответствующий флажок.
4. Выберите предпочитаемый метод фильтрации и в зависимости от выбора создайте соответствующие правила.

   - **Разрешить обмен мгновенными сообщениями со всеми контактами, кроме перечисленных в списке**

     В этом случае необходимо указать идентификаторы мгновенных сообщений, которые необходимо заблокировать (люди, с которыми запрещено общаться вашим детям).

   - **Заблокировать обмен мгновенными сообщениями со всеми контактами, за исключением контактов в списке**

     В этом случае необходимо указать идентификаторы мгновенных сообщений, с которыми детям явным образом разрешено обмениваться сообщениями.Например, можно разрешить обмен мгновенными сообщениями с членами семьи, друзьями из школы или соседями.

Второй параметр рекомендуется выбрать, если ваш ребенок еще не достиг возраста 14 лет.

Создание правил контроля службы мгновенных сообщений (IM)

Чтобы разрешить или заблокировать обмен сообщениями с контактом, выполните следующие действия:

1. Нажмите **Блокировать идентификатор мгновенных сообщений** или **Разрешить идентификатор мгновенных сообщений**.
2. Введите адрес электронной почты или имя пользователя IM контакта в поле **Эл. почта или IM ID:**.
3. Выберите IM-программу, с которой ассоциирован контакт.
4. Выберите желаемое действие для этого правила — **Разрешить** или **Блокировать**
5. Нажмите **Завершить**, чтобы добавить правило.

Управление правилами контроля службы мгновенных сообщений (IM)

Настроенные правила IM-контроля приведены в таблице в нижней части окна.

Чтобы удалить правило, выделите его и нажмите **Удалить**.

Чтобы изменить правило, выберите его и нажмите **Редактировать** или дважды щелкните на нем мышью.Внесите необходимые изменения в окне конфигурации.

19.2. Контроль детской активности

BitDefender помогает вам отслеживать, что ваши дети делают на компьютере, даже когда вы уходите.

Если включена функция родительского контроля, журнал активности детей ведется по умолчанию. Таким образом, вы в любой момент сможете узнать, какие именно веб-сайты посещали дети, какие приложения использовали, какие действия были заблокированы родительским контролем и пр.

Также можно настроить BitDefender для отправки уведомлений по электронной почте при блокировке каких-либо действий функцией родительского контроля.

19.2.1. Проверка журналов родительского контроля

Чтобы проверить, чем занимались дети на компьютере, можно просмотреть журналы родительского контроля.Выполните следующие действия:

1. Откройте BitDefender.
2. Перейдите по ссылке **Просмотреть журналы** в правом нижнем углу окна.

3. Выберите **Родительский контроль** в меню с левой стороны.

Замечание
Эти журналы также можно открыть в окне "Родительский контроль". Для этого нужно выбрать команду **Просмотреть журналы**.

Если ваши дети используют отдельный компьютер, можно настроить домашнюю сеть BitDefender для доступа к журналам родительского контроля из удаленного расположения (с вашего компьютера).Для получения дополнительной информации перейдите к «*Домашняя сеть*» (p. 161).

В журналах функций родительского контроля отображены подробные сведения обо всех действиях детей на компьютере и в Интернете.Информация распределена по нескольким вкладкам:

Общие
Предоставляет общие сведения о последних действиях детей (часто посещаемые веб-сайты и часто используемые приложения).

Доступна фильтрация данных по пользователям и по периодам.

Журнал приложения
Позволяет просмотреть список последних использованных детьми приложений.

Дважды щелкните события в списке, чтобы просмотреть более подробную информацию.Чтобы удалить запись из журнала, дважды щелкните на ней и выберите **Удалить**.

Журнал
Позволяет просмотреть последние посещенные детьми веб-сайты.

Доступна фильтрация данных по пользователям и по периодам.

Другие события
Предоставляет подробные сведения об активности функции родительского контроля (например, время включения или выключения родительского контроля, блокировка событий и т. д.).

Дважды щелкните события в списке, чтобы просмотреть более подробную информацию.Чтобы удалить запись из журнала, дважды щелкните на ней и выберите **Удалить**.

19.2.2. Настройка уведомлений по электронной почте

Получение уведомлений по электронной почте при блокировке действия родительским контролем:

1. Откройте BitDefender.

2. Перейдите в раздел настроек родительского контроля. Для этого выполните следующие действия (в зависимости от режима пользовательского интерфейса):

   Интерфейс "Опытный пользователь"
   Перейдите на вкладку **Безопасность** и выберите **Родительский контроль** в области быстрых задач в левой части окна.

   Интерфейс "Эксперт"
   Выберите **Родительский контроль** в меню с левой стороны.

   Замечание
   В интерфейсе "Основной" или "Опытный пользователь" можно создать ярлык для доступа к этим настройкам непосредственно из панели управления.Для получения дополнительной информации перейдите к *«Мои инструменты»* (p. 33).

3. В разделе "Настройки" выберите **Отправить мне отчет об активности по электронной почте**.
4. Появится подсказка о необходимости задать настройки учетной записи вашей электронной почты. Нажмите **Да**, чтобы открыть окно настроек.

   Замечание
   Вы можете открыть окно настройки позднее, нажав **Настройки уведомлений**.

5. Введите адрес электронной почты, на который будут отправляться уведомления.
6. Настройте параметры электронной почты для сервера, используемого для отправки уведомлений по электронной почте.

Для установки настроек электронной почты доступны три параметра:

Использовать текущие настройки почтового клиента
В случае если BitDefender удается импортировать настройки почтового сервера из почтового клиента, этот параметр выбирается по умолчанию.

Нажмите **Тест настроек**, чтобы проверить настройки. Если во время проверки возникают неполадки, вам будут предложены меры по их устранению.

Выберите один из известных серверов
Выберите этот параметр, если ваша учетная запись электронной почты использует одну из веб-служб электронной почты, перечисленных в списке.

Нажмите **Тест настроек**, чтобы проверить настройки. Если во время проверки возникают неполадки, вам будут предложены меры по их устранению.

Я хочу самостоятельно настроить параметры сервера

Если настройки почтового сервера известны, выберите этот параметр и установите настройки:

- **Исходящий SMTP-сервер** — введите адрес почтового сервера, используемого для отправки сообщений.
- Если сервер FTP использует другой порт, нежели 25, введите его в соответствующее поле.
- Если сервер требует аутентификацию, выберите **Мой SMTP-сервер требует аутентификацию**, отметьте флажок и введите ваши имя пользователя и пароль в соответствующие поля.

Нажмите **Тест настроек**, чтобы проверить настройки. Если во время проверки возникают неполадки, вам будут предложены меры по их устранению.

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

19.3. Удаленный родительский контроль

С помощью функции удаленного родительского контроля можно отслеживать действия детей и изменять настройки родительского контроля, даже находясь вдали от дома.Для этого потребуется только компьютер с доступом в Интернет и веб-браузер.

Функция удаленного родительского контроля позволяет тактично и незаметно проверить, чем занимаются дети в Интернете.

19.3.1. Обязательные требования для использования удаленного родительского контроля

Для использования функции удаленного родительского контроля необходимо соблюдение следующих обязательных требований:

1. На компьютере детей рекомендуется установить BitDefender Internet Security 2011 или BitDefender Total Security 2011.
2. Активация продукта с помощью учетной записи BitDefender.
3. Включение удаленного родительского контроля.
4. Компьютер, с которого осуществляется доступ к функции удаленного родительского контроля, должен быть подключен к Интернету.

19.3.2. Включение удаленного родительского контроля

Включение удаленного родительского контроля:

1. Выполните вход в систему, где установлен BitDefender, используя учетную запись администратора.Можно использовать ту же учетную запись, которую вы использовали при установке продукта.
2. Откройте BitDefender.
3. Перейдите в раздел настроек родительского контроля. Для этого выполните следующие действия (в зависимости от режима пользовательского интерфейса):

   Интерфейс "Опытный пользователь"
   Перейдите на вкладку **Безопасность** и выберите **Родительский контроль** в области быстрых задач в левой части окна.

   Интерфейс "Эксперт"
   Выберите **Родительский контроль** в меню с левой стороны.

   Замечание

   В интерфейсе "Основной" или "Опытный пользователь" можно создать ярлык для доступа к этим настройкам непосредственно из панели управления.Для получения дополнительной информации перейдите к *«Мои инструменты»* (p. 33).

4. Для включения удаленного родительского контроля установите соответствующий флажок.Функция удаленного родительского контроля будет включена для всех пользовательских учетных данных, созданных в системе.

19.3.3. Доступ к функции удаленного родительского контроля

Доступ к функции удаленного родительского контроля можно осуществить из учетной записи BitDefender.

1. На компьютере, подключенном к Интернету, откройте веб-браузер и перейдите по следующему адресу:

   http://myaccount.bitdefender.com

2. Выполните вход в свою учетную запись BitDefender, используя свое имя пользователя и пароль.
3. Перейдите на вкладку **Родительский контроль** для доступа к панели управления модуля удаленного родительского контроля.
4. Можно просмотреть все учетные записи пользователей, для которых включена функция удаленного родительского контроля.

Чтобы проверить, какие действия были заблокированы для конкретной учетной записи пользователя с момента вашего последнего входа в систему, перейдите по ссылке к списку существующих оповещений.

Для просмотра сведений о недавней активности детей перейдите по ссылке **Недавняя активность** для соответствующей учетной записи.

Чтобы изменить настройки родительского контроля для конкретной учетной записи пользователя, перейдите по ссылке **Настройки** соответствующей учетной записи.

19.3.4. Удаленное отслеживание активности детей

Для удаленного отслеживания активности детей на компьютере и в Интернете необходимо предварительно включить на компьютере детей функцию удаленного родительского контроля.Для получения дополнительной информации перейдите к *«Включение удаленного родительского контроля»* (p. 121).

Чтобы удаленно проверить, чем занимаются дети за компьютером:

1. На компьютере, подключенном к Интернету, откройте веб-браузер и перейдите по следующему адресу:

   http://myaccount.bitdefender.com

2. Выполните вход в свою учетную запись BitDefender, используя свое имя пользователя и пароль.
3. Перейдите на вкладку **Родительский контроль** для доступа к панели управления модуля удаленного родительского контроля.
4. Чтобы проверить, какие действия были заблокированы для конкретной учетной записи пользователя с момента вашего последнего входа в систему, перейдите по ссылке к списку существующих оповещений.Для просмотра сведений о недавней активности детей перейдите по ссылке **Недавняя активность** для соответствующей учетной записи.

На странице "Оповещения" можно просмотреть список веб-сайтов, приложений или контактов в службах мгновенных сообщений, которые были заблокированы с момента последнего посещения.

На странице недавней активности приведены подробные сведения о недавней активности детей:

- которые являются наиболее популярными и часто блокируемыми веб-сайтами.
- которые являются наиболее популярными и часто блокируемыми приложениями.

- которые являются наиболее часто блокируемыми контактами из службы мгновенных сообщений с наибольшим числом обращений.

Пользователи могут самостоятельно заблокировать веб-сайт, приложение или идентификатор службы мгновенных сообщений, нажав на соответствующую ссылку **Заблокировать**.

Чтобы снять ограничения, нажмите на соответствующую ссылку **Разрешить**.

19.3.5. Удаленное изменение настроек родительского контроля

Для удаленного изменения настроек родительского контроля, заданных для учетных записей детей, необходимо активировать на их компьютере функцию удаленного родительского контроля.Для получения дополнительной информации перейдите к *«Включение удаленного родительского контроля»* (p. 121).

Удаленное изменение настроек родительского контроля:

1. На компьютере, подключенном к Интернету, откройте веб-браузер и перейдите по следующему адресу:

   http://myaccount.bitdefender.com

2. Выполните вход в свою учетную запись BitDefender, используя свое имя пользователя и пароль.

3. Перейдите на вкладку **Родительский контроль** для доступа к панели управления модуля удаленного родительского контроля.

4. Можно просмотреть все учетные записи пользователей, для которых включена функция удаленного родительского контроля.Чтобы изменить настройки родительского контроля для конкретной учетной записи пользователя, перейдите по ссылке **Настройки** соответствующей учетной записи.

На странице "Настройки" отображены списки веб-сайтов, приложений и идентификаторов мгновенных сообщений, которые явным образом заблокированы родительским контролем.Чтобы снять ограничения, нажмите на соответствующую ссылку **Разрешить**.

Сведения о настройке ограничений см. в следующих разделах:

«Ограничение доступа в Интернет по времени» (p. 124)
«Блокирование веб-сайтов» (p. 124)
«Блокировка приложений» (p. 124)
«Блокирование IM-контактов» (p. 125)

Ограничение доступа в Интернет по времени

Выберите в меню параметр, чтобы задать время, когда детям разрешен доступ в Интернет.Ограничение доступа в Интернет в заданные периоды:

1. Выберите **Создать расписание доступа в Интернет**.
2. Задайте в сетке периоды, в течение которых доступ в Интернет будет заблокирован.Можно щелчком мыши отметить отдельные клетки или нажать на клетку и перетащить, чтобы задать более длительный период.Чтобы перейти к новому выбору, нажмите **Заблокировать все** или **Разрешить все**.
3. Выберите **Подтвердить изменения**.Данные изменения будут настроены и применены для компьютера вашего ребенка после следующей синхронизации с веб-сайтом удаленного родительского контроля (макс. в течение 10 мин.).

Блокирование веб-сайтов

Блокировка веб-сайта:

1. Нажмите **Заблокировать другой веб-сайт**.
2. Введите адрес веб-сайта в соответствующее поле. Если требуется заблокировать один из наиболее часто посещаемых веб-сайтов, просто выберите его из меню.
3. Нажмите **Заблокировать**.Веб-сайт будет добавлен в список заблокированных веб-сайтов.Данное правило будет настроено и применено для компьютера вашего ребенка после следующей синхронизации с веб-сайтом удаленного родительского контроля (макс. в течение 10 мин.).

Если вы передумали, нажмите на соответствующую ссылку **Разрешить**.

Блокировка приложений

Блокирование приложения:

1. Нажмите **Заблокировать другое приложение**.
2. Из списка часто используемых приложений выберите приложение, которое будет заблокировано.
3. Нажмите **Заблокировать**.Приложение будет добавлено в список заблокированных приложений.Данное правило будет настроено и применено для компьютера вашего ребенка после следующей синхронизации с веб-сайтом удаленного родительского контроля (макс. в течение 10 мин.).

Если вы передумали, нажмите на соответствующую ссылку **Разрешить**.

Блокирование IM-контактов

Блокировка обмена мгновенными сообщениями с заданными контактами:

1. Нажмите **Заблокировать другой контакт**.
2. Введите идентификатор мгновенных сообщений в соответствующее поле. Если требуется заблокировать один из наиболее активных идентификаторов мгновенных сообщений, выберите его в меню.
3. Нажмите **Заблокировать**.Идентификатор службы мгновенных сообщений будет добавлен в список заблокированных идентификаторов службы мгновенных сообщений.Данное правило будет настроено и применено для компьютера вашего ребенка после следующей синхронизации с веб-сайтом удаленного родительского контроля (макс. в течение 10 мин.).

Если вы передумали, нажмите на соответствующую ссылку **Разрешить**.

20. Контроль личных данных

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

Контроль личных данных включает следующие компоненты:

- Контроль личных данных — эта функция позволяет блокировать отправку личных данных с компьютера без согласия пользователя. Данная функция сканирует электронную почту и мгновенные сообщения, отправленные с компьютера, и все остальные данные, отправляемые через веб-страницы; и блокирует любые сведения, защищенные созданными правилами контроля личных данных.
- Контроль реестра — спрашивает разрешения всякий раз, когда какая-либо программа пытается менять запись в реестре для загрузки при запуске системы.
- Контроль cookie — запрашивает разрешение всякий раз, когда новый веб-сайт пытается записать файл cookie.
- Контроль сценариев — запрашивает разрешение всякий раз, когда веб-сайт пытается инициировать выполнение сценария или другого активного контента.

По умолчанию включена только функция контроля личных данных.Во избежание несанкционированной отправки конфиденциальной информации необходимо настроить соответствующие правила контроля личных данных.Для получения дополнительной информации перейдите к «*Настройка контроля личных данных*» (p. 129).

Остальные компоненты функции контроля личных данных являются интерактивными. Если они включены, на экране будут отображаться окна оповещений с запросом на разрешение или запрет конкретных действий при открытии новых веб-сайтов или установке новых программ. По этой причине данные компоненты используются, как правило, опытными пользователями.

20.1. Настройка уровня защиты

Уровень защиты позволяет легко и удобно включать или отключать компоненты контроля личных данных.

Настройка уровня защиты:

1. Откройте BitDefender, нажмите **Параметры** в верхнем правом углу окна и выберите интерфейс **Эксперт**.
2. Перейдите в раздел **Контроль личных данных > Состояние**.
3. Убедитесь в том, что включен контроль личных данных.
4. Доступны два параметра:
   - Чтобы установить желаемый уровень защиты, перетащите бегунок в требуемое положение.Нажмите **По умолчанию**, чтобы установить бегунок в уровень по умолчанию.

     Воспользуйтесь описанием справа от шкалы, чтобы выбрать тот уровень защиты, который оптимально соответствует требованиям к безопасности.
   - Вы можете настроить уровень защиты, нажав **Изменить**.В появившемся окне выберите элементы защиты, которые вы хотите включить, и нажмите **ОК**.

20.2. Контроль личных данных

Контроль личных данных защищает вас от кражи данных при подключении к сети.

Рассмотрим простой пример: пользователь создал правило контроля личных данных, которое обеспечивает защиту номера кредитной карты.Если в ваш компьютер каким-то образом проникли шпионские программы, они не смогут выполнить отправку номера кредитной карты по электронной почте, посредством служб мгновенных сообщений или через веб-страницы. Кроме того, дети не смогут воспользоваться номером кредитной карты для покупок в Интернете или раскрыть этот номер людям, с которыми они познакомились в сети.

Дополнительные сведения см. в следующих разделах:

- «*О контроле личных данных*» (p. 127).
- «*Настройка контроля личных данных*» (p. 129).
- «*Управление правилами*» (p. 131).

20.2.1. О контроле личных данных

Обеспечение безопасности конфиденциальной информации — это важный вопрос, волнующий каждого. С развитием интернет-коммуникаций развиваются и методы кражи информации, а также новые методы введения людей в заблуждение с целью получения личной информации.

Независимо от того, адрес ли это вашей электронной почты или номер вашей кредитной карты, вы можете пострадать при утечке этой информации: вас могут засыпать спамом или ваш счет может быть опустошен.

Контроль личных данных защищает вас от кражи данных при подключении к сети.Основываясь на созданных вами правилах, контроль личных данных сканирует веб-трафик, электронную почту и трафик мгновенных сообщений на совпадение с определенным набором символов (например, номер вашей кредитной карты). В случае совпадения соответствующая веб-страница, сообщение электронной почты или IM-сообщение блокируется.

Вы можете создать правила для защиты любой информации, которую вы считаете личной или конфиденциальной, — от своего телефонного номера или адреса электронной почты до сведений о своем банковском счете.Многопользовательская поддержка позволяет пользователям разных учетных записей Windows настраивать и использовать свои личные правила защиты данных.Если ваша учетная запись Windows является учетной записью администратора, правила, которые вы создаете, могут быть сконфигурированы для применения в момент, когда другие пользователи компьютера входят в свои учетные записи пользователей Windows.

Зачем нужен контроль личных данных?

- Функция защиты личных данных очень эффективна при блокировании клавиатурных шпионов.Этот тип вредоносного ПО записывает все ваши нажатия клавиш и отправляет их по Интернету злоумышленнику (хакеру).В украденных данных хакер может найти личную информацию, такую как номера банковских счетов и пароли, и использовать ее в личных целях.

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

- Функция защиты личных данных может защитить вас от попыток фишинга (попыток похитить персональную информацию).Самые распространенные попытки фишинга используют фальсификацию адреса электронной почты, провоцируя вас отсылать информацию на поддельную веб-страницу.

  Например, вы можете получить электронное сообщение якобы от вашего банка с просьбой срочно обновить информацию о вашем банковском счете.В этом сообщении будет 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), если вы явно не укажете исключение для этой веб-страницы.

- С помощью правил контроля личных данных можно предотвратить раскрытие детьми личной информации (например, домашнего адреса или номера телефона) людям, с которыми они познакомились в Интернете. Кроме того, если создано правило для защиты кредитной карты, дети не смогут воспользоваться ей для покупки товаров в Интернете без согласия родителей.

20.2.2. Настройка контроля личных данных

Если вы хотите использовать контроль личных данных, необходимо выполнить следующие шаги:

1. Откройте BitDefender, нажмите **Параметры** в верхнем правом углу окна и выберите интерфейс **Эксперт**.
2. Перейти в раздел **Контроль личных данных > Личные данные**.
3. Убедитесь в том, что включен контроль личных данных.

   Замечание
   Если не удается настроить параметр, перейдите на вкладку **Состояние** и включите функцию контроля личных данных.

4. Создайте правила для защиты ваших данных.Для получения дополнительной информации перейдите к *«Создание правил защиты личных данных»* (p. 129).
5. При необходимости определите особые исключения для созданных вами правил.Например, если вы создали правило для защиты номера кредитной карты, добавьте в список исключений веб-сайты, на которых обычно используется кредитная карта.Для получения дополнительной информации перейдите к *«Определение исключений»* (p. 131).

Создание правил защиты личных данных

Чтобы создать новое правило защиты данных, нажмите кнопку **Добавить** и следуйте указаниям мастера настроек.Навигация по мастеру осуществляется с помощью кнопок **Далее** и **Назад**.Для выхода из мастера нажмите **Отмена**.

1. **Окно приветствия**
2. **Установка типа правила и данных**

   Вам необходимо настроить следующие параметры:

   - **Имя правила** — введите имя правила в поле для редактирования.
   - **Тип правила** — выберите тип правила (адрес, имя, кредитная карта, PIN-код и т. д.).

- **Данные правила** — введите данные, которые вы хотите защитить, в это поле для редактирования.К примеру, если вы хотите защитить номер вашей кредитной карты, введите его полностью или частично здесь.

  Важно

  Если вы введете менее трех символов, вам будет предложено уточнить данные. Рекомендуется вводить минимум три символа, чтобы избежать ошибочного блокирования сообщений и веб-страниц.

Все введенные вами данные шифруются. Для дополнительной безопасности не вводите полностью данные, которые вы хотите защитить.

3. **Выберите типы трафика и пользователей**

   a. Выберите тип трафика, который будет проверяться BitDefender.

   - **Проверять веб-трафик (HTTP-трафик)** — сканирует HTTP-трафик (веб-трафик) и блокирует исходящие данные в соответствии с правилами.
   - **Проверка трафика эл. почты (SMTP-трафика)** — проверяет SMTP-трафик (почтовый трафик) и блокирует исходящие электронные сообщения, содержащие данные правила.
   - **Проверка IM-трафика** — сканирует трафик мгновенных сообщений и блокирует исходящие сообщения в соответствии с правилами.

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

   b. Укажите пользователей, к которым применимы данные правила.

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

4. **Опишите правило**

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

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

С этого момента любые попытки отправить указанные данные (по электронной почте, через службу мгновенных сообщений или через веб-страницу) будут блокироваться. При этом будет выводиться оповещение о том, что BitDefender заблокировал отправку личных данных.

Определение исключений

Бывают случаи, когда вам необходимо определить исключения к определенным правилам конфиденциальности.Например, вы создаете правило, предотвращающее отправку номера вашей кредитной карты через HTTP (веб). Каждый раз, когда номер вашей кредитной карты будет отправляться на веб-сайт с вашей учетной записи, страница будет блокироваться. Если, например, вы хотите совершить покупку в интернет-магазине (в безопасности которого вы уверены), вам необходимо будет создать исключение из этого правила.

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

Чтобы добавить исключение, выполните следующие действия:

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

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

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

20.2.3. Управление правилами

Управление правилами контроля личных данных:

1. Откройте BitDefender, нажмите **Параметры** в верхнем правом углу окна и выберите интерфейс **Эксперт**.
2. Перейти в раздел **Контроль личных данных > Личные данные**.

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

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

Чтобы редактировать правило, необходимо 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 **OK**, чтобы сохранить изменения.

20.3. Контроль реестра

Реестр – важнейший компонент операционной системы Windows. В нем хранятся настройки, установленные программы, информация пользователя и прочее.

В разделе **Реестр** также определяется, какие программы необходимо автоматически загружать при запуске Windows. Многие программы-шпионы пользуются этим, чтобы автоматически запускаться при включении компьютера.

Функция **Управление реестром** позволяет следить за реестром операционной системы Windows. Это очень полезно для обнаружения программ класса троян. Вы будете получать сообщение всякий раз, когда какая-либо программа будет менять запись в реестре, для того чтобы загружаться при запуске системы.Для получения дополнительной информации перейдите к *«Оповещения реестра»* (p. 41).

Настройка управления реестром:

1. Откройте BitDefender, нажмите **Параметры** в верхнем правом углу окна и выберите интерфейс **Эксперт**.
2. Перейти в раздел **Контроль личных данных > Реестр**.
3. Для включения функции управления реестром установите соответствующий флажок.

Замечание
Если не удается настроить параметр, перейдите на вкладку **Состояние** и включите функцию контроля личных данных.

Управление правилами

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

20.4. Контроль Cookie

Файлы Cookie встречаются в Интернете очень часто. Это небольшие файлы, хранящиеся на вашем компьютере. Сайты в сети создают такие файлы, чтобы отслеживать некоторую информацию о вас.

Файлы cookie созданы, чтобы сделать жизнь пользователя легче. Например, с их помощью веб-сайт запоминает ваше имя и ваши настройки, и вам не нужно вводить их при каждом посещении.

Но файлы истории обращений также могут раскрывать определенную информацию о вас, отслеживая ваши перемещения в сети.

В этом случае рекомендуется использовать функцию управления cookie.Если функция управления cookie включена, система будет запрашивать разрешение каждый раз, когда веб-сайт запрашивает или устанавливает cookie.Для получения дополнительной информации перейдите к *«Оповещения cookie»* (p. 42).

Настройка управления cookie:

1. Откройте BitDefender, нажмите **Параметры** в верхнем правом углу окна и выберите интерфейс **Эксперт**.
2. Перейдите в раздел **Контроль личных данных > Cookie**.
3. Для включения функции управления cookie установите соответствующий флажок.

   Замечание
   Если не удается настроить параметр, перейдите на вкладку **Состояние** и включите функцию контроля личных данных.

4. Можно настроить правила для регулярно посещаемых веб-сайтов, но это не обязательно.В зависимости от ответа правила создаются автоматически в окне оповещения.

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.

Создание правил вручную

Чтобы создать новое правило вручную, нажмите кнопку **Добавить** и настройте параметры правила в окне конфигурации.Вы можете установить следующие настройки:

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

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

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

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

Замечание

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

Нажмите **Завершить**.

Управление правилами

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

20.5. Контроль сценариев

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

Если функция управления сценариями включена, будет выведен запрос на разрешение при каждой попытке запуска веб-сайтом сценариев или другого активного содержимого.Для получения дополнительной информации перейдите к «*Оповещения сценария*» (p. 41).

Настройка управления сценарием:

1. Откройте BitDefender, нажмите **Параметры** в верхнем правом углу окна и выберите интерфейс **Эксперт**.
2. Перейдите в раздел **Контроль личных данных > Сценарий**.
3. Для включения функции управления сценарием установите соответствующий флажок.

   Замечание
   Если не удается настроить параметр, перейдите на вкладку **Состояние** и включите функцию контроля личных данных.

4. Можно настроить правила для регулярно посещаемых веб-сайтов, но это не обязательно.В зависимости от ответа правила создаются автоматически в окне оповещения.

Создание правил вручную

Чтобы создать новое правило вручную, нажмите кнопку **Добавить** и настройте параметры правила в окне конфигурации.Вы можете установить следующие настройки:

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

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

Нажмите **Завершить**.

Управление правилами

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

21. Брандмауэр

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

Замечание

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

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

21.1. Настройки защиты

Чтобы включить, отключить или настроить защиту брандмауэра, откройте BitDefender и в зависимости от используемого режима пользовательского интерфейса выполните следующие действия:

Интерфейс "Опытный пользователь"
: Перейдите на вкладку **Безопасность** и выберите **Настроить брандмауэр** в области быстрых задач в левой части окна.В открывшемся окне перейдите на вкладку **Настройки**.

Интерфейс "Эксперт"
: Перейдите в раздел **Брандмауэр > Настройки**.

Важно

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

В верхней части раздела представлены статистические данные по обнаруженной активности.

В нижней части раздела отображается статистика BitDefender по входящему и исходящему трафику. График показывает объем интернет-трафика за последние две минуты.

Замечание

График отображается только в интерфейсе "Эксперт".

21.1.1. 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.

- Разрешить все
- Разрешенные программы
- Отчет
- Запретить все

При выборе действия отображается его краткое описание.

21.1.2. Конфигурация дополнительных настроек брандмауэра

В интерфейсе "Эксперт" можно задать дополнительные настройки брандмауэра. Для этого следует перейти в раздел **Дополнительные настройки**.

Доступны следующие варианты:

- **Включить общий доступ к подключению к Интернету (ICS)** — включает поддержку общего доступа к подключению к Интернету (ICS).

  Замечание
  Этот параметр не включает автоматически функцию ICS на вашей системе, а только позволяет устанавливать соединения подобного типа, если данная функция включена в операционной системе.

- **Проверка приложений, измененных с момента создания правила брандмауэра** — проверяет каждое приложение, которое пытается подключиться к Интернету, на предмет изменений, которые могли произойти с момента добавления правила контроля доступа. Если приложение было изменено, оповещение предложит вам разрешить или блокировать доступ приложений к Интернету.

  Замечание
  Вредоносные программы могут изменять приложения.Рекомендуем включать этот параметр и разрешать 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.

Приложения с цифровой подписью считаются надежными и имеют более высокую степень безопасности.Вы можете выбрать параметр **Игнорировать изменения приложений с цифровой подписью** для того, чтобы разрешить измененным приложениям с подписью доступ в Интернет без вашего уведомления о данном событии.

- **Показывать 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.
- **Включить сторонние 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.

21.2. Правила доступа к приложению

Для управления правилами брандмауэра, координирующими доступ приложений к сетевым ресурсам и Интернету, откройте BitDefender и, в зависимости от режима просмотра пользовательского интерфейса, выполните следующие действия:

Интерфейс "Опытный пользователь"
: Перейдите на вкладку **Безопасность** и выберите **Настроить брандмауэр** в области быстрых задач в левой части окна.Выберите вкладку **Программы** в открывшемся окне.

Интерфейс "Эксперт"
: Перейдите в раздел **Брандмауэр > Программы**.

Интерфейс "Опытный пользователь" предоставляет доступ к базовым настройкам конфигурации. Для доступа к более детальным пользовательским настройкам рекомендуется использовать интерфейс "Эксперт".

21.2.1. Просмотр текущих правил

Здесь представлены программы (процессы), для которых в таблице созданы правила брандмауэра.

В интерфейсе "Эксперт" можно просмотреть подробные сведения о каждом из правил, указанных в столбцах таблицы.Чтобы видеть правила, созданные для определенного приложения, щелкните на кнопке "+" около соответствующего приложения.Снимите флажок **Скрыть системные процессы**, если вы также хотите видеть правила, касающиеся системы или процессов BitDefender.

- **Типы процессов/сети** — 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 или Интернету через определенный адаптер (например, беспроводный 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. Он 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-адреса. 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.Обратите внимание на следующие события:

Событие	Описание
Подключение	Предварительный обмен стандартными сообщениями, используемыми протоколами на основе соединений (такими

Событие	Описание
	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.
Прослушивание	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.

21.2.2. Автоматическое добавление правил

Если включена функция **Брандмауэр**, BitDefender отслеживает все приложения и автоматически создает правило при попытке приложения подключиться к Интернету.В зависимости от приложения и настроек брандмауэра BitDefender процедура выполняется автоматически или при участии пользователя.

Если выбран интерфейс "Основной" или "Опытный пользователь", все попытки подключения со стороны неизвестных приложений будут блокироваться.

При выборе интерфейса "Эксперт" в окне оповещения выводится запрос на выполнение действия каждый раз, когда неизвестное приложение пытается подключиться к Интернету.

В появившемся окне вы увидите следующее: приложение, пытающееся получить доступ в Интернет, 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.

Важно

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

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.

21.2.3. Добавление правил вручную

Создание правил вручную может осуществляться различными способами в зависимости от используемого режима просмотра пользовательского интерфейса.

Интерфейс "Опытный пользователь"

1. Нажмите **Обзор** на вкладке **Добавить новую программу**.
2. Найдите программу, для которой требуется создать правило, и нажмите **Открыть**.
3. Нажмите **Добавить правило**.

   Обратите внимание, что теперь правило отображается в таблице.
4. Выберите действие в столбце **Действие**: разрешить или запретить доступ.

   Действие будет применено ко всем параметрам правила.

Интерфейс "Эксперт"

1. Нажмите кнопку **Добавить правило**.Появится окно настроек.
2. Настройте главные и расширенные параметры надлежащим образом.
3. Нажмите **OK**, чтобы добавить новое правило.

Правила можно изменить только в процессе настройки брандмауэра в интерфейсе "Эксперт".Чтобы изменить существующее правило, выполните следующую процедуру:

1. Нажмите кнопку **Редактировать правило** или дважды щелкните мышью на правиле.Появится окно настроек.
2. Настройте главные и расширенные параметры надлежащим образом.
3. Нажмите **OK**, чтобы сохранить сделанные изменения.

Настройка основных параметров

Вкладка **Общие** окна конфигурации позволяет настраивать основные параметры правил.

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 хотите применить правило к TCP, выберите **TCP**.
  - Если вы хотите применить правило к UDP, выберите **UDP**.
  - 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.Обратите 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.
Прослушивание	Состояние, в котором приложение наблюдает за сетью, ожидая установки соединения или получения информации от другого приложения.

- **Типы адаптера.** Выберите типы адаптера, 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 **Дополнительные** окна конфигурации позволяет настраивать расширенные параметры правил.

Вы можете установить следующие дополнительные параметры:

- **Направление.** Выберите из меню направление трафика, к которому будет применяться правило.

Направление	Описание
Исходящий	Правило применяется только к исходящему трафику.
Входящий	Правило применяется только к входящему трафику.
Оба	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 IP-адрес этого компьютера.

- 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**).Термин "строгие правила" означает, что BitDefender будет запрашивать действие пользователя каждый раз, когда приложение, запрашивая доступ к сетевым или интернет-ресурсам, противоречит родительскому процессу.

21.2.4. Расширенное управление правилами

Чтобы просматривать и редактировать правила, управляющие приложениями, нажмите кнопку **Дополнительно**, которая отображается при настройке брандмауэра в интерфейсе "Эксперт".

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 котором отмечаются правила, очень важен.

Для удаления правила его необходимо выделить и нажать 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 кнопку **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 наименьший приоритет.

Нажмите **Закрыть**, чтобы закрыть окно.

21.2.5. Удаление и переустановка правил

Удаление и повторная настройка правил возможна только при настройке брандмауэра в интерфейсе "Эксперт".

Для удаления правила необходимо выбрать его и нажать кнопку **Удалить правило**.Вы можете выбрать и удалить одновременно несколько правил.

Если требуется удалить все правила, созданные для конкретного приложения, выберите нужное приложение из списка и нажмите кнопку **Удалить правило**.

Если хотите загрузить набор правил по умолчанию для выбранного уровня доверия, нажмите **Сбросить правила**.

21.3. Настройки сети

Чтобы задать настройки подключения для продукта, откройте BitDefender и в зависимости от используемого режима интерфейса пользователя выполните следующие действия:

Интерфейс "Опытный пользователь"
: Перейдите на вкладку **Безопасность** и выберите **Настроить брандмауэр** в панели быстрых задач в левой части окна. В открывшемся окне перейдите на вкладку **Сеть**.

Интерфейс "Эксперт"
: Перейдите в раздел **Брандмауэр > Сеть**.

В столбцах таблицы **Конфигурация сети** представлены подробные сведения о сети, к которой подключен компьютер. С помощью этих сведений можно настроить параметры подключения:

- **Адаптер** — сетевой адаптер, который ваш компьютер использует для подключения к сети и Интернету.
- **Тип сети** — тип сети, к которой подключен адаптер.В зависимости от конфигурации сетевого адаптера, BitDefender может автоматически выбрать тип сети или запросить более подробные сведения.

  Изменить тип можно, нажав на стрелку ▾ в столбце **Тип сети** и выбрав из списка один из доступных типов.

Тип сети	Описание
Доверенные (разрешить все)	Отключение брандмауэра для определенного адаптера.
Домашний/рабочий	Разрешение всего трафика между вашим компьютером и компьютерами в локальной сети.
Общедоступный	Весь трафик фильтруется.

Тип сети	Описание
Ненадежные (блокировать все)	Полное блокирование трафика сети и Интернета через соответствующий адаптер.

- **VPN** — используется ли соединение типа VPN.

  Для трафика, поступающего через VPN-соединения, применяется тип фильтрации, отличный от фильтрации трафика, проходящего через другие сетевые соединения.При использовании VPN-соединения нажмите на стрелку в столбце **VPN** и выберите **Да**.

В интерфейсе "Эксперт" отображаются два дополнительных столбца:

- **Режим невидимки** — параметр, определяющий возможность быть обнаруженным другими компьютерами.

  Для настройки режима невидимки нажмите стрелку в колонке **Режим невидимки** и выберите нужный вариант.

Режим "Невидимка"	Описание
Вкл.	Невидимый режим включен.Ваш компьютер невидим из локальной сети и 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.

- **Общие** — определяет, применяются ли общие правила к этому соединению.

  При изменении IP-адреса сетевого адаптера BitDefender соответствующим образом изменит тип сети.Если требуется сохранить тот же тип, нажмите стрелку в столбце **Общие** и выберите **Да**.

21.3.1. 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 разрешен.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 **Сетевых зон** приведены текущие сетевые зоны для каждого адаптера.

Чтобы добавить зону, выберите адаптер и нажмите **Добавить зону**.Появится новое окно.

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. Нажмите **OK**.

21.4. Устройства

Для управления устройствами, подключенными к сети, откройте BitDefender и выполните следующие действия (в зависимости от режима пользовательского интерфейса):

Интерфейс "Опытный пользователь"
: Перейдите на вкладку **Безопасность** и выберите **Настроить брандмауэр** в области быстрых задач в левой части окна.В открывшемся окне перейдите на вкладку **Устройства**.

Интерфейс "Эксперт"
: Перейдите в раздел **Брандмауэр > Устройства**.

В таблице перечислены принтеры, факсы и сканеры, обнаруженные в сети, а также действия по умолчанию, заданные для них.Чтобы изменить статус устройства, дважды щелкните в таблице и в открывшемся окне выберите одно из следующих действий: разрешить или заблокировать обмен данными с устройством.

Для управления списком устройств используйте доступные кнопки:

- **Добавить** — добавление устройства, не отображаемого в списке.
- **Удалить** — удалить выбранное устройство из списка.
- **Обновить устройства** — запуск нового сканирования сети для обновления списка устройств.

21.5. Контроль соединений

Чтобы отслеживать текущую активность в сети или в Интернете (с использованием протоколов TCP и UDP) с сортировкой по приложениям или открыть журнал брандмауэра BitDefender, выполните следующие действия:

1. Откройте BitDefender, нажмите **Параметры** в верхнем правом углу окна и выберите интерфейс **Эксперт**.
2. Перейдите в раздел **Брандмауэр > Активность**.

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:

- Показывает исходящее подключение.
- Показывает входящее подключение.
- Показывает открытый порт на вашем компьютере.

Это окно отображает активность соединения с сетью/Интернетом в реальном времени. По мере того как соединения или порты закрываются, соответствующие пункты вначале тускнеют, а затем исчезают из списка.То же самое происходит и со статистическими данными для определенного приложения, генерирующего трафик или имеющего открытые порты, которые вы закрыли.

Подробный список событий, относящихся к использованию модуля брандмауэра (включение/выключение брандмауэра, блокирование трафика, изменение параметров) или созданных действиями, обнаруженными данным модулем (сканирование портов, блокировка попыток подключения или трафика в соответствии с правилами), см. в журнале брандмауэра BitDefender. Для просмотра журнала нажмите кнопку **Показать журнал**.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 **Расширить словесное наполнение лога**.

21.6. Поиск и устранение неисправностей брандмауэра

В случае возникновения проблемы, которая предположительно была вызвана брандмауэром BitDefender, мастер поиска и устранения неисправностей поможет ее устранить.

Для запуска мастера откройте BitDefender и выполните следующие действия (в зависимости от используемого режима пользовательского интерфейса):

Интерфейс "Опытный пользователь"

Перейдите на вкладку **Безопасность** и выберите **Настроить брандмауэр** в области быстрых задач в левой части окна.Перейдите на вкладку **Настройки** в открывшемся окне и выберите **Поиск и устранение неисправностей**.

Интерфейс "Эксперт"

Перейдите в раздел **Брандмауэр > Настройки** и нажмите **Поиск и устранение неполадок**.

С помощью этого мастера можно быстро устранить неисправности подключения, связанные с конфигурацией брандмауэра.

- Сбой при выводе на печать.
- Сбой при попытке доступа к компьютеру в сети.
- Сбой при попытке доступа в Интернет.

Если ни одна из описанных ситуаций не соответствует вашей проблеме, выберите **Другие проблемы брандмауэра**, чтобы перейти к окну **Инструмент поддержки**.

Дополнительные сведения о мастере см. в разделе Поиск и устранение неполадок данного руководства.

22. Уязвимости

Важный шаг в защите вашего компьютера от злоумышленников и вредоносного ПО состоит в том, чтобы держать операционную систему и используемые приложения в обновленном состоянии.Более того, чтобы предотвратить несанкционированный 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.

22.1. Поиск уязвимостей

Проверить систему на наличие уязвимостей и осуществить их поэтапное устранение можно с помощью мастера **Поиск уязвимостей**.Для запуска мастера откройте BitDefender и выполните следующие действия (в зависимости от используемого режима пользовательского интерфейса):

Интерфейс "Опытный пользователь"
: Перейдите на вкладку **Безопасность** и выберите **Сканирование на наличие уязвимостей** в области быстрых задач в левой части окна.

Интерфейс "Эксперт"
: Перейдите в раздел **Уязвимости > Статус** и нажмите **Проверить сейчас**.

Для устранения уязвимостей системы выполните следующую процедуру, состоящую из шести шагов.Навигация по мастеру осуществляется с помощью кнопки **Далее**. Для выхода из мастера нажмите **Отмена**.

1. **Защитить ваш компьютер**

   Выберите уязвимости для проверки.

2. **Сканировать выбранные угрозы...**

   Подождите, пока BitDefender завершит проверку системы на наличие уязвимостей.

3. **Обновления Windows**

   Вы можете просмотреть список важных и второстепенных обновлений Windows, которые в данный момент не установлены на вашем компьютере.Выберите обновления для установки.

4. **Обновления приложений**

   Если приложение нуждается в обновлении, щелкните появившуюся ссылку, чтобы загрузить последнюю версию.

5. **Слабые пароли**

Вы можете просмотреть список учетных записей Windows, установленных на вашем компьютере, и уровень защиты, обеспечиваемый их паролями.Нажмите **Устранить**, чтобы изменить все слабые пароли.

6. **Сводка**

   Здесь можно просмотреть результаты операции.

22.2. Состояние

Чтобы проверить текущий статус уязвимости и включить или отключить автоматическое сканирование на наличие уязвимостей, выполните следующие действия:

1. Откройте BitDefender, нажмите **Параметры** в верхнем правом углу окна и выберите интерфейс **Эксперт**.
2. Перейдите в раздел **Уязвимость > Состояние**.

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

Для автоматического получения уведомлений об уязвимостях системы или приложений параметр **Автоматическое сканирование на наличие уязвимостей** должен быть включен.

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

- Если доступны обновления Windows, нажмите **Установить** в колонке **Действие** для установки.
- Если приложение устарело, нажмите **Дополнительная информация** для просмотра сведений о версии и ссылки на веб-страницу поставщика, где вы сможете загрузить и установить последнюю версию приложения.
- Если пароль учетной записи пользователя Windows недостаточно надежен, нажмите **Просмотреть и исправить**, чтобы изменить пароль при следующем входе в систему, или измените пароль самостоятельно.Чтобы пароль был сильным, используйте комбинации символов в верхнем и нижнем регистре, числа и специальные символы (такие как, например, #, $ или @).
- Если в Windows включена функция автозапуска носителя, выберите **Исправить** для ее отключения.

22.3. Настройки

Для настройки параметров автоматической проверки на наличие уязвимостей выполните следующие действия:

1. Откройте BitDefender, нажмите **Параметры** в верхнем правом углу окна и выберите интерфейс **Эксперт**.
2. Перейдите в раздел **Уязвимости > Настройки**.
3. Установите флажки, соответствующие системным уязвимостям, наличие которых должно регулярно проверяться.
   - **Критические обновления Windows**
   - **Регулярные обновления Windows**
   - **Обновления приложений**
   - **Слабые пароли**
   - **Автозапуск носителя**

Замечание

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

23. Шифрование чата

Содержание мгновенных сообщений должно оставаться конфиденциальным для вас и ваших собеседников.Благодаря шифрованию сообщений вы можете быть уверены в том, что в случае перехвата отправляемых или получаемых вами сообщений злоумышленники не смогут прочесть их содержимое.

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

- У вашего собеседника установлена версия BitDefender, которая поддерживает шифрование мгновенных сообщений, и эта функция включена в используемой программе мгновенных сообщений;
- 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 приложение для чата, поддерживающее Yahoo Messenger или MSN.

Настройка шифрования мгновенных сообщений:

1. Откройте BitDefender, нажмите **Параметры** в верхнем правом углу окна и выберите интерфейс **Эксперт**.
2. Перейдите в раздел **Шифрование > Шифрование чата**.

Замечание

Шифрование обмена мгновенными сообщениями с каждым из собеседников в чате можно легко настроить с помощью панели инструментов BitDefender в окне чата.

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 программ мгновенного обмена сообщениями, для которых шифрование выключено.Чтобы удалить контакт из списка, выберите его и нажмите кнопку **Удалить**.
- **Текущие подключения** — список текущих соединений обмена сообщениями (идентификаторы пользователей и соответствующие программы мгновенных

сообщений), а также наличие или отсутствие шифрования.Соединение может быть не зашифровано по следующим причинам:

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

23.1. Отключение шифрования для отдельных пользователей

Для отключения шифрования для отдельного пользователя выполните следующую процедуру:

1. Для открытия окна конфигурации нажмите кнопку **Добавить**.
2. Введите в поле ввода ID вашего контакта.
3. Выберите программу мгновенных сообщений, связанную с данным контактом.
4. Нажмите **OK**.

23.2. Панель инструментов BitDefender в окне чата

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

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

Замечание

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

Щелчок на панели инструментов BitDefender вызывает следующие параметры:

- **Навсегда отменить шифрование для контакта.**
- **Предложить собеседнику использовать шифрование.** Чтобы зашифровать ваше общение, ваш собеседник должен установить BitDefender и использовать совместимую IM-программу.
- **Добавить контакт в черный список родительского контроля.** Если вы добавите контакт в черный список родительского контроля, вы не сможете больше получать сообщения от этого контакта (при включенном родительском контроле).Чтобы удалить контакт из черного списка, нажмите на панель инструментов и выберите **Удалить контакт из черного списка родительского контроля**.

24. Режим игры/режим ноутбука

Режим игры/ноутбука позволяет настраивать специальные режимы работы BitDefender:

- Режим игры временно изменяет параметры продукта с целью минимизации потребления ресурсов при игре.
- Режим ноутбука предотвращает выполнение запланированных заданий при работе ноутбука от батареи с целью экономии заряда батареи.
- Режим "Без оповещений" временно изменяет настройки продукта для минимизации воздействия на работу системы в процессе просмотра видеозаписей или презентаций.

24.1. Режим игры

Режим игры изменяет параметры настроек системы защиты для того, чтобы снизить до минимума воздействие на компьютер во время игры.При включении режима игры применяются следующие настройки:

- Все предупреждения и всплывающие окна BitDefender будут отключены.
- Режим защиты BitDefender в реальном времени будет установлен как **Разрешающий**.
- Брандмауэр BitDefender установлен в режим **Разрешить все**.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**.

По умолчанию BitDefender автоматически входит в режим игры при запуске игры, находящейся в списке известных игр BitDefender, или когда приложение разворачивается на полный экран.Вы можете войти в режим игры вручную с помощью сочетания клавиш по умолчанию `Ctrl+Alt+Shift+G`.Настоятельно рекомендуется выходить из режима игры по завершении игры (вы можете воспользоваться тем же сочетанием клавиш `Ctrl+Alt+Shift+G`).

Замечание

Находясь в режиме игры, вы будете видеть букву G поверх значка BitDefender.

Настройка режима игры:

1. Откройте BitDefender, нажмите **Параметры** в верхнем правом углу окна и выберите интерфейс **Эксперт**.
2. Перейдите в раздел **Режим игры/ноутбука > Режим игры**.

Вверху раздела отображается состояние режима игры.Для изменения текущего статуса можно нажать **Режим игры включен** или **Режим игры выключен**.

24.1.1. Настройка автоматического перехода в режим игры

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

- **Использовать список игр предлагаемых BitDefender** — для автоматического входа в режим игры при запуске игры из списка известных игр BitDefender.Для просмотра этого списка нажмите **Управление играми**, затем **Список игр**.
- **Действие в полноэкранном режиме** — можно выбрать автоматический переход в режим игры или в режим "Без оповещений" при переключении приложения в полноэкранный режим.
- **Спрашивать о добавлении приложения в список игр** — вывод запроса на добавление нового приложения в список игр при выходе из полноэкранного режима.Добавив новое приложение в список игр, при следующем его запуске BitDefender автоматически перейдет в режим игры.

Замечание

Если автоматическое переключение BitDefender в режим игры нежелательно, снимите флажок **Автоматический режим игры включен**.

24.1.2. Управление списком игр

BitDefender автоматически переходит в режим игры при запуске приложения из списка игр.Для просмотра и управления списком игр нажмите **Управление играми**.Появится новое окно.

Новые приложения автоматически добавляются в список при следующих условиях:

- Вы запускаете игру из списка игр, известных программе BitDefender.Для просмотра списка нажмите **Список игр**.
- Выйдя из полноэкранного режима, вы добавляете приложение в список игр из появившегося окна.

Если вы хотите отключить автоматический режим игры для отдельного приложения из списка, снимите соответствующий флажок.Следует отключить автоматический режим игры для обычных приложений, которые переходят в

полноэкранный режим, таких как, например, веб-браузеры и проигрыватели видео.

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

- **Добавить** — добавление нового приложения в список игр.
- **Удалить** — удаление приложения из списка игр.
- **Редактировать** — редактирование существующего приложения в списке игр.

24.1.3. Добавление и редактирование игр в списке

При добавлении записей в список игр или их редактировании откроется новое окно.

Нажмите **Обзор**, чтобы выбрать приложение, или введите полный путь к приложению в поле ввода.

Если вы не хотите автоматически переходить в игровой режим при запуске выбранного приложения, нажмите **Выключить**.

Нажмите **OK**, чтобы добавить новую запись в список игр.

24.1.4. Настройка параметров режима игры

Для настройки режима работы при запланированных заданиях воспользуйтесь следующими параметрами:

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

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

Чтобы автоматически отключать брандмауэр BitDefender, находясь в игровом режиме, воспользуйтесь следующей процедурой:

1. Нажмите **Дополнительные настройки**.Появится новое окно.
2. **Установить брандмауэр на режим "Разрешить все" (режим игры), находясь в игре**.

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

24.1.5. Изменение горячих клавиш режима игры

Можно переключиться в режим игры вручную, используя установленный по умолчаниюCtrl+Alt+Shift+Gгорячая клавиша.Чтобы изменить горячие клавиши, необходимо выполнить следующие шаги:

1. Нажмите **Дополнительные настройки**.Появится новое окно.
2. Используя параметр **Использовать горячие клавиши**, задайте желаемую горячую клавишу:
   - Выберите клавиши, которые вы хотите изменить, используя клавиши Control (Ctrl), Shift (Shift) или Alternate (Alt).
   - В поле редактирования укажите букву с клавишей, которую вы хотите использовать.

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

   Замечание
   Сняв флажок **Использовать горячую клавишу**, вы отключите использование данной горячей клавиши.

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

24.2. Режим ноутбука

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

В режиме ноутбука запланированные задания не выполняются по умолчанию.

BitDefender замечает, когда ваш ноутбук переключается на питание от батареи, и автоматически переходит в режим ноутбука.Таким же образом BitDefender автоматически выходит из режима ноутбука, когда обнаруживает, что ноутбук уже не работает от батареи.

Настройка режима ноутбука:

1. Откройте BitDefender, нажмите **Параметры** в верхнем правом углу окна и выберите интерфейс **Эксперт**.
2. Перейдите в раздел **Режим игры/ноутбука > Режим ноутбука**.

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

24.2.1. Настройка параметров режима ноутбука

Для настройки режима работы при запланированных заданиях воспользуйтесь следующими параметрами:

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

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

24.3. Режим "Без оповещений"

Режим "Без оповещений" временно изменяет настройки безопасности таким образом, чтобы максимально сократить их влияние на производительность системы.В режиме "Без оповещений" применяются следующие настройки:

- Все предупреждения и всплывающие окна BitDefender будут отключены.
- Брандмауэр BitDefender установлен в режим **Разрешить все**.Это означает, что все новые соединения (входящие и исходящие) автоматически разрешаются, независимо от используемого порта и протокола.
- Запланированные задания проверки отключены по умолчанию.

По умолчанию для BitDefender настроено автоматическое переключение в режим "Без оповещений" при просмотре видеозаписей или презентаций либо при работе приложений в полноэкранном режиме.По завершении просмотра видеозаписи или презентации настоятельно рекомендуется отключить режим "Без оповещений".

Замечание

В режиме "Без оповещений" можно заметить незначительное изменение небольшого значка BitDefender, расположенного рядом с часами в области оповещений.

Настройка режима "Без оповещений":

1. Откройте BitDefender, нажмите **Параметры** в верхнем правом углу окна и выберите интерфейс **Эксперт**.
2. Перейдите в раздел **Режим игры/ноутбука > Режим "Без оповещений"**.

В верхней части раздела отображается статус режима "Без оповещений".Для изменения текущего статуса можно нажать **Режим "Без оповещений" включен** или **Режим "Без оповещений" выключен**.

24.3.1. Настройка действия в полноэкранном режиме

Вы можете установить следующие параметры:

- **Действие в полноэкранном режиме** — можно выбрать автоматический переход в режим игры или в режим "Без оповещений" при переключении приложения в полноэкранный режим.

Замечание

Если вы не хотите, чтобы BitDefender автоматически переходил в режим "Без оповещений", снимите флажок **Действие в полноэкранном режиме**.

24.3.2. Настройка параметров режима "Без оповещений"

Для настройки режима работы при запланированных заданиях воспользуйтесь следующими параметрами:

- **Включить этот модуль для изменения запланированных задач антивирусного сканирования** — предотвращение запуска запланированных задач в режиме "Без оповещений".Вы можете выбрать один из следующих параметров:

Настройка	Описание
Пропустить задачу	Никогда не запускать запланированное задание.
Отложить задачу	Выполнять запланированное задание непосредственно после выхода из режима "Без оповещений".

25. Домашняя сеть

Модуль "Домашняя сеть" позволяет управлять обновлениями BitDefender, установленными на ваших домашних компьютерах, с одного компьютера.Для доступа к модулю домашней сети BitDefender выполните следующие действия (в зависимости от используемого режима пользовательского интерфейса):

Интерфейс "Опытный пользователь"
Перейдите на вкладку **Сеть**.

Интерфейс "Эксперт"
Перейдите в раздел **Домашняя сеть**.

Замечание
Также можно добавить ярлык для раздела Мои инструменты.

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

1. Включить систему управления домашней сетью BitDefender на компьютере.Настройте свой компьютер в качестве сервера.
2. Подключите каждый компьютер, которым вы хотите управлять, к сети (установите пароль).Настройте каждый компьютер как "стандартный".
3. Вернитесь к своему компьютеру и добавьте те компьютеры, которыми вы хотите управлять.

25.1. Включение сети BitDefender

Чтобы включить функцию домашней сети BitDefender, выполните следующие действия:

1. Нажмите **Управление сетью**.Появится окно настройки пароля для управления домашней сетью.
2. Введите пароль в каждом из полей ввода.
3. Настройка роли компьютера в домашней сети BitDefender:
   - **Компьютер-"сервер"** — установите этот параметр на том компьютере, с которого будет осуществляться управление остальными компьютерами.
   - **Стандартный компьютер** — установите этот параметр на всех компьютерах, которые будут управляться компьютером, выполняющим роль сервера.
4. Нажмите **OK**.

На карте сети будет отображаться имя компьютера.

Отобразится кнопка **Отключить сеть**.

25.2. Добавление компьютеров в сеть BitDefender

Компьютер будет автоматически добавлен в сеть, если он соответствует следующим требованиям:

- функция управления домашней сетью BitDefender была включена для этого модуля.
- для роли было задано значение "Стандартный компьютер".
- пароль, заданный при включении сети, совпадает с паролем, заданным для компьютера-"сервера".

Замечание

В интерфейсе "Эксперт" можно в любое время выполнить сканирование домашней сети на наличие компьютеров, удовлетворяющих критериям. Для этого нажмите кнопку **Автоматическое обнаружение**.

Чтобы вручную добавить компьютер в домашнюю сеть BitDefender с компьютера, выполняющего роль сервера, выполните следующие действия:

1. Нажмите **Добавить компьютер**.
2. Введите пароль для управления домашней сетью и нажмите **OK**.Появится новое окно.

   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. Выполните одно из следующих действий:
   - Выберите из списка имя добавляемого компьютера.
   - Введите IP-адрес или имя добавляемого компьютера в соответствующем поле.
4. Нажмите **Добавить**.Появится окно ввода пароля к управлению домашней сетью для соответствующего компьютера.
5. Введите пароль управления домашней сетью на соответствующем компьютере.
6. Нажмите **OK**.Если вы ввели правильный пароль, имя выбранного компьютера появится на карте сети.

25.3. 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, отобразятся краткие сведения о нем (имя, IP-адрес, число проблем, влияющих на безопасность системы, состояние регистрации BitDefender).

Если щелкнуть мышью на имени компьютера на карте сети, вы увидите список административных задач, которые можно запустить на удаленном компьютере.

- **Зарегистрировать BitDefender на этом компьютере**

  Позволяет зарегистрировать BitDefender на этом компьютере с помощью лицензионного ключа.

- **Установить пароль настроек на удаленном ПК**

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

- **Запустить задачу сканирования по требованию.**

  Позволяет запустить сканирование по требованию на удаленном компьютере. Вы можете выполнить любую из следующих задач сканирования: сканирование моих документов, системное сканирование или глубокое системное сканирование.

- **Устранить все проблемы на этом ПК**

  Позволяет исправить проблемы, влияющие на безопасность этого компьютера, с помощью мастера Устранить все угрозы.

- **Просмотр журнала/событий**

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

- **Обновить сейчас**

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

- **Установить профиль родительского контроля**

  Позволяет задать на этом компьютере возрастную категорию для веб-фильтра родительского контроля.

- **Установить в качестве сервера обновлений для этой сети**

  Позволяет установить этот компьютер, как сервер обновлений для всех продуктов BitDefender, установленных на компьютерах в сети.Использование этого параметра позволит снизить интернет-трафик, так как только один компьютер в сети будет подключаться к Интернету для загрузки обновлений.

- **Удалить ПК из домашней сети**

  Позволяет удалить ПК из сети.

Если для BitDefender выбран интерфейс "Опытный пользователь", нажав на соответствующие кнопки, можно одновременно запустить несколько заданий на всех управляемых компьютерах.

- **Сканировать все файлы** — позволяет сканировать все управляемые компьютеры одновременно.
- **Обновление файлов** — позволяет обновлять все управляемые компьютеры одновременно.
- **Регистрация** — позволяет зарегистрировать все управляемые компьютеры сразу.

Перед запуском задания на определенном компьютере появится окно ввода пароля управления домашней сетью.Введите пароль для управления домашней сетью и нажмите **OK**.

Замечание

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

26. Обновление

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

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

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

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

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

Обновления происходят следующим путем:

- **Обновления модуля антивируса** — при появлении новых угроз необходимо обновить файл вирусных сигнатур для обеспечения беспрерывной защиты от них. Этот тип обновления также известен как **Обновление определений вирусов**.
- **Обновление защиты от спама** — к эвристическому и URL-фильтру будут добавлены новые правила, а к 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** — сигнатуры новых программ-шпионов будут добавлены в базу данных. Этот тип обновления также известен как **Обновление модуля антишпиона**.
- **Обновления программного продукта** — при выпуске новой версии программы в новую версию добавляются новые функции и методы проверки, что только улучшает работу программы. Этот тип обновления также известен как **Обновление программы**.

26.1. Процедура обновления

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

Для обновления BitDefender необходимо выполнить следующие действия (в зависимости от режима пользовательского интерфейса):

Интерфейс "Основной"
Щелкните значок **Обновить сейчас** в области "Защита компьютера".

Интерфейс "Опытный пользователь"
Перейдите на вкладку **Безопасность** и выберите **Обновить сейчас** в области быстрых задач в левой части окна.

Интерфейс "Эксперт"
Перейти в раздел **Обновление > Обновление**.

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

Важно
Может потребоваться перезагрузка компьютера для завершения обновления. Рекомендуется сделать это как можно раньше.

Замечание

Если вы подключаетесь к Интернету по телефонной линии, лучше всего регулярно обновлять BitDefender по запросу.Для получения дополнительной информации перейдите к *«Обновление BitDefender при низкой скорости интернет-соединения»* (p. 192).

26.2. Настройка параметров обновления.

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

Настройка параметров обновления:

1. Откройте BitDefender, нажмите **Параметры** в верхнем правом углу окна и выберите интерфейс **Эксперт**.
2. Перейдите в раздел **Обновление > Настройки**.

3. Установите требуемые настройки.Для того чтобы узнать, на что влияет настройка, подержите курсор мыши над ней. Внизу окна появится подсказка.
4. Нажмите **Применить**, чтобы сохранить сделанные изменения.

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

Настройки обновления сгруппированы в четыре категории: **Настройки местоположения обновления**, **Настройки автоматического обновления**, **Настройки ручного обновления** и **Дополнительные настройки**. Каждая из категорий будет описана отдельно.

26.2.1. Настройки местоположения обновления

Чтобы настроить местоположение обновлений, используйте параметры 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 Интернетом через прокси-сервер.

Для более надежных и быстрых обновлений вы можете настроить два места обновления: **основное местоположение обновлений** и **альтернативное местоположение обновлений**. По умолчанию это `http://upgrade.bitdefender.com`.

Чтобы изменить местоположение обновления, введите URL-адрес локального зеркала в поле **URL**, соответствующем месту, которое вы хотите изменить.

Замечание

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

Если компания использует прокси-сервер для выхода в Интернет, поставьте отметку в поле **Использовать прокси**, а затем нажмите **Настройки прокси** для изменения настроек прокси.Дополнительные сведения см. в«Настройки соединения» (p. 60)

26.2.2. Настройки автоматического обновления

Чтобы настроить процесс обновлений, автоматически выполняемый BitDefender, используйте параметры в категории **Настройки автоматического обновления**.

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

Чтобы указать, как необходимо проводить процесс автоматического обновления, выберите один из следующих параметров:

- **Обновление без оповещений** — BitDefender автоматически загружает и устанавливает обновления.
- **Запрос перед загрузкой обновлений** — каждый раз, когда появится новое обновление, будет выводиться запрос вашего подтверждения перед загрузкой.
- **Запрос перед установкой обновлений** — каждый раз, когда будет загружено обновление, вам будет приходить запрос перед его установкой.

26.2.3. Настройка обновления вручную

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

- **Обновление без оповещений** — обновление вручную будет выполняться автоматически в фоновом режиме.
- **Запрос перед загрузкой обновлений** — каждый раз, когда появится новое обновление, будет выводиться запрос вашего подтверждения перед загрузкой.

26.2.4. Изменение дополнительных настроек

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

- **Перезагрузить позже** — если для завершения установки обновления необходимо выполнить перезапуск компьютера, программное обеспечение при выборе данного параметра будет продолжать 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 обновлять во время выполнения сканирования** — обновление BitDefender не выполняется в процессе выполнения сканирования. Таким образом, процесс обновления BitDefender не будет нарушать ход выполнения заданий сканирования.

Замечание

Если BitDefender будет проводить обновление во время сканирования, процесс сканирования будет прерван.

- **Не обновлять, если режим игры включен** — обновление BitDefender при включенном режиме игры не выполняется.Таким образом вы можете минимизировать влияние продукта на работу системы во время игр.
- **Разрешить совместный доступ к обновлениям** — чтобы снизить влияние сетевого трафика на производительность системы в процессе обновлений, воспользуйтесь функцией совместного доступа к обновлениям.
- **Отправить файлы BitDefender с компьютера** — BitDefender предусматривает возможность для пользователей BitDefender обмениваться последними вирусными сигнатурами.

Как?

27. Сканирование файлов и папок

Сканировать с помощью BitDefender легко.Существует несколько способов настроить BitDefender для сканирования файлов и папок на наличие вирусов и других вредоносных программ:

- Использование контекстного меню Windows
- Использование задач сканирования
- Использование панели активности сканирования

После начала сканирования появится мастер сканирования на антивирусы и проведет вас через весь процесс.Для получения дополнительной информации перейдите к *«Мастер антивирусного сканирования»* (p. 73).

Замечание

Сведения о сканировании с использованием BitDefender в безопасном режиме загрузки Windows см. в *«Сканирование компьютера в безопасном режиме»* (p. 207).

27.1. Использование контекстного меню Windows

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

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

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

27.2. Использование задач сканирования

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

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

Запуск заданий сканирования в простом режиме

В интерфейсе "Основной" доступен запуск нескольких предварительно настроенных заданий сканирования.Нажмите кнопку **Безопасность** и выберите требуемое задание сканирования.Следуйте подсказкам мастера сканирования на антивирусы.

Запуск заданий сканирования в интерфейсе "Опытный пользователь"

В интерфейсе "Опытный пользователь" можно запустить несколько предварительно настроенных задач проверки. Также можно настроить и запустить настраиваемые задачи сканирования для проверки конкретных файлов на компьютере с помощью настраиваемых параметров сканирования.Выполните следующие действия, чтобы запустить задание сканирования из интерфейса "Опытный пользователь":

1. Щелкните вкладку **Безопасность**.
2. В области быстрых задач слева нажмите **Полное сканирование системы** и выберите требуемое задание сканирования.Для настройки и запуска пользовательского сканирования нажмите **Пользовательское сканирование**.
3. Следуйте подсказкам мастера сканирования на антивирусы.Для запуска пользовательских задач необходимо запустить мастера пользовательского сканирования.

Запуск заданий сканирования в интерфейсе "Эксперт"

В интерфейсе "Эксперт" можно запустить все предварительно настроенные задания сканирования, а также изменить параметры сканирования для этих заданий. Кроме того, если требуется сканировать определенные расположения на компьютере, можно создавать настраиваемые задания сканирования.Для запуска задания в интерфейсе "Эксперт" выполните следующие действия:

1. Нажмите **Антивирус** в левом меню.
2. Нажмите на вкладку **Сканирование вирусов**.Здесь вы можете найти набор задач по умолчанию и создать свои собственные.
3. Дважды щелкните на задание сканирования, которое требуется запустить.
4. Следуйте подсказкам мастера сканирования на антивирусы.

27.3. Использование панели активности сканирования

Панель активности сканирования

В окне **График активности** графически показано, как проходит проверка вашей системы на наличие вирусов.По умолчанию это небольшое окно доступно для отображения только в интерфейсе Эксперт.

Вы можете использовать панель активности сканирования для быстрого сканирования файлов и папок.Перетащите файл или папку, которую надо проверить, на панель активности сканирования.Следуйте подсказкам мастера сканирования на антивирусы.

Замечание

Для получения дополнительной информации перейдите к *«Панель активности сканирования»* (p. 21).

28. Создание настраиваемого задания сканирования

Для создания задания сканирования откройте BitDefender и выполните следующие действия (в зависимости от режима пользовательского интерфейса):

Интерфейс "Опытный пользователь"

Перейдите на вкладку **Безопасность** и выберите **Настраиваемое сканирование** в области быстрых задач в левой части окна.

Откроется мастер, с помощью которого можно создать задание сканирования.Навигация по мастеру осуществляется с помощью кнопок **Далее** и **Назад**.Для выхода из мастера нажмите **Отмена**.

1. **Добро пожаловать!**
2. **Выбор объекта**

   Нажмите **Добавить объект**, чтобы выбрать файлы или папки для сканирования.

   Нажмите **Дополнительные настройки**.На вкладке **Обзор** с помощью бегунка настройте параметры сканирования.Если требуется детальная настройка параметров сканирования, нажмите **Настроить**.Перейдите на вкладку **Планировщик**, чтобы выбрать время запуска задания.
3. **Завершить**

   Здесь можно ввести имя задания и добавить сканирование в область быстрых задач (необязательно).

   Нажмите **Начать сканирование**, чтобы создать задание и запустить мастер сканирования.

Интерфейс "Эксперт"

1. Перейдите на вкладку **Антивирус > Сканирование вирусов**.
2. Нажмите **Новое задание**. После этого откроется новое окно.

   Замечание

   Также можно щелкнуть правой кнопкой мыши на предварительно определенном задании сканирования (например, **Глубокое сканирование системы**) и выбрать **Клонировать задание**.Данная функция полезна при создании новых заданий, поскольку позволяет изменять настройки дубликата задания.
3. На вкладке **Обзор** введите имя задания и с помощью бегунка задайте параметры сканирования.

Если требуется детальная настройка параметров сканирования, нажмите **Настроить**.

4. Перейдите на вкладку **Пути** для выбора объекта сканирования. Нажмите **Добавить элементы**, чтобы выбрать папки или файлы для сканирования.
5. Перейдите на вкладку **Планировщик**, чтобы выбрать время запуска задания.
6. Нажмите **OK**, чтобы сохранить задание.Новое задание отобразится под заданиями, определенными пользователем, после чего его можно редактировать, удалить или запустить из этого окна.

29. Создание расписания сканирования компьютера

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

Чтобы запланировать сканирование вашего компьютера проделайте эти действия:

1. Откройте BitDefender.
2. В зависимости от режима пользовательского интерфейса выполните следующие действия:

   Интерфейс "Опытный пользователь"
   Перейдите на вкладку **Безопасность** и выберите **Настроить антивирус** в области быстрых задач в левой части окна.

   Интерфейс "Эксперт"
   Нажмите **Антивирус** в левом меню.
3. Нажмите на вкладку **Сканирование вирусов**.Здесь вы можете найти набор задач по умолчанию и создать свои собственные.
   - Системные задачи доступны для запуска в любой учетной записи Windows.
   - Пользовательские задачи доступны только тем пользователям, которые их создали.

   По умолчанию вы можете запланировать следующие задачи сканирования:

   Сканирование
   Проверка всей системы, кроме архивов.При настройках по умолчанию проводится проверка на все типы вирусного ПО, кроме руткитов.

   Быстрое сканирование
   Функция быстрого сканирования использует технологию "облачного" сканирования для распознавания вредоносных программ, запущенных в системе.Быстрое сканирование занимает, как правило, менее минуты. Быстрое сканирование использует лишь незначительную часть системных ресурсов, которые используются в процессе стандартного вирусного сканирования.

   Сканирование объектов, выполняемое при загрузке
   Проверка элементов, запускающихся при входе пользователя в систему.Чтобы использовать эту задачу, надо запланировать ее запуск на загрузку системы.По умолчанию проверка элементов автозапуска отключена.

Глубокое сканирование системы
Проверка всей системы.В конфигурации по умолчанию производится проверка на все виды вредоносных программ, угрожающих безопасности вашей системы, а именно на наличие вирусов, программ-шпионов, рекламного ПО, руткитов и проч.

Мои документы
Используйте данное задание для проверки основных папок пользователя: Мои документы, Рабочий стол и Автозагрузка. Это позволит обеспечить безопасность ваших документов, безопасность рабочего пространства и запуск незараженных программ при загрузке.

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

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

   Замечание
   Например, для того чтобы проверять ваш компьютер каждую субботу в два часа ночи, настройте планирование следующим образом:
   a. Выберите **Периодически**.
   b. В поле **Каждые** введите 1 и затем выберите **недель** в меню.Таким образом, задание будет запускаться раз в неделю.
   c. Установите в качестве даты запуска первую субботу.
   d. Установите временем начала 2:00:00 ночи.
6. Нажмите **OK**, чтобы сохранить изменения.Задача запустится автоматически в заданный день и время.Если ваш компьютер выключен, в запланированное время задача запустится, когда вы включите компьютер.

30. Создание учетных записей пользователя Windows

Учетная запись пользователя Windows представляет собой единый профиль, который объединяет все настройки, привилегии и личные файлы каждого из пользователей.

С помощью учетных записей Windows администратор домашнего компьютера может управлять доступом каждого из пользователей.

Создание и настройка учетных записей пользователей выполняются в том случае, когда компьютером пользуются и родители, и дети. Родители могут настроить учетные записи для каждого из детей.

Выберите имеющийся тип операционной системы, чтобы определить способ создания учетных записей Windows.

- Windows XP:
  1. Выполните вход в систему с учетными данными администратора.
  2. Нажмите "Пуск", выберите "Панель управления", затем выберите "Учетные записи пользователей".
  3. Нажмите "Создать новую учетную запись".
  4. Введите имя пользователя. Можно использовать имя и фамилию, только имя или псевдоним. После этого нажмите "Далее".
  5. В качестве типа учетной записи выберите "Ограниченная" и нажмите "Создать учетную запись". Учетные записи с ограниченными правами подходят для детей, так как они не позволяют вносить изменения в систему и устанавливать определенные приложения.
  6. Будет создана новая учетная запись, после чего она появится в списке на экране "Управление учетными записями".
- Windows Vista или Windows 7:
  1. Выполните вход в систему с учетными данными администратора.
  2. Нажмите "Пуск", выберите "Панель управления", затем выберите "Учетные записи пользователей".
  3. Нажмите "Создать новую учетную запись".
  4. Введите имя пользователя. Можно использовать имя и фамилию, только имя или псевдоним. После этого нажмите "Далее".
  5. В качестве типа учетной записи выберите "Стандартная" и нажмите "Создать учетную запись". Учетные записи с ограниченными правами подходят для детей, так как они не позволяют вносить изменения в систему и устанавливать определенные приложения.

6. Будет создана новая учетная запись, после чего она появится в списке на экране "Управление учетными записями".

Замечание

После создания новых учетных записей пользователя можно создать для них пароли.

31. Обновление BitDefender с использованием прокси-сервера

Как правило, BitDefender автоматически выполняет поиск и импорт настроек прокси-сервера из системы.Если для подключения к Интернету используется прокси-сервер, возможно, потребуется узнать настройки прокси-сервера и соответствующим образом настроить BitDefender.Инструкции для этой процедуры см. в «*Просмотр сведений о настройках прокси-сервера.*» (p. 222).

По завершении поиска настроек прокси-сервера выполните следующие действия:

1. Откройте BitDefender, нажмите **Параметры** в верхнем правом углу окна и выберите интерфейс **Эксперт**.
2. Перейдите в раздел **Общие > Настройки**.
3. Выберите **Настройки прокси-сервера** в разделе **Настройки подключения**.
4. Задайте настройки прокси-сервера в соответствующих полях.
5. Нажмите **OK**.

Замечание

Если эта информация не помогла, вы можете обратиться в поддержку BitDefender, как указано в секции «*Поддержка*» (p. 212).

32. Обновление до другой версии продукта BitDefender 2011.

Используя BitDefender 2011, вы сможете легко обновлять BitDefender до более новых версий.

Рассмотрим следующий сценарий: пользователь в течение некоторого времени использовал BitDefender Internet Security 2011 2011, а недавно решил обновить свой продукт до версии BitDefender Total Security 2011 и установить доступные дополнительные функции.

Вам необходимо просто приобрести лицензионный ключ для продукта BitDefender 2011, который вы планируете обновить, и ввести его в окне регистрации текущего установленного продукта BitDefender 2011.

Выполните следующие действия:

1. Откройте BitDefender.
2. Перейдите по ссылке **Сведения о лицензии** в нижней части окна.Откроется окно регистрации.
3. Введите лицензионный ключ и нажмите **Зарегистрировать сейчас**.
4. BitDefender выведет сообщение о том, что данный лицензионный ключ относится к другому продукту, и предложит установить этот продукт.Перейдите по соответствующей ссылке и выполните последовательность действий из трех шагов, чтобы обновить продукт.

   a. **Подтвердить**

   b. **Выполняется обновление**

      Дождитесь, пока BitDefender завершит процесс обновления.Это может занять несколько минут.

   c. **Обновление завершено**

      Процесс завершен. Возможно, потребуется перезагрузка системы.

Устранение неполадок и получение справки

33. Устранение неполадок

В данной главе приведено описание некоторых проблем, с которыми пользователь может столкнуться при использовании BitDefender, а также даны различные варианты их решений.Большинство проблем можно устранить, настроив параметры продукта соответствующим образом.

Если проблема не описана в этом разделе или предлагаемые решения не подходят для ее устранения, обратитесь в службу технической поддержки BitDefender (контактные данные приведены в тексте главы) «*Поддержка*» (p. 212).

33.1. Проблемы установки

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

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

33.1.1. Ошибки подтверждения установки

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

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

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

33.1.2. Сбой установки

Возможны несколько вариантов сбоя установки:

- В процессе установки появляется экран ошибки.Может отобразиться запрос об отмене установки или кнопка запуска инструмента удаления, с помощью которого выполняется очистка системы.

Замечание
Сразу же после начала установки может отобразиться уведомление о нехватке свободного места на диске для установки BitDefender. В этом случае необходимо освободить требуемый объем дискового пространства в разделе,

где планируется установить BitDefender, а затем возобновить или повторно запустить установку.

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

Для устранения неполадок и установки BitDefender выполните следующие действия:

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

   В этом случае самым простым решением является полное удаление из системы и последующая повторная установка BitDefender.Для получения дополнительной информации перейдите к «*Полное удаление BitDefender.*» (p. 222).

2. **Проверьте возможные причины, помешавшие установке.** Прежде чем приступить к переустановке продукта, определите и устраните возможные причины, которые могли привести к сбою установки:

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

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

      - Воспользуйтесь диском-реаниматором BitDefender для проверки компьютера и устраните все возможные угрозы.Для получения дополнительной информации перейдите к «*Диск-реаниматор BitDefender*» (p. 203).
      - Откройте окно Internet Explorer, перейдите к www.bitdefender.com и запустите онлайн-сканирование (нажмите **онлайн-сканирование**).

3. Попробуйте установить BitDefender еще раз.Рекомендуется загружать и запускать последнюю версию установочного файла с www.bitdefender.com.
4. Если снова происходит сбой установки, обратитесь в BitDefender за поддержкой, как описано в «*Поддержка*» (p. 212).

33.2. Работа системы замедлена

Как правило, после установки программного обеспечения безопасности допускается незначительное снижение быстродействия системы.

Если работа системы значительно замедлена, это может быть вызвано одной из следующих причин:

- **В системе установлены другие решения безопасности, помимо BitDefender.**

  Хотя BitDefender выполняет поиск и удаление программ безопасности, обнаруженных во время установки, рекомендуется удалить остальные антивирусные программы заранее, перед установкой BitDefender.Для получения дополнительной информации перейдите к *«Удаление других решений безопасности»* (p. 220).

- **Не соблюдены минимальные системные требования для запуска BitDefender.**

  Если компьютер не соответствует минимальным системным требованиям, это может стать причиной медленной работы системы, особенно при одновременной работе нескольких приложений.Для получения дополнительной информации перейдите к *«Минимальные системные требования»* (p. 2).

- **Избыточная фрагментация жестких дисков.**

  Во время выполнения фрагментации файлов доступ к файлам замедляется и снижается производительность системы.

  Чтобы выполнить дефрагментацию диска, используя средства операционной системы Windows, перейдите из меню Windows "Пуск" по следующему пути: **Пуск → Программы → Служебные → Системные инструменты → Дефрагментация диска**.

33.3. Сканирование не начинается

Неисправности такого типа могут возникать вследствие двух основных причин:

- **Установленная ранее версия BitDefender, которая не была удалена полностью, или некорректно установленная версия BitDefender**.

  В этом случае самым простым решением является полное удаление из системы и последующая повторная установка BitDefender.Для получения дополнительной информации перейдите к *«Полное удаление BitDefender.»* (p. 222).

- **В системе установлены другие решения безопасности, помимо BitDefender**.

  В этом случае выполните следующие действия:

1. Удалите другое решение безопасности.Для получения дополнительной информации перейдите к *«Удаление других решений безопасности»* (p. 220).
2. Удалить BitDefender из системы полностью.
3. Повторная установка BitDefender на компьютер.

Если эта информация не помогла, вы можете обратиться в поддержку BitDefender, как указано в секции *«Поддержка»* (p. 212).

33.4. Не удается использовать приложение

Возникает проблема при попытке использовать программу, которая до установки BitDefender работала нормально.

Вы можете столкнуться с одной из следующих ситуаций.

- Может отображаться сообщение BitDefender о том, что одна из программ пытается внести изменения в систему.
- Программа, которую вы пытаетесь использовать, может вывести сообщение об ошибке.

Такие ситуации возникают в случаях, когда модуль активного вирусного контроля ошибочно определяет некоторые приложения как вредоносные.

Активный вирусный контроль представляет собой отдельный модуль BitDefender, который служит для постоянного отслеживания приложений, запущенных в системе, и информирования об их потенциально вредоносном поведении.Поскольку в основе этой функции лежит система эвристического анализа, возможны случаи распознавания активным вирусным контролем легитимных приложений как вирусов.

При возникновении такой ситуации можно исключить соответствующее приложение из мониторинга активного вирусного контроля.

Для добавления программы в список исключений выполните следующие действия:

1. Откройте BitDefender, нажмите **Параметры** в верхнем правом углу окна и выберите интерфейс **Эксперт**.
2. Перейдите в раздел **Антивирус > Щит**.
3. Нажмите **Дополнительные настройки**.
4. В новом окне перейдите на вкладку **Исключения**, нажмите кнопку **Добавить** и перейдите в папку, где находится EXE-файл программы (обычно в папке `C:\Program Files`).
5. Нажмите **OK**, чтобы сохранить изменения, и закройте окно.
6. Закройте окно BitDefender и проверьте, возникает ли проблема по-прежнему.

Если эта информация не помогла, вы можете обратиться в поддержку BitDefender, как указано в секции «*Поддержка*» (p. 212).

33.5. Не удается подключиться к Интернету

В некоторых случаях после установки BitDefender программа больше не может подключиться к Интернету или получить доступ к сетевым службам.

Мастер поиска и устранения неполадок позволяет выявить и устранить неисправности подключения.Для запуска мастера откройте BitDefender и выполните следующие действия (в зависимости от режима пользовательского интерфейса):

Интерфейс "Опытный пользователь"
: Перейдите на вкладку **Безопасность** и выберите **Настроить брандмауэр** в области быстрых задач в левой части окна.Перейдите на вкладку **Настройки** в открывшемся окне и выберите **Поиск и устранение неисправностей**.

Интерфейс "Эксперт"
: Перейдите в раздел **Брандмауэр > Настройки** и нажмите **Поиск и устранение неполадок**.

Для запуска поиска и устранения неисправностей выполните процедуру, состоящую из трех шагов.Навигация по мастеру осуществляется с помощью кнопки **Далее**.Для выхода из мастера нажмите **Отмена**.

1. **Добро пожаловать!**

   Выберите **Сбой при попытке доступа в Интернет**.

2. **Определение проблемы**

   Нажмите **Выбрать приложение** и **Обзор** для поиска EXE-файла программы (как правило, он расположен в каталоге `C:\Program Files`, например Firefox.exe).Нажмите **Добавить**.

3. **Рекомендуемое решение**

   Выберите **Да, разрешить доступ**.Нажмите **Завершить** и проверьте, удалось ли устранить проблему.

Если эта информация не помогла, вы можете обратиться в поддержку BitDefender, как указано в секции «*Поддержка*» (p. 212).

33.6. Не удается использовать принтер

В зависимости от типа сети, к которой подключен компьютер, брандмауэр BitDefender может заблокировать соединение между компьютером и сетевым принтером.

В этом случае рекомендуется настроить для BitDefender возможность автоматически разрешать подключение к соответствующему принтеру.

Мастер поиска и устранения неполадок позволяет выявить и устранить неисправности подключения.Для запуска мастера откройте BitDefender и выполните следующие действия (в зависимости от режима пользовательского интерфейса):

Интерфейс "Опытный пользователь"

Перейдите на вкладку **Безопасность** и выберите **Настроить брандмауэр** в области быстрых задач в левой части окна.Перейдите на вкладку **Настройки** в открывшемся окне и выберите **Поиск и устранение неисправностей**.

Интерфейс "Эксперт"

Перейдите в раздел **Брандмауэр > Настройки** и нажмите **Поиск и устранение неполадок**.

Для запуска поиска и устранения неисправностей выполните процедуру, состоящую из трех шагов.Навигация по мастеру осуществляется с помощью кнопки **Далее**.Для выхода из мастера нажмите **Отмена**.

1. **Добро пожаловать!**

   Выберите **Сбой при выводе на печать**.

2. **Определение проблемы**

   Нажмите **Выбрать принтер**.В списке выберите принтер по имени или по IP-адресу.Если не удается найти устройство в списке, можно вручную ввести IP-адрес в поле редактирования.Нажмите **Добавить**.

3. **Рекомендуемое решение**

   Выберите **Да, разрешить доступ**.Нажмите **Завершить** и проверьте, удалось ли устранить проблему.

Если мастер поиска и устранения неисправностей сообщает о том, что проблема не связана с брандмауэром BitDefender, установленным на компьютере, проверьте следующие возможные причины:

- Совместный доступ к файлу и принтеру на вашем компьютере может быть заблокирован брандмауэром, установленным на другом компьютере.
  - Если используется брандмауэр Windows, его можно настроить, разрешив доступ к файлам и принтерам следующим образом: откройте окно настройки брандмауэра Windows, вкладку **Исключения** и отметьте флажок **Общий доступ к файлам и принтерам**.
  - Если используется другой брандмауэр, обратитесь к его документации или файлу справки.

- Общие условия, которые могут предотвратить использование общего принтера или подключение к нему:
  - Возможно, вам придется войти в учетную запись администратора Windows для доступа к общему принтеру.
  - Разрешения устанавливаются на общий принтер, чтобы разрешить доступ только конкретному компьютеру и пользователям.Если вы хотите открыть общий доступ к вашему принтеру, проверьте разрешения, установленные на принтере, чтобы увидеть, разрешен ли пользователю на другом компьютере доступ к принтеру.Если вы пытаетесь подключиться к общему принтеру, свяжитесь с пользователем другого компьютера для проверки того, есть ли у вас разрешение на подключение к принтеру.
  - Принтер, подключенный к вашему компьютеру или к другому компьютеру, не является общим.
  - Общий принтер не добавлен на компьютер.

  Замечание

  Чтобы научиться управлять принтерами (обеспечивать общий доступ к принтеру, устанавливать или удалять разрешения для принтера, подключаться к сетевому или к общему принтеру), перейдите к центру справки и поддержки Windows (в меню Пуск выберите команду **Справка и поддержка**).

- Доступ к сетевому принтеру для определенных компьютеров или пользователей может быть ограничен. Необходимо проверить у администратора сети наличие разрешений на подключение к этому принтеру.

Если эта информация не помогла, вы можете обратиться в поддержку BitDefender, как указано в секции «*Поддержка*» (p. 212).

33.7. Не удается разрешить совместный доступ к файлам с другого компьютера

В зависимости от типа сети, к которой подключен компьютер, брандмауэр BitDefender может заблокировать соединение между вашим и другим компьютером.Это может привести к тому, что в дальнейшем совместный доступ к этим файлам с другого компьютера будет заблокирован.В этом случае рекомендуется настроить для BitDefender возможность автоматически разрешать подключение к соответствующей системе.

Мастер поиска и устранения неполадок позволяет выявить и устранить неисправности подключения.Для запуска мастера откройте BitDefender и выполните следующие действия (в зависимости от режима пользовательского интерфейса):

Интерфейс "Опытный пользователь"

Перейдите на вкладку **Безопасность** и выберите **Настроить брандмауэр** в области быстрых задач в левой части окна.Перейдите на вкладку **Настройки** в открывшемся окне и выберите **Поиск и устранение неисправностей**.

Интерфейс "Эксперт"

Перейдите в раздел **Брандмауэр > Настройки** и нажмите **Поиск и устранение неполадок**.

Для запуска поиска и устранения неисправностей выполните процедуру, состоящую из трех шагов.Навигация по мастеру осуществляется с помощью кнопки **Далее**.Для выхода из мастера нажмите **Отмена**.

1. **Добро пожаловать!**

   Выберите **Сбой при попытке доступа к компьютеру в сети**.

2. **Определение проблемы**

   Нажмите **Выбрать компьютер**.В списке выберите компьютер по имени или по IP-адресу.Если не удается найти компьютер в списке, можно вручную ввести IP-адрес в поле редактирования.Нажмите **Добавить**.

3. **Рекомендуемое решение**

   Выберите **Да, разрешить доступ**.Нажмите **Завершить** и проверьте, удалось ли устранить проблему.

Если эта информация не помогла, вы можете обратиться в поддержку BitDefender, как указано в секции *«Поддержка»* (p. 212).

33.8. Низкая скорость соединения с Интернетом

Эта ситуация может возникать после установки BitDefender.Проблема может быть вызвана ошибками конфигурации брандмауэра BitDefender.

Для поиска и устранения неисправностей выполните следующие действия:

1. Откройте BitDefender, нажмите **Параметры** в верхнем правом углу окна и выберите интерфейс **Эксперт**.
2. Перейдите в раздел **Брандмауэр > Настройки**.
3. Для временного отключения брандмауэра снимите флажок **Брандмауэр включен**.
4. Проверьте работоспособность подключения к Интернету при отключенном брандмауэре BitDefender.

   - Если восстановить подключение к Интернету все еще не удается, значит эта неисправность вызвана не BitDefender. Необходимо связаться с

поставщиком услуг Интернета и проверить работоспособность подключения на стороне поставщика.

Если поставщик интернет-услуг подтверждает, что на его стороне неполадки с соединением отсутствуют, но проблема продолжает возникать, обратитесь в BitDefender в соответствии с инструкциями в разделе «*Поддержка*» (p. 212).

- Если вам удалось подключиться к Интернету после отключения брандмауэра BitDefender, выполните следующие действия:

  a. Откройте BitDefender, нажмите **Параметры** в верхнем правом углу окна и выберите интерфейс **Эксперт**.

  b. Перейдите в раздел **Брандмауэр > Настройки** и установите соответствующий флажок для включения брандмауэра.

  c. Нажмите **Дополнительные настройки**, выберите **Разрешить совместный доступ к интернет-соединению** и снимите флажок **Блокировать сканирование портов**.

  d. Перейдите на вкладку **Сеть** в главном окне.

  e. Откройте выпадающее меню из столбца **Тип сети** и выберите **Домашняя/Офисная**.

  f. Перейдите в столбец **Общий** и задайте значение **Да**. Задайте для параметра **Режим невидимки** значение **Удаленный**.

  g. Проверьте доступность подключения к Интернету.

Если эта информация не помогла, вы можете обратиться в поддержку BitDefender, как указано в секции «*Поддержка*» (p. 212).

33.9. Обновление BitDefender при низкой скорости интернет-соединения

При низкой скорости интернет-соединения (например, модемного) в процессе обновления могут возникать ошибки.

Для регулярного обновления вирусных сигнатур BitDefender выполните следующие действия:

1. Откройте BitDefender, нажмите **Параметры** в верхнем правом углу окна и выберите интерфейс **Эксперт**.
2. Перейдите в раздел **Обновление > Настройки**.
3. В разделе **Настройка обновления вручную** выберите **Спрашивать перед загрузкой обновлений**.
4. Нажмите **Применить** и перейдите на вкладку **Обновить**.

5. Нажмите **Обновить сейчас**, после чего откроется новое окно.
6. Выберите только **Обновления сигнатур**, затем нажмите **OK**.
7. BitDefender выполнит загрузку и установку только обновлений вирусных сигнатур.

33.10. Обновление BitDefender на компьютере, не подключенном к Интернету

Если компьютер не подключен к Интернету, необходимо загрузить обновления вручную на компьютер, имеющий доступ в Интернет, и затем перенести их на свой компьютер с помощью съемного носителя (например, USB-носителя).

Выполните следующие действия:

1. На компьютере, подключенном к Интернету, откройте веб-браузер и перейдите по следующему адресу:

   www.bitdefender.com/site/view/Desktop-Products-Updates.html
2. В столбце **Обновление вручную** нажмите на ссылку, соответствующую архитектуре используемого продукта и системы.Чтобы узнать, какая версия Windows (32- или 64-разрядная) установлена на компьютере, см. *«Определение используемой версии Windows (32- или 64-разрядная)»* (p. 221).
3. Сохраните в системе файл с именем `weekly.exe`.
4. Перенос загруженных файлов на съемный носитель (например, на USB-носитель), а затем в компьютер.
5. Дважды щелкните мышью на файл и следуйте инструкциям в мастере.

33.11. BitDefender не отвечает

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

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

Ошибка может быть вызвана одной из следующих причин:

- Устанавливается важное обновление.
- временным ошибкам связи BitDefender.
- некоторые из служб BitDefender остановлены.
- другие средства безопасности работают одновременно с BitDefender.

- вирусы в системе мешают нормальному функционированию BitDefender.

Для устранения этой ошибки попробуйте выполнить следующие действия:

1. Несколько минут подождите возможных изменений.Ошибка может быть временной.
2. Перезагрузите компьютер и дождитесь загрузки BitDefender. Откройте BitDefender и проверьте, не устранена ли ошибка.Перезагрузка компьютера обычно решает проблему.
3. Проверьте, не установлены ли другие средства безопасности, так как они могут нарушить нормальное функционирование BitDefender. Если они установлены, рекомендуется удалить все другие решения безопасности, а затем переустановить BitDefender.
4. Если ошибка повторяется, возможно, проблема более серьезна (например, система заражена вирусом, мешающим работать BitDefender).За технической поддержкой обращайтесь к BitDefender по ссылке «*Поддержка*» (p. 212).

33.12. Антиспам работает некорректно

Эта статья поможет вам устранить следующие проблемы, связанные с операциями фильтрации антиспама BitDefender:

- Количество легальных сообщений, помеченных как [спам].
- Многие спам-сообщения не помечены фильтром антиспама.
- Фильтр антиспама не распознает спам-сообщения.

33.12.1. Легальные сообщения помечены как [спам]

Легальные сообщения помечены как [спам] потому, что для антиспама BitDefender они выглядят как спам.Вы можете решить эту проблему соответствующей настройкой фильтра антиспама.

BitDefender автоматически добавляет получателей вашей почты в список друзей.Сообщения электронной почты, полученные от контактов из списка друзей, учитываются как легальные. Они не проверяются фильтром антиспама и никогда не помечаются как [спам].

Автоматическая настройка списка друзей не предотвращает ошибок обнаружения, которые могут возникнуть в следующих случаях:

- Вы получаете большое количество коммерческой почты в результате подписки на различных веб-сайтах.В данном случае решением будет добавить адреса электронной почты, с которых приходят данные сообщения, в список друзей.

- Значительная часть вашей легальной почты от людей, с которыми вы никогда не переписывались, например клиентов, потенциальных партнеров и других.В данном случае необходимы другие решения.

Если вы используете один из почтовых клиентов с интегрированным BitDefender, попробуйте следующие решения:

1. Указать ошибки обнаружения. Используется для тренировки обучающего ядра (Байесовского) фильтра антиспама и помогает предотвратить ошибки обнаружения.Обучающее ядро анализирует указанные сообщения и изучает их структуру. Следующие сообщения электронной почты, содержащие одинаковые части, не будут помечены как [спам].
2. Уменьшение уровня защиты антиспама. При уменьшении уровня защиты фильтру антиспама нужно больше признаков для классификации спам-сообщений электронной почты как спама.Пробуйте использовать это решение, только если большое количество легальной почты (в том числе коммерческие сообщения) неверно определяется как спам.
3. Переподготовка ядра обучения (Байесовского фильтра). Пробуйте это решение, только если предыдущие не принесли результатов.

Замечание

BitDefender интегрируется в наиболее часто используемые почтовые клиенты с помощью простой в использовании антиспам панели инструментов.С полным списком системных требований можно ознакомиться в разделе *«Требования программного обеспечения»* (p. 2).

Если вы используете другой почтовый клиент, вы не сможете указать спам-сообщения и подготовить обучающее ядро. Для решения проблемы попробуйте понизить уровень защиты.

Добавить контакты в список друзей

Если вы используете поддерживаемый почтовый клиент, вы можете легко добавлять отправителей легальной почты в список друзей.Выполните следующие действия:

1. В вашем почтовом клиенте выберите сообщение электронной почты от отправителя, которого вы хотите добавить в список друзей.
2. Нажмите кнопку **Добавить друга** на панели управления антиспама BitDefender.
3. Вам будет предложено подтвердить добавление адресов в список друзей.Выберите **Не показывать это сообщение снова** и нажмите **OK**.

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

Если вы используете другой почтовый клиент, вы можете добавлять контакты в список друзей из интерфейса BitDefender.Выполните следующие действия:

1. Откройте BitDefender, нажмите **Параметры** в верхнем правом углу окна и выберите интерфейс **Эксперт**.
2. Нажмите **Антиспам** в левом меню.
3. Щелкните вкладку **Статус**.
4. Нажмите **Управление друзьями**.Появится окно настроек.
5. Введите адрес электронной почты, с которого хотите всегда получать почту, и нажмите кнопку для добавления адреса в список друзей.
6. Нажмите **OK**, чтобы сохранить изменения, и закройте окно.

Указать ошибки обнаружения

Если вы используете поддерживаемый почтовый клиент, вы можете легко корректировать фильтр антиспама (указывая письма, которые не надо помечать как [спам]). Данные действия улучшат эффективность фильтра антиспама.Выполните следующие действия:

1. Откройте ваш почтовый клиент.
2. Перейдите в папку нежелательной почты, куда помещаются спам-сообщения.
3. Выберите легитимные сообщения, ошибочно помеченные BitDefender как [спам].
4. Нажмите кнопку **Добавить друга** на панели управления антиспама BitDefender для добавления отправителя в список друзей.Вам будет необходимо нажать **OK** для подтверждения.Вы всегда будете получать сообщения от этого адресата, независимо от их содержания.
5. Нажмите кнопку **Не спам** на панели антиспама BitDefender (обычно расположенной в верхней части окна почтового клиента). Это укажет обучающему ядру, что выбранные сообщения не являются спамом, и они будут перемещены в папку "Входящие".Следующие сообщения электронной почты, содержащие одинаковые части, больше не будут помечены как [спам].

Уменьшение уровня защиты антиспама

Для уменьшения уровня защиты антиспама следуйте этим шагам:

1. Откройте BitDefender, нажмите **Параметры** в верхнем правом углу окна и выберите интерфейс **Эксперт**.
2. Нажмите **Антиспам** в левом меню.

3. Щелкните вкладку **Статус**.
4. Переместите ползунок ниже.

Рекомендуется понизить защиту на один уровень и подождать некоторое время, чтобы увидеть результаты.Если много легальной почты все еще помечается как [спам], вы можете понизить уровень защиты. Если вы замечаете, что многие спам-сообщения не были обнаружены, то понижать уровень защиты не следует.

Переобучить обучающее ядро (Байесовское)

Перед тренировкой обучающего ядра (Байесовского) приготовьте одну папку, содержащую только СПАМ-сообщения, и другую, содержащую только легальную почту.Обучающее ядро проанализирует их и выучит характеристики, определяющие спам или легальные сообщения, которые вам обычно приходят. Для того чтобы обучение было эффективным, в каждой папке должно быть более 50 сообщений.

Чтобы сбросить Байесовскую базу данных и переобучить обучающее ядро, следуйте этим шагам:

1. Откройте ваш почтовый клиент.
2. На панели инструментов аниспама BitDefender нажмите кнопку **Мастер** для запуска мастера настройки антиспама.
3. Нажмите **Далее**.
4. Выберите **Пропустить этот шаг** и нажмите **Далее**.
5. Выберите **Очистить базу данных фильтра антиспама** и нажмите **Далее**.
6. Выберите папку, содержащую легальную почту, и нажмите **Далее**.
7. Выберите папку, содержащую СПАМ-сообщения, и нажмите **Далее**.
8. Нажмите **Завершить** для запуска процесса тренировки.
9. Когда обучение закончится, нажмите **Закрыть**.

Обратиться за помощью

Если эта информация не помогла, вы можете обратиться в поддержку BitDefender, как указано в секции *«Поддержка»* (p. 212).

33.12.2. Многие спам-сообщения не обнаружены

Если вы получаете много спам-сообщений, не помеченных как [спам], вы должны настроить антиспам BitDefender для увеличения его эффективности.

Если вы используете один из почтовых клиентов с интегрированным BitDefender, попробуйте одно из следующих решений:

1. Указать необнаруженные спам-сообщения. Используется для тренировки обучающего ядра (Байесовского) фильтра антиспама и обычно улучшает обнаружение.Обучающее ядро анализирует указанные сообщения и изучает их структуру. Следующие сообщения электронной почты, содержащие одинаковые части, будут помечены как [спам].
2. Добавить спамеров в список спамеров. Почтовые сообщения, полученные с адресов из списка спамеров, автоматически помечены как [спам].
3. Увеличение уровня защиты антиспама. При увеличении уровня защиты фильтру антиспама нужно меньше признаков для классификации спам-сообщений электронной почты как спама.
4. Переподготовка ядра обучения (Байесовского фильтра). Используйте это решение, когда обнаружение спама неудовлетворительно и индикация необнаруженных спам-сообщений больше не помогает.

Замечание

BitDefender интегрируется в наиболее часто используемые почтовые клиенты с помощью простой в использовании антиспам панели инструментов.С полным списком системных требований можно ознакомиться в разделе *«Требования программного обеспечения»* (p. 2).

Если вы используете другой почтовый клиент, вы не сможете указать спам-сообщения и подготовить обучающее ядро. Для решения проблемы попробуйте увеличить уровень защиты и добавить спамеров в список спамеров.

Указать необнаруженные спам-сообщения

Если вы используете поддерживаемый почтовый клиент, вы можете легко определить, какие сообщения должны быть определены как спам. Эти действия значительно улучшат эффективность фильтра антиспама.Выполните следующие действия:

1. Откройте ваш почтовый клиент.
2. Перейти к папке "Входящие".
3. Выберите необнаруженные спам-сообщения.
4. Нажмите кнопку **Это спам** на панели антиспама BitDefender (обычно она расположена в верхней части окна почтового клиента). Это укажет обучающему ядру, что выбранные сообщения являются спамом. Они незамедлительно будут помечены как [спам] и перенесены в папку нежелательной почты.Следующие сообщения электронной почты, содержащие одинаковые части, будут помечены как [спам].

Добавить спамеров в список спамеров

Если вы используете поддерживаемый почтовый клиент, вы можете легко добавлять отправителей спама в список спамеров.Выполните следующие действия:

1. Откройте ваш почтовый клиент.
2. Перейдите в папку нежелательной почты, куда помещаются спам-сообщения.
3. Выберите сообщения, помеченные BitDefender как [спам].
4. Нажмите кнопку **Добавить спамера** на панели антиспама BitDefender.
5. Вам будет предложено подтвердить добавление адресов в список спамеров.Выберите **Не показывать это сообщение снова** и нажмите **OK**.

Если вы используете другой почтовый клиент, вы можете вручную добавить спамеров в список с помощью интерфейса BitDefender. Это удобно делать только тогда, когда вы получили несколько писем с одной и той же электронной почты.Выполните следующие действия:

1. Откройте BitDefender, нажмите **Параметры** в верхнем правом углу окна и выберите интерфейс **Эксперт**.
2. Нажмите **Антиспам** в левом меню.
3. Щелкните вкладку **Статус**.
4. Нажмите **Управление спамерами**.Появится окно настроек.
5. Определите адрес электронной почты спамера и нажмите кнопку для добавления адреса в список спамеров.
6. Нажмите **OK**, чтобы сохранить изменения, и закройте окно.

Увеличение уровня защиты антиспама

Для увеличения уровня защиты антиспама выполните следующие действия:

1. Откройте BitDefender, нажмите **Параметры** в верхнем правом углу окна и выберите интерфейс **Эксперт**.
2. Нажмите **Антиспам** в левом меню.
3. Щелкните вкладку **Статус**.
4. Переместите ползунок выше.

Переобучить обучающее ядро (Байесовское)

Перед тренировкой обучающего ядра (Байесовского) приготовьте одну папку, содержащую только СПАМ-сообщения, и другую, содержащую только легальную почту.Обучающее ядро проанализирует их и выучит характеристики,

определяющие спам или легальные сообщения, которые вам обычно приходят. Для того чтобы обучение было эффективным, должно быть более 50 сообщений в каждой папке.

Чтобы сбросить Байесовскую базу данных и переобучить обучающее ядро, следуйте этим шагам:

1. Откройте ваш почтовый клиент.
2. На панели инструментов аниспама BitDefender нажмите кнопку **Мастер** для запуска мастера настройки антиспама.
3. Нажмите **Далее**.
4. Выберите **Пропустить этот шаг** и нажмите **Далее**.
5. Выберите **Очистить базу данных фильтра антиспама** и нажмите **Далее**.
6. Выберите папку, содержащую легальную почту, и нажмите **Далее**.
7. Выберите папку, содержащую СПАМ-сообщения, и нажмите **Далее**.
8. Нажмите **Завершить** для запуска процесса тренировки.
9. Когда обучение закончится, нажмите **Закрыть**.

Обратиться за помощью

Если эта информация не помогла, вы можете обратиться в поддержку BitDefender, как указано в секции «*Поддержка*» (p. 212).

33.12.3. Фильтр антиспама не обнаружил ни одного спам-сообщения

Если нет спам-сообщений, помеченных как [спам], могут быть проблемы в работе антиспама BitDefender.До устранения проблемы убедитесь, что она не вызвана одной из следующих причин:

- Защита антиспама BitDefender доступна только для клиентов электронной почты, настроенной на прием сообщений электронной почты по протоколу POP3.Это значит:
  - Сообщения электронной почты, полученные через веб-службы электронной почты (например, Yahoo, Gmail, Hotmail или другой), не фильтруются BitDefender на предмет спама.
  - Если ваш почтовый клиент настроен на получение сообщений электронной почты с использованием протоколов, отличных от протокола POP3 (например, IMAP4), антиспам BitDefender не проверяет их на предмет спама.

Замечание

POP3 является одним из наиболее широко используемых протоколов для загрузки сообщений электронной почты с почтового сервера.Если вы не знаете, какой протокол использует ваш почтовый клиент для загрузки сообщений электронной почты, спросите того, кто настроил его.

- BitDefender Internet Security 2011 не проверяет трафик POP3 программы Lotus Notes.

Также следует проверить следующие возможные причины:

1. Убедитесь, что антиспам включен.
   a. Откройте BitDefender.
   b. Нажмите кнопку **Параметры** в верхнем правом углу окна и выберите **Установки**.
   c. Проверьте статус антиспама в настройках безопасности.

   Если антиспам выключен, это может быть причиной вашей проблемы.Включите антиспам и проконтролируйте его работу, чтобы проверить, решается ли проблема.

2. Маловероятно, что вы захотите проверить, настроили ли вы (или кто-либо еще) BitDefender, чтобы не отмечать спам-сообщения как [спам].
   a. Откройте BitDefender, нажмите **Параметры** в верхнем правом углу окна и выберите интерфейс **Эксперт**.
   b. Нажмите **Антиспам** в меню слева, затем вкладку **Настройки**.
   c. Убедитесь, что параметр **Помечать спам в теме сообщения** выбран.

Возможным решением может быть переустановка продукта. Однако вместо этого вы можете обратиться за поддержкой в BitDefender, как описано в разделе «*Поддержка*» (p. 212).

33.13. Сбой удаления BitDefender

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

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

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

Для получения дополнительной информации перейдите к *«Полное удаление BitDefender.»* (p. 222).

Если эта информация не помогла, вы можете обратиться в поддержку BitDefender, как указано в секции *«Поддержка»* (p. 212).

34. Удаление вредоносного ПО из системы

Вредоносные программы могут влиять на работу системы различными способами. Работа BitDefender зависит от типа атаки вредоносного ПО.Вследствие того, что поведение вирусов часто изменяется, определить единый шаблон их поведения и действий довольно сложно.

В отдельных случаях BitDefender не удается автоматически удалить вирусы из системы.В таких случаях требуется вмешательство пользователя.

Если проблема не описана в этом разделе или предлагаемые решения не подходят для ее устранения, обратитесь в службу технической поддержки BitDefender (контактные данные приведены в тексте главы) «*Поддержка*» (p. 212).

34.1. Диск-реаниматор BitDefender

Функция **BitDefender Rescue CD** доступна на большинстве установочных CD BitDefender. С помощью этой функции можно выполнить сканирование и лечение всех существующих жестких дисков перед загрузкой операционной системы.Таким образом можно сохранить данные с зараженного компьютера Windows на съемный носитель.

Если у вас нет BitDefender Rescue CD, его можно загрузить в виде ISO-образа отсюда:

http://download.bitdefender.com/rescue_cd/

Загрузите файл с расширением ISO и запишите его на CD или DVD с помощью любого из доступных инструментов.

Сканирование системы с помощью BitDefender Rescue CD

Для сканирования системы с помощью BitDefender Rescue CD выполните следующие действия:

1. Настройка BIOS компьютера для загрузки с CD.
2. Вставьте CD в дисковод и перезагрузите компьютер.
3. Дождитесь, пока отобразится экран BitDefender, и выберите **Запустить BitDefender Rescue CD** с выбранными языковыми настройками.
4. Дождитесь завершения процесса загрузки. Это может занять некоторое время.
5. По завершении процесса загрузки сигнатуры BitDefender обновляются автоматически и выполняется запуск сканирования всех обнаруженных разделов жесткого диска.

Сохранение данных с помощью BitDefender Rescue CD

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.

Чтобы сохранить данные с компьютера на съемный носитель (например, USB-носитель), выполните следующие действия:

1. Настройка BIOS компьютера для загрузки с CD.
2. Вставьте CD в дисковод и перезагрузите компьютер.
3. Дождитесь, пока отобразится экран BitDefender, и выберите **Запустить BitDefender Rescue CD** с выбранными языковыми настройками.
4. Дождитесь завершения процесса загрузки. Это может занять некоторое время.
5. По завершении процесса загрузки сигнатуры BitDefender обновляются автоматически и выполняется запуск сканирования всех обнаруженных разделов жесткого диска.

   Разделы диска отображаются на рабочем столе. Для просмотра содержимого диска в окне, аналогичном окну проводника Windows, дважды щелкните на выбранном диске.

   Замечание

   В BitDefender Rescue CD используются имена разделов, принятые в Linux. Диски, не размеченные ранее под Windows, будут отображаться с именем `[LocalDisk-0]`, что, вероятно, соответствует имени раздела в Windows `(C:)` или `[LocalDisk-1]`, что соответствует `(D:)`, и так далее.

6. Вставьте съемный носитель в USB-порт компьютера.Через несколько секунд откроется окно, в котором отобразится содержимое устройства.
7. Вы можете копировать файлы и папки так же, как обычно делаете это в Windows.

Если эта информация не помогла, вы можете обратиться в поддержку BitDefender, как указано в секции *«Поддержка»* (p. 212).

34.2. Действия в случае обнаружения BitDefender вирусов на компьютере

Обнаружить в компьютере вирус можно одним из следующих способов:

- Выполнено сканирование компьютера. BitDefender обнаружил зараженные элементы.

- Оповещение о вирусе сообщает о блокировке BitDefender одного или нескольких вирусов, проникших в компьютер.

В такой ситуации необходимо обновить BitDefender для получения последних доступных вирусных сигнатур, после чего запустить глубокое сканирование системы.

По завершении глубокого сканирования выберите действие, которое будет выполняться для зараженных файлов ("Лечить", "Удалить", "Переместить в карантин").

Внимание

Если вы считаете, что этот файл является частью операционной системы Windows, или сомневаетесь в том, что файл заражен вирусом, выполните следующие действия и как можно скорее свяжитесь со службой поддержки клиентов BitDefender.

Если выбранное действие не может быть выполнено и в журнале сканирования отображаются сведения об обнаруженном вирусе, который невозможно удалить, необходимо удалить файл(ы) вручную:

Первый метод можно использовать в нормальном режиме:

1. Отключить антивирусную защиту BitDefender в режиме реального времени.Инструкции для этой процедуры см. в «*Включение и отключение защиты в режиме реального времени*» (p. 223).
2. Отображать скрытые объекты в Windows.Инструкции для этой процедуры см. в «*Отображение скрытых объектов в Windows*» (p. 223).
3. Перейдите в папку, где находится зараженный файл (проверьте журнал сканирования), и удалите этот файл.
4. Включить антивирусную защиту BitDefender в режиме реального времени.

В случае, если с помощью первого способа удалить вирус не удалось, выполните следующие действия:

1. Перезагрузите систему и запустите безопасный режим.Инструкции для этой процедуры см. в «*Перезагрузка компьютера в безопасном режиме*» (p. 221).
2. Отображать скрытые объекты в Windows.
3. Перейдите в папку, где находится зараженный файл (проверьте журнал сканирования), и удалите этот файл.
4. Перезагрузите систему и запустите нормальный режим.

Если эта информация не помогла, вы можете обратиться в поддержку BitDefender, как указано в секции «*Поддержка*» (p. 212).

34.3. Как удалить вирус из архива?

Архив представляет собой файл или набор файлов, сжатых в специальном формате в целях уменьшения пространства на диске, требуемого для хранения файлов.

Некоторые из этих форматов являются открытыми, что дает BitDefender возможность просканировать их изнутри и выполнить после этого соответствующие действия для их удаления.

Другие форматы архивов являются частично или полностью закрытыми. BitDefender может только обнаруживать присутствие в них вирусов, не выполняя каких-либо дополнительных действий.

В тех случаях, когда BitDefender выводит уведомление об обнаружении вируса в архиве, не предлагая доступных действий, это означает, что удаление вируса невозможно из-за ограничений, установленных для настроек разрешений архива.

Удалить вирус из архива можно следующим образом:

1. Выявление архива, содержащего вирус, посредством глубокого сканирования системы.
2. Отключить антивирусную защиту BitDefender в режиме реального времени.
3. Перейдите в папку, содержащую архив, и распакуйте его с помощью приложения архивирования (например, WinZip).
4. Найдите зараженный файл и удалите его.
5. Чтобы полностью удалить вирус, удалите исходный архив.
6. Выполните повторное сжатие файлов в новый архив с помощью приложения архивирования (например, WinZip).
7. Включите антивирусную защиту BitDefender в режиме реального времени и запустите глубокое сканирование системы, чтобы проверить систему на наличие других вирусов.

Замечание

Обратите внимание на то, что вирус, содержащийся в архиве, не представляет собой непосредственной угрозы системе, поскольку для заражения системы необходимо, чтобы вирус был распакован и исполнен.

Если эта информация не помогла, вы можете обратиться в поддержку BitDefender, как указано в секции «*Поддержка*» (p. 212).

34.4. Удаление вируса из архива электронной почты.

BitDefender также может выполнять поиск вирусов в базах данных электронной почты и архивах электронной почты, сохраненных на диске.

В отдельных случаях требуется найти зараженное сообщение, используя данные отчета о сканирования, и удалить его вручную.

Удалить вирус из архива электронной почты можно следующим способом:

1. Сканирование базы данных электронной почты с помощью BitDefender.
2. Отключить антивирусную защиту BitDefender в режиме реального времени.
3. Откройте отчет о сканировании и выполните поиск инфицированных сообщений для почтовом клиенте, используя идентификационные данные (тема, адресат, отправитель).
4. Удалить зараженные сообщения.В большинстве клиентов электронной почты удаленные сообщения также перемещаются в папку восстановления, откуда их можно восстановить.Необходимо проверить, чтобы сообщение было также удалено из папки восстановления.
5. Сжать папку, в которой хранится зараженное сообщение.
   - В Outlook Express:В меню "Файл" нажмите "Папка" и выберите "Сжать все папки".
   - В Microsoft Outlook:В меню "Файл" выберите "Управление файлами данных".Выберите файлы личных папок (PST), которые требуется сжать, и нажмите "Настройки".Нажмите "Сжать".
6. Включить антивирусную защиту BitDefender в режиме реального времени.

Если эта информация не помогла, вы можете обратиться в поддержку BitDefender, как указано в секции *«Поддержка»* (p. 212).

34.5. Сканирование компьютера в безопасном режиме

Ручное сканирование BitDefender позволяет сканировать конкретную папку или диск без создания задания сканирования.

Эта функция разработана для использования в безопасном режиме Windows.

Если ваша система заражена устойчивым вирусом, который не удается удалить в нормальном режиме, попробуйте удалить его, запустив Windows в безопасном режиме и просканировав все жесткие диски с помощью функции сканирования вручную BitDefender.

Сведения о загрузке системы в безопасном режиме см. в *«Перезагрузка компьютера в безопасном режиме»* (p. 221).

1. Для сканирования компьютера с помощью BitDefender, используя функцию сканирования вручную, перейдите по следующему пути из меню Windows "Пуск": **Пуск → Программы → BitDefender 2011 → Сканирование BitDefender вручную**.
2. Нажмите **Добавить папку**, чтобы выбрать объект для сканирования. Откроется новое окно.
3. Выберите объект сканирования:
   - чтобы выполнить сканирование рабочего стола, выберите **Рабочий стол**.
   - чтобы сканировать весь жесткий диск, выберите его в папке **Мой компьютер**.
   - для сканирования конкретной папки необходимо найти и выделить ее.
4. Для запуска сканирования нажмите **OK** и **Продолжить**.
5. Следуйте подсказкам мастера сканирования на антивирусы.

34.6. Действия в случае обнаружения BitDefender вируса в заведомо надежном файле

В этих случаях BitDefender ошибочно помечает легитимные файлы как вирусы (ложноположительное обнаружение).Чтобы исправить эту ошибку, добавьте файл в область исключений BitDefender:

1. Отключить антивирусную защиту BitDefender в режиме реального времени.Инструкции для этой процедуры см. в «*Включение и отключение защиты в режиме реального времени*» (p. 223).
2. Отображать скрытые объекты в Windows.Инструкции для этой процедуры см. в «*Отображение скрытых объектов в Windows*» (p. 223).
3. Восстановление файла из области карантина.
4. Вставьте файл в область исключений.
5. Включить антивирусную защиту BitDefender в режиме реального времени.

Если эта информация не помогла, вы можете обратиться в поддержку BitDefender, как указано в секции «*Поддержка*» (p. 212).

34.7. Удаление зараженных файлов из папки System Volume Information

Папка System Volume Information — это зона жесткого диска, созданная операционной системой, которую Windows использует для хранения критической информации о конфигурации системы.

Ядра BitDefender способны распознавать любые зараженные файлы, хранящиеся в папке System Volume Information. Тем не менее, поскольку эта папка является защищенной областью, удалить файлы из нее не всегда возможно.

Зараженные файлы, обнаруженные в папках, содержащих данные восстановления системы, будут отображаться в журнале сканирования следующим образом:

```
?:\System Volume Information\_restore{B36120B2-BA0A-4E5D-…
```

Для незамедлительного полного удаления зараженных файлов из хранилища данных необходимо отключить и снова включить функцию восстановления системы.

При отключении функции восстановления системы все точки восстановления будут удалены.

При повторном включении функции восстановления системы создаются новые точки восстановления в соответствии с требованиями расписания и событий.

Для отключения функции восстановления системы выполните следующие действия:

- **Для Windows XP:**
  1. Перейдите по следующему пути: **Пуск** → **Программы** → **Служебные** → **Инструменты системы** → **Восстановление системы**
  2. Выберите **Настройки восстановления системы** в левой части окна.
  3. Установите флажок **Отключить восстановление системы** для всех дисков и нажмите **Применить**.
  4. Когда отобразится предупреждение об удалении всех существующих точек восстановления, нажмите **Да** для продолжения.
  5. Чтобы включить функцию восстановления системы, необходимо снять флажок **Отключить восстановление системы** для всех дисков и нажать **Применить**.
- **Для Windows Vista:**
  1. Перейдите по следующему пути: **Пуск** → **Панель управления** → **Система и обслуживание** → **Система**
  2. В левой области окна выберите **Защита системы**.

     Если система требует ввода пароля администратора или подтверждения, введите пароль или предоставьте подтверждение.
  3. Чтобы отключить функцию восстановления системы, снимите флажки, соответствующие каждому из дисков, и нажмите **OK**.

4. Чтобы включить функцию восстановления системы, установите флажки, соответствующие каждому из дисков, и нажмите **OK**.

- **Для Windows 7:**

1. Нажмите **Пуск**, щелкните правой кнопкой на значке **Компьютер** и выберите **Свойства**.
2. Перейдите по ссылке **Защита системы** в левой области окна.
3. В разделе параметров **Защита системы** выделите каждую букву диска и нажмите **Настроить**.
4. Выберите **Отключить защиту системы** и нажмите **Применить**.
5. Нажмите **Удалить**, затем, когда отобразится соответствующий запрос, выберите **Продолжить**, после чего нажмите **OK**.

Если эта информация не помогла, вы можете обратиться в поддержку BitDefender, как указано в секции «*Поддержка*» (p. 212).

34.8. Поиск файлов, защищенных паролем, в журнале сканирования

Это просто уведомление, сообщающее о том, что обнаруженные BitDefender файлы защищены паролем или другим типом шифрования.

Чаще всего паролем защищаются следующие элементы:

- Файлы, относящиеся к другому решению безопасности.
- Файлы, которые являются частью операционной системы.

В целях фактического сканирования содержимого эти файлы должны быть извлечены или иным образом дешифрованы.

При извлечении этого содержимого сканер BitDefender в режиме реального времени автоматически выполнит его сканирование в целях обеспечения защиты компьютера.Чтобы просканировать эти файлы с помощью BitDefender, необходимо связаться с поставщиком продукта для получения дополнительной информации о файлах.

Рекомендуется пропустить эти файлы, поскольку они не представляют угрозы для системы.

34.9. Элементы с пометкой "Пропущено" в журнале сканирования.

Все файлы, отображаемые в отчете о сканировании с пометкой "Пропущено", не заражены.

В целях улучшения производительности BitDefender не сканирует файлы, которые не были изменены с момента выполнения последнего сканирования.

34.10. Поиск файлов с избыточным сжатием в журнале сканирования

Элементами с чрезмерным сжатием называются те элементы, которые сканер не может извлечь, либо элементы, дешифрование которых занимает слишком много времени, в результате чего система становится нестабильной.

"Чрезмерное сжатие" означает, что BitDefender пропустил этот архив при сканировании, поскольку для его распаковки потребовался бы слишком большой объем системных ресурсов. При необходимости содержимое такого архива будет сканироваться при доступе к нему в режиме реального времени.

34.11. Почему BitDefender автоматически удалил зараженный файл?

При обнаружении зараженного файла BitDefender автоматически попытается вылечить его.Если файл не удается вылечить, он перемещается в карантин в целях предотвращения распространения вируса.

В случае определенных типов вредоносных программ лечение невозможно, поскольку вредоносным является весь обнаруженный файл. В таких случаях выполняется удаление зараженного файла с диска.

Такая ситуация характерна для файлов установки, загружаемых с ненадежных веб-сайтов.В этой ситуации рекомендуется загрузить установочный файл с веб-сайта производителя или с другого доверенного веб-сайта.

35. Поддержка

BitDefender стремится предоставить своим клиентам быструю и грамотную техподдержку.При возникновении проблем или вопросов, связанных с работой BitDefender, для быстрого поиска решений или ответов доступны несколько интернет-ресурсов.При необходимости можно обратиться в службу поддержки клиентов BitDefender. Представители службы поддержки быстро ответят на все вопросы и окажут необходимую помощь.

35.1. Онлайн-ресурсы

Для устранения проблем и разрешения вопросов, связанных с BitDefender, доступен ряд интернет-ресурсов.

- База знаний BitDefender:http://www.bitdefender.com/help
- Форум техподдержки BitDefender:http://forum.bitdefender.com
- портал компьютерной безопасности Malware City:http://www.malwarecity.com
- видеоруководства

Также можно воспользоваться поисковой системой для получения дополнительных сведения о компьютерной безопасности, продуктах BitDefender и компании.

35.1.1. База знаний BitDefender

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

База знаний BitDefender открыта для всех и снабжена поисковыми средствами, позволяющими легко найти ответ на интересующую вас проблему. Этот ценный массив информации является еще одним источником технических знаний и экспертных решений для клиентов BitDefender. Все обоснованные информационные запросы и отзывы о найденных программных ошибках, поступившие от клиентов BitDefender своевременно находят свое место в базе знаний BitDefender: в виде отчетов об устранении программных ошибок, обновлениях для максимального устранения недоделок и информационных материалов/статей, дополняющих файлы справки программного продукта.

База знаний BitDefender доступна круглосуточно по адресу http://kb.bitdefender.com.

35.1.2. Форум техподдержки BitDefender

Форум техподдержки BitDefender предоставляет пользователям BitDefender простой способ не только получить необходимую помощь, но и помочь другим.

В случае некорректной работы продукта BitDefender (продукт не может удалить отдельные вирусы с компьютера) или возникновения вопросов относительно работы продукта вы можете опубликовать описание проблемы или свой вопрос на форуме.

Специалисты службы технической поддержки BitDefender отслеживают новые сообщения на форуме, что позволяет своевременно реагировать на все вопросы пользователей. На форуме также есть возможность получить ответ или узнать о способах решения проблемы от более опытных пользователей BitDefender.

Перед публикацией своего сообщения о проблеме или вопроса выполните поиск похожих или связанных тем в форуме.

Форум техподдержки BitDefender доступен по адресу http://forum.bitdefender.com на пяти различных языках: английском, немецком, французском, испанском и румынском.Нажмите на ссылку **Защита для дома и офиса**, чтобы перейти в раздел потребительских товаров.

35.1.3. Портал Malware City

Портал Malware City представляет собой наиболее полный источник информации о компьютерной безопасности. Здесь можно найти сведения о различных угрозах, которым подвергается компьютер при подключении к Интернету (вредоносное ПО, фишинговые атаки, спам, киберпреступность).В словаре разъясняются значения терминов компьютерной безопасности, которые незнакомы пользователю.

Для информирования пользователей о последних вирусах, текущих тенденциях развития систем безопасности и других событиях в отрасли компьютерной безопасности регулярно публикуются новые статьи.

Веб-страница Malware City: http://www.malwarecity.com.

35.1.4. Видеоруководства

Видеоруководства предоставляют пошаговые инструкции по процедуре настройки продукта.Они составлены в простом предельно четком стиле, что позволяет ясно изложить смысл сообщения.

Основная цель — обеспечить удобство использования путем предоставления базовой и дополнительной информации о принципах построения систем безопасности, настройке и использовании BitDefender.

Основная цель — обеспечить специализированную поддержку посредством видеоруководств по использованию продукта, в которых приведена информация непосредственно об использовании и настройке BitDefender.

Например, вместо того, чтобы звонить в службу техподдержки BitDefender для получения инструкций или пытаться самостоятельно выполнить сложные процедуры, можно просто ознакомиться с видеоруководством и выполнить представленные в нем пошаговые инструкции.

35.2. Обращение за помощью

В разделе **Поиск и устранение неполадок и помощь** представлена необходимая информация о наиболее часто встречающихся проблемах, с которыми пользователь может столкнуться при использовании продукта.

Если не удалось найти решение проблемы в доступных источниках, вы можете связаться с нами:

- «Свяжитесь с нами непосредственно через интерфейс продукта BitDefender» (p. 214)
- «Свяжитесь с нами через онлайн-базу знаний» (p. 215)

Важно

Для обращения в службу поддержки клиентов BitDefender необходимо предварительно активировать продукт BitDefender.Для получения дополнительной информации перейдите к *«Регистрация и моя учетная запись»* (p. 54).

Свяжитесь с нами непосредственно через интерфейс продукта BitDefender

При наличии работоспособного подключения к Интернету (доступа в Интернет) вы можете обратиться за помощью в службу поддержки клиентов BitDefender непосредственно из интерфейса продукта (окно программы).

Обратиться за техподдержкой можно с помощью интегрированных инструментов поддержки, доступных в интерфейсе продукта.

Для использования возможностей встроенной справки выполните следующие действия:

1. Откройте BitDefender.
2. Перейдите по ссылке **Справка и поддержка** в правом нижнем углу окна.

3. Теперь доступны два параметра:
   - Чтобы найти нужную информацию, запустите поиск по нашей базе данных.
   - Выберите отдел в соответствии с типом возникшей проблемы.

     Служба поддержки клиентов занимается вопросами, связанными с покупкой, лицензиями, возвратами и продлением.

     Техническая поддержка распространяется на проблемы, связанные непосредственно с продуктом и его работоспособностью.

     Борьба с вредоносным ПО — эта функция служит для разрешения вопросов, связанных с вирусами.
4. Ознакомьтесь с содержанием соответствующих статей или документов и попробуйте предложенные варианты решений.
5. Если решить проблему этим способом не удалось, воспользуйтесь ссылкой, приведенной в статье, для запуска инструмента поддержки.
6. Укажите свой адрес электронной почты, выберите нужный отдел и предоставьте краткое описание проблемы.

   Нажмите **Далее**.
7. Подождите несколько минут, пока BitDefender выполнит сбор сведений о продукте. Эта информация поможет нашим техническим специалистам найти эффективное решение вашей проблемы.

   Нажмите **Далее**.
8. Нажмите **Завершить**, чтобы отправить данные в службу поддержки клиентов BitDefender. В ближайшее время с вами свяжется представитель службы поддержки.

Свяжитесь с нами через онлайн-базу знаний

Если не удается найти требуемые сведения посредством продукта BitDefender, обратитесь к нашей базе знаний в Интернете:

1. Перейдите к http://www.bitdefender.com/help.База знаний BitDefender включает в себя статьи, содержащие решения проблем, связанных с BitDefender.
2. Поищите в базе знаний BitDefender статьи, которые могут помочь вам решить вашу проблему.
3. Ознакомьтесь с содержанием соответствующих статей или документов и попробуйте предложенные варианты решений.
4. Если решить проблему этим способом не удалось, воспользуйтесь ссылкой, приведенной в статье, для обращения в службу поддержки клиентов BitDefender.

5. Свяжитесь с техподдержкой BitDefender по электронной почте или телефону.

36. 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 предвосхищения их ожиданий и постоянного улучшения связи с ними. Мы будем рады ответить на все ваши вопросы и решить ваши проблемы – без колебаний обращайтесь к нам за помощью.

36.1. Адреса веб-сайтов

Отдел продаж: sales@bitdefender.com
Техническая поддержка:www.bitdefender.com/help
Документация: documentation@bitdefender.com
Партнерские программы: partners@bitdefender.com
Маркетинг: marketing@bitdefender.com
Отдел по связям со СМИ: pr@bitdefender.com
Вакансии: jobs@bitdefender.com
Лаборатория для вирусов: virus_submission@bitdefender.com
Лаборатория для спама: spam_submission@bitdefender.com
Жалобы: abuse@bitdefender.com
Веб-сайт продукта:http://www.bitdefender.com
FTP-архивы продукта:ftp://ftp.bitdefender.com/pub
Местные дистрибуторы:http://www.bitdefender.com/site/Partnership/list/
База знаний BitDefender:http://kb.bitdefender.com

36.2. Местные дистрибуторы

Местные дистрибьюторы BitDefender готовы ответить на все вопросы коммерческого и общего характера, находящиеся в их компетенции.

Поиск дистрибутора BitDefender в вашей стране:

1. Перейдите к http://www.bitdefender.com/site/Partnership/list/.
2. Контактные данные местных дистрибуторов BitDefender должны отобразиться автоматически. Если этого не произошло, воспользуйтесь инструментом поиска партнеров в меню слева, чтобы выбрать свой регион и страну.
3. Если не удалось найти дистрибутора BitDefender в вашей стране, свяжитесь с нами по адресу электронной почты sales@bitdefender.com.Указывайте адрес электронной почты на английском языке, чтобы мы смогли своевременно обработать ваш вопрос.

36.3. Офисы BitDefender

Сотрудники компании, ответственные за BitDefender, ответят на ваши запросы коммерческого и общего характера, относящейся к сфере их деятельности и географической привязке. Ниже приведены адреса и контактная информация.

США

BitDefender, LLC
PO Box 667588
Pompano Beach, Fl 33066
Телефон (офис и продажи): 1-954-776-6262
Продажи: sales@bitdefender.com
Техническая поддержка: http://www.bitdefender.com/help
Сайт: http://www.bitdefender.com

Германия

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

Великобритания и Ирландия

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

Испания

BitDefender España, S.L.U.
Avda. Diagonal, 357, 1º 1ª
08037 Barcelona
Факс: +34 93 217 91 28
Телефон: +34 902 19 07 65

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

Россия и страны СНГ (кроме Украины)

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

37. Полезная информация

В этой главе представлены некоторые важные процедуры, о которых необходимо знать перед поиском и устранением технических неисправностей.

Для поиска и устранения технических неполадок BitDefender необходимо знание специфики ОС Windows. Таким образом, следующие шаги относятся в основном к операционной системе Windows.

37.1. Удаление других решений безопасности

Главная цель использования решений безопасности — обеспечение защиты и безопасности данных.Что происходит, если на компьютере установлено несколько решений безопасности?

Одновременное использование нескольких решений безопасности на компьютере приводит к нестабильности системы.Установщик BitDefender Internet Security 2011 автоматически распознает другое программное обеспечение безопасности и предлагает удалить его.

Если другие решения безопасности не были удалены во время исходной установки, выполните следующие действия:

- Для **Windows XP**:
  1. Нажмите **Пуск**, перейдите в раздел **Панель управления** и дважды щелкните мышью элемент **Установка и удаление программ**.
  2. Подождите несколько секунд, пока не отобразится список установленного программного обеспечения.
  3. Найдите имя программы, которую следует удалить, и выберите **Удалить**.
  4. Дождитесь завершения процесса удаления, после чего выполните перезагрузку системы.
- Для **Windows Vista** и **Windows 7**:
  1. Нажмите **Пуск**, перейдите в раздел **Панель управления** и дважды щелкните мышью элемент **Программы и функции**.
  2. Подождите несколько секунд, пока не отобразится список установленного программного обеспечения.
  3. Найдите имя программы, которую следует удалить, и выберите **Удалить**.
  4. Дождитесь завершения процесса удаления, после чего выполните перезагрузку системы.

Если удалить другое решение безопасности не удалось, загрузите инструмент удаления с веб-сайта поставщика такого решения или обратитесь

непосредственно в службу поддержки поставщика для получения инструкций по удалению.

37.2. Перезагрузка компьютера в безопасном режиме

Безопасный режим представляет собой операционный диагностический режим, который используется в основном для поиска и устранения неисправностей, негативно влияющих на нормальную работу Windows.Проблема такого типа может быть вызвана любыми причинами — от конфликта драйверов до вирусов, препятствующих нормальной загрузке Windows.В безопасном режиме могут работать только некоторые приложения, Windows загружает только основные драйвера и минимум компонентов операционной системы.Именно поэтому большинство вирусов неактивны при работе Windows в безопасном режиме и их можно легко удалить.

Запуск Windows в безопасном режиме:

1. Перезагрузите компьютер.
2. Для перехода в корневое меню несколько раз нажмите на клавишу **F8** до того, как загрузится Windows.
3. В корневом меню выберите **Безопасный режим** и нажмите **Ввод**.
4. Дождитесь завершения загрузки Windows в безопасном режиме
5. По завершении процесса выводится сообщение подтверждения.Нажмите **OK** для подтверждения.
6. Для запуска Windows в нормальном режиме просто перезагрузите систему.

37.3. Определение используемой версии Windows (32- или 64-разрядная)

Чтобы узнать, какая операционная система установлена на компьютере (32- или 64-разрядная), выполните следующие действия:

- Для **Windows XP**:
  1. Нажмите **Пуск**.
  2. Найдите элемент **Мой компьютер** в меню **Пуск**.
  3. Щелкните правой кнопкой мыши элемент **Мой компьютер** и выберите **Свойства**.
  4. Если под заголовком **Система** отображается **x64 Edition**, это означает, что на компьютере установлена 64-разрядная версия Windows XP.

     Если пометка **x64 Edition** не отображается, это означает, что на компьютере установлена 32-разрядная версия Windows XP.

- Для **Windows Vista** и **Windows 7**:
  1. Нажмите **Пуск**.
  2. Найдите элемент **Компьютер** в меню **Пуск**.
  3. Щелкните правой кнопкой мыши **Компьютер** и выберите **Свойства**.
  4. Войдите в раздел **Система** для просмотра сведений о системе.

37.4. Просмотр сведений о настройках прокси-сервера.

Чтобы найти эти настройки, выполните следующие действия:

- Для Internet Explorer 8:
  1. Откройте Internel Explorer.
  2. Выберите **Сервис** > **Свойства обозревателя**.
  3. На вкладке **Подключения** выберите **Настройки LAN**.
  4. В разделе **Использовать прокси-сервер для LAN** вы увидите **Адрес** и **Порт** прокси-сервера.
- Для Mozilla Firefox 3.6:
  1. Откройте Firefox.
  2. Выберите **Инструменты** > **Параметры**.
  3. На вкладке **Дополнительно** выберите вкладку **Сеть**.
  4. Нажмите **Настройки**.
- Для Opera 10.51:
  1. Откройте Opera.
  2. Выберите **Инструменты** > **Установки**.
  3. На вкладке **Дополнительно** выберите вкладку **Сеть**.
  4. Нажмите кнопку **Прокси-серверы**, чтобы открыть диалоговое окно настроек прокси-сервера.

37.5. Полное удаление BitDefender.

Выполните следующие действия для корректного удаления BitDefender:

1. Перейдите к www.bitdefender.com/uninstall и загрузите инструмент удаления на ваш компьютер.
2. Запустить инструмент удаления, используя права администратора.
3. Перезагрузите компьютер.

37.6. Включение и отключение защиты 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 служб мгновенных сообщений (ICQ, NetMeeting, Yahoo Messenger, MSN Messenger).

Защита BitDefender в режиме реального времени, как правило, включена, и отключать ее не рекомендуется.

При поиске и устранении неисправностей или удалении вируса может потребоваться отключить защиту в режиме реального времени. Таким образом, разрешается одна из следующих ситуаций:

- Снижение быстродействия системы после установки BitDefender
- Некорректная работа одной из программ или приложений после установки BitDefender
- Сообщения об ошибках, которые могли отображаться непосредственно после установки BitDefender

Чтобы временно включить или отключить защиту в режиме реального времени, выполните следующие действия:

1. Откройте BitDefender, нажмите **Параметры** в верхнем правом углу окна и выберите интерфейс **Эксперт**.
2. Перейдите в раздел **Антивирус** > **Щит**.
3. Снимите флажок **Защита в режиме реального времени включена**, чтобы временно отключить антивирусную защиту (или установите этот флажок, если требуется включить защиту).
4. Необходимо подтвердить выбор. Для этого в меню следует выбрать период, на который требуется отключить защиту в режиме реального времени.

Замечание

Последовательность действий для отключения защиты в режиме реального времени BitDefender рекомендуется использовать исключительно в качестве временной меры и только на короткий период времени.

37.7. Отображение скрытых объектов в Windows

Эти инструкции полезны для устранения вредоносного ПО в тех случаях, когда необходимо найти и удалить скрытые зараженные файлы.

Для отображения скрытых объектов в Windows выполните следующие действия:

1. Нажмите **Пуск**, перейдите на вкладку **Панель управления** и выберите **Параметры папки**.
2. Перейдите на вкладку **Просмотр**.
3. Выберите **Показать содержимое системных папок** (только для Windows XP).
4. Выберите **Отображать скрытые файлы и папки**.
5. Снимите флажок **Скрывать расширения для зарегистрированных типов файлов**.
6. Снимите флажок **Скрывать защищенные файлы операционной системы**.
7. Нажмите **Применить**, затем нажмите **ОК**.

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 вопросы и отвечать на них, "нажимать" на кнопки и другими способами 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 ее использование в сети Интернет.

Рекламное ПО

Рекламное ПО часто устанавливается в качестве "нагрузки" к основным приложениям, которые предоставляются бесплатно, при условии что пользователь соглашается установить программу. Поскольку рекламные 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, информация, собираемая некоторыми из этих приложений, может показаться недопустимой для разглашения для тех пользователей, которые недостаточно полно изучили условия лицензионного соглашения.

Архив

Диск или каталог, содержащие запасные файлы.

Файл, содержащий один или несколько файлов в сжатом формате.

Лазейки в системе

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 отображает на экране веб-страницы. Два самых популярных браузера — это Netscape Navigator и Microsoft Internet Explorer. Это графические браузеры, то есть они отображают и изображения, и текст. Кроме того, большинство современных браузеров могут предоставлять мультимедийную информацию, в том числе звук и видео, хотя и требуют установки дополнительных программ и оборудования (plug-ins).

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

Cookie
В сфере интернет-технологий под файлами истории обращений (cookie) 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 мышью. Понятно, почему сейчас так широко обсуждается конфиденциальность данных пользователей и многие чувствуют себя ущемленными в своих правах, будучи уверенными, что их "считывают", как кассир в магазине считывает штрих-код на этикетке. Порой эта точка зрения кажется крайностью, но иногда она полностью отражает действительность.

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

Дисковод считывает данные и записывает их на жесткие диски.

Накопитель на гибких магнитных дисках 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 на периферийное устройство. Обычно этот термин используется по отношению к копированию файла из источника в сети на свой компьютер. Загрузкой также называют копирование файла с сетевого файлового сервера на компьютер в сети.

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

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

Ложное срабатывание
Событие "ложная тревога" появляется, когда программа считает зараженным файл, который таковым на самом деле не является.

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

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

Эвристический метод
Способ обнаружения новых вирусов, основанный на правилах. Этот способ проверки не связан напрямую с определенными образами вирусов. Преимущество эвристической проверки состоит в том, что новый вирус не может обмануть фильтр. Однако он может принять подозрительный код в обычных программах за вирус и выдать так называемое "ложное срабатывание".

IP
Сокращение от Internet Protocol (интернет-протокол) — маршрутизируемый протокол семейства TCP/IP, отвечающий за адресацию, маршрутизацию, фрагментацию и повторную компоновку IP-пакетов.

Прикладная мини-программа Java-апплет
Это программа, написанная на языке Java, работающая только на страницах в сети. Чтобы использовать апплет на странице, вы должны указать 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 мини-программа 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.

Макровирус

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 каждый раз, когда вы открываете документ.

Почтовый клиент

Приложение, которое позволяет вам отправлять и получать электронную почту.

Память

Внутренние устройства хранения информации. Термин "память" относится к запоминающему устройству, например микросхеме. Термин "накопитель" относится к таким устройствам, как диски. В каждом компьютере изначально есть физическая память, называемая оперативной (основной) памятью или RAM.

Неэвристический 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, после чего 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 пробела и количеством замененных пробелов. В этом случае десять пробелов займут всего лишь два байта. И это только один из многих методов архивации файлов.

Путь

Точное местоположение файла на компьютере. Это местоположение обычно описывается средствами иерархической файловой системы сверху вниз.

Маршрут между двумя объектами, например канал связи между двумя компьютерами.

Фишинг

Это 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 пользователя 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 карты). Однако на самом деле такого рода веб-сайт является поддельным и создается для кражи конфиденциальной информации пользователей.

Полиморфный вирус

Это 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 количество обнаруженных подозрительных и зараженных файлов.

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,

притом что их присутствие оставалось скрытым для системных администраторов.

Основной целью руткитов является скрытие процессов, файлов, логинов и журналов. 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 скрывают 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

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 нежелательную рассылку электронных писем, часто коммерческого содержания.

Программа-шпион

Это 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 загрузить в Интернете, 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 загрузке 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. Из-за потребления программами-шпионами памяти и системных ресурсов работа последних в фоновом режиме может приводить к неустойчивой работе системы и ее сбоям.

Элементы запуска

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

Область пиктограмм панели задач

Область уведомлений впервые появилась в операционной системе Windows 95. Она расположена на панели задач Windows, обычно в нижней части экрана, рядом с часами, и содержит маленькие значки, 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 мышью на значке.

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, общепринятые правила объединения сетей и трафик маршрутизации.

Троян

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

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

Обновление

Новая версия программного обеспечения или оборудования разработана для замены устаревшей версии этого продукта. Кроме того, многие

обновления часто определяют, установлена ли на компьютере старая версия данного программного продукта. Если нет, обновление невозможно.

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

Вирус

Это 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.

Определение вируса

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

Червь

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