INTERNET SECURITY 2012

Publication date 2011.08.18

Правовые положения


Bitdefender

Содержание

1. Начало работы

После установки Bitdefender Internet Security 2012 компьютер будет защищен от всех типов вредоносных программ (вирусов, шпионских программ и вирусов-троянов) и интернет-угроз (атак хакеров, фишинга и спама).

Режим "Автопилот" включен по умолчанию, и вам не требуется настраивать никакие параметры.Тем не менее, пользователь может воспользоваться возможностями Bitdefender для отладки и повышения эффективности защиты компьютера.

Bitdefender будет принимать за вас большинство решений, связанных с защитой, и вы редко будете видеть всплывающие уведомления.В окне "События" отображается подробная информация о выполненных действиях и работе программы.Для получения дополнительной информации перейдите к «*События*» (p. 7).

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.

Если вы не зарегистрировали продукт (в том числе не создали учетную запись MyBitdefender), не забудьте сделать это до конца пробного периода.Вы можете создать учетную запись, чтобы получить возможность использования онлайн-функций продукта.Дополнительные сведения о процессе регистрации см. в «*Регистрация программы*» (p. 2).

1.1. Открытие Bitdefender

Для входа в главный интерфейс Bitdefender Internet Security 2012 используйте меню Windows "Пуск": нажмите **Пуск → Все программы → Bitdefender 2012 → Bitdefender Internet Security 2012** или дважды щелкните по значку Bitdefender  в области уведомлений.

Дополнительную информацию об окне и значке Bitdefender в области уведомлений см. в «*Интерфейс Bitdefender*» (p. 14).

1.2. Действия по завершении установки

Если необходимо, чтобы Bitdefender принимал все решения, связанные с обеспечением безопасности, оставьте включенным режим "Автопилот".Для получения дополнительной информации перейдите к «*Автопилот*» (p. 8).

Список задач, которые может потребоваться выполнить после установки:

- Если ваш компьютер подключен к Интернету через прокси-сервер, вам необходимо задать настройки прокси-сервера, как описано в разделе «*Как*

настроить Bitdefender для использования прокси-сервера при подключении к Интернету?» (p. 33).

- Если вы уже установили Bitdefender на несколько компьютеров в домашней сети, вы можете управлять всеми продуктами Bitdefender удаленно с одного компьютера.Для получения дополнительной информации перейдите к *«Карта сети»* (p. 108).
- Если у вас есть дети, вы можете использовать функцию родительского контроля для мониторинга и управления их действиями на компьютере и в Интернете.Родительский контроль включен по умолчанию для ограниченных учетных записей пользователей Windows, и применяются правила фильтрации, ориентированные на подростков.Для получения дополнительной информации перейдите к *«Родительский контроль»* (p. 81).
- Создайте правила защиты данных, чтобы исключить возможность разглашения важных личных данных без вашего ведома.Для получения дополнительной информации перейдите к *«Защита данных»* (p. 77).

1.3. Регистрация программы

Чтобы активировать защиту Bitdefender, вам необходимо зарегистрировать продукт, введя лицензионный ключ и создав учетную запись MyBitdefender.

Лицензионный ключ определяет период времени, в течение которого вы можете пользоваться продуктом.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.Для получения дополнительной информации перейдите к *«Приобретение или продление лицензионных ключей»* (p. 5).Если вы используете пробную версию Bitdefender, вам необходимо зарегистрировать ее с помощью лицензионного ключа, если вы хотите продолжить пользоваться продуктом после окончания пробного периода.

Учетная запись MyBitdefender предоставляет доступ к обновлениям продукта и позволяет использовать онлайн-службы, которые предлагает Bitdefender Internet Security 2012.Если у вас уже есть учетная запись, используйте ее для регистрации продукта Bitdefender.

Учетная запись MyBitdefender предоставляет следующие возможности:

- Регулярно обновляйте продукт.
- Возможность восстановления лицензионного ключа в случае его утери.
- Свяжитесь со службой поддержки клиентов Bitdefender.
- Осуществляйте мониторинг за действиями детей и настраивайте параметры родительского контроля, где бы вы ни находились.

- Защитите свою учетную запись Facebook с помощью Safego.

1.3.1. Ввод лицензионного ключа

Если при установке выбран вариант оценки продукта, вы сможете пользоваться им в течение 30-дневного пробного периода.Чтобы продолжить использование Bitdefender после окончания пробного периода, продукт необходимо зарегистрировать с помощью лицензионного ключа.

Чтобы зарегистрировать продукт с помощью лицензионного ключа или изменить существующий лицензионный ключ, нажмите ссылку **Информация о лицензии**, расположенную в нижней части окна Bitdefender.Откроется окно регистрации.

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

Регистрация Bitdefender Internet Security 2012:

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 на ссылку в окне, чтобы перейти на веб-страницу, на которой его можно будет приобрести.

2. Нажмите **Зарегистрировать сейчас**.

1.3.2. Выполнение входа в MyBitdefender

Если при установке вы указали адрес электронной почты, на него было отправлено письмо с подтверждением.Нажмите на ссылку в электронном сообщении, чтобы завершить регистрацию.

Если вы не зарегистрировались, Bitdefender уведомит вас о необходимости выполнения регистрации.

Важно

Необходимо войти в учетную запись в течение 30 дней после установки Bitdefender.В противном случае Bitdefender не будет обновляться.

Чтобы создать учетную запись MyBitdefender или войти в нее, нажмите ссылку **Завершение регистрации** / **MyBitdefender** в нижней части окна Bitdefender.

Откроется окно MyBitdefender.Выполните действия, соответствующие текущей ситуации.

Я хочу создать учетную запись MyBitdefender

Для создания учетной записи MyBitdefender выполните следующие действия:

1. Выберите **Создать новую учетную запись**.

   Появится новое окно.

2. Введите необходимую информацию в соответствующих полях.Информация, которую вы предоставите, останется конфиденциальной.

   - **Имя**: введите имя пользователя для учетной записи. Это поле является необязательным.
   - **Электронная почта**: введите свой адрес электронной почты.
   - **Пароль**: введите пароль для своей учетной записи.Пароль должен содержать не менее 6 символов.
   - **Подтвердите пароль**: повторно введите пароль.
   - Дополнительно Bitdefender может информировать вас о специальных предложениях и бонусах по электронной почте, указанной в вашей учетной записи.Чтобы включить эту возможность, выберите **Я разрешаю Bitdefender отправлять мне сообщения по электронной почте**.

   Замечание

   После создания учетной записи вы сможете использовать этот адрес электронной почты и пароль для входа в свою учетную запись на http://my.bitdefender.com.

3. Нажмите **Подтвердить**.
4. Чтобы использовать учетную запись, сначала необходимо завершить регистрацию.Проверьте почту и следуйте инструкциям в письме подтверждения, полученном от Bitdefender.

Замечание

Вы можете выполнить вход под учетной записью Facebook или Google.Дополнительные сведения см. в«Я хочу войти, используя свою учетную запись Facebook или Google» (p. 4)

Я хочу войти, используя свою учетную запись Facebook или Google

Для выполнения входа под учетной записью Facebook или Google выполните следующие действия:

1. Нажмите на значок службы, которую требуется использовать для входа.Вы будете перенаправлены на страницу входа этой службы.
2. Следуйте инструкциям, предоставленным выбранной службой, чтобы связать свою учетную запись с Bitdefender.

Замечание

Bitdefender не получает доступ к конфиденциальной информации, такой как пароль учетной записи, под которой выполняется вход, и личная информация о ваших друзьях и контактах.

У меня уже есть учетная запись MyBitdefender

Если вы уже выполняли вход в учетную запись из продукта, Bitdefender определит это и осуществит вход в эту учетную запись.Чтобы перейти в учетную запись, на http://my.bitdefender.com нажмите **Перейти в MyBitdefender**.

Если вам необходимо войти под другой учетной записью, нажмите на соответствующую ссылку и следуйте инструкциям, представленным в предыдущих разделах.

Если у вас уже есть активная учетная запись, но Bitdefender не может ее обнаружить, выполните следующие действия, чтобы войти в эту учетную запись:

1. Введите адрес электронной почты и пароль вашей учетной записи в соответствующих полях.

Замечание

Если вы забыли пароль, нажмите ссылку **Забыли пароль?** и следуйте инструкциям по восстановлению пароля.

2. Нажмите **Вход**.

1.3.3. 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.

Bitdefender сообщит о приближении даты окончания действия текущей лицензии. Следуйте инструкциям в полученном уведомлении, чтобы приобрести новую лицензию.

В любое время можно перейти на страницу, на которой можно приобрести лицензионный ключ, выполнив следующие действия:

1. Откройте окно Bitdefender.

2. Нажмите ссылку **Сведения о лицензии** в нижней части окна Bitdefender, чтобы открыть окно регистрации продукта.
3. Нажмите на ссылку в нижней части окна.

1.4. Устранение неисправностей

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.

К обнаруженным проблемам относится отключение важных настроек защиты и другие условия, представляющие угрозу безопасности. Они сгруппированы по двум категориям:

- **Критические проблемы**: не позволяют Bitdefender защищать вашу систему от вредоносного ПО или представляют серьезную угрозу безопасности.
- **Незначительные (некритические) проблемы** могут повлиять на защиту системы в ближайшем будущем.

Изменение цвета значка Bitdefender в области уведомлений свидетельствует о наличии проблем:

Красный цвет: Существуют критические угрозы безопасности системы. Они требуют немедленного вмешательства и решения.

Желтый цвет: Некритические проблемы влияют на безопасность вашей системы. Вам необходимо проверить и исправить их в ближайшее время.

Также можно навести курсор на значок, и всплывающее окно подтвердит наличие имеющихся проблем.

При открытии окна Bitdefender в области состояния безопасности на верхней панели инструментов будет показано количество и тип проблем, влияющих на систему.

1.4.1. Мастер устранения угроз

Чтобы устранить обнаруженные проблемы, следуйте инструкциям мастера **устранения угроз**.

1. Для того чтобы запустить мастер, сделайте следующее:
   - Нажмите правой кнопкой мыши на значок Bitdefender на панели задач и выберите **Устранить все**.В зависимости от обнаруженных проблем значок отображается красным (критические проблемы) или желтым цветом (некритические проблемы).

- Откройте окно Bitdefender и нажмите в любом месте области состояния безопасности на верхней панели инструментов (например, нажмите кнопку **Устранить все**).

2. Вы можете видеть проблемы, подвергающие риску безопасность вашего компьютера и данных.Выбрано устранение всех текущих проблем.

   Если моментальное устранение определенной проблемы не требуется, снимите флажок из соответствующего поля.Вам будет предложено указать период, на который будет отложено устранение этой проблемы.Выберите нужный вариант в меню и нажмите **OK**.Чтобы остановить мониторинг проблем соответствующей категории, выберите **Постоянно**.

   Для проблемы будет установлен статус **Отложить**, и система не будет предпринимать никаких действий по ее исправлению.

3. 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.** При устранении таких проблем мастер поможет вам успешно завершить задачу.

1.4.2. Настройка оповещений о статусе

Можно настроить систему оповещений в соответствии с требованиями безопасности и задать конкретные проблемы, о которых система будет информировать пользователя.Следуйте инструкции:

1. Откройте окно Bitdefender.
2. Нажмите кнопку **Настройки** на верхней панели инструментов.
3. Нажмите **Общие** в меню слева и перейдите на вкладку **Расширенные**.
4. Нажмите ссылку **Настроить оповещения о статусе**.
5. С помощью переключателей можно включить и отключить оповещения о статусе в соответствии с потребностями.

1.5. События

Bitdefender ведет детальный журнал событий, связанных с активностью программы на компьютере (включая действия компьютеров, мониторинг которых осуществляет функция родительского контроля).События являются важным инструментом для мониторинга и управления защитой

Bitdefender.Например, вы можете проверить, было ли успешным последнее обновление, были ли найдены на вашем компьютере вредоносные программы и т. п.Кроме того, при необходимости можно предпринять дополнительные действия или изменить операции, которые выполнил Bitdefender.

Для открытия окна "События" откройте окно Bitdefender и нажмите кнопку **События** на верхней панели инструментов.

Для упрощения фильтрации событий Bitdefender в меню слева предусмотрены следующие категории:

- **Антивирус**
- **Антиспам**
- **Родительский контроль**
- **Защита данных**
- **Брандмауэр**
- **Карта сети**
- **Обновление**
- **Safego**

Список событий доступен для каждой категории.Чтобы просмотреть информацию об определенном событии в списке, нажмите на него. Событие отобразится в нижней части окна.Для каждого события доступна следующая информация: краткое описание, действие, которое выполнил Bitdefender при возникновении события, а также дата и время события.При необходимости могут быть предоставлены варианты выбора дальнейших действий.

События можно фильтровать по важности.Имеется три типа событий, каждый из которых отмечается особым значком:

Информационные события показывают успешно выполненные операции.
Предупреждающие события указывают на некритические проблемы. Их следует просмотреть и исправить, когда у вас появится для этого время.
Критические события указывают на критические проблемы. Их следует проверить незамедлительно.

Чтобы упростить задачу управления зарегистрированными событиями, в каждом разделе окна "События" можно удалить или пометить все события как прочитанные.

1.6. Автопилот

Для пользователей, которым требуется, чтобы система безопасности обеспечивала защиту и не отвлекала, в Bitdefender Internet Security 2012 предусмотрен режим "Автопилот".

Когда режим "Автопилот" включен, Bitdefender применяет оптимальную конфигурацию безопасности и принимает за вас все решения, связанные с

защитой.Это означает, что не будут отображаться всплывающие окна и уведомления и вам не потребуется настраивать никакие параметры.

В режиме "Автопилот" Bitdefender автоматически исправляет критические проблемы и осуществляет управление:

- Антивирусная защита, реализуемая с помощью резидентного и непрерывного сканирования.
- Защита брандмауэра.
- Защита конфиденциальных данных, обеспечиваемая фильтрами фишинга и вредоносных программ, которые применяются при работе в Интернете.
- Автоматические обновления.

По умолчанию режим "Автопилот" включается после завершения установки Bitdefender.Пока режим "Автопилот" остается включенным, значок Bitdefender в области уведомлений будет иметь вид  .

Чтобы отключить режим "Автопилот", откройте окно Bitdefender и нажмите переключатель **Автопилот** на верхней панели инструментов.

Важно
Если функция "Автопилот" включена, то изменение настроек, которыми она управляет, приведет к отключению функции.

Чтобы просмотреть историю операций, которые были выполнены приложением Bitdefender, пока был включен режим "Автопилот", откройте окно События.

1.7. Режим игры и режим ноутбука

Некоторые режимы работы компьютера, такие как игры или презентации, требуют повышенной бесперебойной реакции и производительности системы.Если ваш ноутбук работает от батареи, лучше отложить ненужные операции, требующие дополнительной электроэнергии, до подключения ноутбука к источнику бесперебойного питания.

Для адаптирования к этим особым ситуациям Bitdefender Internet Security 2012 имеет два специальных режима работы:

- Режим игры
- Режим ноутбука

1.7.1. Режим игры

Режим игры изменяет параметры настроек системы защиты для того, чтобы снизить до минимума воздействие на компьютер во время игры.При включенном режиме игры применяются следующие настройки:

- Все предупреждения и всплывающие окна Bitdefender будут отключены.

- Сканирование при доступе настраивается на уровне защиты **Низкий**.
- Автоматическое сканирование отключено.Функция автоматического сканирования выявляет и использует периоды времени, когда потребление ресурсов системы снижается до определенного уровня, для выполнения регулярного сканирования всей системы.
- Брандмауэр Bitdefender работает в обычном режиме (режим **Повышенная безопасность** отключен).Это означает, что все новые соединения (входящие и исходящие) автоматически разрешаются, независимо от используемого порта и протокола.
- Автоматическое обновление отключено.
- Панель инструментов Bitdefender в веб-браузере отключена, когда вы играете в онлайн-игры.

Находясь в режиме игры, вы будете видеть букву G поверх  значка Bitdefender.

Использование Режима Игры

По умолчанию Bitdefender автоматически входит в режим игры при запуске игры, находящейся в списке известных игр Bitdefender, или когда приложение разворачивается на полный экран.Bitdefender автоматически вернется в нормальный режим работы, когда вы закрываете игру или при выходе приложения из полноэкранного режима.

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

- Щелкните правой кнопкой мыши на значке Bitdefender на панели задач и установите **Включить режим игры**.
- Нажмите `Ctrl+Shift+Alt+G` (горячая клавиша по умолчанию).

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

Изменение горячей клавиши режима игры

Вы можете войти в режим игры вручную с помощью сочетания клавиш по умолчанию `Ctrl+Alt+Shift+G`.Чтобы изменить горячие клавиши, необходимо выполнить следующие шаги:

1. Откройте окно Bitdefender.
2. Нажмите кнопку **Настройки** на верхней панели инструментов.
3. Нажмите **Общие** в меню слева и перейдите на вкладку **Настройки**.

4. С помощью параметра **Включить горячие клавиши режима игры** установите нужную горячую клавишу:

   a. Выберите клавиши, которые вы хотите изменить, используя клавиши Control (`Ctrl`), Shift (`Shift`) или Alternate (`Alt`).

   b. 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
   Чтобы отключить горячую клавишу, отключите параметр **Включить горячие клавиши режима игры**.

Включение и отключение автоматического режима игры

Для включения или отключения автоматического режима игры выполните следующие действия:

1. Откройте окно Bitdefender.
2. Нажмите кнопку **Настройки** на верхней панели инструментов.
3. Нажмите **Общие** в меню слева и перейдите на вкладку **Настройки**.
4. Включите или отключите автоматический режим игры, нажав на соответствующий переключатель.

1.7.2. Режим ноутбука

Режим ноутбука специально предназначен для пользователей портативных компьютеров. Его цель — минимизировать влияние работы Bitdefender на энергопотребление, когда эти устройства работают от батареи.Когда Bitdefender работает в режиме ноутбука, функции автоматического сканирования и автоматического обновления отключены, так как они требуют больших ресурсов системы, что приводит к повышению энергопотребления.

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.

Для включения и отключения автоматического режима ноутбука выполните следующие действия:

1. Откройте окно Bitdefender.
2. Нажмите кнопку **Настройки** на верхней панели инструментов.
3. Нажмите **Общие** в меню слева и перейдите на вкладку **Настройки**.

4. Включите или отключите автоматический режим ноутбука, нажав на соответствующий переключатель.

Если Bitdefender установлен не на ноутбуке, отключите автоматический режим ноутбука.

1.8. Защищенные паролем настройки Bitdefender

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

Чтобы установить пароль для изменения настроек Bitdefender, выполните следующие действия.

1. Откройте окно Bitdefender.
2. Нажмите кнопку **Настройки** на верхней панели инструментов.
3. Нажмите **Общие** в меню слева и перейдите на вкладку **Настройки**.
4. В разделе **Настройки защиты паролем** включите защиту с помощью пароля, нажав на переключатель.
5. Нажмите ссылку **Изменить пароль**.
6. Введите пароль в двух полях и нажмите **OK**.Пароль должен содержать не менее 8 символов.

После установки пароля при попытке изменения настроек Bitdefender будет выдаваться запрос на ввод пароля.

Важно

Запомните пароль или сохраните его в надежном месте.Если вы забыли пароль, вам придется переустановить программу или обратиться за помощью в службу поддержки клиентов Bitdefender.

Чтобы снять защиту с помощью пароля, выполните следующие действия:

1. Откройте окно Bitdefender.
2. Нажмите кнопку **Настройки** на верхней панели инструментов.
3. Нажмите **Общие** в меню слева и перейдите на вкладку **Настройки**.
4. В разделе **Настройки защиты паролем** отключите защиту с помощью пароля, нажав на переключатель.
5. Введите пароль и нажмите **OK**.

1.9. Анонимные отчеты об использовании

По умолчанию Bitdefender отправляет отчеты, содержащие информацию по использованию вами серверов Bitdefender.Эта информация поможет нам

усовершенствовать продукт и предложить в будущем более широкие возможности.Учтите, эти отчеты не содержат конфиденциальных данных, таких как, например, ваше имя, IP-адрес. Также они не могут быть использованы в каких-либо коммерческих целях.

Чтобы отключить отправку анонимных отчетов об использовании, выполните следующие действия:

1. Откройте окно Bitdefender.
2. Нажмите кнопку **Настройки** на верхней панели инструментов.
3. Нажмите **Общие** в меню слева и перейдите на вкладку **Расширенные**.
4. Отключите отправку анонимных отчетов об использовании, нажав на соответствующий переключатель.

1.10. Восстановление или удаление Bitdefender

Если требуется восстановить или удалить Bitdefender Internet Security 2012, пройдите по следующему пути из меню Windows "Пуск": **Пуск → Все программы → Bitdefender 2012 → 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.

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

Для завершения процесса необходимо будет перезагрузить компьютер.

2. Интерфейс Bitdefender

Bitdefender Internet Security 2012 удовлетворяет требованиям как технически подкованных пользователей, так и новичков, так как его графический интерфейс удобен для любой категории пользователей.

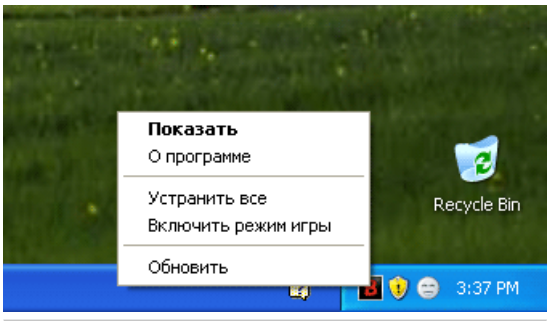
Значок Bitdefender на панели задач позволяет в любой момент времени просмотреть состояние продукта и предоставляет доступ к основным задачам.

Главное окно предоставляет удобный доступ к модулям продукта, важной информации о продукте, а также позволяет выполнять стандартные задачи.

Все необходимые инструменты для детальной настройки Bitdefender и выполнения расширенных задач администрирования доступны в окне настроек.

2.1. Значок на 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**: открытие главного окна Bitdefender.
- **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 неисправностей»* (p. 6).
- **Включить/выключить режим игры** — включает/выключает Режим игры.
- **Обновить сейчас** — запускает немедленное обновление.Состояние обновления можно увидеть на панели "Обновление" в главном окне Bitdefender.

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

 Существуют критические угрозы безопасности системы. Они требуют немедленного вмешательства и решения.

 Некритические проблемы влияют на безопасность системы.Их следует просмотреть и исправить в ближайшее время.

 Продукт работает в Режиме игры.

 Задействована функция Автопилот в Bitdefender.

Если Bitdefender не работает, значок на панели задач отображается на сером фоне:  .Обычно происходит, когда истекает срок действия лицензионного ключа. Также может произойти, когда Bitdefender не отвечает или когда другие ошибки влияют на нормальную работу Bitdefender.

2.2. Главное окно

В главном окне Bitdefender можно выполнять стандартные задачи, быстро устранять проблемы безопасности системы, просматривать информацию о событиях, возникающих при работе продукта, и настраивать параметры продукта.Вам требуется всего несколько раз нажать мышью.

Окно разделено на две основные области:

Верхняя панель инструментов
: Здесь можно посматривать состояние безопасности компьютера и запускать важные задачи.

Область панелей
: Здесь можно управлять основными модулями Bitdefender.

Кроме того, в нижней части окна имеется несколько полезных ссылок:

Ссылка	Описание
Обратная связь	Открывает страницу в браузере, на которой можно заполнить небольшой опрос по опыту использования продукта.Ваши отзывы помогут нам в работе над совершенствованием продуктов Bitdefender.
Завершение регистрации / **MyBitdefender**	Открывает окно учетной записи MyBitdefender, в котором можно создать учетную запись и войти в нее.Для получения обновлений и использования онлайн-функций продукта требуется создать учетную запись MyBitdefender.Дополнительную информацию о создании

Ссылка	Описание
	учетных записей и их преимуществах см. в «*Выполнение входа в MyBitdefender*» (p. 3).
Сведения о лицензии	Откроется окно, в котором отображаются данные о текущем лицензионном ключе. В этом окне также можно зарегистрировать продукт, используя новый лицензионный ключ.
Помощь	Для получения помощи по работе с Bitdefender перейдите по этой ссылке.
	Добавляет вопросительные знаки в различные области окна Bitdefender, чтобы упростить поиск важной информации об элементах интерфейса. Наведите курсор на отметку, чтобы посмотреть краткую информацию о следующем элементе.

2.2.1. Верхняя панель инструментов

Верхняя панель инструментов содержит следующие элементы:

- В **области состояния безопасности** в левой части панели инструментов отображается информация о наличии проблем, которые могут подвергать риску безопасность компьютера, а также предоставляются рекомендации по их разрешению.

  Цвет области состояния безопасности меняется в зависимости от обнаруженных проблем, и отображаются различные сообщения:

  - **Область выделена зеленым цветом.** Нет проблем, требующих разрешения.Ваш компьютер и данные защищены.
  - **Область выделена желтым цветом.** Некритические проблемы влияют на безопасность системы.Их следует просмотреть и исправить в ближайшее время.
  - **Область выделена красным цветом.** Критические проблемы влияют на безопасность системы.Эти проблемы следует разрешить незамедлительно.

  Нажмите кнопку **Просмотреть проблемы** в центре панели инструментов или в любом месте слева от области состояния безопасности, чтобы запустить мастер, который поможет легко устранить любые угрозы с компьютера.Для получения дополнительной информации перейдите к «*Устранение неисправностей*» (p. 6).

- **События**: позволяет просматривать подробную историю событий, произошедших во время работы продукта.Для получения дополнительной информации перейдите к «*События*» (p. 7).
- **Настройки**: вызов окна настроек, в котором можно установить параметры продукта.Для получения дополнительной информации перейдите к «*Окно настроек*» (p. 20).
- **Автопилот** позволяет включить режим "Автопилот", в котором обеспечивается защита без выдачи каких-либо уведомлений и запросов.Для получения дополнительной информации перейдите к «*Автопилот*» (p. 8).

2.2.2. Область панелей

Панели содержат инструменты для управления модулями Bitdefender.

Панели можно расположить нужным образом.Чтобы настроить эту область нужным образом, перетащите отдельные панели, поместив их в требуемые места.

Для перемещения по панелям используйте ползунок под областью панелей или стрелки, расположенные справа и слева.

На каждой панели имеются следующие элементы (сверху вниз):

- Имя модуля.
- Сообщение о состоянии.
- Значок модуля.Нажмите на значок модуля, чтобы настроить его параметры в окне настроек.
- Кнопка, позволяющая выполнять важные задачи, связанные с модулем.
- На некоторых панелях имеется переключатель, разрешающий включать и отключать важные функции модуля.

В этой области доступны следующие панели:

Антивирус

Антивирусная защита — это основа вашей безопасности. Bitdefender обеспечивает защиту в реальном времени и по запросу от всех типов вредоносного ПО, включая вирусы, трояны, шпионские и рекламные программы и т. д.

Панель "Антивирус" предоставляет удобный доступ к важным задачам сканирования.Нажмите **Сканировать** и выберите задачу в раскрывающемся меню:

- Быстрое сканирование
- Сканирование
- Выбор сканирования
- Поиск уязвимостей

- Режим "Реанимация"

Переключатель **Автоскан** позволяет включать и отключать функцию автоматического сканирования.

Дополнительную информацию о задачах сканирования и процедуре настройки защиты антивируса см. в «*Антивирусная защита*» (p. 35).

Брандмауэр

Брандмауэр защищает компьютер, подключенный к сети и Интернету, фильтруя все попытки соединений.

Нажмите **Сведения о сети** на панели "Брандмауэр", чтобы настроить параметры подключения к сети.

С помощью переключателя режима брандмауэра можно включать и отключать защиту брандмауэра.

Внимание

Поскольку при этом возникает риск установки несанкционированных подключений к компьютеру, отключение брандмауэра должно быть только временной мерой.Как можно скорее включите брандмауэр.

Дополнительные сведения о конфигурации брандмауэра см. в «*Брандмауэр*» (p. 97).

Антиспам

Модуль антиспама Bitdefender предотвращает попадание нежелательных писем в почтовый ящик, осуществляя фильтрацию трафика по протоколу POP3.

Нажмите **Управление** на панели "Антиспам" и в раскрывающемся меню выберите "Друзья" или "Спамеры", чтобы изменить соответствующий список адресов.

С помощью переключателя режима антиспама можно включать и отключать защиту антиспама.

Дополнительную информацию о настройке защиты антиспама см. в разделе «*Антиспам*» (p. 63).

Обновление

В условиях, когда кибер-преступники постоянно разрабатывают новые способы причинения вреда, крайне важно регулярно обновлять систему безопасности, чтобы всегда быть на шаг впереди.

По умолчанию Bitdefender автоматически проверяет наличие обновлений каждый час. Для отключения автоматического обновления используйте переключатель **Обновление** на панели "Обновление".

Внимание

Этот аспект является критическим с точки зрения безопасности. Рекомендуем вам отключать автоматическое обновление на как можно меньший промежуток времени. Если автоматическое обновление отключено, вы не защищены от самых последних угроз.

Нажмите кнопку **Обновить сейчас** на панели, чтобы незамедлительно запустить обновление.

Дополнительные сведения о настройке обновлений см. в «*Обновление*» (p. 112).

Родительский

Bitdefender Internet Security 2012 предлагает комплексный набор функций родительского контроля, которые позволят наблюдать за работой детей на компьютере и организовать их защиту.

На панели "Родительский контроль" нажмите **Управление учетными записями**, чтобы настроить параметры учетных записей пользователей Windows на компьютере.

Дополнительную информацию по настройке родительского контроля см. в «*Родительский контроль*» (p. 81).

Анонимность

Модуль защиты личных данных помогает обеспечить конфиденциальность личных данных.Модуль обеспечивает защиту при работе в Интернете от атак фишинга, попыток мошенничества, утечки личных данных.

Нажмите кнопку **Управление правилами** на панели "Защита данных", чтобы перейти в раздел "Защита данных" для настройки правил защиты личных данных.

С помощью переключателя режима антифишинга можно включать и отключать защиту антифишинга.

Дополнительную информацию о настройке Bitdefender для обеспечения конфиденциальности см. в «*Защита данных*» (p. 74).

Карта сети

С помощью карты сети можно легко управлять безопасностью домашних компьютеров с одного компьютера.

Для начала работы нажмите **Управление** на панели карты сети и выберите **Включить сеть**.

После включения сети нажмите **Управление** на панели "Карта сети", чтобы получить доступ к следующим параметрам.

- **Отключить соединение**: отключение сети.

- **Сканировать все**: запуск быстрого сканирования всей системы на управляемых компьютерах.
- **Обновление всех компьютеров**: обновление продуктов Bitdefender на управляемых компьютерах.

Для получения дополнительной информации перейдите к *«Карта сети»* (p. 108).

Safego

Для обеспечения безопасной работы в Facebook вы можете использовать Safego, систему защиты Bitdefender для социальных сетей, непосредственно через интерфейс продукта.

Нажмите **Активировать** для активации и управления Safego через учетную запись Facebook.

Если вы уже активировали Safego, вы сможете просмотреть статистику по активности модуля, нажав кнопку **Просмотр отчетов**.

Для получения дополнительной информации перейдите к *«Защита Safego для социальных сетей»* (p. 117).

2.3. Окно настроек

Окно настроек предоставляет доступ к компонентам и параметрам всех продуктов.Здесь можно настроить различные параметры Bitdefender.

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.

Общие

Позволяет настроить общие параметры продукта, включая настройки пароля, режим игры, режим ноутбука, параметры прокси-сервера и оповещения о статусе.

Антивирус

Позволяет настроить защиту от вредоносного ПО, обнаруживать и устранять уязвимости системы, настраивать исключения сканирования и управлять файлами в карантине.

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.

Защита данных
: Предотвращение кражи данных с вашего компьютера и защита вашей конфиденциальности, когда вы находитесь в режиме онлайн.Настройка защиты для браузера, программ обмена мгновенными сообщениями, управление защитой данных и многое другое.

Брандмауэр
: Позволяет настроить общие параметры и правила брандмауэра, а также параметры обнаружения вторжения и отслеживания сетевой активности.

Карта сети
: Позволяет выполнять настройку и управление обновлениями Bitdefender, установленными на ваших домашних компьютерах, с одного компьютера.

Обновление
: Позволяет подробно настроить процесс обновления.

Кроме того, в нижней части окна имеется несколько полезных ссылок:

Ссылка	Описание
Обратная связь	Открывает страницу в браузере, на которой можно заполнить небольшой опрос по опыту использования продукта.Ваши отзывы помогут нам в работе над совершенствованием продуктов Bitdefender.
Завершение регистрации / **MyBitdefender**	Открывает окно учетной записи MyBitdefender, в котором можно создать учетную запись и войти в нее.Для получения обновлений и использования онлайн-функций продукта требуется создать учетную запись MyBitdefender.Дополнительную информацию о создании учетных записей и их преимуществах см. в *«Выполнение входа в MyBitdefender»* (p. 3).
Сведения о лицензии	Откроется окно, в котором отображаются данные о текущем лицензионном ключе. В этом окне также можно зарегистрировать продукт, используя новый лицензионный ключ.
Помощь	Для получения помощи по работе с Bitdefender перейдите по этой ссылке.
	Добавляет вопросительные знаки в различные области окна Bitdefender, чтобы упростить поиск важной информации об элементах интерфейса. Наведите курсор на отметку, чтобы посмотреть краткую информацию о следующем элементе.

Чтобы вернуться в главное окно, нажмите кнопку **Главная** в правом верхнем углу окна.

3. Советы

В этой главе представлены пошаговые инструкции по настройке стандартных параметров и выполнению типовых задач в Bitdefender.Некоторые разделы включают ссылки на другие разделы, в которых представлена подробная информация.

3.1. Регистрация пробной версии

Если вы установили пробную версию, вы сможете пользоваться ей в течение ограниченного периода времени.Чтобы продолжить использование Bitdefender после завершения пробного периода, вам необходимо зарегистрировать продукт с помощью лицензионного ключа и создать учетную запись MyBitdefender.

- Для регистрации Bitdefender выполните следующие действия:
  1. Откройте окно Bitdefender.
  2. Перейдите по ссылке **Сведения о лицензии** в нижней части окна.Откроется окно регистрации.
  3. Введите лицензионный ключ и нажмите **Зарегистрировать сейчас**.

     Если у вас нет лицензионного ключа, нажмите на ссылку в окне, чтобы перейти на веб-страницу, на которой его можно будет приобрести.
  4. Дождитесь завершения процесса регистрации и закройте окно.
- Для создания учетной записи MyBitdefender выполните следующие действия:
  1. Откройте окно Bitdefender.
  2. Перейдите по ссылке **Завершение регистрации** в нижней части окна.Откроется окно учетной записи.
  3. Выберите соответствующую ссылку, чтобы создать новую учетную запись.
  4. Введите необходимую информацию в соответствующих полях.Информация, которую вы предоставите, останется конфиденциальной.

     Нажмите **Подтвердить**.
  5. Проверьте почту и следуйте инструкциям в полученном письме, чтобы завершить регистрацию.

Замечание

Вы можете использовать предоставленный адрес электронной почты и пароль для входа в учетную запись на http://my.bitdefender.com.

3.2. Как зарегистрировать Bitdefender без подключения к Интернету?

Если вы только что приобрели Bitdefender и у вас нет подключения к Интернету, вы можете зарегистрировать Bitdefender в режиме офлайн.

Чтобы зарегистрировать Bitdefender с помощью лицензионного ключа, выполните следующие действия:

1. Перейдите к компьютеру, который подключен к Интернету.Например, вы можете использовать компьютер друга или компьютер в публичном месте.
2. Перейдите на https://my.bitdefender.com, чтобы создать учетную запись MyBitdefender.
3. Войдите в свою учетную запись и выберите **Выполнить регистрацию в режиме офлайн**.
4. Введите номер приобретенного лицензионного ключа.
5. Нажмите **Подтвердить**, чтобы получить код подтверждения.

   Важно
   Запишите код подтверждения.

6. Введите код подтверждения на компьютере.
7. Откройте окно Bitdefender.
8. Перейдите по ссылке **Сведения о лицензии** в нижней части окна.Откроется окно регистрации.
9. Выберите вариант регистрации продукта с использованием кода подтверждения.
10. В соответствующем поле введите код подтверждения и нажмите **Подтвердить**.
11. Дождитесь завершения процесса регистрации и нажмите **Завершить**.

3.3. Порядок обновления до другой версии продукта Bitdefender 2012

Вы можете легко выполнить переход с одного продукта Bitdefender 2012 на другой.

Рассмотрим следующий сценарий: пользователь в течение некоторого времени использовал Bitdefender Internet Security 2012 2012, а недавно решил обновить его до версии Bitdefender Total Security 2012 и установить доступные дополнительные функции.

Вам необходимо просто приобрести лицензионный ключ для продукта Bitdefender 2012, который вы планируете обновить, и ввести его в окне регистрации текущего установленного продукта Bitdefender 2012.

Следуйте инструкции:

1. Откройте окно 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 процедуру обновления.

3.4. Когда требуется переустановка Bitdefender?

В некоторых ситуациях может потребоваться переустановка Bitdefender.

Типичные ситуации, в которых может потребоваться переустановка Bitdefender:

- вы переустановили операционную систему
- вы приобрели новый компьютер
- вы хотите изменить язык интерфейса Bitdefender

Для выполнения переустановки Bitdefender можно использовать приобретенный установочный диск или загрузить новую версию с веб-сайта Bitdefender.

Во время установки вам будет предложено зарегистрировать продукт с помощью лицензионного ключа.

Если вы не можете найти свой лицензионный ключ, войдите в https://my.bitdefender.com, чтобы получить его.Введите адрес электронной почты и пароль вашей учетной записи в соответствующих полях.

3.5. Когда прекращает действовать защита Bitdefender?

Чтобы посмотреть количество дней до истечения лицензионного ключа, выполните следующие действия.

1. Откройте окно Bitdefender.
2. Перейдите по ссылке **Сведения о лицензии** в нижней части окна.
3. В окне **Регистрация продукта** показано оставшееся число дней.

3.6. Как продлить защиту Bitdefender?

Прежде чем срок действия лицензии Bitdefender закончится, необходимо продлить лицензионный ключ.

- Выполните следующие действия, чтобы перейти на веб-сайт, где можно будет приобрести лицензионный ключ Bitdefender:
  1. Откройте окно Bitdefender.
  2. Перейдите по ссылке **Сведения о лицензии** в нижней части окна.
  3. Нажмите **Нет лицензионного ключа? Купить сейчас!**
  4. В веб-браузере откроется страница, на которой можно будет приобрести лицензионный ключ Bitdefender.

  Замечание
  В качестве альтернативного метода вы можете связаться с продавцом, у которого вы приобрели продукт Bitdefender.

- Для регистрации Bitdefender с использованием нового лицензионного ключа выполните следующие действия:
  1. Откройте окно Bitdefender.
  2. Перейдите по ссылке **Сведения о лицензии** в нижней части окна.Откроется окно регистрации.
  3. Введите лицензионный ключ и нажмите **Зарегистрировать сейчас**.
  4. Дождитесь завершения процесса регистрации и закройте окно.

Для получения дополнительной информации свяжитесь со службой поддержки Bitdefender, как описано в разделе *«Техническая поддержка»* (p. 142).

3.7. Какой продукт Bitdefender я использую?

Чтобы узнать, какая программа Bitdefender установлена, выполните следующие действия:

1. Откройте окно Bitdefender.
2. В верхней части окна отображается один из следующих элементов:
   - Bitdefender Antivirus Plus 2012
   - Bitdefender Internet Security 2012
   - Bitdefender Total Security 2012

3.8. Как выполнить сканирование файла или папки?

Самым простым методом сканирования файлов и папок, который рекомендуется использовать, является нажатие правой кнопкой мыши на объект, сканирование которого требуется выполнить, и выбор пункта меню **Сканировать с помощью Bitdefender**.Для завершения сканирования следуйте инструкциям мастера антивирусного сканирования.Bitdefender автоматически выполняет рекомендуемые действия в отношении обнаруженных файлов.Если после сканирования все еще остались угрозы, вам будет предложено выбрать действия, которые следует предпринять по отношению к ним.Для получения дополнительной информации перейдите к *«Мастер антивирусного сканирования»* (p. 47).

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.

3.9. Как выполнить сканирование системы?

Для осуществления полного сканирования системы выполните следующие действия:

1. Откройте окно Bitdefender.
2. Перейдите на панель **Антивирус**.
3. Нажмите **Сканировать** и в раскрывающемся меню выберите **Сканирование**.
4. Следуйте подсказкам мастера сканирования на антивирусы.Bitdefender автоматически выполняет рекомендуемые действия в отношении обнаруженных файлов.Если после сканирования все еще остались угрозы, вам будет предложено выбрать действия, которые следует предпринять по отношению к ним.Для получения дополнительной информации перейдите к *«Мастер антивирусного сканирования»* (p. 47).

3.10. Как создать пользовательское задание сканирования?

Чтобы выполнить сканирование отдельных папок на компьютере или настроить параметры сканирования, создайте и запустите пользовательское сканирование.

Для создания пользовательской задачи сканирования выполните следующие действия:

1. Откройте окно Bitdefender.
2. Перейдите на панель **Антивирус**.
3. Нажмите **Сканировать** и в раскрывающемся меню выберите вариант **Выбор сканирования**.
4. Нажмите **Добавить объект**, чтобы выбрать файлы или папки для сканирования.
5. Если требуется детальная настройка параметров сканирования, нажмите **Параметры сканирования**.

   Можно легко настроить параметры сканирования с помощью регулировки уровня сканирования. Переместите бегунок в требуемое положение, чтобы задать выбранный уровень сканирования.

   Вы также можете выбрать выключение компьютера по завершении сканирования, если нет обнаруженных угроз.Помните, что это будет поведением по умолчанию при запуске этой задачи.
6. Нажмите **Начало сканирования** и следуйте инструкциям мастера антивирусного сканирования, чтобы выполнить проверку.На этапе завершения сканирования отобразится сообщение, предлагающее выбрать действия, которые будут выполняться для обнаруженных файлов (если есть).
7. Чтобы сохранить задание сканирования для последующего использования, повторно откройте окно конфигурации настраиваемого сканирования.
8. Найдите только что запущенное сканирование в списке **Последние сканирования**.
9. Наведите курсор мыши на имя сканирования и щелкните значок ★, чтобы добавить сканирование в список избранных сканирований.
10. Введите значимое имя сканирования.

3.11. Порядок исключения папки из сканирования

Bitdefender позволяет исключать из сканирования определенные файлы, папки и расширения файлов.

Исключения могут настраивать пользователи, имеющие достаточно большой опыт работы с компьютерами, и только в следующих ситуациях:

- У вас имеется большая папка в системе, в которой хранятся фильмы и музыка.
- У вас имеется большой архив в системе, в котором хранятся различные данные.

- У вас имеется папка для установки разных типов программного обеспечения и приложений в целях тестирования.В результате сканирования папки некоторые данные могут быть потеряны.

Для добавления папки в список исключений выполните следующие действия:

1. Откройте окно Bitdefender.
2. Нажмите кнопку **Настройки** на верхней панели инструментов.
3. Нажмите **Антивирус** в меню слева и перейдите на вкладку **Исключения**.
4. Нажмите ссылку **Исключенные файлы и папки**.
5. Нажмите кнопку **Добавить** в верхней части таблицы исключений.
6. Нажмите кнопку **Обзор**, выберите папку, которую требуется исключить из сканирования, и нажмите **OK**.
7. Нажмите **Добавить**, а затем **OK**, чтобы сохранить изменения и закрыть окно.

3.12. 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. Отключение антивирусной защиты Bitdefender в режиме реального времени:
   a. Откройте окно Bitdefender.
   b. Нажмите кнопку **Настройки** на верхней панели инструментов.
   c. Нажмите **Антивирус** в меню слева и перейдите на вкладку **Экран**.
   d. Нажмите на переключатель, чтобы отключить **резидентное сканирование**.
2. Отображать скрытые объекты в Windows.Инструкции для этой процедуры см. в *«Как отобразить скрытые объекты в Windows?»* (p. 150).
3. Восстановление файла из области карантина:
   a. Откройте окно Bitdefender.
   b. Нажмите кнопку **Настройки** на верхней панели инструментов.
   c. Нажмите **Антивирус** в меню слева и перейдите на вкладку **Карантин**.
   d. Выберите файл и нажмите **Восстановить**.
4. Добавьте файл в список исключений.Инструкции для этой процедуры см. в *«Порядок исключения папки из сканирования»* (p. 28).

5. Включить антивирусную защиту Bitdefender в режиме реального времени.
6. Свяжитесь с нашей службой поддержки, и мы удалим сигнатуру обнаружения.Инструкции для этой процедуры см. в *«Обращение за помощью»* (p. 143).

3.13. Как создать учетную запись 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.

3.14. Как защитить детей от интернет-угроз?

Модуль родительского контроля Bitdefender позволяет ограничить доступ в Интернет и к определенным приложениям, чтобы ваши дети не могли смотреть неподобающие материалы, когда вас нет дома.

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, чат, программы обмена файлами и другие.
- Мгновенные сообщения, отправленные заблокированными IM-контактами.

Для настройки родительского контроля выполните следующие действия:

1. Создайте ограниченные (стандартные) учетные записи Windows для своих детей.Для получения дополнительной информации перейдите к *«Как создать учетную запись пользователя Windows?»* (p. 30).
2. При загрузке системы необходимо выполнить вход в учетную запись администратора.Только пользователи с правами администратора (системные администраторы) могут получить доступ для настройки родительского контроля.
3. Настройте Родительский Контроль для учетной записи Windows, которой пользуются ваши дети.
   a. Откройте окно Bitdefender.
   b. Перейдите на панель **Родительский**.
   c. Нажмите **Учетные записи** и убедитесь, что родительский контроль включен для учетной записи вашего ребенка.
   d. Введите возраст своего ребенка, нажав на одно из полей, соответствующих параметру **Возраст**.Когда пользователь указывает возраст ребенка, автоматически загружаются настройки,

соответствующие данной категории возраста (на основе стандартов детского развития).

e. Если требуется детальная настройка параметров родительского контроля, нажмите **Настройки**.

Дополнительные сведения об использовании родительского контроля см. в *«Родительский контроль»* (p. 81).

3.15. Разблокирование веб-сайтов, заблокированных функцией родительского контроля

Функция родительского контроля Bitdefender позволяет контролировать, к какому содержимому ребенок имеет доступ при использовании компьютера.

Если вы установили в функции родительского контроля возрастную категорию для своего ребенка и используете только одну учетную запись Windows, вы не сможете открывать веб-сайты, классифицированные как неподобающие для данной возрастной категории.

Если доступ к веб-сайту блокируется родительским контролем, можно создать правило, в котором будет явно задано разрешение для доступа к этому сайту.

Чтобы разрешить доступ к веб-сайту, выполните следующие действия:

1. Откройте окно Bitdefender.
2. Перейдите на панель **Родительский**.
3. Нажмите **Учетные записи**.
4. Нажмите кнопку **Настройки**, чтобы определить пользовательские настройки.
5. Нажмите **Разрешить веб-сайт**.
6. Введите адреса сайтов в поле **Веб-сайт**.
7. Выберите нужное действие для этого правила (**Разрешить**) и нажмите **Завершить**, чтобы добавить правило.
8. Запустите браузер и откройте веб-сайт.

3.16. Как защитить личную информацию?

Модуль защиты данных осуществляет мониторинг данных, которые передаются с компьютера через веб-формы, в сообщениях электронной почты и мгновенных сообщениях.

Чтобы исключить отправку личных данных с компьютера, происходящую без вашего ведома, необходимо создать соответствующие правила защиты данных.Правила защиты данных определяют, какая информация будет заблокирована.

Для создания правила защиты данных выполните следующие действия:

1. Откройте окно Bitdefender.
2. Нажмите кнопку **Настройки** на верхней панели инструментов.
3. Нажмите **Защита данных** в меню слева и перейдите на вкладку **Защита данных**.
4. Если функция **Защита данных** отключена, включите ее, используя соответствующий переключатель.
5. Выберите вариант **Добавить правило**, чтобы запустить мастер защиты данных.
6. Следуйте инструкциям мастера.

3.17. Как настроить Bitdefender для использования прокси-сервера при подключении к Интернету?

Если ваш компьютер подключен к Интернету через прокси-сервер, вам необходимо задать настройки прокси-сервера в Bitdefender.Как правило, Bitdefender автоматически выполняет поиск и импорт настроек прокси-сервера из системы.

Важно

Прокси-сервер для домашних подключений к Интернету обычно не используется.Если обновление не выполняется, прежде всего проверьте и настройте параметры подключения Bitdefender к прокси-серверу.Если обновление Bitdefender выполняется, значит настройки подключения продукта к Интернету установлены правильно.

Для управления настройками прокси-сервера выполните следующие действия:

1. Откройте окно Bitdefender.
2. Нажмите кнопку **Настройки** на верхней панели инструментов.
3. Нажмите **Общие** в меню слева и перейдите на вкладку **Расширенные**.
4. В разделе **Настройки прокси** включите использование прокси-сервера, нажав на переключатель.
5. Нажмите ссылку **Управление прокси**.
6. Настройки прокси-сервера можно задать двумя способами:
   - **Импортировать настройки прокси-сервера из браузера по умолчанию**: настройки прокси-сервера для текущего пользователя, извлеченные из браузера по умолчанию. Если прокси-сервер требует ввода имени пользователя и пароля, их необходимо указать в соответствующих полях.

Замечание

Bitdefender может импортировать настройки из самых популярных браузеров, включая последние версии Internet Explorer, Mozilla Firefox и Opera.

- **Пользовательские настройки прокси-сервера** — настройки прокси-сервера, которые вы можете настроить самостоятельно.Должны быть определены следующие настройки:
  - **Адрес** — введите IP-адрес прокси-сервера.
  - **Порт** — введите порт, используемый Bitdefender для подсоединения к прокси-серверу.
  - **Имя пользователя**: введите имя пользователя, опознаваемое прокси-сервером.
  - **Пароль** — введите пароль пользователя, указанного ранее.

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

При управлении подключением к Интернету Bitdefender будет использовать доступные настройки прокси-сервера.

4. 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:

- Проверка при доступе — 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.

  Резидентное сканирование обеспечивает постоянную защиту от вредоносного ПО и является важным компонентом любой программы компьютерной безопасности.

  Важно
  Чтобы предотвратить заражение компьютера вирусами, функция **резидентного сканирования** должна быть включена.

- 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.

  Если функция автоматического сканирования включена, выполнять проверку на вирусы вручную практически не требуется.Функция автоматического сканирования обеспечивает постоянное сканирование компьютера и выполнение необходимых действий при обнаружении вредоносных программ.Функция автоматического сканирования запускается, только когда имеется достаточно системных ресурсов, чтобы производительность компьютера при этом не снижалась.

Bitdefender автоматически сканирует все съемные носители, подключенные к компьютеру, для проверки их безопасности.Для получения дополнительной информации перейдите к *«Автоматическое сканирование съемных носителей»* (p. 51).

Если сканирование определенных файлов или типов файлов выполнять не требуется, опытные пользователи могут настроить исключения сканирования.Для получения дополнительной информации перейдите к *«Настройка исключений сканирования»* (p. 53).

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 *«Управление файлами в карантине»* (p. 55).

В случае заражения компьютера вирусом см. информацию в *«Удаление вредоносного ПО из системы»* (p. 133).Чтобы помочь вам очистить компьютер от вирусов, которые невозможно удалить из операционной системы Windows, Bitdefender предоставляет режим "Реанимация".Это доверенная среда, предназначенная, в частности, для удаления вредоносного ПО, которая позволяет загружать компьютер без запуска Windows.Когда компьютер запущен в режиме "Реанимация", вредоносные программы Windows неактивны, благодаря чему их можно легко удалить.

Чтобы защитить компьютер от неизвестных вредоносных программ, Bitdefender использует функции активного вирусного контроля, расширенную эвристическую технологию, которая осуществляет постоянный мониторинг приложений, запущенных в системе.Активный вирусный контроль автоматически блокирует приложения, демонстрирующие вирусное поведение, чтобы не позволить им нанести вред компьютеру.Время от времени могут блокироваться легальные сообщения. В таких ситуациях можно настроить, чтобы функция активного вирусного контроля не блокировала приложения повторно, создав правила исключения.Дополнительные сведения см. в *«Активный вирусный контроль»* (p. 56).

Многие формы вредоносного ПО предназначены для инфицирования систем путем использования их уязвимостей, таких как отсутствие обновлений операционной системы и устаревшие приложения.Bitdefender помогает легко обнаруживать и устранять уязвимости системы для повышения уровня защиты компьютера от вредоносных программ и хакеров.Для получения дополнительной информации перейдите к *«Устранение уязвимостей системы»* (p. 59).

4.1. Резидентное сканирование (защита в реальном 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.

4.1.1. Проверка вредоносных программ, обнаруженных в режиме резидентного сканирования

Для выполнения проверки вирусов, обнаруженных при резидентном сканировании, выполните следующие действия:

1. Откройте окно Bitdefender.
2. Нажмите кнопку **События** на верхней панели инструментов.
3. Нажмите **Антивирус** в меню слева и перейдите на вкладку **Сканирование на вирусы**.Здесь можно просмотреть все события сканирования на вирусы, включая угрозы, обнаруженные при резидентном сканировании, сканировании по инициативе пользователя, а также изменения статуса автоматического сканирования.
4. Нажмите на событие, чтобы просмотреть сведения о нем.

4.1.2. Регулировка уровня защиты в реальном 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.

Для настройки уровня защиты в реальном времени выполните следующие действия:

1. Откройте окно Bitdefender.
2. Нажмите кнопку **Настройки** на верхней панели инструментов.
3. Нажмите **Антивирус** в меню слева и перейдите на вкладку **Экран**.
4. 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.

4.1.3. Создание настраиваемого уровня защиты

Опытные пользователи могут воспользоваться преимуществами настройки параметров сканирования Bitdefender.Детальную настройку защиты в режиме реального времени можно выполнить, создав настраиваемый уровень защиты.

Для создания настраиваемого уровня защиты выполните следующие действия:

1. Откройте окно Bitdefender.
2. Нажмите кнопку **Настройки** на верхней панели инструментов.

3. Нажмите **Антивирус** в меню слева и перейдите на вкладку **Экран**.
4. Нажмите **Настраиваемый**.
5. Настройте параметры сканирования по своему выбору.
6. 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.
- **Параметры сканирования для используемых файлов.** В Bitdefender можно настроить, чтобы выполнялось только сканирование всех файлов и приложений (файлов программ), вызываемых пользователем.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:

  386; a6p; ac; accda; accdb; accdc; accde; accdp; accdr; accdt; accdu; acl; acr; action; ade; adp; air; app; as; asd; asp; awk; bas; bat; bin; cgi; chm; cla; class; cmd; cnv; com; cpl; csc; csh; dat; dek; dld; dll; doc; docm; docx; dot; dotm; dotx; drv; ds; ebm; esh; exe; ezs; fky; frs; fxp; gadget; grv; hlp; hms; hta; htm; html; iaf; icd; ini; inx; ipf; isu; jar; js; jse; jsx; kix; laccdb; lnk; maf; mam; maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mpp; mpt; mpx; ms; msg; msi; msp; mst; msu; oab; obi; obs; ocx; oft; ole; one; onepkg; ost; ovl; pa; paf; pex; pfd; php; pif; pip; pot; potm; potx; ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; prc; prf; prg; pst; pub; puz; pvd; pwc; py; pyc; pyo; qpx; rbx; rgs; rox; rpj; rtf; scar; scr; script; sct; shb; shs; sldm; sldx; smm; snp; spr; svd; sys; thmx; tlb; tms; u3p; udf; url; vb; vbe; vbs; vbscript; vxd; wbk; wcm; wdm; wiz; wll; wpk; ws; wsf; xar; xl; xla; xlam; xlb; xlc; xll; xlm; xls; xlsb; xlsm; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp

- **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.

При использовании данного варианта вы сможете задать максимально разрешенный размер архивов для резидентного сканирования.Поставьте флажок в соответствующем поле и введите максимальный размер архива (в МБ).

- **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 и исходящие сообщения электронной почты
  - веб-трафик
  - файлы, полученные через Yahoo! 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.

- **Сканировать загрузочные секторы.** Bitdefender можно настроить для сканирования загрузочных секторов жесткого диска.Этот сектор жесткого диска содержит компьютерный код, необходимый для запуска процесса загрузки.Заражение вирусом загрузочного сектора может привести к тому, что диск станет недоступен и вы не сможете загрузить систему и получить доступ к своим данным.

- **Проверить только новые и измененные файлы.** Сканируя только новые и измененные файлы, можно значительно повысить общее быстродействие системы с минимальными потерями в безопасности.

4.1.4. 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

Чтобы восстановить настройки по умолчанию для модуля защиты в режиме реального времени, выполните следующие действия:

1. Откройте окно Bitdefender.
2. Нажмите кнопку **Настройки** на верхней панели инструментов.
3. Нажмите **Антивирус** в меню слева и перейдите на вкладку **Экран**.
4. Нажмите **По умолчанию**.

4.1.5. Включение или отключение защиты в реальном времени

Включите или отключите защиту от вирусов в реальном времени, выполнив следующие действия:

1. Откройте окно Bitdefender.
2. Нажмите кнопку **Настройки** на верхней панели инструментов.
3. Нажмите **Антивирус** в меню слева и перейдите на вкладку **Экран**.
4. Нажмите на переключатель, чтобы включить или отключить резидентное сканирование.
5. Если вы захотите отключить постоянную защиту, то появится окно с предупреждением.Вы должны подтвердить свое намерение, выбрав промежуток времени, на который вы хотите отключить постоянную защиту. Вы можете отключить постоянную защиту на 5, 15 или 30 минут, на час, навсегда или до следующей перезагрузки системы.

Внимание

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

4.1.6. Действия, выполненные в отношении обнаруженных вредоносных программ

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. Поскольку B-HAVE является эвристической технологией анализа, Bitdefender не может точно определить, действительно ли файл заражен вирусом.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.

- Если обнаружен подозрительный файл, он помещается в карантин, чтобы предотвратить возможное заражение.

  По умолчанию файлы в карантине автоматически отправляются в лабораторию Bitdefender, где они анализируются специалистами по вирусам Bitdefender.Если наличие вредоносного ПО подтверждено, выпускается сигнатура, которая позволит удалить вредоносное ПО.

4.2. 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.Сканирование компьютера можно выполнять в любое время, запустив

задачи по умолчанию или собственные (пользовательские) задачи сканирования.Чтобы выполнить сканирование отдельных папок на компьютере или настроить параметры сканирования, создайте и запустите пользовательское сканирование.

4.2.1. Автоскан

Автоматическое сканирование — это процесс сканирования по запросу, который осуществляет проверку всех данных на предмет наличия вредоносного кода и выполняет соответствующие действия при обнаружении вирусов.Функция автоматического сканирования выявляет и использует периоды времени, когда потребление ресурсов системы снижается до определенного уровня, для выполнения регулярного сканирования всей системы.

Преимущества автоматического сканирования:

- Влияние на систему практически отсутствует.
- Предварительное сканирование всего жесткого диска гарантирует быстрое выполнение задач по требованию впоследствии.
- Выполнение резидентного сканирования также может занять продолжительное время.

Для включения или отключения автоматического сканирования выполните следующие действия:

1. Откройте окно Bitdefender.
2. Перейдите на панель **Антивирус**.
3. Нажмите на переключатель, чтобы включить или отключить автоматическое сканирование.

4.2.2. Сканирование файла или папки на предмет наличия вредоносных программ

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.На этапе завершения сканирования отобразится сообщение, предлагающее выбрать действия, которые будут выполняться для обнаруженных файлов (если есть).

4.2.3. Запуск быстрого сканирования

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.

Чтобы запустить быстрое сканирование, выполните следующие действия.

1. Откройте окно Bitdefender.
2. Перейдите на панель **Антивирус**.
3. Нажмите **Сканировать** и в раскрывающемся меню выберите **Быстрое сканирование**.
4. Следуйте инструкциям мастера антивирусного сканирования для выполнения проверки.Bitdefender автоматически выполняет рекомендуемые действия в отношении обнаруженных файлов.Если после сканирования все еще остались угрозы, вам будет предложено выбрать действия, которые следует предпринять по отношению к ним.

4.2.4. Запуск полной проверки системы

Выполняется сканирование всего компьютера на наличие любых типов вредоносных программ, представляющих угрозу для безопасности системы, например вирусов, рекламного и шпионского ПО, руткитов и др.Если функция автоматического сканирования отключена, рекомендуется выполнять полное сканирование системы хотя бы один раз в неделю.

Замечание

Поскольку функция **полного сканирования системы** обеспечивает выполнение детальной проверки всей системы, сканирование может занять длительное время. Поэтому рекомендуется запускать эту задачу, когда компьютер не используется.

Перед запуском полного сканирования системы рекомендуется выполнить следующие действия:

- Убедитесь, что установлены последние обновления вирусных сигнатур для Bitdefender. Если сканирование компьютера выполняется с использованием устаревших сигнатур, Bitdefender не сможет обнаружить новые вирусы, появившиеся с момента последнего обновления.Для получения дополнительной информации перейдите к «*Обновление*» (p. 112).
- Закройте все открытые программы.

Чтобы выполнить сканирование отдельных папок на компьютере или настроить параметры сканирования, создайте и запустите пользовательское сканирование.Для получения дополнительной информации перейдите к «*Настройка и запуск пользовательского сканирования*» (p. 44).

Чтобы запустить полное сканирование системы, выполните следующие действия:

1. Откройте окно Bitdefender.
2. Перейдите на панель **Антивирус**.
3. Нажмите **Сканировать** и в раскрывающемся меню выберите **Сканирование**.
4. Следуйте инструкциям мастера антивирусного сканирования для выполнения проверки.Bitdefender автоматически выполняет рекомендуемые действия в отношении обнаруженных файлов.Если после сканирования все еще остались угрозы, вам будет предложено выбрать действия, которые следует предпринять по отношению к ним.

4.2.5. Настройка и запуск пользовательского сканирования

Для детальной настройки и выполнения сканирования на наличие вредоносных программ выполните следующие действия:

1. Откройте окно Bitdefender.
2. Перейдите на панель **Антивирус**.
3. Нажмите **Сканирование** и в раскрывающемся меню выберите **Выбор сканирования**.
4. При желании можно быстро перезапустить предыдущее настраиваемое сканирование, щелкнув соответствующую запись в списке **Последние сканирования** или **Избранные сканирования**.
5. Нажмите **Добавить объект**, поставьте флажки в полях, соответствующих разделам, которые требуется проверить на вирусы, и нажмите **OK**.
6. Нажмите **Параметры сканирования**, если требуется настроить параметры сканирования.Появится новое окно.Следуйте инструкции:

   a. 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.

   Опытные пользователи могут воспользоваться преимуществами настройки параметров сканирования Bitdefender.Для детальной настройки параметров сканирования нажмите **Пользовательский**. Информация об этих настройках представлена в конце данного раздела.

   b. 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.

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

7. Нажмите **Начало сканирования** и следуйте инструкциям мастера антивирусного сканирования, чтобы выполнить проверку.Процедура сканирования может занять некоторое время в зависимости от выбранных путей сканирования.На этапе завершения сканирования отобразится сообщение, предлагающее выбрать действия, которые будут выполняться для обнаруженных файлов (если есть).

Сохранение настраиваемого сканирования в список избранного

При настройке и запуске настраиваемого сканирования оно автоматически добавляется в ограниченный список последних сканирований. Если вы планируете в будущем повторно использовать настраиваемое сканирование, можно сохранить его в список избранных сканирований, присвоив ему значимое имя.

Чтобы сохранить последнее запущенное настраиваемое сканирование в список избранных сканирований, выполните следующие действия:

1. Откройте окно конфигурации настраиваемого сканирования.
   a. Откройте окно Bitdefender.
   b. Перейдите на панель **Антивирус**.
   c. Нажмите **Сканирование** и в раскрывающемся меню выберите **Выбор сканирования**.
2. Найдите требуемое сканирование в списке **Последние сканирования**.
3. Наведите курсор мыши на имя сканирования и щелкните значок ★, чтобы добавить сканирование в список избранных сканирований.
4. Введите значимое имя сканирования.

Сканирования, сохраненные в список избранного, помечены значком ★.Щелкните этот значок, после чего сканирование будет удалено из списка избранных сканирований.

Информация о параметрах сканирования

Эти сведения могут быть полезными:

- Значение незнакомых терминов можно посмотреть в глоссарии.Также вы можете найти полезную информацию в Интернете.

- **Проверка файлов.** В Bitdefender можно настроить, чтобы выполнялось только сканирование файлов или приложений (файлов программ) всех типов.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: 386; a6p; ac; accda; accdb; accdc; accde; accdp; accdr; accdt; accdu; acl; acr; action; ade; adp; air; app; as; asd; asp; awk; bas; bat; bin; cgi; chm; cla; class; cmd; cnv; com; cpl; csc; csh; dat; dek; dld; dll; doc; docm; docx; dot; dotm; dotx; drv; ds; ebm; esh; exe; ezs; fky; frs; fxp; gadget; grv; hlp; hms; hta; htm; html; iaf; icd; ini; inx; ipf; isu; jar; js; jse; jsx; kix; laccdb; lnk; maf; mam; maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mpp; mpt; mpx; ms; msg; msi; msp; mst; msu; oab; obi; obs; ocx; oft; ole; one; onepkg; ost; ovl; pa; paf; pex; pfd; php; pif; pip; pot; potm; potx; ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; prc; prf; prg; pst; pub; puz; pvd; pwc; py; pyc; pyo; qpx; rbx; rgs; rox; rpj; rtf; scar; scr; script; sct; shb; shs; sldm; sldx; smm; snp; spr; svd; sys; thmx; tlb; tms; u3p; udf; url; vb; vbe; vbs; vbscript; vxd; wbk; wcm; wdm; wiz; wll; wpk; ws; wsf; xar; xl; xla; xlam; xlb; xlc; xll; xlm; xls; xlsb; xlsm; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp

- **Параметры сканирования 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.

- **Сканировать загрузочные секторы.** Bitdefender можно настроить для сканирования загрузочных секторов жесткого диска.Этот сектор жесткого диска содержит компьютерный код, необходимый для запуска процесса загрузки.Заражение вирусом загрузочного сектора может привести к тому, что диск станет недоступен и вы не сможете загрузить систему и получить доступ к своим данным.

- **Проверка памяти.** Выберите этот параметр, чтобы выполнить сканирование программ, выполняющихся в системной памяти.
- **Проверка реестра.** Выберите этот параметр для сканирования ключей реестра.Реестр Windows — это база данных, в которой хранятся настройки и параметры конфигурации для компонентов операционной системы Windows и установленных приложений.
- **Сканировать cookies.** Выберите этот параметр, чтобы включить сканирование файлов cookie, сохраненных браузером на компьютере.
- **Проверить только новые и измененные файлы.** Сканируя только новые и измененные файлы, можно значительно повысить общее быстродействие системы с минимальными потерями в безопасности.
- **Пропускать коммерческие клавиатурные шпионы.** Выберите этот параметр, если вы установили и используете на компьютере коммерческие программы клавиатурных шпионов.Коммерческие клавиатурные шпионы — это законные программы мониторинга компьютеров, базовой функцией которых является запись текста, вводимого с клавиатуры.
- **Проверка на руткиты.** Выберите этот параметр для сканирование на наличие руткитов и объектов, скрытых с помощью такого программного обеспечения.

4.2.6. 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.Следуйте инструкциям мастера для завершения процесса сканирования.

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. Выполнение сканирования

Bitdefender начнет проверку выбранных объектов.В режиме реального времени отображается информация о статусе сканирования и статистике (время с начала сканирования, оценка оставшегося времени и количество обнаруженных угроз).Для просмотра подробных сведений перейдите по ссылке **Подробнее**.

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

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**.

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:

- **Пароль.** Если вы хотите, чтобы Bitdefender проверил архив, выберите этот параметр и введите пароль.Если вы не знаете пароля, выберите любой другой параметр.
- **Не спрашивать пароль и пропустить эти объекты без сканирования.** Выберите этот параметр, чтобы пропустить этот архив.
- **Пропустить все защищенные паролем элементы без их сканирования.** 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.

Выберите требуемый параметр и нажмите **OK** для продолжения сканирования.

Шаг 2. Выбор действий

На этапе завершения сканирования отобразится сообщение, предлагающее выбрать действия, которые будут выполняться для обнаруженных файлов (если есть).

Замечание

При выполнении быстрого сканирования или полного сканирования системы Bitdefender автоматически выполняет рекомендуемые действия в отношении файлов, обнаруженных во время сканирования.Если после сканирования все еще остались угрозы, вам будет предложено выбрать действия, которые следует предпринять по отношению к ним.

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:

Выполнить соотв. действия
Bitdefender выполнит рекомендуемые действия в зависимости от типа обнаруженного файла:

- **Зараженных файлов.** Файлы, распознанные как зараженные вирусом, соответствуют вирусным сигнатурам в базе данных вирусных сигнатур Bitdefender.Bitdefender попытается автоматически удалить вредоносный код из зараженного файла и изменить структуру исходного файла.Эта операция называется "лечение".

  Файлы, которые не удается вылечить, перемещаются в папку карантина во избежание распространения вируса.Добавленные в карантин файлы нельзя выполнять или открывать; таким образом, риск заражения сводится к нулю.Для получения дополнительной информации перейдите к *«Управление файлами в карантине»* (p. 55).

  Важно

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

- **Подозрительные файлы.** Файлы помечены эвристическим анализом как подозрительные. Невозможно вылечить подозрительные файлы, так как процедура лечения недоступна. Такие файлы будут перемещены в карантин во избежание заражения.

  По умолчанию файлы в карантине автоматически отправляются в лабораторию Bitdefender, где они анализируются специалистами по вирусам Bitdefender.Если наличие вредоносного ПО подтверждено, выпускается сигнатура, которая позволит удалить вредоносное ПО.

- **Архивы, содержащие зараженные файлы.**

  - Архивы, содержащие только зараженные файлы, будут удалены автоматически.
  - Если в архиве содержатся как зараженные, так и не зараженные файлы, Bitdefender попытается удалить зараженные файлы при условии, что возможно восстановление архива, содержащего не зараженные файлы.Если восстановить архив невозможно, вы получите уведомление о невозможности выполнения действия во избежание утраты очищенных файлов.

Удалить

Удаляет обнаруженные файлы с диска.

Если зараженные файлы хранятся в архиве вместе с не зараженными, Bitdefender попытается удалить зараженные файлы и восстановить архив, содержащие не зараженные файлы.Если восстановить архив невозможно, вы получите уведомление о невозможности выполнения действия во избежание утраты очищенных файлов.

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

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

Шаг 3. Сводка

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.

Нажмите **Закрыть**, чтобы закрыть окно.

Важно

В большинстве случаев Bitdefender успешно лечит зараженные файлы, которые обнаруживает, или изолирует инфекцию.Тем не менее, существуют проблемы, которые невозможно устранить автоматически.Если потребуется, перезагрузите вашу систему для завершения процесса очистки.Дополнительные сведения и инструкции по удалению вредоносных программ вручную см. в *«Удаление вредоносного ПО из системы»* (p. 133).

4.2.7. Просмотр журналов сканирования

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**.

Чтобы проверить журналы сканирования позднее, выполните следующие действия:

1. Откройте окно Bitdefender.
2. Нажмите кнопку **События** на верхней панели инструментов.
3. Нажмите **Антивирус** в меню слева и перейдите на вкладку **Сканирование на вирусы**.Здесь можно просмотреть все события сканирования на вирусы, включая угрозы, обнаруженные при резидентном сканировании, сканировании по инициативе пользователя, а также изменения статуса автоматического сканирования.

4. В списке событий можно посмотреть недавно выполненные сканирования.Нажмите на событие, чтобы просмотреть сведения о нем.
5. Чтобы открыть журнал сканирования, нажмите **Просмотреть журнал**.Отчет сканирования откроется в вашем web-браузере по умолчанию.

4.3. Автоматическое сканирование съемных носителей

Bitdefender автоматически определяет подключение съемного запоминающего устройства к компьютеру и выполняет его сканирование в фоновом режиме.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

Автоматическое сканирование можно настроить отдельно для каждой категории накопителей.Автоматическое сканирование сопоставленных сетевых дисков по умолчанию отключено.

4.3.1. Как он работает?

При обнаружении съемного носителя Bitdefender запускает операцию его сканирования на вирусы в фоновом режиме (если функция автоматического сканирования для этого типа устройств включена).В области уведомлений появится значок сканирования Bitdefender .Вы можете щелкнуть по этому значку, чтобы открыть окно сканирования и наблюдать прогресс проверки.

Если режим "Автопилот" включен, процесс сканирования не будет отвлекать вас.Информация о сканировании будет зарегистрирована и доступна только в окне События.

Если режим "Автопилот" отключен:

1. Откроется всплывающее окно с уведомлением о том, что новое устройство было обнаружено и выполняется его сканирование.
2. В большинстве случаев Bitdefender автоматически удаляет обнаруженное вредоносное ПО или изолирует зараженные файлы, помещая их в карантин.Если после сканирования остались неразрешенные угрозы, вам будет предложено выбрать действия, которые следует предпринять по отношению к ним.

Замечание
Обратите внимание, что в отношении инфицированных или подозрительных файлов, обнаруженных на CD/DVD, никакие действия не выполняются.

Действия также не выполняются в отношении инфицированных или подозрительных файлов, обнаруженных на назначенных сетевых дисках, если у пользователя нет соответствующих прав.

3. После завершения сканирования отображается окно с результатами, в котором указывается, безопасно ли использовать файлы на съемных носителях.

Следующая информация может оказаться вам полезной:

- Соблюдайте осторожность при использовании зараженных CD/DVD, так как удалить вредоносное ПО с дисков невозможно (носители доступны только для чтения).Убедитесь, что защита в реальном времени включена, чтобы предотвратить распространение вредоносных программ в системе.Рекомендуется скопировать все важные данные с диска в систему и затем избавиться от диска.
- В некоторых случаях Bitdefender не может удалять вирусы из определенных файлов по причине юридических или технических ограничений. Например, это могут быть файлы, заархивированные с помощью собственной технологии (при этом архив не может быть воссоздан корректно).

  Инструкции по обработке вредоносного ПО см. в *«Удаление вредоносного ПО из системы»* (p. 133)

4.3.2. Управление сканированием съемных носителей

Для управления автоматическим сканированием съемных носителей выполните следующие действия:

1. Откройте окно Bitdefender.
2. Нажмите кнопку **Настройки** на верхней панели инструментов.
3. Нажмите **Антивирус** в меню слева и перейдите на вкладку **Исключения**.
4. В разделе **Устройства, обнаруженные при сканировании** выберите типы устройств хранения, которые требуется сканировать автоматически.Нажмите на переключатель, чтобы включить или отключить автоматическое сканирование.

Для обеспечения наилучшей защиты рекомендуется включить автоматическое сканирование для всех типов съемных носителей.

Параметры сканирования предварительно настроены для достижения наилучших результатов обнаружения.Если обнаружены зараженные файлы, Bitdefender попытается их вылечить (удалить вредоносный код) или переместить в карантин. Если не удастся выполнить ни одну из этих операций, мастер антивирусного сканирования разрешит выбрать другие действия,

которые будут выполнены с зараженными файлами.Параметры сканирования стандартны, и вы не можете их изменить.

4.4. Настройка исключений сканирования

Bitdefender позволяет исключать определенные файлы, папки и расширения файлов из сканирования. Эта функция предназначена для того, чтобы исключить помехи для вашей работы и повысить производительность системы.Исключения могут быть использованы пользователями, которые имеют большой опыт работы с компьютерами, или в случае получения соответствующих рекомендаций от представителя Bitdefender.

Вы можете настроить исключения, которые будут применяться только для резидентного сканирования или сканирования по запросу либо в обоих случаях.Объекты не будут проверяться, если они исключены из списка входного сканирования, независимо от того, используются ли они вами, либо 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**.

4.4.1. Исключение файлов или папок из сканирования

Для исключения отдельных файлов или расширений файлов из сканирования выполните следующие действия:

1. Откройте окно Bitdefender.
2. Нажмите кнопку **Настройки** на верхней панели инструментов.
3. Нажмите **Антивирус** в меню слева и перейдите на вкладку **Исключения**.
4. Активируйте исключения сканирования для файлов, используя соответствующий переключатель.
5. Нажмите ссылку **Исключенные файлы и папки**.В открывшемся окне можно управлять файлами и папками, исключенными из сканирования.
6. Добавьте исключения, выполнив следующие действия:
   a. Нажмите кнопку **Добавить** в верхней части таблицы исключений.
   b. Нажмите **Обзор**, выберите файл или папку, которые требуется исключить из сканирования, и нажмите **OK**.Также путь к файлу или папке можно ввести (или скопировать и вставить) в поле редактирования.
   c. По умолчанию указанный файл или папка исключаются из резидентного сканирования и сканирования по запросу. Чтобы изменить правила применения исключений, выберите другой параметр.

d. Нажмите **Добавить**.

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

4.4.2. Исключение расширений файлов из сканирования

Если расширение файлов исключено из сканирования, Bitdefender больше не будет сканировать файлы с таким расширением, независимо от их местоположения на компьютере.Исключение также применяется к файлам на съемных носителях, таких как CD, DVD, USB-устройства и сетевые диски.

Важно

Соблюдайте осторожность при исключении расширений из сканирования, так как в результате этого компьютер может стать уязвимым для вредоносного ПО.

Для исключения расширений файлов из сканирования выполните следующие действия.

1. Откройте окно Bitdefender.
2. Нажмите кнопку **Настройки** на верхней панели инструментов.
3. Нажмите **Антивирус** в меню слева и перейдите на вкладку **Исключения**.
4. Активируйте исключения сканирования для файлов, используя соответствующий переключатель.
5. Нажмите ссылку **Исключенные расширения**.В открывшемся окне сканирования можно управлять расширениями файлов, исключенными из сканирования.
6. Добавьте исключения, выполнив следующие действия:
   a. Нажмите кнопку **Добавить** в верхней части таблицы исключений.
   b. Введите расширения, которые требуется исключить из сканирования, разделив их точкой с запятой (;).Пример:

      ```
      txt;avi;jpg
      ```

   c. По умолчанию все файлы с заданными расширениями исключаются из резидентного сканирования и сканирования по запросу. Чтобы изменить правила применения исключений, выберите другой параметр.
   d. Нажмите **Добавить**.
7. Нажмите **OK**, чтобы сохранить изменения, и закройте окно.

4.4.3. Управление исключениями сканирования

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

Для управления исключениями сканирования выполните следующие действия:

1. Откройте окно Bitdefender.
2. Нажмите кнопку **Настройки** на верхней панели инструментов.
3. Нажмите **Антивирус** в меню слева и перейдите на вкладку **Исключения**.Для управления исключениями сканирования используйте параметры в разделе **Файлы и папки**.
4. Чтобы удалить или изменить исключения сканирования, нажмите на одну из доступных ссылок.Выполните следующие действия:
   - Чтобы удалить запись из таблицы, выберите ее и нажмите кнопку **Удалить**.
   - Чтобы изменить запись в таблице, дважды нажмите на ней левой кнопкой мыши (или нажмите кнопку **Редактировать**).Откроется новое окно, в котором можно будет изменить расширение или путь к исключению и тип сканирования, из которого вы хотите его исключить. Внесите необходимые изменения и нажмите **Изменить**.
5. Чтобы отключить исключения сканирования, используйте соответствующий переключатель.

4.5. Управление файлами в карантине

Bitdefender изолирует зараженные вирусами файлы, которые невозможно вылечить, и подозрительные файлы в безопасной области, называемой карантином.Вирус, изолированный в карантинной зоне, не может причинить никакого вреда, так как его нельзя запустить или открыть для чтения.

По умолчанию файлы в карантине автоматически отправляются в лабораторию Bitdefender, где они анализируются специалистами по вирусам Bitdefender.Если наличие вредоносного ПО подтверждено, выпускается сигнатура, которая позволит удалить вредоносное ПО.

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

Для проверки и управления файлами в карантине выполните следующие действия:

1. Откройте окно Bitdefender.
2. Нажмите кнопку **Настройки** на верхней панели инструментов.
3. Нажмите **Антивирус** в меню слева и перейдите на вкладку **Карантин**.
4. Bitdefender автоматически управляет файлами в карантине в соответствии с настройками карантина по умолчанию.Вы можете изменить настройки

карантина в соответствии со своими потребностями, однако это делать не рекомендуется.

Сканировать карантин после обновления определений вирусов
Оставьте этот параметр включенным, чтобы сканирование файлов в карантине выполнялось автоматически после обновления определений вирусов.Очищенные файлы автоматически возвращаются на свое место.

Отправить файлы в карантине в Bitdefender для дальнейшего анализа
Оставьте этот параметр включенным, чтобы файлы, помещенные в карантин, автоматически отправлялись в лабораторию Bitdefender.Специалисты по вирусам Bitdefender проанализируют образцы файлов.Если наличие вредоносного ПО подтверждено, выпускается сигнатура, которая позволит удалить вредоносное ПО.

Удалять содержимое старше {30} дн.
По умолчанию файлы в карантине, созданные более 30 дней назад, удаляются автоматически.Чтобы изменить интервал, введите новое значение в соответствующем поле.Чтобы отключить автоматическое удаление старых файлов в карантине, введите 0.

5. 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**.

4.6. Активный вирусный контроль

Функция активного вирусного контроля Bitdefender — это инновационная технология проактивного обнаружения, использующая расширенные эвристические методы выявления новых потенциальных угроз в режиме реального времени.

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 общая оценка для процесса достигает установленного порогового значения, процесс признается опасным и автоматически блокируется.

Если режим "Автопилот" отключен, будут отображаться всплывающие окна с уведомлениями о блокировке приложений.В противном случае приложения будут заблокированы без уведомления.В окне События можно посмотреть, какие приложения были найдены активным вирусным контролем.

4.6.1. Проверка обнаруженных приложений

Для просмотра приложений, обнаруженных функцией активного вирусного контроля, выполните следующие действия:

1. Откройте окно Bitdefender.
2. Нажмите кнопку **События** на верхней панели инструментов.
3. Нажмите **Антивирус** в меню слева и перейдите на вкладку **Активный вирусный контроль**.
4. Нажмите на событие, чтобы просмотреть сведения о нем.
5. Если вы доверяете приложению, вы можете настроить, чтобы активный вирусный контроль не блокировал его, нажав кнопку **Разрешить и отслеживать**.Активный вирусный контроль продолжит мониторинг исключенных приложений. Если будет обнаружено выполнение подозрительных действий исключенным приложением, событие будет зарегистрировано в журнале и передано в облако Bitdefender как ошибка обнаружения.

4.6.2. Включение и отключение активного вирусного контроля

Чтобы включить или отключить активный вирусный контроль, выполните следующие действия:

1. Откройте окно Bitdefender.
2. Нажмите кнопку **Настройки** на верхней панели инструментов.
3. Нажмите **Антивирус** в меню слева и перейдите на вкладку **Экран**.
4. Нажмите на переключатель, чтобы включить или отключить активный вирусный контроль.

4.6.3. Настройка защиты с помощью активного вирусного контроля

Если вы замечаете, что функция активного вирусного контроля часто обнаруживает легальные приложения, установите более низкий уровень защиты.

Для настройки защиты с помощью функции активного вирусного контроля выполните следующие действия:

1. Откройте окно Bitdefender.
2. Нажмите кнопку **Настройки** на верхней панели инструментов.
3. Нажмите **Антивирус** в меню слева и перейдите на вкладку **Экран**.
4. Убедитесь, что активный вирусный контроль включен.
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.

Замечание

При установке более высокого уровня защиты для функции активного вирусного контроля будет требоваться меньше признаков вирусного поведения для регистрации процесса как вредоносного. В результате этого повысится количество приложений, признанных вредоносными. При этом также повышается вероятность ошибочных результатов (чистые приложения отмечаются как вредоносные).

4.6.4. Управление исключенными процессами

Вы можете настроить правила исключения для доверенных приложений, чтобы активный вирусный контроль не блокировал их, когда они выполняют операции с признаками вредоносного поведения.Активный вирусный контроль продолжит мониторинг исключенных приложений. Если будет обнаружено выполнение подозрительных действий исключенным приложением, событие будет зарегистрировано в журнале и передано в облако Bitdefender как ошибка обнаружения.

Для управления исключениями процесса активного вирусного контроля выполните следующие действия:

1. Откройте окно Bitdefender.
2. Нажмите кнопку **Настройки** на верхней панели инструментов.
3. Нажмите **Антивирус** в меню слева и перейдите на вкладку **Исключения**.
4. Нажмите ссылку **Исключенные процессы**.В открывшемся окне можно управлять исключениями процессов функции активного антивирусного контроля.

Замечание

Исключения процессов также применяются к системе обнаружения вторжений, входящей в брандмауэр Bitdefender.

5. Добавьте исключения, выполнив следующие действия:
   a. Нажмите кнопку **Добавить** в верхней части таблицы исключений.
   b. Нажмите **Обзор**, выберите приложение, которое требуется исключить, и нажмите **OK**.
   c. Оставьте выбранным параметр **Разрешить**, чтобы функция активного вирусного контроля не блокировала приложение.
   d. Нажмите **Добавить**.
6. Чтобы удалить или изменить исключения, выполните следующие действия:
   - Чтобы удалить запись из таблицы, выберите ее и нажмите кнопку **Удалить**.

- Чтобы изменить запись в таблице, дважды нажмите на ней левой кнопкой мыши (или нажмите кнопку **Редактировать**).Внесите необходимые изменения и нажмите **Изменить**.

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

4.7. Устранение уязвимостей системы

Важный шаг в защите вашего компьютера от злоумышленников и вредоносного ПО состоит в том, чтобы держать операционную систему и используемые приложения в обновленном состоянии.Рассмотрите вариант отключения настроек Windows, которые делают систему более уязвимой к вредоносному ПО.Более того, чтобы предотвратить несанкционированный доступ к компьютеру, каждую учетную запись Windows необходимо снабдить сильным паролем (паролем, который трудно угадать).

Bitdefender предоставляет два простых способа устранения уязвимостей системы:

- Проверить систему на наличие уязвимостей и устранить их можно с помощью мастера **поиска уязвимостей**.
- Используя функцию автоматического мониторинга уязвимостей, в окне События можно просматривать и устранять обнаруженные уязвимости.

Поиск и устранение уязвимостей системы следует выполнять каждую неделю или один раз в две недели.

4.7.1. Сканирование системы на наличие уязвимостей

Чтобы устранить уязвимости системы, используя мастер поиска уязвимостей, выполните следующие действия:

1. Откройте окно Bitdefender.
2. Перейдите на панель **Антивирус**.
3. Нажмите **Сканировать** и выберите **Поиск уязвимостей**.
4. 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**.
   a. **Защитите свой ПК**

      Выберите уязвимости для проверки.

   b. **Наличие неисправностей**

      Подождите, пока Bitdefender завершит проверку системы на наличие уязвимостей.

   c. **Обновления Windows**

Вы можете просмотреть список важных и второстепенных обновлений Windows, которые в данный момент не установлены на вашем компьютере.Выберите обновления для установки.

Чтобы начать установку выбранных обновлений, нажмите **Далее**.Обратите внимание, что установка обновлений может занять некоторое время и для завершения установки некоторых из них потребуется перезагрузка системы.Если требуется, выполните перезагрузку системы при первой возможности.

d. **Обновления приложения**

Если приложение нуждается в обновлении, щелкните появившуюся ссылку, чтобы загрузить последнюю версию.

e. **Ненадежные 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.Вы можете выбрать, чтобы пользователю был выдан запрос на изменение пароля при следующем входе в систему, или изменить пароль самостоятельно в настоящий момент.Чтобы пароль был сильным, используйте комбинации символов в верхнем и нижнем регистре, числа и специальные символы (такие как, например, #, $ или @).

f. **Резюме**

Здесь можно просмотреть результаты операции.

4.7.2. Использование автоматического мониторинга уязвимостей

Bitdefender регулярно сканирует в фоновом режиме систему на наличие уязвимостей. Сведения об обнаруженных проблемах регистрируются в окне События.

Чтобы просмотреть и исправить обнаруженные проблемы, выполните следующие действия:

1. Откройте окно Bitdefender.
2. Нажмите кнопку **События** на верхней панели инструментов.
3. Нажмите **Антивирус** в меню слева и перейдите на вкладку **Уязвимости**.
4. Вы можете просмотреть подробные сведения об обнаруженных уязвимостях системы.В зависимости от проблемы, для того чтобы устранить конкретную уязвимость, предпримите следующие действия:
   - Если доступны обновления для Windows, нажмите **Обновить**, чтобы запустить мастер проверки уязвимостей и установить обновления.

- Если приложение устарело, нажмите **Обновить**, чтобы найти ссылку на веб-страницу поставщика, с которой можно установить последнюю версию приложения.
- Если для учетной записи Windows установлен слабый пароль, нажмите **Исправить пароль**, чтобы принудить пользователя сменить пароль при следующем входе в систему, или смените его сами.Чтобы пароль был сильным, используйте комбинации символов в верхнем и нижнем регистре, числа и специальные символы (такие как, например, #, $ или @).
- Если функция автозапуска Windows включена, нажмите **Отключить**, чтобы отключить ее.

Для настройки параметров мониторинга уязвимостей выполните следующие действия:

1. Откройте окно Bitdefender.
2. Нажмите кнопку **Настройки** на верхней панели инструментов.
3. Нажмите **Антивирус** в меню слева и перейдите на вкладку **Уязвимости**.
4. Нажмите на переключатель, чтобы включить или отключить автоматический поиск уязвимостей.

Важно

Для автоматического получения уведомлений об уязвимостях системы или приложений параметр **Автоматическая проверка на наличие уязвимостей** должен быть включен.

5. Используя соответствующие переключатели, выберите уязвимости системы, которые требуется регулярно проверять.

   Критические обновления Windows

   Проверьте, установлены ли последние критические обновления безопасности для операционной системы Windows, выпущенные корпорацией Microsoft.

   Регулярные обновления Windows

   Проверьте, установлены ли последние обновления безопасности для Windows, выпущенные корпорацией Microsoft.

   Обновления приложения

   Проверьте, обновлены ли основные веб-приложения, установленные в системе.Устаревшие приложения могут быть использованы вредоносными программами, что делает компьютер уязвимым для атак извне.

   Ненадежные пароли

   Проверьте, насколько легко можно подобрать пароли, установленные для учетных записей Windows.Если установлены пароли, которые сложно

подобрать (надежные пароли), хакерам будет непросто проникнуть в вашу систему.Сильный пароль включает символы в верхнем и нижнем регистре, числа и специальные символы (например, #, $ или @).

Автозапуск носителя

Проверьте статус функции автозапуска Windows.Эта функция обеспечивает возможность автоматического запуска приложений с CD, DVC, USB-устройств и других внешних устройств.

Некоторые типы вредоносных программ используют функцию автозапуска, чтобы автоматически передавать вирус со съемного носителя на компьютер. Поэтому рекомендуется отключить данную функцию в Windows.

Замечание

Если мониторинг определенных уязвимостей отключен, соответствующие проблемы больше не будут регистрироваться в окне "События".

5. 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 «*О модуле "Антиспам"*» (p. 63).

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.

5.1. О модуле "Антиспам"

5.1.1. Фильтры модуля Антиспам

Механизм ядра антиспама Bitdefender состоит из нескольких разных фильтров, надежно защищающих папку входящих сообщений от спама: Список друзей,

Список спамеров, Фильтр символов, Фильтры ссылок, Фильтр сигнатур, Фильтр NeuNet (эвристический) и "Облачная" технология распознавания.

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 ссылок

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 ссылок проверяет все URL-адреса в сообщении на наличие их в базе данных. В случае совпадения сообщение помечается как СПАМ.

Фильтр сигнатур

Специалисты по спаму Bitdefender постоянно анализируют сообщения спама в естественных условиях и выпускают сигнатуры спама, чтобы обеспечить возможность их обнаружения.

Фильтр сигнатур проверяет электронную почту, используя сигнатуры спама из локальной базы данных.Если обнаружено совпадение, сообщение помечается как СПАМ.

Замечание

Фильтр сигнатур, в отличие от других фильтров, нельзя отключить без отключения защиты антиспама.

NeuNet (эвристический) фильтр

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.В зависимости от результатов анализа сообщению электронной почты присваивается рейтинг спама.

Если оценка спама превышает пороговый уровень, письмо считается СПАМОМ.Пороговый уровень определяется уровнем чувствительности антиспама.Для получения дополнительной информации перейдите к «*Настройка уровня чувствительности*» (p. 71).

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.

"Облачная" технология распознавания

Функция обнаружения в облаке использует облачные службы Bitdefender для обеспечения эффективной и всегда актуальной защиты от спама.

Электронные сообщения в облаке проверяются, только если локальные фильтры антиспама не позволяют получить конкретный результат.

5.1.2. Работа модуля "Антиспам"

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**.

Фильтр ссылок 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 сигнатур проверяет электронную почту, используя сигнатуры спама из локальной базы данных.Если обнаружено совпадение, сообщение помечается 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.

Если оценка спама превышает пороговый уровень, письмо считается СПАМОМ.Пороговый уровень определяется уровнем защиты антиспама.Для получения дополнительной информации перейдите к *«Настройка уровня чувствительности»* (p. 71).

Если локальные фильтры антиспама не позволяют получить конкретный результат, выполняется проверка письма в облаке, по итогам которой определяется, является ли письмо спамом.

5.1.3. Обновления антиспама

При каждом обновлении в базу данных добавляются сигнатуры известных адресов электронной почты и ссылок, являющихся спамом.Это поможет повысить эффективность Антиспама.

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

5.1.4. Поддерживаемые почтовые клиенты и протоколы

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

- Microsoft Outlook 2007/2010
- Microsoft Outlook Express и Почта Windows (в 32-разрядных системах)
- Mozilla Thunderbird 3.0.4

5.2. Включение и отключение защиты антиспама

Для включения или отключения защиты антиспама выполните следующие действия:

1. Откройте окно Bitdefender.

2. Перейдите на панель **Антиспам**.
3. Нажмите на переключатель, чтобы включить или отключить защиту антиспама.

5.3. Использование панели инструментов антиспама в окне почтового клиента

В верхней части вашей почтовой программы вы можете заметить 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 *«Поддерживаемые почтовые клиенты и протоколы»* (p. 66).

Ниже приводится описание каждой кнопки панели инструментов Bitdefender:

Это спам: показывает, что выбранное сообщение является спамом.Сообщение будет незамедлительно перемещено в папку **Спам**.Если облачные службы антиспама включены, в облако Bitdefender будет отправлено сообщение для дальнейшего анализа.

Не спам: показывает, что выбранное сообщение электронной почты не является спамом и Bitdefender не должен помечать его.Письмо будет перемещено из папки **Спам** в папку **Входящие**.Если облачные службы антиспама включены, в облако Bitdefender будет отправлено сообщение для дальнейшего анализа.

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. 70).

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. 69).

Настройки: открытие окна, в котором можно настроить фильтры антиспама и параметры панели управления.

5.3.1. Отображение обнаружения ошибок

Если вы используете поддерживаемый почтовый клиент, вы можете легко корректировать фильтр антиспама, указывая, какие письма не следует помечать как [спам]. Это поможет повысить эффективность фильтра антиспама.Следуйте инструкции:

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 инструментов антиспама Bitdefender (обычно расположена в верхней части окна почтового клиента).Письмо будет перемещено в папку "Входящие".

5.3.2. Обозначение необнаруженных сообщений спама

Если вы используете поддерживаемый почтовый клиент, вы можете легко указать, какие сообщения должны были быть определены как спам. Это позволит существенно повысить эффективность фильтра антиспама.Следуйте инструкции:

1. Откройте ваш почтовый клиент.
2. Перейти к папке "Входящие".
3. Выберите необнаруженные спам-сообщения.
4. Нажмите кнопку **Это спам** на панели инструментов антиспама Bitdefender (обычно расположена в верхней части окна почтового клиента). Они будут помечены как [спам] и перемещены в папку спама.

5.3.3. Настройка параметров панели инструментов

Чтобы настроить панель управления антиспама для почтового клиента, нажмите кнопку **Настройки** на панели инструментов и перейдите на вкладку **Панель инструментов**.

Настройки сгруппированы по двум категориям:

- В категории **Правила электронной почты** можно настроить правила обработки сообщений спама, обнаруженных продуктом Bitdefender.
  - **Переместить сообщение в папку "Удаленные"** (только для Microsoft Outlook Express/Почта Windows)

    Замечание
    В Microsoft Outlook/Mozilla Thunderbird обнаруженные сообщения спама автоматически помещаются в папку "Спам", расположенную в папке "Удаленные"/"Корзина".

  - **Пометить спам-сообщения как прочтенные**: письма спама автоматически отмечаются как прочитанные, чтобы они не отвлекали пользователей при поступлении.
- В категории **Уведомления** можно настроить отображение окна подтверждения при нажатии кнопок **Добавить спамера** и **Добавить друга** на панели инструментов антиспама.Окна подтверждения позволяют предотвращать случайное добавление отправителей электронной почты в списки друзей и спамеров.

5.4. 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 окно Bitdefender.
  2. Перейдите на панель **Антиспам**.

3. Нажмите **Управление** и в меню выберите **Друзья**.

Чтобы добавить адрес электронной почты, выберите параметр **Эл. почта**, введите адрес и нажмите **Добавить**.Адрес должен иметь следующую структуру: name@domain.com.

Чтобы добавить адреса электронной почты с определенного домена, выберите параметр **Имя домена**, введите имя домена и нажмите **Добавить**.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, нажмите соответствующую ссылку **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 **OK**, чтобы сохранить изменения, и закройте окно.

5.5. 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 окно Bitdefender.
2. Перейдите на панель **Антиспам**.
3. Нажмите **Управление** и в меню выберите **Спамеры**.

Чтобы добавить адрес электронной почты, выберите параметр **Эл. почта**, введите адрес и нажмите **Добавить**.Адрес должен иметь следующую структуру: name@domain.com.

Чтобы добавить адреса электронной почты с определенного домена, выберите параметр **Имя домена**, введите имя домена и нажмите **Добавить**.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, нажмите соответствующую ссылку **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 **OK**, чтобы сохранить изменения, и закройте окно.

5.6. Настройка уровня чувствительности

Если вы заметили, что некоторые легальные письма помечаются как спам или многие сообщения спама не распознаются, для решения этой проблемы можно

настроить уровень чувствительности антиспама.Тем не менее, вместо того, чтобы изменить отдельно уровень чувствительности, рекомендуется сначала прочитать «*Фильтр антиспама работает некорректно*» (p. 125) и следовать инструкциям по устранению проблемы.

Для настройки уровня чувствительности антиспама выполните следующие действия:

1. Откройте Bitdefender.
2. Нажмите кнопку **Настройки** на верхней панели инструментов.
3. Нажмите **Антиспам** в меню слева, затем вкладку **Настройки**.
4. Воспользуйтесь описанием справа от шкалы, чтобы выбрать уровень чувствительности, оптимально соответствующий вашим требованиям безопасности.В описании также приведены сведения о дополнительных действиях, которые необходимо выполнить во избежание проблем или в целях повышения эффективности распознавания спама.

5.7. Настройка локальных фильтров антиспама

Как описано в «*О модуле "Антиспам"*» (p. 63), для распознавания спама Bitdefender использует комбинацию из нескольких различных фильтров антиспама.Фильтры антиспама предварительно настроены в целях обеспечения эффективной защиты.

Важно

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

Для настройки локальных фильтров антиспама выполните следующие действия:

1. Откройте окно Bitdefender.
2. Нажмите кнопку **Настройки** на верхней панели инструментов.
3. Нажмите **Антиспам** в меню слева, затем вкладку **Настройки**.
4. Используйте переключатели, чтобы включить или отключить локальные фильтры антиспама.

Если вы используете Microsoft Outlook/Outlook Express/Windows Mail/Thunderbird, локальные фильтры антиспама можно настроить непосредственно из почтового клиента.Нажмите кнопку **Настройки** на панели инструментов антиспама

Bitdefender (обычно расположена в верхней части окна почтового клиента) и затем перейдите на вкладку **Антиспам-фильтры**.

5.8. Настройка обнаружения в облаке

Функция обнаружения в облаке использует облачные службы Bitdefender для обеспечения эффективной и всегда актуальной защиты от спама.

Для настройки обнаружения в облаке выполните следующие действия:

1. Откройте окно Bitdefender.
2. Нажмите кнопку **Настройки** на верхней панели инструментов.
3. Нажмите **Антиспам** в меню слева и перейдите на вкладку **Облако**.
4. Нажмите на переключатель, чтобы включить или отключить обнаружение в облаке.
5. Примеры законных сообщений и спама можно отправить в облако Bitdefender при обнаружении ошибок и пропущенных сообщений спама. Это позволит повысить точность распознавания спама Bitdefender.Настройте отправку образцов сообщений электронной почты в облако Bitdefender, выбрав нужные параметры.

Если вы используете Microsoft Outlook/Outlook Express/Windows Mail/Thunderbird, функцию обнаружения в облаке можно настроить непосредственно из почтового клиента.Нажмите кнопку **Настройки** на панели инструментов антиспама Bitdefender (обычно расположена в верхней части окна почтового клиента) и перейдите на вкладку **Настройки облака**.

6. Защита данных

Кибер-преступники постоянно стремятся получить доступ к вашей личной информации.Поскольку угрозы существуют практически во всех областях, связанных с работой в Интернете, отсутствие надлежащей защиты для электронной почты, мгновенных сообщений и веб-браузеров может приводить к возникновению утечки информации, подвергая риску вашу конфиденциальность.

Модуль защиты личных данных Bitdefender устраняет эти угрозы с помощью различных компонентов.

- Антифишинг — комплексный набор функций, обеспечивающих защиту при работе в Интернете, включая предотвращение отправки личной информации через мошеннические сайты, замаскированные под законные.
- Защита данных помогает гарантировать, что ваша личная информация не будет отправлена с вашего компьютера без вашего ведома.Модуль сканирует электронную почту и мгновенные сообщения, отправляемые с компьютера, а также данные, передаваемые через веб-страницы, и блокирует любые фрагменты информации, защищенной созданными вами правилами защиты данных.
- Шифрование чата: шифрование мгновенных сообщений для того, чтобы их содержимое было доступно только вам и вашим собеседникам.

6.1. 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
- Google Chrome
- Safari
- Opera
- Yahoo! Messenger

Для настройки параметров антифишинга выполните следующие действия:

1. Откройте окно Bitdefender.
2. Нажмите кнопку **Настройки** на верхней панели инструментов.
3. Нажмите **Защита данных** в меню слева и перейдите на вкладку **Антифишинг**.

Настройки сгруппированы по двум категориям.

Функции панели инструментов

Нажмите на переключатели, чтобы включить или отключить:

- Отображение панели инструментов Bitdefender в браузере.
- Модуль оптимизации поиска присваивает рейтинг для результатов поиска в системах Google, Bing и Yahoo! и ссылок из Facebook и Twitter, размещая значок перед каждым результатом:

  Эту веб-страницу посещать не следует.

  Эта веб-страница может содержать опасную информацию. Соблюдайте осторожность, если вы решите открыть ее.

  Эта страница безопасна для посещения.
- Сканирование веб-трафика SSL.

  При более сложных атаках для ввода пользователей в заблуждение может использоваться защищенный интернет-трафик.Поэтому рекомендуется включить сканирование SSL.

Защита для веб-браузеров

Нажмите на переключатели, чтобы включить или отключить:

- Защита от мошенничества.
- Защита от фишинга.
- Защита для мгновенных сообщений.

Можно создать список веб-сайтов, для которых сканирование антифишингом Bitdefender выполняться не будет.Список должен содержать только веб-сайты, которым вы полностью доверяете.Например, добавьте туда веб-сайты, где вы совершаете интернет-покупки.

Для настройки белого списка антифишинга и управления им нажмите ссылку **Белый список**.Появится новое окно.

Чтобы добавить сайт в белый список, введите его адрес в соответствующем поле и нажмите **Добавить**.

Чтобы удалить веб-сайт из списка, выберите его в списке и нажмите соответствующую ссылку **Удалить**.

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

6.1.1. Защита Bitdefender в веб-браузере

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

- Internet Explorer

- Mozilla Firefox
- Google Chrome
- Safari
- Opera

Панель инструментов Bitdefender отличается от стандартной панели инструментов браузера.В браузере появляется только небольшой значок перетаскивания в верхней части каждой веб-страницы.Нажмите, чтобы показать панель инструментов.

Верхняя панель инструментов Bitdefender содержит следующие инструменты:

Рейтинг страницы

В зависимости от результатов классификации просматриваемой веб-страницы системой Bitdefender в левой части панели инструментов отображается один из следующих рейтингов:

- Появляется сообщение "Страница является небезопасной" на красном фоне: следует незамедлительно закрыть веб-страницу.
- Сообщение "Рекомендуется соблюдать осторожность" на оранжевом фоне: эта веб-страница может включать опасное содержимое.Соблюдайте осторожность, если вы решите посетить его.
- Сообщение "Эта страница безопасна" на зеленом фоне: эта страница является безопасной для просмотра.

Sandbox

Нажмите , чтобы запустить браузер в изолированной от операционной системы среде Bitdefender.Это позволяет предотвратить использование браузерными угрозами уязвимостей браузера для получения контроля над системой.Используйте Sandbox при посещении веб-страниц, которые могут содержать вредоносное ПО.

Замечание
Sandbox недоступен на компьютерах с ОС Windows XP.

Настройки

Нажмите , чтобы включить или отключить отдельные функции.

- Фильтр фишинга
- Фильтр вредоносных программ
- Оптимизация поиска

Выключатель питания

Чтобы полностью включить или отключить функции панели инструментов, нажмите справа от панели инструментов.

6.1.2. Уведомления Bitdefender в браузере

Если открываемый веб-сайт классифицируется как небезопасный, он блокируется и в браузере отображается страница предупреждения.

На этой странице содержится такая информация, как URL веб-сайта и обнаруженные угрозы.

Вам необходимо принять решение по дальнейшим действиям. Доступные варианты:

- Закройте веб-страницу.
- Игнорируя предупреждение, перейдите на веб-страницу, нажав кнопку **Я осознаю риск. Перейти все равно.**
- Добавьте страницу в белый список антифишинга, нажав **Добавить в белый список**.Системы антифишинга Bitdefender больше не выполняют сканирование страницы.

6.2. Защита данных

Функция защиты данных позволяет предотвратить утечку важных данных во время работы в Интернете.

Рассмотрим простой пример: пользователь создал правило защиты данных, которое обеспечивает защиту номера кредитной карты.Если шпионская программа каким-либо образом была установлена на компьютер, она не сможет отправлять номера кредитных карт по электронной почте, через мгновенные сообщения и веб-сайты.Кроме того, ваши дети не смогут совершать с ее помощью покупки в Интернете и сообщать номер карты людям, с которыми они познакомились по Интернету.

6.2.1. О защите данных

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.

Основываясь на созданных вами правилах, модуль защиты данных сканирует веб-трафик, электронную почту и трафик мгновенных сообщений на совпадение с определенным набором символов (например, с номером вашей кредитной карты). В случае совпадения соответствующая веб-страница, сообщение электронной почты или мгновенное сообщение блокируются.

Вы можете создать правила для зашиты информации, которую вы считаете личной или конфиденциальной, от своего телефонного номера или адреса электронной почты до сведений о своем банковском счете.Многопользовательская поддержка обеспечивает возможность настройки и использования индивидуальных правил для разных учетных записей Windows.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.

6.2.2. Настройка защиты данных

Если требуется использовать функцию защиты данных, выполните следующие действия:

1. Откройте окно Bitdefender.
2. Нажмите кнопку **Настройки** на верхней панели инструментов.
3. Нажмите **Защита данных** в меню слева и перейдите на вкладку **Защита данных**.
4. Убедитесь, что защита данных включена.
5. Создайте правила для защиты ваших данных.Для получения дополнительной информации перейдите к «*Создание правил защиты данных*» (p. 78).

Создание правил защиты данных

Чтобы создать правило, нажмите кнопку **Добавить правило** и следуйте инструкциям мастера настройки.Навигация по мастеру осуществляется с помощью кнопок **Далее** и **Назад**.Для выхода из мастера нажмите **Отмена**.

1. **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 карточки, 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.

2. **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 же 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.

3. **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.

Теперь при попытке отправить указанные данные (по электронной почте, в мгновенных сообщениях или через веб-страницы) операцию выполнить не удастся.В окне События будет показана запись, указывающая на то, что Bitdefender заблокировал отправку личных данных.

6.2.3. Управление правилами

Управление правилами защиты данных:

1. Откройте окно Bitdefender.
2. Нажмите кнопку **Настройки** на верхней панели инструментов.
3. Нажмите **Защита данных** в меню слева и перейдите на вкладку **Защита данных**.

В этом окне вы видите список правил, приведенный в таблице.

Для удаления правила необходимо выбрать его и нажать кнопку **Удалить правило**.

Чтобы изменить правило, выберите его и нажмите кнопку **Редактировать**. Откроется новое окно.Здесь вы можете изменять название, описание и параметры правила (тип, данные и вид трафика). Нажмите **OK**, чтобы сохранить изменения.

6.3. 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 установлен продукт Bitdefender, который поддерживает шифрование чата, и эта функция включена в используемой программе мгновенных сообщений.
- Вы и ваш собеседник в чате используете Yahoo! Messenger.

Важно

Bitdefender не применяет шифрование диалогов, если один из пользователей чата использует веб-приложение, например Meebo.

Настройка шифрования мгновенных сообщений:

1. Откройте окно Bitdefender.
2. Нажмите кнопку **Настройки** на верхней панели инструментов.
3. Нажмите **Защита данных** в меню слева и перейдите на вкладку **Шифрование**.

По умолчанию шифрование чата включено.Для отключения шифрования чата используйте соответствующий переключатель.

7. 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.

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.

7.1. 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 *«Как создать учетную запись пользователя Windows?»* (p. 30).

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 *«Защищенные паролем настройки Bitdefender»* (p. 12).

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 окно Bitdefender.
3. Нажмите кнопку **Настройки** на верхней панели инструментов.
4. Нажмите **Родительский контроль** в меню слева и перейдите на вкладку **Учетные записи**.Здесь можно проверить и настроить параметры родительского контроля для каждой учетной записи пользователя Windows.Если функция родительского контроля включена, вы можете посмотреть выбранную возрастную категорию и состояние родительского контроля (подробнее будет описано позднее).

Настройка родительского контроля для конкретной учетной записи пользователя:

1. Для включения родительского контроля для этой учетной записи пользователя установите соответствующий флажок.
2. Введите возраст своего ребенка, нажав на одно из полей, соответствующих параметру **Возраст**.Когда пользователь указывает возраст ребенка, автоматически загружаются настройки, соответствующие данной категории возраста (на основе стандартов детского развития).
3. Если требуется детальная настройка параметров родительского контроля, нажмите **Настройки**.Перейдите на вкладку конфигурации соответствующей функции родительского контроля:

   - **Сеть**: фильтрация операций и настройка ограничений времени доступа к Интернету с использованием функции Веб-контроль.
   - **Приложения**: настройка блокировки или ограничения к доступа к определенным приложениям функцией контроля приложений.
   - **Ключевые слова**: фильтрация веб-сайтов, почты и мгновенных сообщений на основе ключевых слов с помощью модуля контроля ключевых слов.
   - **Службы мгновенных сообщений (IM)**: настройка контроля мгновенных сообщений для разрешения или блокировки чатов с определенными контактами служб мгновенных сообщений Yahoo! Messenger.
   - **Категории**: блокировка определенных категорий содержимого веб-страниц с помощью фильтра категорий.

   Чтобы закрыть окно настроек родительского контроля, нажмите кнопку X в правом верхнем углу окна.Установленные настройки сохраняются автоматически.

Для настройки параметров отслеживания активности и удаленного родительского контроля перейдите на вкладку **Настройки**.Настройте параметры отслеживания по своему выбору:

Отправлять отчеты 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 *«Мониторинг активности детей»* (p. 89).

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. 91).

7.1.1. Веб-контроль

Функция веб-контроля помогает блокировать веб-сайты с неподобающим содержимым и устанавливать ограничения на доступ к Интернету.

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. 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.
5. Можно установить ограничения по времени для работы детей в Интернете.Для получения дополнительной информации перейдите к «Ограничение доступа в Интернет по времени» (p. 84).

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, выберите его и нажмите **Удалить**.

Чтобы изменить правило, дважды щелкните по нему (или выберите правило и нажмите **Изменить**).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 **Предел доступа в Интернет**.
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.Чтобы перейти к новому выбору, нажмите **Заблокировать все** или **Разрешить все**.
4. Нажмите **Сохранить**.

Замечание

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

7.1.2. 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 **Блокировать** или **Ограничить**.
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.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**.
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, выберите его и нажмите **Удалить**.

Чтобы изменить правило, дважды щелкните по нему (или выберите правило и нажмите **Изменить**).Внесите необходимые изменения в окне конфигурации.

7.1.3. 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.Кроме того, вы можете гарантировать, что они не будут передавать личную информацию (например, домашний адрес или номер телефона) людям, с которыми они познакомились в Интернете.

Замечание

Функция контроля ключевых слов в службе обмена мгновенными сообщениями доступна только для Yahoo! 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, чтобы предотвратить отображение неподобающих слов и отправку важной информации.

Создание правил контроля ключевых слов

Чтобы заблокировать слово или фразу, следуйте этим шагам:

1. Нажмите **Блокировать ключевое слово**.
2. Настроить информацию о ключевых словах.
   - **Категория слова**: введите в этом поле имя правила.
   - **Ключевое слово**: введите в этом поле слово или фразу, которые требуется блокировать.Если требуется, чтобы система находила только слова целиком, поставьте флажок в поле **Совпадение слов целиком**.
3. Выберите тип фильтрации.
   - **Блокировать просмотр**: выберите этот параметр для создаваемых правил, чтобы предотвратить отображение неподобающих слов.
   - **Блокировать отправку**: выберите этот параметр для создаваемых правил, чтобы предотвратить отправку важной информации.
4. Выберите тип трафика, который должен сканировать Bitdefender на наличие определенного слова.

Настройка	Описание
Сеть	Блокируются веб-страницы, содержащие ключевое слово.
E-mail	Блокируются электронные сообщения, содержащие ключевое слово.
IM клиент	Блокируются мгновенные сообщения, содержащие ключевое слово.

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

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.

Управление правилами контроля ключевых слов

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

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

Чтобы изменить правило, дважды щелкните по нему (или выберите правило и нажмите **Изменить**).Внесите необходимые изменения в окне конфигурации.

7.1.4. Контроль Службы Мгновенных Сообщений

Контроль службы мгновенных сообщений (IM) позволяет указать, с кем из IM-контактов могут беседовать ваши дети.

Замечание
Контроль служб обмена мгновенными сообщениями доступен только для Yahoo! Messenger.

Настройка IM-контроля для отдельных пользовательских учетных записей:

1. Откройте окно настроек родительского контроля Bitdefender для этой учетной записи пользователя.
2. Перейдите на вкладку **Службы мгновенных сообщений (IM)**.
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

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 желаемое действие для этого правила — **Разрешить** или **Блокировать**
4. Нажмите **Завершить**, чтобы добавить правило.

Управление правилами контроля мгновенных сообщений

Настроенные правила IM-контроля приведены в таблице в нижней части окна.

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

Чтобы изменить правило, дважды щелкните по нему (или выберите правило и нажмите **Изменить**).Внесите необходимые изменения в окне конфигурации.

7.1.5. Фильтр категорий

Фильтр категорий выполняет динамическую фильтрацию доступа к веб-сайтам на основе их содержимого.При включении функции родительского контроля и вводе возраста ребенка для фильтра категорий автоматически будет настроена блокировка категорий веб-сайтов, посещение которых детьми этого возраста считается недопустимым.Эта конфигурация подходит в большинстве случаев.

Если вы хотите контролировать информацию, которую ваш ребенок просматривает в Интернете, вы можете настроить, чтобы фильтр категорий блокировал отдельные категории веб-сайтов.

Для проверки и детальной настройки параметров фильтра категорий для определенной учетной записи пользователя выполните следующие действия:

1. Откройте окно настроек родительского контроля Bitdefender для этой учетной записи пользователя.
2. Перейдите на вкладку **Категории**.
3. По умолчанию функция контроля категорий включена.Вы можете отключить контроль категорий и самостоятельно настроить список блокируемых веб-сайтов, используя Веб-контроль, однако этого делать не рекомендуется.
4. Вы можете проверить, какие веб-категории блокируются или ограничиваются автоматически для текущих заданных возрастных групп.Например, если категория "Поисковые системы" имеет статус **заблокировано**, ваш ребенок не сможет пользоваться поисковыми системами.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.

7.2. Мониторинг активности детей

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.

7.2.1. Проверка журналов родительского контроля

Чтобы проверить, чем занимались дети на компьютере, можно просмотреть журналы родительского контроля.Следуйте инструкции:

1. Откройте окно Bitdefender.
2. Нажмите кнопку **События** на верхней панели инструментов.
3. Выберите **Родительский контроль** в меню с левой стороны.

Замечание

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 «*Карта сети*» (p. 108).

В журналах функций родительского контроля отображены подробные сведения обо всех действиях детей на компьютере и в Интернете.Информация распределена по нескольким вкладкам:

События

Предоставляет подробные сведения об активности функции родительского контроля (например, время включения или выключения родительского контроля, блокировка событий и т. д.).

Нажмите на событие, чтобы просмотреть сведения о нем.

Использование приложения

Позволяет просмотреть список последних использованных детьми приложений.

Доступна фильтрация данных по пользователям и по периодам.Нажмите на событие, чтобы просмотреть сведения о нем.

Журнал

Позволяет просмотреть последние посещенные детьми веб-сайты.

Доступна фильтрация данных по пользователям и по периодам.Нажмите на событие, чтобы просмотреть сведения о нем.

7.2.2. Настройка уведомлений по электронной почте

Получение уведомлений по электронной почте при блокировке действия родительским контролем:

1. Откройте окно Bitdefender.
2. Нажмите кнопку **Настройки** на верхней панели инструментов.
3. Нажмите **Родительский контроль** в меню слева и перейдите на вкладку **Настройки**.
4. Включите параметр **Отправлять отчеты об активности по электронной почте**, используя соответствующий переключатель.
5. 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**.

6. Введите адрес электронной почты, на который будут отправляться уведомления.
7. 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.

   Выберите один из известных серверов
   Выберите этот параметр, если ваша учетная запись электронной почты использует одну из веб-служб электронной почты, перечисленных в списке.

   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.
   - Если для сервера требуется защищенное SSL-соединение, поставьте флажок в поле **Использовать SSL**.
8. Нажмите **Тест настроек**, чтобы проверить настройки. Если во время проверки возникают неполадки, вам будут предложены меры по их устранению.
9. Нажмите **OK**, чтобы сохранить изменения, и закройте окно.

7.3. 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.

7.3.1. Обязательные требования для использования удаленного родительского контроля

Для использования функции удаленного родительского контроля необходимо соблюдение следующих обязательных требований:

1. Установите на компьютер детей Bitdefender Internet Security 2012 или Bitdefender Total Security 2012.
2. Не забудьте выполнить регистрацию продукта, связав его со своей учетной записью MyBitdefender.Для получения дополнительной информации перейдите к *«Регистрация программы»* (p. 2).
3. Включение удаленного родительского контроля.
4. Компьютер, с которого осуществляется доступ к функции удаленного родительского контроля, должен быть подключен к Интернету.

7.3.2. 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 окно Bitdefender.
3. Нажмите кнопку **Настройки** на верхней панели инструментов.
4. Нажмите **Родительский контроль** в меню слева и перейдите на вкладку **Настройки**.
5. Включите удаленный родительский контроль с помощью соответствующего переключателя.Функция удаленного родительского контроля будет включена для всех пользовательских учетных данных, созданных в системе.

7.3.3. Доступ к функции удаленного родительского контроля

Для доступа к функции удаленного родительского контроля войдите в MyBitdefender.

1. На компьютере, подключенном к Интернету, откройте веб-браузер и перейдите по следующему адресу:

   https://my.bitdefender.com

2. Войдите в свою учетную запись, указав свое имя пользователя и пароль.
3. На панели "Службы" нажмите **Поддержка для родителей**, чтобы перейти к панели управления удаленного родительского контроля.

4. Вы можете видеть все компьютеры, для которых включен удаленный родительский контроль, и соответствующие учетные записи пользователей.Для каждой учетной записи пользователя имеется три кнопки:

   - **Уведомления**: просмотр операций, которые были заблокированы для соответствующей учетной записи пользователя с момента последнего входа.
   - **Активность**: проверка недавней активности детей.
   - **Настройки**: изменение настроек родительского контроля для соответствующей учетной записи пользователя.

   По нажатии на любую из этих кнопок откроется страница "Удаленный родительский контроль" для данной учетной записи пользователя.

7.3.4. 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. 92).

Чтобы удаленно проверить, чем занимаются дети за компьютером:

1. На компьютере, подключенном к Интернету, откройте веб-браузер и перейдите по следующему адресу:

   https://my.bitdefender.com

2. Войдите в свою учетную запись, указав свое имя пользователя и пароль.
3. На панели "Службы" нажмите **Поддержка для родителей**, чтобы перейти к панели управления удаленного родительского контроля.
4. Найдите учетную запись, которую использует ваш ребенок, и нажмите одну из следующих кнопок:

   - **Уведомления**: просмотр операций, которые были заблокированы для соответствующей учетной записи пользователя с момента последнего входа.
   - **Активность**: проверка недавней активности детей.

На странице "Оповещения" можно просмотреть список веб-сайтов, приложений или контактов в службах мгновенных сообщений, которые были заблокированы с момента последнего посещения.Чтобы снять ограничение, нажмите соответствующую кнопку **Разрешить**.

На странице активности представлены 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 кнопку **Блокировать**.

Для фильтрации отображаемых записей нажмите на меню **Показать** и выберите нужный вариант.

7.3.5. 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. 92).

Удаленное изменение настроек родительского контроля:

1. На компьютере, подключенном к Интернету, откройте веб-браузер и перейдите по следующему адресу:

   https://my.bitdefender.com

2. Выполните вход в свою учетную запись Bitdefender, используя свое имя пользователя и пароль.
3. На панели "Службы" нажмите **Поддержка для родителей**, чтобы перейти к панели управления удаленного родительского контроля.Можно просмотреть все учетные записи пользователей, для которых включена функция удаленного родительского контроля.
4. Найдите учетную запись, которую использует ваш ребенок, и нажмите одну из следующих кнопок:
   - **Уведомления**: просмотр списка последних заблокированных операций и снятие ограничений.
   - **Активность**: проверка недавней активности детей и блокировка нежелательных действий.
   - **Настройки**: изменение настроек родительского контроля для соответствующей учетной записи пользователя.
5. Установите и снимите ограничения в соответствии со своими потребностями.

Ограничение доступа в Интернет по времени

Вы можете настроить время, когда ребенок может пользоваться Интернетом, с помощью параметров **графика веб-доступа** на странице **Настройки**.

Ограничение доступа в Интернет в заданные периоды:

1. Задайте в сетке периоды, в течение которых доступ в Интернет будет заблокирован.Чтобы перейти к новому выбору, нажмите **Заблокировать все** или **Разрешить все**.
2. Нажмите **Сохранить**.

Чтобы полностью заблокировать доступ к Интернету, нажмите ссылку **Запретить все** в сетке времени, а затем нажмите ссылку **Сохранить**.

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. Перейдите на страницу **Настройки**.
2. В соответствующем поле укажите веб-сайт.
3. Нажмите **Подтвердить**.Веб-сайт будет добавлен в список действий, ожидающих выполнения.Если вы передумали, нажмите соответствующую кнопку **Отменить действие**.

Замечание

Также можно перейти на страницу **Активность**, просмотреть список посещенных веб-сайтов и нажать соответствующую кнопку **Блокировать** для веб-сайта, который необходимо заблокировать.

Данное правило будет настроено и применено для компьютера вашего ребенка после следующей синхронизации с веб-сайтом удаленного родительского контроля (макс. в течение 10 мин.).

Блокировка контактов мгновенных сообщений

Блокировка обмена мгновенными сообщениями с заданными контактами:

1. Перейдите на страницу **Настройки**.
2. В соответствующем поле введите код мгновенного сообщения.
3. Нажмите **Заблокировать**.Идентификатор мгновенного сообщения будет добавлен в список действий, ожидающих выполнения.Если вы передумали, нажмите соответствующую кнопку **Отменить действие**.

Замечание

Кроме того, вы можете перейти на страницу **Активность**, просмотреть список контактов мгновенных сообщений, с которыми общался ваш ребенок, и нажать соответствующую кнопку **Блокировать** при обнаружении нежелательного контакта.

Данное правило будет настроено и применено для компьютера вашего ребенка после следующей синхронизации с веб-сайтом удаленного родительского контроля (макс. в течение 10 мин.).

Блокировка приложений

Блокирование приложения:

1. Перейдите на страницу **Активность**.
2. Просмотрите список приложений, к которым был осуществлен доступ, и нажмите на соответствующую кнопку **Блокировать**, если найдете нежелательное приложение.

Данное правило будет настроено и применено для компьютера вашего ребенка после следующей синхронизации с веб-сайтом удаленного родительского контроля (макс. в течение 10 мин.).

Разблокирование веб-сайтов, приложений и контактов мгновенных сообщений

На странице "Уведомления" отображены списки веб-сайтов, приложений и идентификаторов мгновенных сообщений, которые были заблокированы родительским контролем.Чтобы снять ограничение, нажмите соответствующую кнопку **Разрешить**.Данное ограничение будет удалено с детского компьютера после следующей синхронизации с веб-сайтом удаленного родительского контроля (макс. в течение 10 мин.).

8. Брандмауэр

Брандмауэр защищает компьютер от установки неавторизованных соединений.Фактически он выполняет функции охранника на входе: отслеживает попытки подключения и определяет, какие подключения следует разрешить, а какие требуется заблокировать.

Замечание

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

Если на компьютере установлена ОС Windows Vista или Windows 7, Bitdefender автоматически назначает тип сети для каждого обнаруживаемого сетевого подключения.На компьютерах с ОС Windows XP будет предложено выбрать тип сети.Дополнительную информацию о настройках брандмауэра для каждого типа сети и процедуре изменения настроек сети см. в *«Настройка параметров подключения к сети»* (p. 98).

Брандмауэр Bitdefender использует набор правил для фильтрации данных, передаваемых в вашу систему и из нее.Правила сгруппированы по 3 категориям:

Общие правила

Правила, определяющие протоколы, подключение по которым разрешено.

Используется набор правил по умолчанию, обеспечивающих оптимальную защиту.Вы можете изменить правила, чтобы разрешить или запретить подключения по определенным протоколам.

Правила приложения

Правила, определяющие доступ приложений к ресурсам сети и Интернету.

В обычных условиях Bitdefender автоматически создает правило каждый раз, когда приложение пытается получить доступ к Интернету.Правила для приложений можно добавить и изменить вручную.

Правила адаптера

Правила, определяющие, может ли компьютер быть подключен к другим определенным компьютерам.

Вам необходимо создать правила, разрешающие или запрещающие трафик.

Дополнительную защиту предоставляет система обнаружения вторжений (IDS).Система обнаружения вторжений осуществляет мониторинг активности сети и системы, выявляя вредоносные операции и нарушения политики.Модуль может обнаруживать и блокировать попытки изменения критических системных файлов, файлов Bitdefender и записей реестров, установку вредоносных драйверов и атаки путем DLL.

По умолчанию для Bitdefender настроено автоматическое выполнение рекомендуемых действий по обеспечению безопасности без вывода оповещений.Если вы хотите получать уведомления и принимать решения относительно действий, выполняемых при отправке приложением запроса на доступ в Интернет или обнаружении подозрительного поведения приложения, необходимо переключиться в Режим повышенной безопасности.

8.1. Включение или отключение защиты брандмауэра

Чтобы включить или отключить защиту брандмауэра, выполните следующие действия:

1. Откройте окно Bitdefender.
2. Перейдите на панель **Брандмауэр**.
3. Нажмите на переключатель "Брандмауэр".

Внимание

Поскольку при этом возникает риск установки несанкционированных подключений к компьютеру, отключение брандмауэра должно быть только временной мерой.Как можно скорее включите брандмауэр.

8.2. Настройка параметров подключения к сети

Для просмотра и изменения настроек подключения к сети выполните следующие действия:

1. Откройте окно Bitdefender.
2. Перейдите на панель **Брандмауэр**.
3. Нажмите **Сведения о сети**.

Появится новое окно.На графике в верхней части окна в реальном времени отображается информация о входящем и исходящем трафике.

Под графиком для каждого сетевого подключения отображается следующая информация.

- **Тип сети**: введите тип сети, к которой подключен компьютер.Bitdefender применяет базовые настройки брандмауэра в зависимости от типа сети, к которой вы подключены.

  Чтобы изменить тип, откройте раскрывающееся меню **Тип сети** и выберите один из доступных типов в списке.

Тип сети	Описание
Надежное	Отключение брандмауэра для определенного адаптера.

Тип сети	Описание
Домашний/рабочий	Разрешение всего трафика между вашим компьютером и компьютерами в локальной сети.
Публичный	Весь трафик фильтруется.
Ненадежный	Полное блокирование трафика сети и Интернета через соответствующий адаптер.

- **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**.

8.3. Система обнаружения вторжений

Для настройки системы обнаружения вторжений выполните следующие действия:

1. Откройте окно Bitdefender.
2. Нажмите кнопку **Настройки** на верхней панели инструментов.
3. Нажмите **Брандмауэр** в меню слева и перейдите на вкладку **Настройки**.
4. Чтобы включить систему обнаружения вторжений, нажмите на соответствующий переключатель.
5. Чтобы установить желаемый уровень агрессивности, переместите бегунок в требуемое положение.Воспользуйтесь описанием справа от шкалы, чтобы

выбрать уровень, наиболее точно соответствующий требованиям безопасности.

В окне События вы можете посмотреть, какие приложения были найдены системой обнаружения вторжений.

Если имеются приложения, которым вы доверяете и которые не система обнаружения вторжений не должна сканировать, для них можно добавить правила исключения.Чтобы исключить приложение из сканирования, выполните действия, описанные в разделе *«Управление исключенными процессами»* (p. 58).

Замечание

Операция системы обнаружения вторжений относится к активному вирусному контролю.Правила исключения процессов применяются для обеих систем.

8.4. Настройка параметров трафика

Для настройки параметров трафика выполните следующие действия:

1. Откройте окно Bitdefender.
2. Нажмите кнопку **Настройки** на верхней панели инструментов.
3. Нажмите **Брандмауэр** в меню слева и перейдите на вкладку **Настройки**.

В разделе **Трафик** можно включить и отключить следующие функции.

- **Включить общий доступ к подключению к Интернету (ICS)**: включение поддержки 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.

- **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.

- **Расширить ведение журнала**: расширение информации, регистрируемой в журнале брандмауэра.

  Bitdefender ведет журнал 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).Журнал можно открыть в окне **Активность брандмауэра**, нажав кнопку **Показать лог**.

- **Отслеживать Wi-Fi-соединения** — если вы подключены к беспроводным сетям, этот параметр будет отображать сведения о сетевых событиях (например, когда новый компьютер подключается к сети).

8.5. Общие правила

При передаче данных через Интернет используются определенные протоколы.

Общие правила позволяют настраивать протоколы, по которым разрешена передача трафика.Для изменения правил выполните следующие действия:

1. Откройте окно Bitdefender.
2. Нажмите кнопку **Настройки** на верхней панели инструментов.
3. Нажмите **Брандмауэр** в меню слева и перейдите на вкладку **Расширенные**.
4. В разделе "Правила брандмауэра" нажмите **Общие правила**.

Появится новое окно.Отображаются текущие правила.

Чтобы изменить правило, нажмите на соответствующую ссылку в столбце **Действие** и выберите **Разрешить** или **Запретить**.

DNS по UDP/TCP
Разрешить или запретить DNS по UDP и TCP.

По умолчанию этот тип подключения разрешен.

Входящий ICMP/ICMPv6
Разрешите или запретите сообщения ICMP/ICMPv6.

Сообщения ICMP часто используются хакерами для проведения атак на компьютерные сети.По умолчанию этот тип подключения запрещен.

Отправка сообщений электронной почты
Разрешите или запретите отправку электронных сообщений по SMTP.

По умолчанию этот тип подключения разрешен.

HTTP веб-просмотра
Разрешить или запретить просмотр по протоколу HTTP.

По умолчанию этот тип подключения разрешен.

Входящие подключения к удаленному рабочему столу
Разрешить или запретить другим компьютерам доступ с помощью подключений к удаленному рабочему столу.

По умолчанию этот тип подключения разрешен.

Трафик проводника Windows по протоколу HTTP/FTP
Разрешить или запретить трафик HTTP и FTP из Windows Explorer.

По умолчанию этот тип подключения запрещен.

8.6. Правила приложения

Для просмотра и управления правилами брандмауэра, которые контролируют доступ к сетевым ресурсам и Интернету, нажмите **Правила приложения**.

1. Откройте окно Bitdefender.
2. Нажмите кнопку **Настройки** на верхней панели инструментов.
3. Нажмите **Брандмауэр** в меню слева и перейдите на вкладку **Расширенные**.
4. В разделе "Правила брандмауэра" нажмите **Правила приложения**.

Здесь представлены программы (процессы), для которых в таблице созданы правила брандмауэра.Чтобы просмотреть правила, созданные для определенного приложения, нажмите кнопку "+" возле соответствующего приложения или дважды щелкните по нему.

Для каждого правила отображается следующая информация:

- **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).
- **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.

Протокол	Описание
Число	Означает определенный IP-протокол (отличный от TCP и UDP).Полный список назначенных номеров IP-протокола можно увидеть на странице http://www.iana.org/assignments/protocol-numbers.

- **Действие**: определяет, разрешен или запрещен доступ данному приложению к сети или Интернету при определенных обстоятельствах.

Для управления правилами используйте кнопки в нижней части окна:

- **Добавить правило**: открытие окна Добавить правило приложения, в котором можно будет создать новое правило.
- **Редактировать правило**: открытие окна Редактировать правило приложения, в котором можно изменить настройки выбранного правила.
- **Удалить правило**: удаление выбранного правила.

Добавление/редактирование правил приложений

Чтобы добавить или изменить правило приложения, нажмите соответствующую кнопку.Откроется новое окно. Далее выполните следующие действия:

- **Путь к программе.** Нажмите **Обзор** и выберите приложение, к которому вы хотите применить правила.
- **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.
- **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.
- **Тип сети.** Выберите тип сети, для которого будет назначено правило.
- **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.

Событие	Описание
Трафик	Поток данных между двумя компьютерами.
Прослушивание	Состояние, в котором приложение наблюдает за сетью, ожидая установки соединения или получения информации от другого приложения.

- **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 http://www.iana.org/assignments/protocol-numbers.

- **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.
- **Разрешение.** Выберите одно из доступных разрешений:

Разрешение	Описание
Разрешить	Указанному приложению будет разрешен доступ в сеть/Интернет при определенных обстоятельствах.

Разрешение	Описание
Запретить	Указанному приложению будет запрещен доступ в сеть/Интернет при определенных обстоятельствах.

8.7. Правила адаптера

Для каждого сетевого подключения можно настроить особые доверенные и ненадежные зоны.

Доверенная зона — это устройство, которому вы полностью доверяете, например компьютер или принтер.Разрешен весь трафик между вашим компьютером и доверенным устройством.Чтобы открыть доступ к ресурсам для определенных компьютеров в небезопасной беспроводной сети, добавьте их в список разрешенных компьютеров.

Ненадежная зона — это устройство, подключение которого к вашему компьютеру вы хотите полностью исключить.

Для просмотра зон сетевых адаптеров и управления ими выполните следующие действия:

1. Откройте окно Bitdefender.
2. Нажмите кнопку **Настройки** на верхней панели инструментов.
3. Нажмите **Брандмауэр** в меню слева и перейдите на вкладку **Расширенные**.
4. В разделе "Правила брандмауэра" нажмите **Правила адаптера**.

Появится новое окно.Отображаются текущие сетевые зоны для каждого адаптера.

Для управления зонами используйте кнопки в верхней части окна:

- **Добавить зону**: открытие окна Добавить IP-адрес, в котором можно создать новую зону для выбранного адаптера.
- **Редактировать зону**: открытие окна Редактировать правило, в котором можно изменить настройки выбранной зоны.
- **Удалить зону**: удаление выбранной зоны.

Добавление/изменение зон

Чтобы добавить или изменить зону, нажмите соответствующую кнопку.Откроется новое окно со списком IP-адресов устройств, подключенных к сети.Выполните следующие действия:

1. Выберите IP-адрес компьютера, который требуется добавить, или введите адрес или диапазон адресов в текстовом поле.

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**, чтобы сохранить изменения, и закройте окно.

8.8. Мониторинг сетевой активности

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 окно Bitdefender.
2. Нажмите кнопку **Настройки** на верхней панели инструментов.
3. Нажмите **Брандмауэр** в меню слева и перейдите на вкладку **Расширенные**.
4. В разделе "Сетевая активность" нажмите **Активность брандмауэра**.

Появится новое окно.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.

Возле каждого подключения отображается значок.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, которое генерирует трафик, или имеются открытые порты и 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**.Файл журнала

расположен в каталоге ?\Program Files\Common Files\Bitdefender\Bitdefender Firewall\bdfirewall.txt.

8.9. Использование режима повышенной безопасности

Bitdefender Internet Security 2012 специально разработан с целью наименьшего влияния на рабочий процесс.В обычных условиях нет необходимости принимать решения о том, следует ли запретить или разрешить установку соединения или выполнение действий приложениями, запущенными в системе.Bitdefender принимает за вас все решения.

Если вы хотите полностью контролировать процесс принятия решений, выполните следующие действия:

1. Откройте окно Bitdefender.
2. Нажмите кнопку **Настройки** на верхней панели инструментов.
3. Нажмите **Брандмауэр** в меню слева и перейдите на вкладку **Расширенные**.
4. Включите **Режим повышенной безопасности** с помощью соответствующего переключателя.

При переключении в режим повышенной безопасности отобразится оповещение, предлагающее выполнить определенное действие при возникновении одной из следующих ситуаций:

- Приложение пытается установить соединение с Интернетом.
- Приложение пытается выполнить действие, которое Система обнаружения вторжений или Активный вирусный контроль считает подозрительным.

В оповещении указывается подробная информация о приложении и обнаруженном поведении.Необходимо **Разрешить** или **Запретить** действие с помощью соответствующей кнопки.

9. Карта сети

Модуль "Домашняя сеть" позволяет управлять обновлениями Bitdefender, установленными на ваших домашних компьютерах, с одного компьютера.

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

1. Включите сеть Bitdefender на своем компьютере.Настройте компьютер, чтобы он выполнял роль **сервера**.
2. Подключите каждый компьютер, которым вы хотите управлять, к сети (установите пароль).Установите, чтобы все компьютеры работали как **стандартные**.
3. Вернитесь к своему компьютеру и добавьте те компьютеры, которыми вы хотите управлять.

9.1. Включение сети Bitdefender

Чтобы включить функцию сети Bitdefender, выполните следующие действия:

1. Откройте окно Bitdefender.
2. Нажмите кнопку **Настройки** на верхней панели инструментов.
3. Нажмите **Карта сети** в меню слева.
4. Нажмите **Управление сетью**.Вам будет предложено установить пароль управления для сетевой карты.
5. Введите пароль в каждом из полей ввода.
6. Настройка роли компьютера в сетевой карте 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.
7. Нажмите **OK**.

   На карте сети будет отображаться имя компьютера.

   Отобразится кнопка **Отключить соединение**.

Замечание

Карту сети можно также включить в главном окне Bitdefender:

1. Откройте окно Bitdefender.
2. Перейдите на панель **Карта сети**.

3. Нажмите **Управление** и в раскрывающемся меню выберите **Включить сеть**.

9.2. Добавление компьютеров в сеть Bitdefender

Компьютер будет автоматически добавлен в сеть, если он соответствует следующим требованиям:

- карта сети 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

Вы можете в любой момент выполнить сканирование карты сети на наличие компьютеров, удовлетворяющих критериям. Для этого нажмите кнопку **Автоматическое обнаружение**.

Чтобы вручную добавить компьютер в карту сети Bitdefender с компьютера, выполняющего роль сервера, выполните следующие действия:

1. Откройте окно Bitdefender.
2. Нажмите кнопку **Настройки** на верхней панели инструментов.
3. Нажмите **Карта сети** в меню слева.
4. Нажмите **Добавить компьютер**.
5. Введите пароль управления 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.

6. Выполните одно из следующих действий:
   - Выберите из списка имя добавляемого компьютера.
   - Введите IP-адрес или имя добавляемого компьютера в соответствующем поле.
7. Нажмите **Добавить**.
8. Введите пароль управления, установленный на соответствующем компьютере.

9. Нажмите **OK**.Если вы ввели правильный пароль, имя выбранного компьютера появится на карте сети.

9.3. Управление сетью Bitdefender

После успешного создания карты сети Bitdefender всеми продуктами Bitdefender можно будет управлять с компьютера, выполняющего роль сервера.

Для запуска нескольких задач на всех управляемых компьютерах выполните следующие действия:

1. Откройте окно Bitdefender.
2. Перейдите на панель **Карта сети**.
3. Нажмите **Управление** и в раскрывающемся меню выберите соответствующие кнопки:
   - **Отключить соединение**: позволяет отключить сеть.
   - **Сканировать все** — позволяет сканировать все управляемые компьютеры одновременно.
   - **Обновление всех компьютеров** - позволяет обновлять все управляемые компьютеры одновременно.

Перед запуском задания на определенном компьютере будет выдан запрос на ввод локального пароля управления.Введите пароль управления и нажмите **OK**.

Для просмотра всей карты сети и получения доступа ко всем задачам управления выполните следующие действия:

1. Откройте окно Bitdefender.
2. Нажмите кнопку **Настройки** на верхней панели инструментов.
3. Нажмите **Карта сети** в меню слева.

Если навести курсор мыши на компьютер на карте сети, будет показана краткая информация о нем (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 продукт
Позволяет зарегистрировать Bitdefender на этом компьютере с помощью лицензионного ключа.

Настроить пароль для параметров продукта
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: быстрое сканирование или полное сканирование системы.

Исправить все проблемы
Позволяет исправить проблемы, влияющие на безопасность этого компьютера, с помощью мастера Устранить все угрозы.

Обновить
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 компьютер из карты сети
Позволяет удалить ПК из сети.

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.

10. 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**.В случае обнаружения обновление будет автоматически загружено и установлено на ваш компьютер.

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

Для обеспечения защиты компьютера от новых угроз необходимо, чтобы функция автоматического обновления была включена.

В определенных ситуациях требуется ваше вмешательство для поддержания защиты Bitdefender в актуальном состоянии:

- Если ваш компьютер подключен к Интернету через прокси-сервер, вам необходимо задать настройки прокси-сервера, как описано в разделе *«Как настроить Bitdefender для использования прокси-сервера при подключении к Интернету?»* (p. 33).
- Если вы не подключены к Интернету, вы можете обновить Bitdefender вручную, как описано в разделе *«Мой компьютер не подключен к Интернету. Как обновить Bitdefender?»* (p. 124).Файл обновления вручную выпускается один раз в неделю.
- При низкой скорости подключения к Интернету во время загрузки обновлений могут возникать ошибки.Инструкции по устранению таких ошибок см. в *«Обновление Bitdefender при низкой скорости подключения к Интернету»* (p. 124).
- Если вы подключаетесь к Интернету по телефонной линии, лучше всего регулярно обновлять Bitdefender по запросу.Для получения дополнительной информации перейдите к *«Выполнение обновления»* (p. 113).

10.1. Проверьте, установлены ли последние обновления Bitdefender

Чтобы проверить, установлены ли последние обновления защиты Bitdefender, выполните следующие действия.

1. Откройте окно Bitdefender.
2. Перейдите на панель **Обновление**.
3. Время последнего обновления отображается под именем панели.

Для получения дополнительной информации о последних обновлениях просмотрите события обновления:

1. В главном окне на верхней панели инструментов нажмите **События**.
2. В меню слева нажмите **Обновление**.

Можно посмотреть список выбранных обновлений и информацию о них (была ли установка выполнена успешно и требуется ли для завершения установки перезагрузка компьютера).Если требуется, выполните перезагрузку системы при первой возможности.

10.2. Выполнение обновления

Для выполнения обновления требуется подключение к Интернету.

Чтобы запустить обновление, выполните одно из следующих действий:

- Откройте окно Bitdefender и на панели **Обновление** нажмите **Обновить**.
- Щелкните правой кнопкой мыши на значке Bitdefender на панели задач и выберите **Обновить**.

Модуль обновления подключится к серверу обновлений Bitdefender для проверки наличия обновлений.Если будет обнаружено обновление, вам будет предложено подтвердить его установку или же обновление начнется автоматически, в зависимости от настроек обновления.

Важно
Может потребоваться перезагрузка компьютера для завершения обновления. Рекомендуется сделать это как можно раньше.

10.3. Включение и отключение автоматического обновления

Для включения и отключения автоматического обновления выполните следующие действия:

1. Откройте окно Bitdefender.

2. Перейдите на панель **Обновление**.
3. Нажмите на переключатель, чтобы включить или отключить автоматическое обновление.
4. Если вы решите отключить автоматическое обновление, появится окно предупреждения.Вы должны подтвердить свое намерение, выбрав промежуток времени, на который вы хотите отключить автоматическое обновление. Вы можете отключить на 5, 15 или 30 минут, на час, навсегда или до следующей перезагрузки системы.

Внимание

Этот аспект является критическим с точки зрения безопасности. Рекомендуем вам отключать автоматическое обновление на как можно меньший промежуток времени. Если автоматическое обновление отключено, вы не защищены от самых последних угроз.

10.4. 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.

Настройки обновления по умолчанию подходят для большинства пользователей, и обычно изменять их не требуется.

Для настройки параметров управления выполните следующие действия:

1. Откройте окно Bitdefender.
2. Нажмите кнопку **Настройки** на верхней панели инструментов.
3. В меню слева нажмите **Обновление**.
4. Настройте параметры необходимым образом.

Расположение обновления

В Bitdefender настроено получение обновлений с серверов обновлений Bitdefender в Интернете.Обновления доступны на веб-сайте `http://upgrade.bitdefender.com`, при открытии которого автоматически происходит перенаправление на ближайший сервер обновлений Bitdefender в вашем регионе.

Не изменяйте расположение обновлений, если только такие инструкции не были получены от представителя Bitdefender или сетевого администратора (если вы подключены к офисной сети).

Если Bitdefender установлен у вас дома на нескольких компьютерах, вы можете создать домашнюю сеть Bitdefender и назначить один из компьютеров сервером

обновлений.Подробная информация представлена в *«Карта сети»* (p. 108).Программа Bitdefender, установленная на компьютере, назначенном сервером обновлений, будет получать обновления из Интернета. Программы Bitdefender, установленные на остальных компьютерах, будут получать обновления с локального сервера обновлений (путь к обновлениям в их настройках автоматически будет изменен соответствующим образом).Эта конфигурация предназначена для снижения интернет-трафика и оптимизации обновлений.

Вы можете вновь вернуть общий веб-сайт обновлений, нажав кнопку **По умолчанию**.

Обновить правила обработки

Предусмотрено три способа загрузки и установки обновлений:

- **Обновление без оповещений** — Bitdefender автоматически загружает и устанавливает обновления.
- **Запросить разрешение перед загрузкой**: каждый раз при появлении новых обновлений будет выводиться запрос на подтверждение перед его загрузкой.
- **Запросить разрешение перед установкой**: после загрузки обновлений будет выдаваться запрос для подтверждения установки.

Для завершения установки некоторых обновлений требуется перезагрузка.По умолчанию, если обновление требует перезагрузки, Bitdefender продолжит работу со старыми файлами до тех пор, пока пользователь не перезагрузит компьютер. Это позволяет предотвратить прерывание работы пользователя процессом обновления Bitdefender.

Если вы хотите, чтобы система выдавала запрос, когда обновление требует перезагрузки, отключите параметр **Отложить перезагрузку**, нажав на соответствующий переключатель.

Обновление P2P

Помимо обычного механизма обновления в Bitdefender также используется система интеллектуального распространения обновлений, работающая на основе протокола одноранговогo обновления (P2P), для передачи обновлений сигнатур вредоносного ПО пользователям Bitdefender.

Включить и отключить параметры обновления P2P можно с помощью соответствующих переключателей.

Использовать систему обновления P2P

Включите этот параметр, чтобы загрузить обновления сигнатуры вирусов от других пользователей Bitdefender, используя систему обновлений

P2P.Bitdefender использует порты 8880–8889 для одноранговогo обновления.

Рассылка файлов Bitdefender

Включите этот параметр, чтобы предоставить другим пользователям Bitdefender доступ к последним сигнатурам вредоносных программ, имеющихся на вашем компьютере.

11. Защита Safego для социальных сетей

Вы доверяете своим друзьям в Интернете.Доверяете ли вы их компьютерам?Используйте защиту Safego для социальных сетей, чтобы защитить свою учетную запись и своих друзей от интернет-угроз.

Safego — это приложение для Facebook, разработанное Bitdefender для обеспечения защиты учетных записей социальной сети.Модуль выполняет сканирование ссылок, которые вы получаете от друзей в Facebook, и мониторинг настроек конфиденциальности вашей учетной записи.

Замечание

Для использования этой функции требуется учетная запись MyBitdefender. Для получения дополнительной информации перейдите к *«Регистрация программы»* (p. 2).

Основные функции:

- автоматически сканирует сообщения в ленте новостей на наличие вредоносных ссылок.
- защищает вашу учетную запись от интернет-угроз.

  При обнаружении сообщений или комментариев, являющихся спамом, фишингом или вредоносной программой, вы получаете предупреждающее сообщение.
- предупреждает ваших друзей о подозрительных ссылках в их фидах новостей.
- помогает создать безопасную сеть друзей с помощью функции **Другомер**.
- получить состояние безопасности системы с помощью Bitdefender QuickScan.

Для использования Safego из продукта Bitdefender выполните следующие действия:

1. Откройте окно Bitdefender.
2. Перейдите на панель **Safego**.
3. Нажмите **Активировать**.Вы будете перенаправлены в учетную запись.

   Если вы уже активировали Safego, вы сможете просмотреть статистику по активности модуля, нажав кнопку **Просмотр отчетов**.
4. Используйте параметры учетной записи Facebook для подключения к приложению Safego.
5. Разрешите Safego доступ к своей учетной записи Facebook.

12. 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) *«Техническая поддержка»* (p. 142).

12.1. Система работает медленно

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 *«Как удалить другие решения безопасности?»* (p. 148).

- **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.

- **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**.

12.2. 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 выполните следующие действия:

  1. Полностью удалить Bitdefender из системы:
     a. Перейдите к http://www.bitdefender.com/uninstall и загрузите инструмент удаления на ваш компьютер.
     b. Запустить инструмент удаления, используя права администратора.
     c. Перезагрузите компьютер.
  2. Повторная установка Bitdefender на компьютер.

- **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 «*Как удалить другие решения безопасности?*» (p. 148).
  2. Полностью удалить Bitdefender из системы:
     a. Перейдите к http://www.bitdefender.com/uninstall и загрузите инструмент удаления на ваш компьютер.
     b. Запустить инструмент удаления, используя права администратора.
     c. Перезагрузите компьютер.
  3. Повторная установка Bitdefender на компьютер.

Если эта информация не помогла, вы можете обратиться в поддержку Bitdefender, как указано в секции «*Обращение за помощью*» (p. 143).

12.3. 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 окно Bitdefender.
2. Нажмите кнопку **Настройки** на верхней панели инструментов.
3. Нажмите **Антивирус** в меню слева и перейдите на вкладку **Исключения**.
4. Нажмите ссылку **Исключенные процессы**.В открывшемся окне можно управлять исключениями процессов функции активного антивирусного контроля.
5. Добавьте исключения, выполнив следующие действия:
   a. Нажмите кнопку **Добавить** в верхней части таблицы исключений.
   b. Нажмите **Обзор**, выберите приложение, которое требуется исключить, и нажмите **OK**.
   c. Оставьте выбранным параметр **Разрешить**, чтобы функция активного вирусного контроля не блокировала приложение.
   d. Нажмите **Добавить**.

Если эта информация не помогла, вы можете обратиться в поддержку Bitdefender, как указано в секции *«Обращение за помощью»* (p. 143).

12.4. Не удается подключиться к Интернету

В некоторых случаях после установки Bitdefender программа или веб-браузер больше не могут подключиться к Интернету или получить доступ к сетевым службам.

В этом случае рекомендуется настроить в Bitdefender возможность автоматически разрешать подключение к соответствующему приложению.

1. Откройте окно Bitdefender.
2. Нажмите кнопку **Настройки** на верхней панели инструментов.
3. Нажмите **Брандмауэр** в меню слева и перейдите на вкладку **Расширенные**.
4. В разделе "Правила брандмауэра" нажмите **Правила приложения**.

5. Чтобы добавить правило приложения, нажмите на соответствующую кнопку.
6. Нажмите **Обзор** и выберите приложение, к которому вы хотите применить правила.
7. Выберите все доступные типы сетей.
8. Перейдите в раздел **Разрешение** и выберите **Разрешить**.

Закройте Bitdefender, откройте приложение и снова попробуйте подключиться к Интернету.

Если эта информация не помогла, вы можете обратиться в поддержку Bitdefender, как указано в секции *«Обращение за помощью»* (p. 143).

12.5. Не удается получить доступ к устройству в сети

В зависимости от типа сети, к которой подключен компьютер, брандмауэр Bitdefender может заблокировать соединение между вашей системой и другим устройством (другим компьютером или принтером).После этого вы больше не сможете предоставлять доступ к файлам и распечатывать их.

В этом случае рекомендуется настроить в Bitdefender возможность автоматически разрешать подключение к соответствующему устройству.Для каждого подключения к сети можно настроить особую доверенную зону.

Доверенная зона — это устройство, которому вы полностью доверяете.Разрешается весь трафик между вашим компьютером и доверенным устройством.Чтобы предоставить доступ к ресурсам для определенных устройств, например для компьютеров или принтеров, добавьте их в доверенные зоны.

Для добавления сетевых адаптеров в доверенную зону выполните следующие действия:

1. Откройте окно Bitdefender.
2. Нажмите кнопку **Настройки** на верхней панели инструментов.
3. Нажмите **Брандмауэр** в меню слева и перейдите на вкладку **Расширенные**.
4. В разделе "Правила брандмауэра" нажмите **Правила адаптера**.
5. Чтобы добавить зону, нажмите соответствующую кнопку.Откроется новое окно со списком IP-адресов устройств, подключенных к сети.
6. Выберите IP-адрес компьютера или принтера, который требуется добавить, или введите адрес или диапазон адресов в текстовом поле.
7. Перейдите в раздел **Разрешение** и выберите **Разрешить**.

Если вы по-прежнему не можете подключиться к устройству, эта проблема может быть связана с Bitdefender.

Проверьте другие возможные причины, такие как:

- 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 *«Обращение за помощью»* (p. 143).

12.6. Низкая скорость подключения к Интернету

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 окно Bitdefender.
2. Перейдите на панель **Брандмауэр** и нажмите на переключатель, чтобы отключить его.
3. Проверьте подключение к Интернету при отключенном брандмауэре Bitdefender.
   - Если подключение к Интернету все еще работает медленно, значит Bitdefender не является причиной этой неисправности. Свяжитесь с поставщиком услуг Интернета, чтобы проверить подключение 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 «*Обращение за помощью*» (p. 143).
   - Если вам удалось подключиться к Интернету после отключения брандмауэра Bitdefender, выполните следующие действия:
     a. Откройте окно Bitdefender.
     b. Перейдите на панель **Брандмауэр** и нажмите на переключатель, чтобы включить его.
     c. Нажмите кнопку **Настройки** на верхней панели инструментов.
     d. Нажмите **Брандмауэр** в меню слева и перейдите на вкладку **Настройки**.
     e. Перейдите к параметру **Совместное использование интернет-соединения** и нажмите на переключатель, чтобы включить его.
     f. Перейдите к **Блокировать сканирование портов** и нажмите на переключатель, чтобы отключить его.
     g. Нажмите кнопку **Главная** на верхней панели инструментов.
     h. Перейдите на панель **Брандмауэр** и нажмите **Сведения о сети**.
     i. Перейдите в раздел **Тип сети** и выберите **Домашний/рабочий**.
     j. Перейдите в раздел **Режим невидимки** и выберите для него тип **Удаленный**. Для параметра **Общие** выберите значение **Да**.
     k. Закройте Bitdefender, перезагрузите систему и проверьте скорость подключения к Интернету.

Если эта информация не помогла, вы можете обратиться в поддержку Bitdefender, как указано в секции «*Обращение за помощью*» (p. 143).

12.7. Обновление Bitdefender при низкой скорости подключения к Интернету

При низкой скорости интернет-соединения (например, модемного) в процессе обновления могут возникать ошибки.

Для регулярного обновления вирусных сигнатур Bitdefender выполните следующие действия:

1. Откройте окно Bitdefender.
2. Нажмите кнопку **Настройки** на верхней панели инструментов.
3. Нажмите **Обновление** в меню слева и перейдите на вкладку **Обновление**.
4. В разделе **Обновить правила обработки** выберите **Запросить разрешение перед загрузкой**.
5. Нажмите кнопку **Главная** на верхней панели инструментов.
6. Перейдите на панель **Обновление** и нажмите **Обновить**.
7. Выберите только **Обновления сигнатур**, затем нажмите **OK**.
8. Bitdefender выполнит загрузку и установку только обновлений вирусных сигнатур.

12.8. Мой компьютер не подключен к Интернету. Как обновить Bitdefender?

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).

Следуйте инструкции:

1. На компьютере, подключенном к Интернету, откройте веб-браузер и перейдите по следующему адресу:

   http://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. 149).
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 левой кнопкой мыши на файле и следуйте инструкциям мастера.

12.9. Службы Bitdefender не отвечают

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, информируя о том, что службы Bitdefender не отвечают.
- 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.

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.

   Для получения дополнительной информации перейдите к *«Как удалить другие решения безопасности?»* (p. 148).

Если ошибка продолжает возникать, свяжитесь с нашей службой поддержки, как описано в разделе *«Обращение за помощью»* (p. 143).

12.10. Фильтр антиспама 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.

12.10.1. 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.

1. Если вы используете один из почтовых клиентов с интегрированным Bitdefender, покажите ошибки обнаружения.

   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 *«Поддерживаемые почтовые клиенты и протоколы»* (p. 66).

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.

Добавить контакты в список друзей

Если вы используете поддерживаемый почтовый клиент, вы можете легко добавлять отправителей легальной почты в список друзей.Следуйте инструкции:

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.Следуйте инструкции:

1. Откройте окно Bitdefender.
2. Перейдите на панель **Антиспам**.
3. Нажмите **Управление** и в меню выберите **Друзья**.Появится окно настроек.
4. Введите адрес электронной почты, с которого вы хотите всегда получать письма, и нажмите **Добавить**.Можно добавить любое необходимое число адресов электронной почты.
5. Нажмите **OK**, чтобы сохранить изменения, и закройте окно.

Показать ошибки обнаружения

Если вы используете поддерживаемый почтовый клиент, вы можете легко корректировать фильтр антиспама, указывая, какие письма не следует помечать как [спам]. Это поможет повысить эффективность фильтра антиспама.Следуйте инструкции:

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 инструментов антиспама Bitdefender (обычно расположена в верхней части окна почтового клиента).Письмо будет перемещено в папку "Входящие".

Уменьшить уровень защиты антиспама

Для уменьшения уровня защиты антиспама следуйте этим шагам:

1. Откройте окно Bitdefender.

2. Нажмите кнопку **Настройки** на верхней панели инструментов.
3. Нажмите **Антиспам** в меню слева.
4. Переместите ползунок ниже.

12.10.2. Многие сообщения спама остаются необнаруженными

Если вы получаете много спам-сообщений, не помеченных как [спам], вы должны настроить антиспам Bitdefender для увеличения его эффективности.

Попробуйте следующие решения:

1. Если вы используете один из почтовых клиентов с интегрированным Bitdefender, укажите необнаруженные сообщения спама.

   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 *«Поддерживаемые почтовые клиенты и протоколы»* (p. 66).

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.

Указать необнаруженные сообщения спама

Если вы используете поддерживаемый почтовый клиент, вы можете легко указать, какие сообщения должны были быть определены как спам. Это позволит существенно повысить эффективность фильтра антиспама.Следуйте инструкции:

1. Откройте ваш почтовый клиент.
2. Перейти к папке "Входящие".
3. Выберите необнаруженные спам-сообщения.
4. Нажмите кнопку **Это спам** на панели инструментов антиспама Bitdefender (обычно расположена в верхней части окна почтового клиента). Они будут помечены как [спам] и перемещены в папку спама.

Добавить спамеров в список спамеров

Если вы используете поддерживаемый почтовый клиент, вы можете легко добавлять отправителей спама в список спамеров.Следуйте инструкции:

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.Следуйте инструкции:

1. Откройте окно Bitdefender.
2. Перейдите на панель **Антиспам**.
3. Нажмите **Управление** и в меню выберите **Спамеры**.Появится окно настроек.
4. Введите адрес электронной почты спамера и нажмите **Добавить**.Можно добавить любое необходимое число адресов электронной почты.
5. Нажмите **OK**, чтобы сохранить изменения, и закройте окно.

Увеличение уровня защиты антиспама

Для увеличения уровня защиты антиспама выполните следующие действия:

1. Откройте окно Bitdefender.
2. Нажмите кнопку **Настройки** на верхней панели инструментов.
3. Нажмите **Антиспам** в левом меню.
4. Переместите ползунок выше.

12.10.3. Фильтр антиспама не обнаруживает ни одно сообщение спама

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 может быть отключена.Чтобы посмотреть состояние защиты антиспама, откройте окно Bitdefender и установите переключатель на панели **Антиспам**.

  Если модуль антиспама выключен, это может быть причиной возникшей проблемы.Нажмите на переключатель, чтобы включить защиту антиспама.

- 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 2012 не проверяет трафик POP3 программы Lotus Notes.

Возможным решением может быть переустановка продукта. Однако вместо этого вы можете обратиться за поддержкой в Bitdefender, как описано в разделе «*Техническая поддержка*» (p. 142).

12.11. 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 системы, выполните следующие действия:

1. Перейдите к http://www.bitdefender.com/uninstall и загрузите инструмент удаления на ваш компьютер.
2. Запустить инструмент удаления, используя права администратора.
3. Перезагрузите компьютер.

Если эта информация не помогла, вы можете обратиться в поддержку Bitdefender, как указано в секции *«Обращение за помощью»* (p. 143).

12.12. Моя система не загружается после установки Bitdefender

Если вы установили Bitdefender и система больше не загружается в нормальном режиме, это может происходить по нескольким причинам.

Наиболее вероятно, что проблема вызвана тем, что ранее установленная версия Bitdefender не была удалена корректно или в системе имеется другая программа безопасности.

Любую ситуацию можно разрешить следующим образом:

- **Вы использовали Bitdefender ранее и не удалили продукт корректно.**

  Для решения этой проблемы выполните следующие действия:

  1. Перезагрузите систему и запустите безопасный режим.Инструкции для этой процедуры см. в *«Перезагрузка компьютера в безопасном режиме»* (p. 149).
  2. Удалите Bitdefender из системы:
     a. Перейдите к http://www.bitdefender.com/uninstall и загрузите инструмент удаления на ваш компьютер.
     b. Запустить инструмент удаления, используя права администратора.
     c. Перезагрузите компьютер.
  3. Перезагрузите систему в нормальном режиме и переустановите Bitdefender.

- **Ранее было установлено другое решение безопасности, которое не было удалено корректно.**

  Для решения этой проблемы выполните следующие действия:

  1. Перезагрузите систему и запустите безопасный режим.Инструкции для этой процедуры см. в *«Перезагрузка компьютера в безопасном режиме»* (p. 149).
  2. Удалите Bitdefender из системы:
     a. Перейдите к http://www.bitdefender.com/uninstall и загрузите инструмент удаления на ваш компьютер.
     b. Запустить инструмент удаления, используя права администратора.
     c. Перезагрузите компьютер.

3. Чтобы корректно удалить другие программы, с соответствующего веб-сайта запустите инструмент удаления программы или свяжитесь с разработчиком для получения инструкций по удалению.
4. Перезагрузите систему в нормальном режиме и переустановите Bitdefender.

Вы уже выполнили описанные выше действия, но проблему разрешить не удалось.

Для решения этой проблемы выполните следующие действия:

1. Перезагрузите систему и запустите безопасный режим.Инструкции для этой процедуры см. в «*Перезагрузка компьютера в безопасном режиме*» (p. 149).
2. Используйте функцию восстановления системы Windows, чтобы вернуться к состоянию системы до установки продукта Bitdefender.Инструкции для этой процедуры см. в «*Как использовать функцию восстановления системы в Windows?*» (p. 150).
3. Перезагрузите систему в нормальном режиме и свяжитесь со службой поддержки, как описано в разделе «*Обращение за помощью*» (p. 143).

13. 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.

- «*Режим "Реанимация" Bitdefender*» (p. 133)
- «*Действия в случае обнаружения Bitdefender вирусов на компьютере*» (p. 135)
- «*Как удалить вирус из архива?*» (p. 136)
- «*Как очистить от вирусов архив электронной почты?*» (p. 137)
- «*Что делать, если имеются подозрения о том, что файл является опасным?*» (p. 138)
- «*Удаление зараженных файлов из папки System Volume Information*» (p. 139)
- «*Поиск защищенных паролями файлов в журнале сканирования*» (p. 140)
- «*Поиск пропущенных элементов в журнале сканирования*» (p. 141)
- «*Поиск файлов с избыточным сжатием в журнале сканирования.*» (p. 141)
- «*Почему Bitdefender автоматически удалил зараженный файл?*» (p. 141)

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) «*Техническая поддержка*» (p. 142).

13.1. Режим "Реанимация" Bitdefender

Режим "Реанимация" — это функция Bitdefender, которая позволяет выполнять сканирование и лечение всех разделов жесткого диска вне среды операционной системы.

После установки Bitdefender Internet Security 2012 режим "Реанимация" можно будет использовать, даже когда не удается запустить Windows.

Запуск системы в режиме "Реанимация"

В режим "Реанимация" можно перейти двумя способами:

Из окна Bitdefender

Для перехода в режим "Реанимация" из Bitdefender выполните следующие действия:

1. Перейдите на панель **Антивирус**.
2. Нажмите **Сканировать** и в раскрывающемся меню выберите **Режим "Реанимация"**.

   Появится окно подтверждения. Нажмите **Да**, чтобы перезагрузить компьютер.
3. После перезагрузки компьютера появится меню с предложением выбрать операционную систему.Выберите **Образ реанимации Bitdefender** и нажмите клавишу **Enter**, чтобы загрузить среду Bitdefender, в которой можно будет выполнить очистку раздела Windows.
4. При появлении запроса нажмите клавишу **Enter** и выберите разрешение экрана, наиболее близкое к разрешению, которое вы обычно используете.Затем снова нажмите **Enter**.

   Режим реанимации Bitdefender будет запущен через несколько минут.

Загружайте компьютер в режиме "Реанимация"

Если Windows больше не запускается, вы можете загрузить компьютер в режиме реанимации Bitdefender, выполнив следующие действия.

Замечание

Этот метод недоступен на компьютерах с ОС Windows XP.

1. Включите или перезагрузите компьютер и начните нажимать клавишу **пробела** на клавиатуре, прежде чем появится логотип Windows.
2. Появится запрос на выбор запускаемой операционной системы.Нажмите клавишу **TAB**, чтобы перейти в область инструментов.Выберите **Образ реанимации Bitdefender** и нажмите клавишу **Enter**, чтобы загрузить среду Bitdefender, в которой можно будет выполнить очистку раздела Windows.
3. При появлении запроса нажмите клавишу **Enter** и выберите разрешение экрана, наиболее близкое к разрешению, которое вы обычно используете.Затем снова нажмите **Enter**.

   Режим реанимации Bitdefender будет запущен через несколько минут.

Сканирование системы в режиме "Реанимация"

Чтобы запустить сканирование системы в режиме "Реанимация", выполните следующие действия:

1. Перейдите в режим "Реанимация", как описано в разделе «Запуск системы в режиме "Реанимация"» (p. 133).
2. Появится логотип Bitdefender, и начнется копирование антивирусных систем.

3. Откроется окно приветствия.Нажмите **Продолжить**.
4. Установка обновления вирусных сигнатур запущена.
5. После завершения обновления появится окно "Сканер антивируса Bitdefender по запросу".
6. Нажмите **Сканировать**, в открывшемся окне выберите объект сканирования и нажмите **Открыть**, чтобы начать сканирование.

   Рекомендуется выполнить сканирование всего раздела Windows.

   Замечание

   При работе в режиме "Реанимация" используются имена разделов в стиле Linux.Разделы диска отображаются следующим образом: `sda1`, вероятно соответствующий разделу типа Windows `(C:)`; `sda2`, соответствующий диску `(D:)`, и т. д.

7. Дождитесь завершения сканирования. Если будут обнаружены вредоносные программы, следуйте инструкциям для устранения угрозы.
8. Чтобы выйти из режима "Реанимация", щелкните правой кнопкой мыши по пустой области рабочего стола, в появившемся меню нажмите **Выход** и выберите перезагрузку или выключение компьютера.

13.2. 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 полное сканирование системы.

По завершении полного 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. Отключение антивирусной защиты Bitdefender в режиме реального времени:
   a. Откройте окно Bitdefender.
   b. Нажмите кнопку **Настройки** на верхней панели инструментов.
   c. Нажмите **Антивирус** в меню слева и перейдите на вкладку **Экран**.
   d. Нажмите на переключатель, чтобы отключить **резидентное сканирование**.
2. Отображать скрытые объекты в Windows.Инструкции для этой процедуры см. в «*Как отобразить скрытые объекты в Windows?*» (p. 150).
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. 149).
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 «*Обращение за помощью*» (p. 143).

13.3. 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 полного сканирования системы.
2. Отключение антивирусной защиты Bitdefender в режиме реального времени:
   a. Откройте окно Bitdefender.
   b. Нажмите кнопку **Настройки** на верхней панели инструментов.
   c. Нажмите **Антивирус** в меню слева и перейдите на вкладку **Экран**.
   d. Нажмите на переключатель, чтобы отключить **резидентное сканирование**.
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 полное 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 *«Обращение за помощью»* (p. 143).

13.4. Как очистить от вирусов архив 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. Отключение антивирусной защиты Bitdefender в режиме реального времени:
   a. Откройте окно Bitdefender.
   b. Нажмите кнопку **Настройки** на верхней панели инструментов.
   c. Нажмите **Антивирус** в меню слева и перейдите на вкладку **Экран**.
   d. Нажмите на переключатель, чтобы отключить **резидентное сканирование**.
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 *«Обращение за помощью»* (p. 143).

13.5. Что делать, если имеются подозрения о том, что файл является опасным?

Вы можете подозревать, что файл, содержащийся в системе, является опасным, даже если продукт Bitdefender не обнаружил его.

Для проверки защиты системы выполните следующие действия:

1. Запустите **полное сканирование системы** с помощью Bitdefender.Инструкции для этой процедуры см. в *«Как выполнить сканирование системы?»* (p. 27).

2. Если при сканировании угрозы обнаружены не были, но у вас все еще имеются сомнения и вы хотите убедиться в безопасности определенного файла, свяжитесь с нашей службой поддержки.

   Инструкции для этой процедуры см. в *«Обращение за помощью»* (p. 143).

13.6. 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 *«Обращение за помощью»* (p. 143).

13.7. Поиск защищенных паролями файлов 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.

13.8. Поиск пропущенных элементов 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.

13.9. 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.

13.10. 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.

14. Получение справки

14.1. Техническая 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.

14.1.1. Онлайн-ресурсы

Для устранения проблем и разрешения вопросов, связанных с Bitdefender, доступен ряд интернет-ресурсов.

- Центр поддержки Bitdefender:http://www.bitdefender.com/help
- Форум техподдержки Bitdefender:http://forum.bitdefender.com
- портал компьютерной безопасности Malware City:http://www.malwarecity.com

Также можно воспользоваться поисковой системой для получения дополнительных сведения о компьютерной безопасности, продуктах Bitdefender и компании.

Центр поддержки Bitdefender

Центр помощи Bitdefender — это интернет-хранилище информации о продуктах Bitdefender.Здесь хранятся в удобном для доступа формате отчеты о результатах текущих операций по технической поддержке и исправлению ошибок, выполняемых службой поддержки и разработки Bitdefender, а также статьи по предотвращению заражения вирусами, управлению решениями Bitdefender с подробными разъяснениями, а также другая информация.

Центр поддержки Bitdefender доступен для всех, и поиск по нему можно осуществлять без каких-либо ограничений.Bitdefender содержит обширную информацию, предоставляя клиентам необходимые технические сведения.Все действительные запросы информации и отчеты об ошибках, поступающие от клиентов Bitdefender, поступают в центр поддержки Bitdefender, и в справочные ресурсы по продукту включаются отчеты об исправлении ошибок, обходные решения и информационные статьи.

Центр поддержки Bitdefender доступен круглосуточно по адресу http://www.bitdefender.com/help.

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.

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.

14.1.2. Обращение за помощью

В разделе **Устранение неполадок** представлена необходимая информация о наиболее часто возникающих проблемах, с которыми пользователь может столкнуться при работе с продуктом.

Если не удалось найти решение проблемы в доступных источниках, вы можете связаться с нами:

- «Свяжитесь с нами через интерфейс Bitdefender» (p. 144)
- «Свяжитесь с нами через онлайн-центр поддержки» (p. 144)

Важно

Для обращения в службу поддержки клиентов Bitdefender необходимо предварительно зарегистрировать продукт Bitdefender.Для получения дополнительной информации перейдите к *«Регистрация программы»* (p. 2).

Свяжитесь с нами через интерфейс Bitdefender

При наличии рабочего подключения к Интернету вы можете обратиться за помощью в службу поддержки клиентов Bitdefender непосредственно из интерфейса продукта.

Следуйте инструкции:

1. Откройте окно Bitdefender.
2. Нажмите ссылку **Справка и поддержка** в правом нижнем углу окна.
3. Для выбора доступны следующие параметры:
   - Ознакомьтесь с содержанием соответствующих статей или документов и попробуйте предложенные варианты решений.
   - Чтобы найти нужную информацию, запустите поиск по нашей базе данных.
   - Нажмите кнопку **Контакты службы технической поддержки**, чтобы запустить инструмент поддержки и связаться с отделом технической поддержки.Навигация по мастеру осуществляется с помощью кнопки **Далее**. Для выхода из мастера нажмите **Отмена**.
     a. Поставьте флажок в поле для принятия условий соглашения и нажмите **Далее**.
     b. Заполните форму отправки, указав необходимые данные:
        i. Введите свой адрес электронной почты.
        ii. Введите свое полное имя.
        iii. Выберите страну в соответствующем меню.
        iv. Введите описание возникшей проблемы.
     c. Подождите несколько минут, пока Bitdefender выполнит сбор сведений о продукте. Эта информация поможет нашим техническим специалистам найти эффективное решение вашей проблемы.
     d. Нажмите **Завершить**, чтобы отправить данные в службу поддержки клиентов Bitdefender. В ближайшее время с вами свяжется представитель службы поддержки.

Свяжитесь с нами через онлайн-центр поддержки

Если не удается найти требуемые сведения с помощью продукт Bitdefender, воспользуйтесь нашим онлайн-центром поддержки.

1. Перейдите к http://www.bitdefender.com/help.В центре поддержки Bitdefender имеется множество статей, содержащих решения проблем, связанных с работой Bitdefender.
2. Выберите продукт в левом столбце и выполните в центре поддержки Bitdefender поиск статей, в которых может быть описано решение вашей проблемы.
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.

14.2. 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.

14.2.1. Веб-адреса

Отдел продаж: sales@bitdefender.com
Центр поддержки:http://www.bitdefender.com/help
Документация: documentation@bitdefender.com
Местные дистрибуторы:http://www.bitdefender.com/partners
Партнерская программа: partners@bitdefender.com
Отдел по связям со СМИ: pr@bitdefender.com
Вакансии: jobs@bitdefender.com
Отправка вирусов: virus_submission@bitdefender.com
Отправка спама: spam_submission@bitdefender.com
Жалобы: abuse@bitdefender.com
Веб-сайт:http://www.bitdefender.ru

14.2.2. Местные дистрибьюторы

Местные дистрибьюторы Bitdefender готовы ответить на все вопросы коммерческого и общего характера, находящиеся в их компетенции.

Россия и страны СНГ (кроме Украины)
Aflex Distribution
127566, г. Москва, Алтуфьевское шоссе, д. 48, корп. 1

Тел \ факс: +7 (495) 988-22-68
Продажи: sales@bitdefender.ru
Сайт: http://www.bitdefender.ru
Центр поддержки: http://www.bitdefender.ru/support

14.2.3. 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.ru

Великобритания и Ирландия

Genesis Centre Innovation Way
Stoke-on-Trent, Staffordshire
ST6 4BF
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

Германия

Bitdefender GmbH
Airport Office Center
Robert-Bosch-Straße 2
59439 Holzwickede
Deutschland
Офис: +49 2301 91 84 0
Продажи: vertrieb@bitdefender.de
Техническая поддержка: http://kb.bitdefender.de
Сайт: http://www.bitdefender.de

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: http://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

15. 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.

15.1. Как удалить другие решения 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 2012 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.

15.2. 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 меню загрузки выберите **Безопасный режим** или **Безопасный режим с загрузкой сетевых драйверов**, если требуется доступ к Интернету.
4. Нажмите клавишу **Enter** и дождитесь 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.

15.3. 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, значит 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.

15.4. Как использовать функцию восстановления системы в Windows?

Если не удается загрузить компьютер в нормальном режиме, загрузитесь в безопасном режиме и используйте функцию восстановления системы, чтобы восстановить систему на момент времени, когда компьютер загружался без ошибок.

Для выполнения восстановления системы войдите в Windows под учетной записью администратора.

Для восстановления системы выполните следующие действия:

- Для Windows XP:
  1. Запустите Windows в безопасном режиме.
  2. В Windows нажмите **Пуск → Все программы → Служебные → Восстановление системы**.
  3. На странице **восстановления системы** выберите параметр **Восстановление предшествующего состояния компьютера** и нажмите кнопку "Далее".
  4. Следуйте инструкциям мастера, чтобы перезагрузить систему в обычном режиме.
- Для Windows Vista и Windows 7:
  1. Запустите Windows в безопасном режиме.
  2. Перейдите по следующему пути в меню Windows "Пуск": **Все программы → Стандартные → Служебные → Восстановление системы**.
  3. Следуйте инструкциям мастера, чтобы перезагрузить систему в обычном режиме.

15.5. Как отобразить скрытые объекты 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.

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.

E-mail

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

IP

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

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.

Архив

Диск, лента или каталог, содержащие резервные файлы.

Файл, содержащий один или несколько файлов в сжатом формате.

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).

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.

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 (floppy drive) работает с гибкими дисками.

Дисковод может быть встроенным, то есть находиться в корпусе компьютера, или же внешним, то есть находиться в отдельном корпусе и подключаться к компьютеру.

Загрузка

Копирование данных (обычно целых файлов) из основного местоположения 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.

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.

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.

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.

Клавиатурный шпион

Клавиатурные шпионы — это приложения, которые регистрируют все, что вводится с клавиатуры.

Клавиатурные шпионы по сути не являются вредоносным ПО. Их можно использовать в законных целях, например для контроля за действиями сотрудников или детей. Однако все чаще они используются кибер-мошенниками со злоумышленными намерениями (например, для сбора частных данных, таких как учетные данные и номера карт социального страхования).

Командная строка

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

Лазейки в системе (Backdoor)

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

Ложное срабатывание

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

Макро-вирус

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

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

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.

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.

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.

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.

Почтовый клиент

Приложение, которое позволяет вам отправлять и получать электронную почту.

Прикладная минипрограмма 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.

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.

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.

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.

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.

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.

Сигнатура вируса

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

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.

Спам

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

Сценарий

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

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.

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.

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.

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

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".

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.

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.