Bitdefender ANTIVIRUS PLUS

РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

Bitdefender Antivirus Plus
Руководство пользователя

Дата публикации 07/23/2018

Правовое положение

Bitdefender

Содержание

УСТАНОВКА

1. ПОДГОТОВКА К УСТАНОВКЕ

Перед установкой Bitdefender Antivirus Plus завершите эти приготовления для обеспечения беспрепятственной установки:

- Убедитесь, что компьютер, на котором вы собираетесь установить Bitdefender, соответствует минимальным системным требованиям. Если компьютер не соответствует минимальным системным требованиям, Bitdefender не будет установлен, либо не будет работать должным образоми это приведет к замедлению работы и нестабильности системы С полным списком системных требований можно ознакомиться в разделе«*Системные требования*» (p. 3).
- Войдите в систему под учетной записью администратора.
- Удалите с компьютера все остальные аналогичные программы. При обнаружении подобных программ во время установки программы Bitdefender Вы получите уведомление об их удалении. Одновременный запуск двух программ безопасности может повлиять на их работу и вызвать серьезные проблемы с системой. Во время установки защитник Windows будет отключен.
- Рекомендуется обеспечить подключение компьютера к Интернету во время установки, даже если установка выполняется с CD- или DVD-диска. Если доступны новые версии файлов приложения, включенные в пакет установки, Bitdefender можно загрузить и установить их.

2. СИСТЕМНЫЕ ТРЕБОВАНИЯ

Вы можете установить Bitdefender Antivirus Plus только на компьютеры, использующие следующие операционные системы:

- Windows 7 с пакетом обновления 1
- Windows 8
- Windows 8.1
- Windows 10

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

Примечание

Выполните следующую инструкцию, чтобы узнать, какая операционная система установлена на вашем компьютере и получить информацию по аппаратному обеспечению:

- В **Windows 7**, нажмите правую кнопку мыши на **Компьютер** на рабочем столе и выберите **Свойства** из выпадающего списка.
- На экране пуск в **Windows 8**, найдите **Компьютер** (например, можно вводить "Компьютер" непосредственно в стартовом окне) и затем нажмите на значок правой кнопкой мыши. В **Windows 8.1**, найдите **Этот компьютер**.

  Выберите **Свойства** в нижнем меню. Посмотрите пункт **Система**, чтобы найти информацию о вашем типе системы.
- В **Windows 10**, нажмите **Система** в поле поиска на панели задач и нажмите на его значок. Посмотрите пункт **Система**, чтобы найти информацию о вашем типе системы.

2.1. Минимальные системные требования

- 2 ГБ свободного пространства на жестком диске
- Двухъядерный процессор 1.6 ГГц
- 1 ГБ памяти (ОЗУ)

2.2. Рекомендуемые системные требования

- 2,5 ГБ свободного пространства на жестком диске (не менее 800 МБ на системном диске)
- Intel CORE Duo (2 ГГц) или аналогичный

- 2 ГБ памяти (ОЗУ)

2.3. Требования к программному обеспечению

Для использования Bitdefender и всех его функций компьютер должен соответствовать следующим требованиям к программному обеспечению:

- Microsoft Edge 40 и более новые версии
- Internet Explorer 10 и более новые версии
- Mozilla Firefox 51 более новые версии
- Google Chrome 34 и более новые версии

3. УСТАНОВКА ПРОДУКТА BITDEFENDER

Вы можете установить Bitdefender с установочного диска, или с помощью веб-инсталлятора, который можно загрузить на ваш компьютер с Bitdefender Central.

Если Ваша покупка охватывает более чем один компьютер (например, Вы приобрели Bitdefender Antivirus Plus для 3 ПК), повторите процесс установки и зарегистрируйте продукт с помощью лицензионного ключа на каждом компьютере. Вам нужно использовать аккаунт, который содержит активную подписку на ваш Bitdefender.

3.1. Установка из Bitdefender Central

Из аккаунта Bitdefender Central вы можете скачать установочный комплект, соответствующий приобретенной подписке. Как только процесс установки завершен, Bitdefender Antivirus Plus будет активирован.

Для скачивания Bitdefender Antivirus Plus из Bitdefender Central необходимо:

1. Войдите в ваш Bitdefender Central.
2. Выберите панель **Мои устройства**, затем нажмите **УСТАНОВИТЬ ЗАЩИТУ**.
3. Выберите одну из двух доступных опций:

   - **Защитить это устройство**

     Выберите этот параметр и сохраните установочный файл.

   - **Защитить другие устройства**

     Выберите этот параметр и нажмите кнопку **ОТПРАВИТЬ ССЫЛКУ ДЛЯ ЗАГРУЗКИ**. Введите адрес электронной почты в соответствующем поле и нажмите **ОТПРАВИТЬ ПИСЬМО**. Обратите внимание, что сгенерированная ссылка на скачивание действительна только в течение 24 часов. Если срок действия ссылки истечет, необходимо создать новую, следуя тем же инструкциям.

Проверьте введенную учетную запись на устройстве, на котором хотите установить Bitdefender, и нажмите соответствующую кнопку загрузки.

4. Подождите окончания загрузки, затем запустите программу установки.

Проверка установки

Сначала Bitdefender проверит вашу систему для подтверждения установки.

Если система не соответствует минимальным требованиям для установки Bitdefender, вы получите уведомление об исправлениях, которые необходимо внести перед продолжением работы.

При обнаружении несовместимой антивирусной программы или более ранней версии Bitdefender, отобразится запрос на ее удаление из системы. Следуйте инструкциям по удалению программного обеспечения из системы. Это позволяет избежать возникновения проблем в будущем. Для завершения удаления обнаруженных антивирусных программ может потребоваться перезагрузка.

В Bitdefender Antivirus Plus инсталляционный пакет постоянно обновляется.

Примечание
Загрузка установочных файлов может занять много времени, особенно на медленных интернет-соединениях.

Если установка прошла проверку, появится мастер установки. Выполните следующие шаги для установки Bitdefender Antivirus Plus.

Шаг 1 - Bitdefender установка

Прежде чем приступать к установке, необходимо принять Соглашение о подписке. Ознакомьтесь с Соглашением о Подписке и условиями использования Bitdefender Antivirus Plus.

Если вы не согласны с этими условиями, закройте окно. Процедура установки будет прервана и Вы выйдете из программы установки.

Две дополнительные задачи могут быть выполнены во время этого шага:

- Включите параметр **Отправлять отчеты о продукте**. При разрешении этой опции, отчеты с информацией о том, как вы используете продукт, отправляются на серверы Bitdefender. Эта информация необходима для усовершенствования продукта, и с ее помощью мы сможем предоставить более широкие знания в области использования этого продукта. Следует отметить, что в этих отчетах не содержится конфиденциальная информация, такая как ваше имя или IP-адрес, и они не будут использоваться в коммерческих целях.
- Выберите язык, который вы хотите использовать в продукте.

Нажмите кнопку **УСТАНОВИТЬ**, чтобы запустить процесс установки продукта Bitdefender.

Шаг 2 - Ход выполнения установки

Дождитесь завершения установки. Отображаются подробные сведения о ходе выполнения.

Выполняется проверка критических областей системы на наличие угроз, загрузка и установка актуальных версий файлов приложений, а также запуск служб Bitdefender. Выполнение этого шага может занять несколько минут. Нажмите кнопку **ПРОПУСТИТЬ СКАНИРОВАНИЕ** если Вы хотите сканировать систему позже. Дополнительные сведения о проведении сканирования системы см.в «*Запуск проверки системы*» (p. 84)

Шаг 3 - Установка завершена

Ваш Bitdefender продукт успешно установлен.

Отображается сводная информация по установке. Если во время установки обнаружены и удалены угрозы, может потребоваться перезагрузка системы. Нажмите **НАЧАТЬ ПОЛЬЗОВАТЬСЯ Bitdefender** чтобы продолжить.

Шаг 4 - Начать

В окне **Начать** Вы можете увидеть подробную информацию о Вашей активной подписке.

Нажмите **ЗАКОНЧИТЬ** чтобы перейти в Bitdefender Antivirus Plus интерфейс.

3.2. Установка продукта с установочного диска

Чтобы установить Bitdefender с установочного диска, вставьте диск в оптический привод.

В течение нескольких секунд должен появится экран приветствия. Следуйте инструкциям для начала установки.

Если экран приветствия не отображается, используйте проводник Windows для перехода в корневой каталог диска, и дважды щелкните файл autorun.exe.

Если у Вас медленная скорость Интернет-соединения или система не подключена к Интернету, нажмите кнопку **Установить с CD/DVD**. В этом случае продукт Bitdefender будет установлен с диска и более новая версия будет загружена с помощью серверов обновления Bitdefender.

Проверка установки

Сначала Bitdefender проверит вашу систему для подтверждения установки.

Если система не соответствует минимальным требованиям для установки Bitdefender, вы получите уведомление об исправлениях, которые необходимо внести перед продолжением работы.

При обнаружении несовместимой антивирусной программы или более ранней версии Bitdefender, отобразится запрос на ее удаление из системы. Следуйте инструкциям по удалению программного обеспечения из системы. Это позволяет избежать возникновения проблем в будущем. Для завершения удаления обнаруженных антивирусных программ может потребоваться перезагрузка.

Примечание
Загрузка установочных файлов может занять много времени, особенно на медленных интернет-соединениях.

Если установка прошла проверку, появится мастер установки. Выполните следующие шаги для установки Bitdefender Antivirus Plus.

Шаг 1 - Bitdefender Установка

Прежде чем приступать к установке, необходимо принять Соглашение о подписке. Ознакомьтесь с Соглашением о Подписке и условиями использования Bitdefender Antivirus Plus.

Если вы не согласны с этими условиями, закройте окно. Процедура установки будет прервана и Вы выйдете из программы установки.

Две дополнительные задачи могут быть выполнены во время этого шага:

- Включите параметр **Отправлять отчеты о продукте**. При разрешении этой опции, отчеты с информацией о том, как вы используете продукт, отправляются на серверы Bitdefender. Эта информация необходима для усовершенствования продукта, и с ее помощью мы сможем предоставить более широкие знания в области использования этого продукта. Следует отметить, что в этих отчетах не содержится конфиденциальная информация, такая как ваше имя или IP-адрес, и они не будут использоваться в коммерческих целях.
- Выберите язык, который вы хотите использовать в продукте.

Нажмите кнопку **УСТАНОВИТЬ**, чтобы запустить процесс установки продукта Bitdefender.

Шаг 2 - Ход выполнения установки

Дождитесь завершения установки. Отображаются подробные сведения о ходе выполнения.

Идет проверка наиболее важных областей системы на наличие угроз и запуск служб Bitdefender. Выполнение этого шага может занять несколько минут. Нажмите кнопку **ПРОПУСТИТЬ СКАНИРОВАНИЕ** если Вы хотите сканировать систему позже. Дополнительные сведения о проведении сканирования системы см.в «*Запуск проверки системы*» (p. 84)

Шаг 3 - Установка завершена

Отображается сводная информация по установке. Если во время установки обнаружены и удалены угрозы, может потребоваться перезагрузка системы. Нажмите **НАЧАТЬ ПОЛЬЗОВАТЬСЯ Bitdefender** чтобы продолжить.

Шаг 4 - Аккаунт Bitdefender

После завершения начальной настройки, появится окно аккаунта Bitdefender. Учетная запись Bitdefender требуется для того, чтобы активировать продукт и использовать его онлайн возможности. Для получения более подробной информации, обратитесь к «*Bitdefender Central*» (p. 33).

Выполните действия, соответствующие текущей ситуации.

- **Я хочу создать учетную запись Bitdefender**

  1. Введите необходимую информацию в соответствующих полях. Информация, которую вы предоставите, останется конфиденциальной. Пароль должен содержать не менее 8 символов и содержать цифру.
  2. Прежде чем продолжить, вы должны принять условия использования. Внимательно ознакомьтесь с пунктом "Условия использования", поскольку в нем приведены условия, на которых вы можете использовать Bitdefender.

     Кроме того, вы можете ознакомиться с Политикой конфиденциальности.
  3. Нажмите **СОЗДАТЬ УЧЕТНУЮ ЗАПИСЬ**.

  > **Примечание**
  > После создания учетной записи можно использовать представленный адрес электронной почты и пароль для входа в учетную запись https://central.bitdefender.com или в приложение Bitdefender Central при том условии, что оно установлено на одном из устройств Android или iOS. Для установки приложения Bitdefender Central на устройство Android необходимо войти в Google Play, найти Bitdefender Central и нажать на соответствующую опцию установки. Для установки приложения Bitdefender Central на устройство iOS необходимо войти в App Store, найти Bitdefender Central и нажать на соответствующую опцию установки.

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

  1. Нажмите **Войти**, затем введите адрес электронной почты и пароль для Вашей учетной записи Bitdefender.

     Нажмите **Войти** чтобы продолжить.

2. Если вы забыли пароль учетной записи или просто хотите сбросить уже установленный, нажмите ссылку **Забыл пароль**. Введите адрес вашей электронной почты, затем нажмите кнопку **ЗАБЫЛ ПАРОЛЬ**. Проверьте электронную почту учетной записи и следуйте приведенным инструкциям для установки нового пароля Вашей учетной записи Bitdefender

> **Примечание**
> Если у вас уже есть учетная запись MyBitdefender, вы можете использовать ее, чтобы войти в свою учетную запись Bitdefender. Если вы забыли свой пароль, то сначала нужно перейти https://my.bitdefender.com, чтобы сбросить его. Затем, используйте обновленные учетные данные для входа в вашу учетную запись Bitdefender.

- **Я хочу войти, используя свою учетную запись Microsoft, Facebook или Google**

  Чтобы войти используйте свою учетную запись Microsoft, Facebook или Google:

  1. Выберите службу, которую вы хотите использовать. Вы будете перенаправлены на страницу входа этой службы.
  2. Следуйте инструкциям, предоставленным выбранной службой, чтобы связать свою учетную запись с Bitdefender.

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

Шаг 5 - Активация вашего продукта

> **Примечание**
> Этот шаг появляется, если вы выбрали создать новую учетную запись Bitdefender на предыдущем шаге или если вы вошли в систему с помощью учетной записи с истекшим сроком подписки.

Требуется активное подключение к Интернету для завершения активации вашего продукта.

Выполните действия, соответствующие текущей ситуации:

- У меня есть код активации

  В этом случае для регистрации продукта необходимо выполнить следующие действия:

  1. Введите код активации в поле **У меня есть код активации** и затем нажмите **Продолжить**.

     Примечание
     Вы можете найти код активации:
     - на этикетке компакт- или DVD-диска.
     - на регистрационной карточке продукта;
     - в электронном письме о совершении покупки.

  2. **Я хочу оценить Bitdefender**

     В этом случае вы сможете использовать продукт в течение 30-и дней. Для использования пробного периода, выберите **У меня нет подписки, я хочу попробовать продукт бесплатно**, затем нажмите кнопку **Продолжить**.

Шаг 6 - Начать

В окне **Начать** Вы можете увидеть подробную информацию о Вашей активной подписке.

Нажмите **ЗАКОНЧИТЬ** чтобы перейти в Bitdefender Antivirus Plus интерфейс.

НАЧАЛО РАБОТЫ

4. ОСНОВЫ

Установка Bitdefender Antivirus Plus обеспечивает защиту от всех типов угроз, таких как вирусы, шпионские программы и программы-вымогатели, эксплойты, бот-сети и трояны.

Приложение использует технологию Фотон для повышения скорости и производительности процесса сканирования угроз. Он работает путем исследования установленных в системе приложений и определяет какие из них нуждаются в сканировании, минимизируя таким образом влияние на производительность системы.

Подключение к публичным точкам в таких местах как аэропорты, торговые центры, кафе или отели без защиты могут представлять опасность для Вашего устройства и личных данных. Главным образом потому, что мошенники могут следить за Вашей деятельностью и найти подходящий момент для хищения личных данных, кроме того Ваш IPадрес находится у всех на виду. В следствие этого,Ваше устройство может стать жертвой кибератак в будущем. Чтобы избежать подобные негативные последствия установите и используйте приложение«*VPN*» (p. 127).

Можете отслеживать пароли и учетные данные, сохранив их в «*Защита ваших учетных данных при помощи параметра "Менеджер паролей"*» (p. 119) Хранилище. Используя один мастер-пароль Вы можете защитить персональные данные от злоумышленников, которые могут попытаться вывести Ваши денежные средства.

Чтобы обеспечить защиту от потенциальных мошенников и нарушителей во время подключения устройства к незащищенной точке доступа, Bitdefender проводит анализ уровня безопасности и, если это необходимо, предлагает необходимые решения для повышения безопасности Ваших действий в сети. Для получения инструкций как сохранить в безопасности персональные данные см.«*Советник безопасности Wi-Fi*» (p. 109)

Ваши личные файлы, хранящиеся локально, например, документы, фотографии или видеоматериалы, а также те файлы, которые хранятся на облаке, остаются под надежной защитой от самого опасного на сегодняшний день вредоносного ПО, а именно, вируса-вымогателя. Информацию о том, как перенести личные файлы в хранилище см. «*Safe Files*» (p. 113).

Файлы, зашифрованные вымогателем, могут быть восстановлены без выплаты запрашиваемого выкупа. Сведения о восстановлении зашифрованных файлов см. в «*Ransomware Remediation*» (p. 116).

В то время как вы работаете, играете в игры или смотрите фильмы, Bitdefender может предложить вам непрерывную работу путем отсрочки задач по обслуживанию, устраняя перебои и регулировки системой визуальных эффектов. Вы можете извлечь выгоду из всего этого, активизировав и сконфигурировав «*Профили*» (p. 139).

Bitdefender будет принимать за вас большинство решений, связанных с защитой, и вы редко будете видеть всплывающие уведомления. Подробная информация о принятых мерах и информация о работе программы, отображена в окне Уведомления. Для получения более подробной информации, обратитесь к «*Уведомления*» (p. 16).

Время от времени необходимо открывать Bitdefender и устранять существующие неполадки. Возможно, вам придется настроить отдельные элементы Bitdefender или принять профилактические меры для защиты вашего компьютера и данных.

Чтобы использовать онлайн-возможности Bitdefender Antivirus Plus и управлять своими подписками и устройствами, войдите в Вашу учетную запись Bitdefender. Для получения более подробной информации, обратитесь к «*Bitdefender Central*» (p. 33).

В разделе «Советы» (p. 44) вы найдете пошаговые инструкции о том, как выполнять общие задачи. Если у вас возникли проблемы при использовании Bitdefender, проверьте раздел «*Решение общих вопросов.*» (p. 147) для возможного решения наиболее распространенных проблем.

4.1. Откройте окно Bitdefender.

Выполните следующую процедуру, чтобы войти в главный интерфейс Bitdefender Antivirus Plus:

- В **Windows 7**:
  1. Нажмите **Пуск** и перейдите в **Все программы**.
  2. Нажмите **Bitdefender**.
  3. Нажмите **Bitdefender Antivirus Plus** или дважды нажмите на Bitdefender иконку в области уведомлений.
- В **Windows 8 и Windows 8.1**:

Введите Bitdefender в Стартовом окне Windows (например, можно вводить "Bitdefender" непосредственно в стартовом окне) и затем нажмите на его значок. В качестве альтернативы, откройте приложение рабочего стола и затем дважды щелкните иконку Bitdefender в области уведомлений.

- В **Windows 10**:

  Выберите "Bitdefender" в поле поиска на панели задач, а затем щелкните на его значок. В качестве альтернативы, нажмите дважды на Bitdefender иконку в области уведомлений.

Дополнительную информацию об окне и значке Bitdefender, расположенных в области уведомлений, см. в *«Интерфейс Bitdefender»* (p. 21).

4.2. Уведомления

Bitdefender ведет подробный журнал событий, касающихся его автивности, которые он выполняет на вашем компьютере. Всякий раз, когда происходит что-то, имеющее отношение к безопасности системы и данных, новое сообщение добавляется в события Bitdefender, таким же образом, как новые сообщения электронной почты, входят в ваш почтовый ящик.

Уведомления являются важным инструментом для мониторинга и управления защитой Bitdefender. Например, вы можете легко проверить, успешно ли было выполнено обновление, были ли обнаружены угрозы или неисправности на компьютере и т.д. Кроме того, при необходимости можно предпринять дополнительные действия или изменить операции, которые выполнил Bitdefender.

Чтобы открыть журнал уведомлений, нажмите **Уведомления** в меню Bitdefender интерфейс. При каждом важном событии счетчик будет отмечать его на значке .

В зависимости от типа и серьезности, уведомления группируются в:

- **Критичные** события указывают на критичные проблемы. Их следует проверить незамедлительно.
- **Опасные** события указывают на некритичные проблемы. Их следует проверить и исправить в ближайшее время.

- **Информационные** события показывают успешно выполненные операции.

Нажмите каждую вкладку, чтобы найти более подробную информацию о сгенерированных событиях. Краткие сведения отображаются с помощью одинарного нажатия по каждому названию события, а именно: краткое описание, действие принятое Bitdefender с ним, когда это случилось, и дата и время, когда это произошло. При необходимости могут быть предоставлены варианты выбора дальнейших действий.

Чтобы упростить задачу управления зарегистрированными событиями, окно Уведомления предоставляет опции для удаления или пометить как прочитанные все события в этом разделе.

4.3. Профили

Некоторые режимы работы компьютера, такие как онлайн игры или видео-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.

Профили Bitdefender перенаправляет больше системных ресурсов в запущенные приложения, временно изменив настройки защиты и регулировку конфигурации системы. Следовательно, влияние системы на вашу деятельность сведена к минимуму.

Для адаптации к различным видам деятельности, Bitdefender предлагает использовать следующие профили:

Профиль Работа
: Оптимизирует эффективность вашей работы путем выявления и корректировки параметров продукта и системы.

Профиль "Фильм"
: Усиливает визуальные эффекты и устраняет перебои при просмотре фильмов.

Профиль Игры
: Усиливает визуальные эффекты и устраняет перебои когда вы играете в игры.

Профиль публичный Wi-Fi
: Применяемые параметры продукта обеспечивают полную защиту при подключении к небезопасной публичной сети.

Профиль Режим работы от батарей
: Применяет параметры продукта и удерживает фоновые активности для экономии заряда батареи.

4.3.1. Настройка автоматической активации профилей

Для простоты использования, вы можете настроить Bitdefender для управления рабочим профилем. В этом случае, Bitdefender автоматически определяет, какую деятельность вы выполняете и применяет настройки оптимизации системы и продукта.

Чтобы разрешить Bitdefender активировать профили необходимо:

1. Нажмите **Настройки** в меню навигации интерфейс Bitdefender.
2. Выберите вкладку **Profiles**.
3. Используйте соответствующий переключатель чтобы включить **Активировать профиль автоматически**

Если вы не хотите чтобы некоторые профили активировались автоматически, выключите соответсвующий переключатель.

Чтобы вручную активировать профиль, включите соответствующий переключатель. Только один профиль можно активировать за один раз.

Для получения подробной информации о профилях, пожалуйста, обратитесь к«*Профили*» (p. 139)

4.4. Защищенные паролем настройки Bitdefender

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

Установить защиту паролем для настроек Bitdefender:

1. Нажмите **Настройки** в меню навигации интерфейс Bitdefender.
2. В окне **Общие** включите **Защита паролем**.

3. Введите пароль в двух полях и затем нажмите **OK**. Пароль должен содержать не менее 8 символов.

После установки пароля при попытке изменения параметров настроек Bitdefender будет запрашивать пароль.

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.

Удалить защиту паролем:

1. Нажмите **Настройки** в меню навигации интерфейс Bitdefender.
2. В окне **Общие** отключите **Защита паролем**.
3. Введите пароль и затем нажмите **OK**

Примечание

Чтобы изменить пароль вашего продукта, нажмите **Изменить пароль**. Введите текущий пароль и нажмите **OK**. В новом окне, которое появится введите новый пароль, который вы хотите использовать, чтобы ограничить доступ к вашим Bitdefender параметрам.

4.5. Отчеты о продукте

Отчеты о продукте включают сведения о применении установленного продукта Bitdefender. Эта информация поможет нам усовершенствовать продукт и предложить в будущем более широкие возможности.

Обратите внимание, что эти отчеты не используются в коммерческих целях и не содержат таких конфиденциальных данных как: ваше имя или IP-адрес,

Если в процессе установки вы дали согласие на отправление таких отчетов на серверы Bitdefender и теперь хотите остановить процесс:

1. Нажмите **Настройки** в меню навигации интерфейс Bitdefender.
2. Выберите вкладку **Advanced**.
3. Отключите **Отчеты о продукте**.

4.6. Уведомления о специальных предложениях

Если имеются рекламные предложения, Bitdefender уведомит вас через всплывающее окно. Это дает Вам возможность воспользоваться выгодными ценами и сохранить Ваши устройства защищенными в течение более длительного периода времени.

Чтобы включить или отключить специальные предложения и уведомления о продуктах:

1. Нажмите **Настройки** в меню навигации интерфейс Bitdefender.
2. В окне **Общие** нажмите на соответствующий переключатель.

Опция специальные предложения и уведомления о продуктах включена по умолчанию.

4.7. Служба сканирования вредоносных программ

Bitdefender интегрируется с Microsoft Antimalware Scan Interface (AMSI), чтобы ваши устройства были защищены от динамических сценариев на основе вредоносных программ и нетрадиционных путей кибератаки. AMSI представляет собой универсальный стандарт интерфейса, благодаря которому приложения и службы могут интегрироваться с продуктами Bitdefender.

Чтобы включить или выключить интеграцию с Antimalware Scan Interface:

1. Нажмите **Настройки** в меню навигации интерфейс Bitdefender.
2. В окне **Общие** нажмите на соответствующий переключатель.

Параметр интеграции с Antimalware Scan Interface доступен только в Windows 10 и включен по умолчанию.

5. ИНТЕРФЕЙС BITDEFENDER

Bitdefender Antivirus Plus удовлетворяет требованиям как технически подкованных пользователей, так и новичков. Его графический пользовательский интерфейс предназначен для удовлетворения каждой категории пользователей.

Чтобы пройти через интерфейс Bitdefender, в верхней левой части экрана отображается мастер ввода, содержащий сведения о том, как взаимодействовать с продуктом и как его настроить. Выберите правую угловую скобку, чтобы продолжить навигацию по руководству, или **Пропустить тур** для закрытия мастера.

значок области уведомлений Bitdefender доступен в любое время, независимо от ваших действий.

В главном окне содержатся сведения о состоянии вашей безопасности. Здесь Автопилот отображает различные типы рекомендаций, которые помогут вам улучшить безопасность и повысить производительность вашего устройства. Кроме того, вы можете добавить быстрые действия, которые используете чаще всего. Таким образом, в нужный момент они будут всегда под рукой.

Из меню навигации, расположенном слева, можно перейти к вашей учетной записи Bitdefender, области настроек, уведомлениям и разделам Bitdefender для детальной настройки и дополнительных административных задач. Также вы можете связаться со службой поддержки в случае возникновения вопросов.

Если Вы хотите постоянно следить за важными сведениями о безопасности и иметь быстрый доступ к ключевым параметрам, добавьте Виджет безопасности на Рабочий стол.

5.1. Значок области уведомлений

Чтобы быстрее управлять всем продуктом, в области уведомлений можно использовать значок Bitdefender .

Примечание

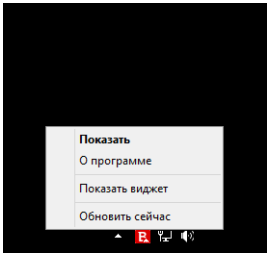
Значок Bitdefender может быть невидимым в любое время. Для того, чтобы значок постоянно отображался:

- В **Windows 7, Windows 8 и Windows 8.1**:

1. Нажмите стрелку в правом нижнем углу экрана.
2. Нажмите **Настроить...**, чтобы открыть окно Значки Области Уведомлений.
3. Выберите опцию **Показать значки и уведомления** для иконки **Bitdefenderагент**.

- В **Windows 10**:
  1. Щелкните правой кнопкой мыши панель задач и выберите **Свойства**.
  2. Нажмите **Настроить** в окне Панель задач.
  3. Нажмите в окне **Выберите отображение значков и уведомлений на панели задач** ссылку **Уведомления & действия**.
  4. Включите переключатель рядом с **Bitdefender agent**.

Двойной щелчок по этому значку открывает приложение Bitdefender. Кроме того, щелкнув правой кнопкой мыши по иконке, контекстное меню позволит Вам быстро управлять продуктом Bitdefender.



Значок панели задач

- **Показать** - открытие главного окна Bitdefender.
- **О программе** открывает окно, из которого можно получить сведения о Bitdefender, ознакомиться с Соглашением о подписке и третьих сторонах, Политикой конфиденциальности, найти помощь в решении возникших проблем.
- **Скрыть / Показать Виджет Безопасности** - включает / отключает Виджет Безопасности.
- **Обновить сейчас** - запускает немедленное обновление. Состояние обновления можно увидеть на панели "Обновления" в главном Bitdefender окне.

Значок области уведомлений Bitdefender информирует о проблемах, влияющих на Ваш компьютер, или о том, как работает продукт, отображая Специальный символ следующим образом:

Проблемы, влияющие на безопасность вашей системы, отсутствуют.

Критические проблемы влияют на безопасность вашей системы. Они требуют немедленного вмешательства и должны быть исправлены как можно скорее.

Если Bitdefender не работает, значок области уведомлений отображается на сером фоне: B. Подобное обычно происходит при истечении срока действия лицензионного ключа. Также это может произойти, когда Bitdefender не отвечает или когда другие ошибки влияют на нормальную работу Bitdefender.

5.2. Меню навигации

В левой части интерфейса Bitdefender находится меню навигации, которое позволяет быстро получить доступ к функциям и инструментам Bitdefender, необходимым для обработки вашего продукта. В этой области доступны следующие вкладки:

- **Панель управления**. Здесь можно быстро устранить проблемы безопасности, просмотреть рекомендации, соответствующие потребностям системы и шаблонам использования, а также выполнить быстрые действия.
- **Защита**. Здесь вы можете запустить и настроить антивирусное сканирование, восстановить данные, если они были зашифрованы программой-вымогателем, настроить защиту во время навигации в Интернете, перейти к настройкам брандмауэра, защите файлов и приложений от атак программ-вымогателей.
- **Приватность**. Здесь вы можете создавать менеджеры паролей для ваших учетных записей, совершать онлайн-платежи в безопасной среде, перейти к приложению VPN и защитить доступ к веб-камере.
- **Уведомления**. Отсюда вы получаете доступ к сгенерированным уведомлениям.
- **Моя учетная запись**. Здесь можно получить доступ к учетной записи Bitdefender для проверки подписок и выполнения задач безопасности на управляемых устройствах. Доступны сведения об учетной записи Bitdefender и использовании подписки.
- **Параметры**. Отсюда Вы можете получить доступ к общим настройкам.

- **Поддержка**. Отсюда, когда нужна помощь в решении проблем с Вашим Bitdefender Antivirus Plus, Вы можете обратиться в отдел технической поддержки Bitdefender.

5.3. Панель управления

Окно "Панель управления" позволяет выполнять общие задачи, быстро устранять проблемы безопасности, просматривать информацию о работе продукта и получать доступ к панелям для настройки параметров продукта.

Вам требуется всего несколько раз нажать мышью.

Это окно включает три основные области:

Область состояния безопасности
: Здесь можно проверить состояние безопасности компьютера.

Autopilot
: Здесь вы можете проверить рекомендации "Автопилота", чтобы обеспечить надлежащую функциональность системы.

Быстрые действия
: Здесь Вы можете запускать различные задачи, чтобы защитить систему.

5.3.1. Область состояния безопасности

Bitdefender использует Систему слежения в целях обнаружения проблем, которые могут отразиться на безопасности Вашего компьютера и личных данных и сообщает Вам о них. К обнаруженным проблемам относится отключение важных параметров настроек защиты и другие условия, представляющие угрозу безопасности.

При обнаружении любой проблемы, влияющей на безопасность вашего компьютера, в верхней части Bitdefender интерфейса появляется статус безопасности, обозначенный красным цветом. Отображаемый статус указывает на характер проблем, влияющих на вашу систему. Значок области уведомлений поменяется на , также можно навести курсор на значок и всплывающее окно подтвердит наличие имеющихся проблем.

Поскольку обнаруженные проблемы представляют серьезную угрозу безопасности и могут препятствовать защите Bitdefender,

рекомендуется как можно скорее обратить на них внимание и исправить. Чтобы устранить проблему, нажмите кнопку рядом с обнаруженной проблемой.

5.3.2. Autopilot

Bitdefender "Автопилот" будет выступать в качестве вашего персонального советника по вопросам безопасности, чтобы обеспечить эффективную работу и защиту. Исходя из выполняемых вами действий, будь то проведение онлайн-платежей, игры или просмотр видео, Bitdefender "Автопилот" конфигурирует контекстуальные рекомендации. Предлагаемые рекомендации также могут быть связаны с действиями, которые необходимо выполнить для поддержания работоспособности продукта в полном объеме.

Чтобы приступить к использованию предлагаемой функции или внести улучшения в ваш продукт, нажмите соответствующую кнопку.

Отключение уведомлений режима "Автопилот"

Чтобы привлечь ваше внимание к рекомендациям режима "Автопилот", продукт Bitdefender использует всплывающее окно для уведомлений.

Чтобы отключить уведомления режима "Автопилот":

1. Нажмите **Настройки** в меню навигации интерфейс Bitdefender.
2. В окне **Общие** отключите **Уведомления о рекомендациях**.

5.3.3. Быстрые действия

Используя быстрые действия, можно быстро запускать важные задачи для защиты вашей системы и улучшения работы.

Bitdefender по умолчанию предусматривает некоторые быстрые действия, которые можно заменить на другие часто используемые действия. Чтобы заменить быстрое действие:

1. Нажмите значок + в правом верхнем углу карточки, которую хотите удалить.
2. Укажите задачу, которую хотите добавить в основной интерфейс, и нажмите кнопку **ДОБАВИТЬ**.

Задачи, которые вы можете добавить в основной интерфейс:

- **Быстрое Сканирование**. Запустите быстрое сканирование, чтобы оперативно выявить возможные угрозы на вашем компьютере.
- **Сканирование системы**. Запустите быстрое сканирование чтобы убедиться, что компьютер очищен от угроз.
- **Сканирование Уязвимостей**. Проверьте компьютер на наличие уязвимостей, чтобы убедиться, что все установленные приложения, вместе с операционной системой, обновляются и должным образом функционируют.
- **Проверка безопасности Wi-Fi**. Откройте "Советник по безопасности Wi-Fi", чтобы проверить подключенную беспроводную сеть на предмет безопасности и наличие уязвимостей.
- **Кошельки**. Обзор и управление вашими кошельками.
- **Открыть Safepay**. Откройте Bitdefender Safepay™, чтобы защитить ваши конфиденциальные данные во время онлайн-транзакций.
- **Открыть VPN**. Откройте Bitdefender VPN, чтобы добавить дополнительный уровень защиты при подключении к Интернету
- **Уничтожитель файлов**. Запустите средство «Файловый шредер» для удаления следов конфиденциальных данных с вашего компьютера.
-

Чтобы начать защиту дополнительных устройств с помощью Bitdefender:

1. Нажмите **Установить на другом устройстве**.

   Вы будете перенаправлены на веб-страницу учетной записи Bitdefender. Убедитесь, что вы вошли с вашими учетными данными.

2. В появившемся окне нажмите **Отправить ссылку для скачивания**.

3. Введите адрес электронной почты в соответствующем поле и нажмите **ОТПРАВИТЬ ПИСЬМО**. Обратите внимание, что сгенерированная ссылка на скачивание действительна только в течение 24 часов. Если срок действия ссылки истечет, необходимо создать новую, следуя тем же инструкциям.

   Проверьте введенную учетную запись на устройстве, на котором хотите установить Bitdefender, и нажмите соответствующую кнопку загрузки.

В зависимости от вашего выбора будут установлены следующие продукты Bitdefender:

- Bitdefender Antivirus Plusна устройствах на базе Windows.
- Bitdefender Антивирус для Mac на устройствах на базе macOS.

- Bitdefender Мобильная безопасность на устройствах на базе Android.
- Bitdefender Мобильная безопасность на устройствах на базе iOS.

5.4. Разделы Bitdefender

Продукт Bitdefender поставляется с распределенными в два раздела полезными функциями, которые помогут вам оставаться защищенным во время игр, просмотра веб-страниц, работы или совершении онлайн-платежей.

Если вы хотите получить доступ к функциям определенного раздела или начать настройку продукта, используйте следующие значки, расположенные в меню навигации в интерфейсе Bitdefender:

- Защита
- Приватность

5.4.1. **Защита**

В разделе "Защита" можно установить дополнительные параметры безопасности, настроить "Безопасные файлы" и "Предотвращение сетевых угроз", проверить и устранить потенциальные уязвимости системы и оценить уровень безопасности подключенных беспроводных сетей.

Функции, которыми вы можете управлять в разделе Защита:

АНТИВИРУС

Антивирусная защита — это основа вашей безопасности. Bitdefender защищает вас в режиме реального времени и по требованию от всевозможных угроз, таких как вирусы, трояны, шпионское по, рекламное по и т.д.

Из функции Антивирус вы можете легко получить доступ к следующим задачам сканирования:

- Быстрое сканирование
- Сканирование системы
- Управление сканированием
- Режим Восстановления (Rescue Environment в Windows 10)

Дополнительную информацию о задачах сканирования и процедуре настройки защиты антивируса см. в «*Антивирусная защита*» (p. 77).

ПРЕДОТВРАЩЕНИЕ СЕТЕВЫХ УГРОЗ

"Предотвращение сетевых угроз" помогает вам оставаться защищенным от фишинговых атак, попыток мошенничества и утечек ваших персональных данных во время серфинга в Интернете.

Для получения дополнительных сведений о настройке Bitdefender для защиты вашей веб-активности, пожалуйста, обратитесь «*Предотвращение сетевых угроз*» (p. 102).

АКТИВНЫЙ КОНТРОЛЬ УГРОЗ

Активный Контроль Угроз эффективно защищает вашу систему от угроз, таких как вымогатели, шпионские программы и трояны, путем анализа поведения всех установленных приложений. Подозрительные процессы идентифицируются и, при необходимости, блокируются.

Для получения более подробной информации о том, как защитить вашу систему от угроз, обратитесь к «*АКТИВНЫЙ КОНТРОЛЬ УГРОЗ*» (p. 100).

УЯЗВИМОСТИ

Функция Уязвимость помогает сохранить операционную систему и приложения, которые вы регулярно используете в актуальном состоянии, и определить небезопасные Беспроводные сети, к которым вы подключаетесь.

Нажмите **Сканирование Уязвимости** в функции Уязвимость, чтобы начать идентификацию критических обновлений Windows, приложений обновления, слабые пароли, принадлежащие к учетным записям Windows и беспроводных сетей, которые не являются безопасными.

Нажмите **"Безопасность Wi-Fi"**, чтобы просмотреть список подключенных беспроводных сетей вместе с оценкой репутации каждой из них и ознакомиться с возможными действиями, которые можно предпринять, чтобы оставаться в безопасности от так называемых "ищеек".

Для получения более подробной информации о настройке защиты от уязвимостей, пожалуйста, обратитесь в «*Уязвимости*» (p. 105).

БЕЗОПАСНЫЕ ФАЙЛЫ

Функция «Безопасные файлы» гарантирует, что ваши личные файлы останутся защищенными от атак вируса-вымогателя.

Дополнительные сведения о том, как настроить безопасные файлы для защиты личных файлов от атак вымогателей, см. «*Safe Files*» (p. 113).

RANSOMWARE REMEDIATION

Функция "Ransomware Remediation" окажет помощь в восстановлении файлов в случае их шифрования программой-вымогателем.

Дополнительные сведения о восстановлении зашифрованных файлов см. в разделе «*Ransomware Remediation*» (p. 116).

5.4.2. Приватность

В разделе Конфиденциальность вы можете открыть приложение Bitdefender VPN, защитить свои онлайн-транзакции и обеспечить безопасность вашего просмотра.

Функции, которыми вы можете управлять в разделе Конфиденциальность:

VPN

VPN обеспечивает защиту Вашей онлайн-активности и скрывает Ваш IP-адрес каждый раз, когда вы подключаетесь к незащищенным беспроводным сетям, находясь в аэропортах, торговых центрах, кафе или отелях. Кроме того, можно получить доступ к содержимому, которое обычно ограничено в определенных областях.

Для получения дополнительной информации об этой функции см. «*VPN*» (p. 127).

Кошелек WALLET

Bitdefender "Менеджер паролей" помогает отслеживать ваши пароли, защищать вашу конфиденциальность и обеспечивать безопасную работу в Интернете.

Дополнительную информацию по настройке родительского контроля см. в «*Защита ваших учетных данных при помощи параметра "Менеджер паролей"*» (p. 119).

БЕЗОПАСНЫЙ ПЛАТЕЖ

Браузер Bitdefender Safepay™ поможет вам сохранить ваш Интернет-банкинг, онлайн-шопинг и любой другой тип онлайн-транзакций частным и безопасным.

Для получения более подробной информации о Bitdefender Safepay™, пожалуйста, обратитесь «*Безопасный платеж - безопасность для онлайн-транзакций*» (p. 130).

ЗАЩИТА ДАННЫХ

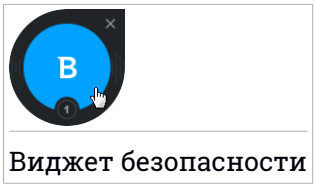
Функция защиты данных позволяет постоянно удалять файлы. Нажмите **Шредер файлов** на панели «Защита данных» для запуска мастера, который позволит полностью удалить файлы из Вашей системы.

Для получения более подробной информации о настройке Защита личных данных, пожалуйста, обратитесь «*Защита данных*» (p. 135).

5.5. Виджет безопасности

Виджет безопасности является быстрым и простым способом для контроля и управления Bitdefender Antivirus Plus. Добавление этого небольшого и ненавязчивого виджета на рабочий стол позволяет увидеть важную информацию и выполнить ключевые задачи в любое время:

- откройте главное окно Bitdefender.
- Мониторинг активности сканирования в режиме реального времени.
- Отслеживайте состояние безопасности системы и устраняйте существующие проблемы.
- показывает, когда идет процесс обновления.
- Просмотр уведомлений и получение доступа к последним событиям, о которых сообщает Bitdefender.
- сканирование файлов и папок с помощью перетаскивания одного или нескольких элементов на виджет.



Виджет безопасности

Общее состояние безопасности вашего компьютера отображается **в центре** виджета. Состояние обозначается цветом и формой значка, которые отображаются в этой области.

Критические проблемы влияют на безопасность системы.

Они требуют немедленного вмешательства и решения. Щелкните значок состояния, чтобы начать исправление проблем, о которых сообщалось.

Некритические проблемы влияют на безопасность системы. Их следует проверить и исправить в ближайшее время. Щелкните значок состояния, чтобы начать исправление проблем, о которых сообщалось.

Ваша система защищена.

При выполнении задачи проверки по требованию отображается анимированный значок.

При сообщении о проблемах щелкните значок состояния, чтобы запустить мастер устранения неполадок.

Нижняя сторона виджета отображает счетчик непрочитанных событий (число выдающихся событий Bitdefender, если таковые имеются). Щелкните счетчик событий, например 1 для одного непрочитанного события, чтобы открыть окно Уведомления. Для получения более подробной информации, обратитесь к «*Уведомления*» (p. 16).

5.5.1. Сканирование файлов и папок

Вы можете использовать Виджет безопасности для быстрого сканирования файлов и папок. Перетащите файл или папку, которую Вы хотите просканировать и поместите его в **Виджет безопасности**.

Появится Мастер сканирования и проведет вас через процесс сканирования. Параметры сканирования предварительно настроены

для достижения наилучших результатов обнаружения и они не могут быть изменены. При обнаружении инфицированных файлов, Bitdefender попробует вылечить их (удалить вредоносный код). Если действие не будет успешно, то Мастер сканирования даст вам возможность определить дальнейшие действия по отношению к файлам.

5.5.2. Показать / скрыть Виджет безопасности

Если вы больше не хотите видеть виджет, нажмите .

Для того, чтобы восстановить значок Виджета безопасности, воспользуйтесь одним из предложенных способов:

- Из области уведомлений:
  1. Правой кнопкой мыши щелкните по значку Bitdefender в области уведомлений.
  2. Нажмите **Виджет безопасности** в появившемся контекстном меню.
- Из интерфейса Bitdefender:
  1. Нажмите **Настройки** в меню навигации интерфейс Bitdefender.
  2. В окне **Общие** включите **Виджет безопасности**.

Виджет безопасности Bitdefender по умолчанию отключен.

6. BITDEFENDER CENTRAL

Bitdefender Central представляет собой платформу с доступом к онлайн-функциям и службам продукта, где также можно удаленно выполнять важные задачи на устройствах с установленным Bitdefender. Вы можете войти в учетную запись Bitdefender с любого компьютера, подключенного к интернету, перейдя к https://central.bitdefender.com или непосредственно из приложения Bitdefender Central на устройствах Android и iOS.

Чтобы установить приложение Bitdefender Central на устройства:

- **На Android**-выполните поиск Bitdefender Central в Google Play, затем загрузите и установите приложение. Выполните необходимые действия для завершения установки.
- **На iOS**-выполните поиск Bitdefender Central в App Store, затем загрузите и установите приложение. Выполните необходимые действия для завершения установки.

После того как вы вошли в систему, вы можете начать делать следующее:

- Скачать и установить Bitdefender на операционные системы Windows, OS X and Android . Продукты, доступные для скачивания:
  - Bitdefender Antivirus Plus
  - Антивирус Bitdefender для Mac
  - Bitdefender Mobile Security для Android
  - Bitdefender Мобильная безопасность для iOS
- Управление и обновление своей Bitdefender подпиской.
- Добавлять новые устройства к сети и управлять ими, где бы вы не находились.

6.1. Доступ к Bitdefender Central

Есть несколько способов доступа к Bitdefender Central:

- Из интерфейса Bitdefender:
  1. Нажмите **Моя учетная запись** в меню навигации интерфейса Bitdefender.

2. Нажмите **Переход в Bitdefender Central**.
3. Войдите в свою учетную запись Bitdefender, используя свой адрес электронной почты и пароль.

- Из вашего веб-браузера:
  1. Откройте веб-браузер на любом устройстве с доступом к Интернету.
  2. Перейти к: https://central.bitdefender.com.
  3. Войдите в свою учетную запись Bitdefender, используя свой адрес электронной почты и пароль.
- С устройства Android или iOS:

  Откройте установленное приложение Bitdefender Central.

Примечание
В этом материале предоставлены инструкции, доступные на веб-платформе.

6.2. Мои подписки

Платформа Bitdefender Central дает возможность легко управлять имеющимися подписками на всех ваших устройствах.

6.2.1. Проверка доступных подписок

Проверка доступных подписок:

1. Войдите в ваш Bitdefender Central.
2. Выберите панель **Мои подписки**.

Здесь находится информация о наличии подписок и количестве устройств, которыми вы управляете.

Вы можете добавить новое устройство к подписки или продлить имеющуюся, выбрав карточку подписки.

Примечание
Вы можете иметь одну или несколько подписок на вашем аккаунте при условии, что они предназначены для различных платформ (Windows, Mac OS X или Android).

6.2.2. Добавить новое устройство

Если ваша подписка охватывает более одного устройства, вы можете добавить новое устройство и установить на нем Bitdefender Antivirus Plus следующим образом:

1. Войдите в ваш Bitdefender Central.
2. Выберите панель **Мои устройства**, затем нажмите **УСТАНОВИТЬ ЗАЩИТУ**.
3. Выберите одну из двух доступных опций:
   - **Защитить это устройство**

     Выберите этот параметр и сохраните установочный файл.
   - **Защитить другие устройства**

     Выберите этот параметр и нажмите кнопку **ОТПРАВИТЬ ССЫЛКУ ДЛЯ ЗАГРУЗКИ**. Введите адрес электронной почты в соответствующем поле и нажмите **ОТПРАВИТЬ ПИСЬМО**. Обратите внимание, что сгенерированная ссылка на скачивание действительна только в течение 24 часов. Если срок действия ссылки истечет, необходимо создать новую, следуя тем же инструкциям.

     Проверьте введенную учетную запись на устройстве, на котором хотите установить Bitdefender, и нажмите соответствующую кнопку загрузки.
4. Подождите окончания загрузки, затем запустите программу установки.

6.2.3. Продлить подписку

Если вы не выберете автоматическое продления Bitdefender подписки, вы можете вручную продлить ее, выполнив следующие действия:

1. Войдите в ваш Bitdefender Central.
2. Выберите панель **Мои подписки**.
3. Выбрать нужную карточку подписки.
4. Нажмите **ОБНОВИТЬ** чтобы продолжить.

В веб-браузере откроется веб-страница, на которой можно продлитьBitdefender.

6.2.4. Активировать подписку

Подписка может быть активирована в процессе установки, используя вашу учетную запись Bitdefender. Вместе с запуском процесса активации начнется обратный отсчет срока действия.

Если вы приобрели код активации от одного из наших реселлеров или получили его в качестве подарка, то можете добавить его к Вашей подписке Bitdefender, при условии, что они предназначены для одного и того же продукта.

Активация подписки с помощью кода активации:

1. Войдите в ваш Bitdefender Central.
2. Выберите панель **Мои подписки**.
3. Нажмите кнопку**АКТИВИРОВАТЬ КОД**, затем введите код в соответствующем поле.
4. Нажмите кнопку **Активировать**, чтобы продолжить.

Подписка активирована. Перейдите на панель **Мои устройства** и выберите **УСТАНОВИТЬ ЗАЩИТУ** чтобы установить продукт на одно из ваших устройств.

6.3. Мои устройства

Область **Мои устройства** в вашем Bitdefender Central дает возможность установить, управлять и принимать удаленные действия в Bitdefender на любом устройстве, при условии, что оно включено и подключено к Интернету. Карточки устройства отображают имя устройства, состояние защиты и риски безопасности, влияющие на защиту устройств.

для просмотра списка устройств, отсортированных в соответствии с их статусом или пользователями, щелкните стрелку раскрывающегося списка в правом верхнем углу экрана.

Чтобы легко определять ваши устройства, вы можете настроить имя устройства:

1. Войдите в ваш Bitdefender Central.
2. Выберите **Мои устройства** на панели справа.

3. Нажмите на желаемую карточку устройства, затем значок ⋮ в правом верхнем углу экрана.
4. Выберите **Настройки**.
5. Введите новое имя в поле **Имя устройства**, затем нажмите **Сохранить**.

Вы можете создать и назначить владельца для каждого из ваших устройств для лучшего управления:

1. Войдите в ваш Bitdefender Central.
2. Выберите **Мои устройства** на панели справа.
3. Нажмите на желаемую карточку устройства, затем значок ⋮ в правом верхнем углу экрана.
4. Выберите **Профиль**.
5. Нажмите **Добавить владельца** , затем заполните соответствующие поля. Настройте профиль, добавив фотографию и выбрав дату рождения.
6. Нажмите **ДОБАВИТЬ** чтобы сохранить профиль.
7. Выберите нужного владельца из списка **Владелец устройства**, затем нажмите кнопку **НАЗНАЧИТЬ**.

Для удаленного обновления Bitdefender на устройстве Windows:

1. Войдите в ваш Bitdefender Central.
2. Выберите **Мои устройства** на панели справа.
3. Нажмите на желаемую карточку устройства, затем значок ⋮ в правом верхнем углу экрана.
4. Выберите **Обновление**.

Для других возможностей удаленного управления и информации о вашем Bitdefender на конкретном устройстве, выберите нужную карточку устройства.

После того, как вы нажмете на карточку устройства, будут доступны следующие вкладки:

- **Панель инструментов**. В этом окне можно просмотреть подробную информацию о выбранном устройстве, проверить его состояние

защиты, а также состояние VPN Bitdefender и и количество заблокированных угроз в течение последних семи дней. Состояние защиты может быть зеленым, если на устройстве нет проблем, связанных с устройством; желтым, когда устройству требуется Ваше внимание; красным, когда устройство подвержено риску. При возникновении проблем, повреждающих устройство, нажмите стрелку раскрывающегося списка в верхней области состояния, для получения более подробной информации. Здесь можно вручную исправить проблемы, влияющие на безопасность устройств.

- **Защита**. Из этого окна вы можете удаленно запустить быстрое сканирование или системное сканирование на ваших устройствах. Нажмите кнопку **СКАНИРОВАТЬ**, чтобы начать процесс. Вы также можете проверить, когда на устройствах выполнялось последнее сканирование и просмотреть отчет последней проверки с наиболее важной информацией.Для получения более подробной информации об этих двух процессов сканирования, пожалуйста, обратитесь «*Запуск проверки системы*» (p. 84) и «*Запуск быстрого сканирования*» (p. 84).
- **Уязвимости**. Чтобы проверить устройство на наличие уязвимостей, например отсутствующие обновления Windows, устаревшие приложения или слабые пароли нажмите кнопку **СКАНИРОВАТЬ** на вкладке Уязвимость. Уязвимости не могут быть устранены удаленно. В случае, если обнаружена уязвимость, необходимо запустить новую проверку на устройстве, а затем выполнить Рекомендуемые действия. Нажмите **Дополнительная информация** чтобы получить доступ к подробному отчету о найденных проблемах. Для получения более подробной информации об этой функции, пожалуйста, обратитесь к «*Уязвимости*» (p. 105).

6.4. Моя учетная запись

В области **Моя учетная запись** у вас есть возможность персонализировать свой профиль, изменить пароль, связанный с вашей учетной записью, управлять сеансами входа в систему и справочными сообщениями Bitdefender Central.

Как только вы нажмете значок в верхней правой части экрана и выберите **Моя учетная запись**, у вас появятся следующие вкладки:

- **Профиль** - здесь вы можете добавлять и редактировать информацию об учетной записи.

- **Изменить пароль** - здесь Вы можете изменить пароль, связанный с Вашей учетной записью.
- **Управление сеансом** - здесь Вы можете просматривать и управлять последними неактивными и активными сеансами входа в систему, запущенными на устройствах, связанных с Вашей учетной записью.
- **Настройки** - здесь можно включать и отключать справочные сообщения Bitdefender Central и включить/отключить уведомления о сделанных снимках.

6.5. Уведомления

Чтобы помочь Вам узнать о том, что происходит на устройствах, связанных с Вашей учетной записью, значок 🔔 находится на иконке "рука" Как только Вы нажмете на него, Вы увидите изображение, содержащее информацию о деятельности продуктов Bitdefender, установленных на Ваших устройствах.

7. ПОДДЕРЖКА BITDEFENDER В ОБНОВЛЕННОМ СОСТОЯНИИ

Каждый день появляются и обнаруживаются новые угрозы. Поэтому очень важно постоянно обновлять Bitdefender и поддерживать базу данных угроз в актуальном состоянии.

Если вы подключаетесь к Интернету через широкополосное соединения или DSL, Bitdefender берет на себя решение вопросов безопасности самостоятельно. По умолчанию, он проверяет наличие обновлений при запуске компьютера и каждый **час** в дальнейшем. В случае обнаружения обновлений, они будут автоматически загружены и установлены 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. 70).
- Если вы подключаетесь к Интернету по телефонной линии, лучше всего регулярно обновлять Bitdefender по запросу. Для получения более подробной информации, обратитесь к *«Выполнение обновления»* (p. 41).

7.1. Проверьте, установлены ли последние обновления Bitdefender

Чтобы проверить время последнего обновления вашего Bitdefender:

1. Нажмите **Уведомления** в меню навигации интерфейсBitdefender.

2. На вкладке **ВСЕ**, выберите уведомления относительно последнего обновления.

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.

7.2. Выполнение обновления

Для выполнения обновления требуется подключение к Интернету.

Чтобы приступить к обновлению, нажмите правой кнопкой мыши на Bitdefender значок в области уведомлений и выберите **Обновить сейчас**.

Функция 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 параметров обновления.

> **Важно**
> Возможно, потребуется перезагрузить компьютер после завершения обновления. Рекомендуется сделать это сразу.

Вы также можете выполнить обновления устройств удаленно, при условии, что они включены и подключены к сети Интернет.

Для удаленного обновления Bitdefender на устройстве Windows:

1. Войдите в ваш Bitdefender Central.
2. Выберите **Мои устройства** на панели справа.
3. Нажмите на желаемую карточку устройства, затем значок в правом верхнем углу экрана.
4. Выберите **Обновление**.

7.3. Включение и отключение автоматического обновления

Чтобы включить или выключить автоматическое обновление:

1. Нажмите **Настройки** в меню навигации интерфейс Bitdefender.

2. Выберите вкладку **Update**.
3. Включите или выключите соответствующий переключатель.
4. Появится окно предупреждения. Необходимо подтвердить выбор. Для этого в меню следует выбрать период, на который требуется отключить автообнолвение. Вы можете отключить автоматическое обновление на 5, 15 или 30 минут, на час, навсегда или до следующей перезагрузки системы.

Предупреждение
Это критическая проблема безопасности. Рекомендуется отключать автоматическое обновление на как можно меньший промежуток времени. В случае, если автоматическое обновление Bitdefender отключено, вы не будете защищены от самых последних угроз.

7.4. 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.

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

Чтобы настроить параметры обновления:

1. Нажмите **Настройки** в меню навигации интерфейс Bitdefender.
2. Выберите вкладку **Update** и измените настройки в соответствии с вашими предпочтениями.

Частота обновлений

Bitdefender настроен для проверки обновлений каждый час. Чтобы изменить частоту обновлений, перетащите ползунок по шкале, чтобы установить желаемый период времени, когда обновление должно произойти.

Обновить правила обработки

Если доступно обновление, Bitdefender автоматически загружает и внедряет его без уведомления. Отключите параметр **Тихое обновление**,

если хотите получать уведомления о каждом новом доступном обновлении.

Для завершения установки некоторых обновлений требуется перезагрузка.

По умолчанию если обновление требует перезагрузку, Bitdefender продолжит работу со старыми файлами до тех пор, пока пользователь не перезагрузит компьютер. Это предотвращает вмешательство процесса обновления Bitdefender в работу пользователя.

Если вы хотите получать уведомления о том,что обновлению требуется перезагрузка, включите **Перезапуск уведомлений**.

7.5. Постоянные обновления

Чтобы убедиться, что Вы используете последнюю версию, Ваш Bitdefender автоматически проверяет наличие обновлений продукта. Эти обновления могут привести к новым возможностям и улучшениям, устранить проблемы с продуктом или автоматически обновить новую версию. Когда новая версия Bitdefender поставляется через обновление, настраиваемые параметры сохраняются, а процедура удаления и переустановки пропускается.

Эти обновления требуют перезагрузки системы, чтобы начать установку новых файлов. Когда обновление продукта будет завершено, всплывающее окно сообщит Вам о перезапуске системы. Если Вы пропустите это уведомление, Вы можете нажать кнопку **ПЕРЕЗАПУСТИТЬ СЕЙЧАС** в окне Уведомления, где упоминается самое последнее обновление, или вручную перезапустить систему.

Примечание

Обновления, включая новые функции и усовершенствования, будут доставлены только пользователям, у которых установлен Bitdefender 2018.

СОВЕТЫ

8. УСТАНОВКА

8.1. Как установить Bitdefender на второй компьютер?

Если подписка, которую вы приобрели охватывает более чем один компьютер, вы можете использовать свою учетную запись Bitdefender для регистрации на втором компьютере.

Установить Bitdefender на второй компьютер:

1. Нажмите на **Установить на другом устройстве** в нижнем левом углу интерфейса Bitdefender.

   Вы будете перенаправлены на веб-страницу учетной записи Bitdefender. Убедитесь, что вы вошли с вашими учетными данными.

2. В появившемся окне нажмите **Отправить ссылку для скачивания**.

3. Введите адрес электронной почты в соответствующем поле и нажмите **ОТПРАВИТЬ ПИСЬМО**. Обратите внимание, что сгенерированная ссылка на скачивание действительна только в течение 24 часов. Если срок действия ссылки истечет, необходимо создать новую, следуя тем же инструкциям.

   Проверьте введенную учетную запись на устройстве, на котором хотите установить Bitdefender, и нажмите соответствующую кнопку загрузки.

4. Запустите Bitdefender продукт, который вы скачали.

Новое устройство, на котором вы установили Bitdefender появится на панели оповещения Bitdefender Central.

8.2. Как переустановить Bitdefender?

Типичные ситуации, в которых может потребоваться переустановка Bitdefender:

- вы переустановили операционную систему.
- Вы хотите исправить проблемы, которые могут привести к замедлению и сбоям.

- ваш продукт Bitdefender не запускается или не работает должным образом.

В случае, если одна из упомянутых ситуаций - Ваша ситуация, выполните следующие действия:

- В **Windows 7**:
  1. Нажмите **Пуск** и перейдите в **Все программы**.
  2. Найдите из списка **Bitdefender Antivirus Plus** и выберите **Удалить**.
  3. Нажмите **ПЕРЕУСТАНОВИТЬ** в появившемся окне.
  4. Для завершения процесса необходимо перезагрузить компьютер.
- В **Windows 8 и Windows 8.1**:
  1. На стартовом экране Windows найдите **Панель управления** (например, можно начать ввод "Панель управления" непосредственно на начальном экране), а затем щелкните его значок.
  2. Нажмите **Удалить программу** или **Программы и компоненты**.
  3. Найдите из списка **Bitdefender Antivirus Plus** и выберите **Удалить**.
  4. Нажмите **ПЕРЕУСТАНОВИТЬ** в появившемся окне.
  5. Для завершения процесса необходимо перезагрузить компьютер.
- В **Windows 10**:
  1. Нажмите **Пуск**, выберите Настройки.
  2. Нажмите иконку **Система** в области Настройки, затем выберите **Программы & компоненты**.
  3. Найдите из списка **Bitdefender Antivirus Plus** и выберите **Удалить**.
  4. Нажмите **Удалить** снова, чтобы подтвердить выбор.
  5. Щелкните **УДАЛИТЬ**.
  6. Для завершения процесса необходимо перезагрузить компьютер.

Примечание

Следуя этой процедуре переустановки, настраиваемые параметры сохраняются и доступны в новом установленном продукте. Другие настройки могут быть возвращены к их конфигурации по умолчанию.

8.3. На каком веб-сайте можно загрузить Bitdefender?

Можно установить Bitdefender с установочного диска или с помощью веб-установщика, который можно загрузить на компьютер с платформы Bitdefender Central.

Примечание
Перед установкой необходимо удалить любые антивирусные программы, установленные на вашем компьютере. Одновременное использование нескольких решений безопасности на компьютере приводит к нестабильности системы.

Чтобы установить Bitdefender из Bitdefender Central:

1. Войдите в ваш Bitdefender Central.
2. Выберите панель **Мои устройства**, затем нажмите **УСТАНОВИТЬ ЗАЩИТУ**.
3. Выберите одну из двух доступных опций:
   - **Защитить это устройство**

     Выберите этот параметр и сохраните установочный файл.
   - **Защитить другие устройства**

     Выберите этот параметр и нажмите кнопку **ОТПРАВИТЬ ССЫЛКУ ДЛЯ ЗАГРУЗКИ**. Введите адрес электронной почты в соответствующем поле и нажмите **ОТПРАВИТЬ ПИСЬМО**. Обратите внимание, что сгенерированная ссылка на скачивание действительна только в течение 24 часов. Если срок действия ссылки истечет, необходимо создать новую, следуя тем же инструкциям.

     Проверьте введенную учетную запись на устройстве, на котором хотите установить Bitdefender, и нажмите соответствующую кнопку загрузки.
4. Запустите Bitdefender продукт, который вы скачали.

8.4. Как изменить язык продукта Bitdefender?

Если вы хотите использовать Bitdefender на другом языке, вам придется переустановить продукт с выбранным языком.

Чтобы пользоваться Bitdefender на другом языке:

1. Удалите Bitdefender, выполнив следующие действия:
   - В **Windows 7**:
     a. Нажмите **Пуск**, перейдите в раздел **Панель управления** и дважды щелкните мышью по элементу **Программы и функции**.
     b. Найдите из списка **Bitdefender Antivirus Plus** и выберите **Удалить**.
     c. Нажмите кнопку **УДАЛИТЬ** в появившемся окне.
     d. Дождитесь завершения процесса удаления, после чего выполните перезагрузку системы.
   - В **Windows 8 и Windows 8.1**:
     a. На стартовом экране Windows найдите **Панель управления** (например, можно начать ввод "Панель управления" непосредственно на начальном экране), а затем щелкните его значок.
     b. Нажмите **Удалить программу** или **Программы и компоненты**.
     c. Найдите из списка **Bitdefender Antivirus Plus** и выберите **Удалить**.
     d. Нажмите кнопку **УДАЛИТЬ** в появившемся окне.
     e. Дождитесь завершения процесса удаления, после чего выполните перезагрузку системы.
   - В **Windows 10**:
     a. Нажмите **Пуск**, выберите Настройки.
     b. Нажмите иконку **Система** в области Настройки, затем выберите **Установленные приложения**.
     c. Найдите из списка **Bitdefender Antivirus Plus** и выберите **Удалить**.
     d. Нажмите **Удалить** снова, чтобы подтвердить выбор.
     e. Нажмите кнопку **УДАЛИТЬ** в появившемся окне.

f. Дождитесь завершения процесса удаления, после чего выполните перезагрузку системы.

2. Изменение языка в Bitdefender Central:
   a. Войдите в ваш Bitdefender Central.
   b. Нажмите иконку в верхней правой части экрана.
   c. Нажмите **Моя учетная запись** в слайд-меню.
   d. Выберите вкладку **Профиль**.
   e. Выберите язык из раскрывающееся окна списка **Язык**, а затем нажмите кнопку **СОХРАНИТЬ**.
3. Скачать установочный файл:
   a. Выберите панель **Мои устройства**, затем нажмите **УСТАНОВИТЬ ЗАЩИТУ**.
   b. Выберите одну из двух доступных опций:
      - **Защитить это устройство**

        Выберите этот параметр и сохраните установочный файл.
      - **Защитить другие устройства**

        Выберите этот параметр и нажмите кнопку **ОТПРАВИТЬ ССЫЛКУ ДЛЯ ЗАГРУЗКИ**. Введите адрес электронной почты в соответствующем поле и нажмите **ОТПРАВИТЬ ПИСЬМО**. Обратите внимание, что сгенерированная ссылка на скачивание действительна только в течение 24 часов. Если срок действия ссылки истечет, необходимо создать новую, следуя тем же инструкциям.

        Проверьте введенную учетную запись на устройстве, на котором хотите установить Bitdefender, и нажмите соответствующую кнопку загрузки.
4. Запустите Bitdefender продукт, который вы скачали.

Примечание
Эта процедура переустановки навсегда удалит настроенные параметры.

8.5. Как пользоваться лицензионным ключом для Bitdefender после обновления Windows?

Эта ситуация появляется при обновлении операционной системы и в случае, если вы хотите дальше использовать лицензионный ключ для Bitdefender.

Если вы используете предыдущую версию Bitdefender, вы можете бесплатно обновить ее до последней версии Bitdefender, как показано ниже:

- От предыдущей версии Антивируса Bitdefender до последней доступной версии Антивируса Bitdefender.
- От предыдущей версии Bitdefender Интернет-безопасности до последней версии Bitdefender Интернет-безопасности.
- От предыдущей версии Bitdefender Интернет-безопасности до последней версии Bitdefender Интернет-безопасности.

Существует 2 варианта развития событий:

- Вы обновили операционную систему через службу Windows Update и обнаружили, что Bitdefender больше не работает.

  В этом случае необходимо переустановить продукт, выполнив следующие действия:

  - В **Windows 7**:

    1. Нажмите **Пуск**, перейдите в раздел **Панель управления** и дважды щелкните мышью по элементу **Программы и функции**.
    2. Найдите из списка **Bitdefender Antivirus Plus** и выберите **Удалить**.
    3. Нажмите **ПЕРЕУСТАНОВИТЬ** в появившемся окне.
    4. Дождитесь завершения процесса удаления, после чего выполните перезагрузку системы.

       Откройте интерфейс Вашего нового установленного продукта Bitdefender, чтобы получить доступ к его функциям.

  - В **Windows 8 и Windows 8.1**:

    1. На стартовом экране Windows найдите **Панель управления** (например, можно начать ввод "Панель управления"

непосредственно на начальном экране), а затем щелкните его значок.

2. Нажмите **Удалить программу** или **Программы и компоненты**.
3. Найдите из списка **Bitdefender Antivirus Plus** и выберите **Удалить**.
4. Нажмите **ПЕРЕУСТАНОВИТЬ** в появившемся окне.
5. Дождитесь завершения процесса удаления, после чего выполните перезагрузку системы.

   Откройте интерфейс Вашего нового установленного продукта Bitdefender, чтобы получить доступ к его функциям.

- В **Windows 10**:

1. Нажмите **Пуск**, выберите Настройки.
2. Нажмите иконку **Система** в области Настройки, затем выберите **Установленные приложения**.
3. Найдите из списка **Bitdefender Antivirus Plus** и выберите **Удалить**.
4. Нажмите **Удалить** снова, чтобы подтвердить выбор.
5. Нажмите **ПЕРЕУСТАНОВИТЬ** в появившемся окне.
6. Дождитесь завершения процесса удаления, после чего выполните перезагрузку системы.

   Откройте интерфейс Вашего нового установленного продукта Bitdefender, чтобы получить доступ к его функциям.

Примечание

Следуя этой процедуре переустановки, настраиваемые параметры сохраняются и доступны в новом установленном продукте. Другие настройки могут быть возвращены к их конфигурации по умолчанию.

- Вы обновили систему и хотите дальше использовать систему защиты Bitdefender. Таким образом, вам необходимо переустановить продукт, используя последнюю версию.

  Чтобы решить эту ситуацию:

1. Скачать установочный файл:
   a. Войдите в ваш Bitdefender Central.

b. Выберите панель **Мои устройства**, затем нажмите **УСТАНОВИТЬ ЗАЩИТУ**.

c. Выберите одну из двух доступных опций:

- **Защитить это устройство**

  Выберите этот параметр и сохраните установочный файл.

- **Защитить другие устройства**

  Выберите этот параметр и нажмите кнопку **ОТПРАВИТЬ ССЫЛКУ ДЛЯ ЗАГРУЗКИ**. Введите адрес электронной почты в соответствующем поле и нажмите **ОТПРАВИТЬ ПИСЬМО**. Обратите внимание, что сгенерированная ссылка на скачивание действительна только в течение 24 часов. Если срок действия ссылки истечет, необходимо создать новую, следуя тем же инструкциям.

  Проверьте введенную учетную запись на устройстве, на котором хотите установить Bitdefender, и нажмите соответствующую кнопку загрузки.

2. Запустите Bitdefender продукт, который вы скачали.

Для получения дополнительной информации о процессе установки Bitdefender, пожалуйста, обратитесь к «*Установка продукта Bitdefender*» (p. 5).

8.6. Как перейти к последней версии Bitdefender?

Теперь обновление до новейшей версии возможно без процедуры удаления и переустановки вручную. Более точно, новый продукт, включая новые функции и основные улучшения продукта поставляется через обновление продукта и, если у вас уже есть активная подписка Bitdefender, продукт автоматически активируется.

Если вы используете версию 2018 года, можно обновить продукт до новейшей версии, выполнив следующие действия:

1. Нажмите **ПЕРЕЗАПУСТИТЬ СЕЙЧАС** в уведомлении, которое Вы получите с информацией об обновлении. Если Вы пропустите его, откройте окно Уведомления, наведите указатель на самое последнее обновление, а затем нажмите кнопку **ПЕРЕЗАПУСТИТЬ СЕЙЧАС**. Подождите, пока компьютер перезагрузится.

Появится окно **Новинки** с информацией о новых и улучшенных функциях.

2. Нажмите ссылку **Подробнее** и Вы будете перенаправлены на нашу специальную страницу с более подробной информацией и полезными статьями.
3. Закройте окно **Новинки** для доступа к интерфейсу новой установленной версии.

Пользователи, которые хотят обновить бесплатно Bitdefender 2016 или более позднюю версию до последней версии Bitdefender, должны удалить свою текущую версию с панели управления, а затем загрузить последний установочный файл из Bitdefender по следующему адресу: https://www.bitdefender.com/Downloads/. Активация возможна только при наличии действительной подписки.

9. ПОДПИСКИ

9.1. Как активировать подписку на Bitdefender, используя лицензионный ключ?

Если у вас есть действующий лицензионный ключ и Вы хотите использовать его для активации подписки на Bitdefender Antivirus Plus, есть два возможных варианта:

- Вы обновили предыдущую версию Bitdefender на новую:
  1. После завершения обновления до Bitdefender Antivirus Plus вам будет предложено войти в свою учетную запись Bitdefender.
  2. Нажмите **Войти**, затем введите адрес электронной почты и пароль для Вашей учетной записи Bitdefender.
  3. Нажмите **Войти** чтобы продолжить.
  4. На экране вашего аккаунта появится уведомление о том, что подписка была создана. Созданная подписка будет действительна в течение оставшихся дней на вашем лицензионном ключе и для того же количества пользователей.

     На устройствах, использующих предыдущие версии Bitdefender и зарегистрированных с помощью лицензионного ключа, необходимо активировать продукт с той же учетной записью Bitdefender.
- Bitdefender ранее не устанавливался в системе:
  1. Как только процесс установки будет завершен, вам будет предложено войти в свой аккаунт Bitdefender.
  2. Нажмите **Войти**, затем введите адрес электронной почты и пароль для Вашей учетной записи Bitdefender.
  3. Нажмите **ВОЙТИ** чтобы продолжить и затем нажмите кнопку **ЗАКОНЧИТЬ** чтобы перейти к интерфейсу Bitdefender Antivirus Plus.
  4. Нажмите **Моя учетная запись** в меню навигации интерфейса Bitdefender.
  5. Нажмите **Активировать сейчас**.

     Появится новое окно.
  6. Нажмите ссылку **Получить бесплатное обновление сейчас!**.

7. Введите лицензионный ключ в соответствующее поле и нажмите **ОБНОВИТЬ МОЙ ПРОДУКТ**. Подписка с тем же временем активности и количеством пользователей вашего лицензионного ключа связана с вашей учетной записью.

10. BITDEFENDER CENTRAL

10.1. Как войти в Bitdefender Central, используя другую учетную запись?

Вы создали новую учетную запись Bitdefender и хотите использовать ее с этого момента.

Для того, чтобы успешно использовать другую учетную запись:

1. Нажмите **Моя учетная запись** в меню навигации интерфейса Bitdefender.
2. Чтобы изменить учетную запись, связанную с компьютером, нажмите в правом верхнем углу экрана кнопку **Переключить учетную запись**.
3. Введите адрес электронной почты и пароль Вашей учетной записи в соответствующие поля, затем нажмите **ВОЙТИ**.

Примечание

Продукт Bitdefender с устройства автоматически изменяется в соответствии с подпиской, связанной с новой учетной записью Bitdefender.

Если нет доступной подписки, связанной с новой учетной записью Bitdefender, или вы хотите перенести ее из предыдущей учетной записи, вы можете связаться с Bitdefender для поддержки, как описано в разделе «*Обращение за помощью*» (p. 173).

10.2. Как отключить справочные сообщения Bitdefender Central?

Чтобы помочь понять, что полезно для каждого параметра в Bitdefender Central, на панели мониторинга отображаются сообщения справки.

Если вы хотите прекратить просмотр такого рода сообщений:

1. Войдите в ваш Bitdefender Central.
2. Нажмите иконку в верхней правой части экрана.
3. Нажмите **Моя учетная запись** в слайд-меню.
4. Щелкните на вкладке **Настройки**.
5. Отключить опцию **Включение/выключение сообщений**.

10.3. Я забыл пароль, установленный для учетной записи Bitdefender. Как сбросить его?

Существует две возможности установить новый пароль для вашей учетной записи Bitdefender:

- Из интерфейса Bitdefender:
  1. Нажмите **Моя учетная запись** в меню навигации интерфейса Bitdefender.
  2. Нажмите в правом верхнем углу экрана **Переключить учетную запись**.

     Появится новое окно.
  3. Нажмите **Забыл пароль**.
  4. Введите адрес электронной почты, используемый для создания учетной записи Bitdefender, а затем нажмите кнопку **ЗАБЫЛ ПАРОЛЬ**.
  5. Проверьте электронную почту и перейдите по указанной ссылке.

     Откроется окно Bitdefender СБРОС ПАРОЛЯ.
  6. Введите свой адрес электронной почты и новый пароль в соответствующие поля. Пароль должен быть длиной не менее 8 символов и содержать числа.
  7. Нажмите **СБРОС ПАРОЛЯ**.
- Из вашего веб-браузера:
  1. Перейти к: https://central.bitdefender.com.
  2. Нажмите **Забыл пароль**.
  3. Введите адрес вашей электронной почты, затем нажмите кнопку **ЗАБЫЛ ПАРОЛЬ**.
  4. Проверьте электронную почту учетной записи и следуйте приведенным инструкциям для установки нового пароля Вашей учетной записи Bitdefender

Чтобы получить доступ к Вашей учетной записи Bitdefender с этого момента, введите свой адрес электронной почты и новый пароль, который Вы только что установили.

10.4. Как управлять сеансами входа в систему, связанными с моей учетной записью Bitdefender?

В Bitdefender аккаунт Вы можете просмотреть последние неактивные и активные сеансы в работе системы на устройствах, запущенные на устройствах, связанных с вашей учетной записью. Кроме того, Вы можете выйти удаленно, выполнив следующие шаги:

1. Войдите в ваш Bitdefender Central.
2. Нажмите иконку в верхней правой части экрана.
3. Нажмите **Моя учетная запись** в слайд-меню.
4. Выберите вкладку **Управление сеансами**.
5. В области **Активные сеансы** выберите параметр **ВЫЙТИ** рядом с устройством, на котором Вы хотите завершить сеанс работы

11. СКАНИРОВАНИЕ С BITDEFENDER

11.1. Как выполнить сканирование файла или папки?

Самый простой способ сканирования файла или папки — щелкнуть правой кнопкой мыши объект, который требуется сканировать, указать Bitdefender и выбрать **Сканировать с Bitdefender** из меню.

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.

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.
- Сканирование общей сетевой папки перед копированием файлов на компьютер.

11.2. Как выполнить сканирование системы?

Чтобы выполнить полную проверку системы:

1. Нажмите **Защита** в меню навигации интерфейса Bitdefender.
2. В области **АНТИВИРУС** нажмите **Системное сканирование**.
3. Для завершения сканирования следуйте инструкциям мастера сканирования системы. 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 более подробной информации, обратитесь к «*Мастер антивирусного сканирования*» (p. 89).

11.3. Как составить график сканирования?

Вы можете настроить свой Bitdefender таким образом, чтобы сканирование критических мест системы начиналось до того, как Вы приступите к работе.

Чтобы запланировать сканирование:

1. Нажмите **Защита** в меню навигации интерфейса Bitdefender.
2. В области **АНТИВИРУС** нажмите **УПРАВЛЕНИЕ СКАНИРОВАНИЕМ**.
3. Выберите тип сканирования, который требуется запланировать: "Полное сканирование системы" или "Быстрое сканирование", а затем нажмите **ПАРАМЕТРЫ СКАНИРОВАНИЯ**.

   Кроме того, можно создать тип сканирования в соответствии с вашими потребностями, щелкнув **НОВАЯ ЗАДАЧА ПОЛЬЗОВАТЕЛЯ**.
4. Включить параметр **Расписание**.

   Выберите один из предложенных вариантов, чтобы установить расписание:

   - При запуске системы
   - Один раз
   - Периодически

В окне **Цели сканирования** вы можете выбрать местоположения, которые хотите сканировать Этот параметр доступен только в том случае, вы решите создать новое пользовательское сканирование.

11.4. Как создать пользовательское задание сканирования?

Если требуется сканировать определенные местоположения на компьютере или настроить параметры сканирования, настройте и запустите настраиваемую задачу сканирования.

Для создания пользовательской задачи сканирования выполните следующие действия:

1. Нажмите **Защита** в меню навигации интерфейса Bitdefender.
2. В области **АНТИВИРУС** нажмите **УПРАВЛЕНИЕ СКАНИРОВАНИЕМ**.

3. Нажмите **НОВАЯ ЗАДАЧА ПОЛЬЗОВАТЕЛЯ**. В окне **Основное** введите имя для сканирования и выберите сканируемые местоположения.
4. Если вы хотите настроить дополнительный параметры сканирования, выберите вкладку **Расширенное**.

   Настроить параметры сканирования можно легко, с помощью регулировки уровня сканирования. Перетащите ползунок по шкале, чтобы задать требуемый 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.
5. Нажмите **ОК**, чтобы сохранить изменения, и закройте окно.
6. Используйте соответствующий переключатель, если требуется задать расписание для задачи сканирования.
7. Для выполнения проверки нажмите **НАЧАТЬ СКАНИРОВАНИЕ** и следуйте инструкциям мастера сканирования. На этапе завершения сканирования отобразится сообщение, предлагающее выбрать действия, которые будут выполняться для обнаруженных файлов (если есть).
8. При желании можно быстро перезапустить предыдущее пользовательское сканирование, щелкнув соответствующую запись в доступном списке.

11.5. Порядок исключения папки из сканирования.

Bitdefender допускает исключение из сканирования определенных файлов, папок и расширений 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.

Чтобы добавить папку в "Список исключений":

1. Нажмите **Защита** в меню навигации интерфейса Bitdefender.
2. На панели **АНТИВИРУС** нажмите **Настройки**.
3. Выберите вкладку **Исключения**.
4. Выберите в меню **Список файлов и папок, исключенных из сканирования** и затем нажмите **Добавить**.
5. Нажмите **ОБЗОР**, выберите папку, которую хотите исключить из сканирования, затем выберите тип сканирования, из которого ее необходимо исключить.
6. Нажмите **ДОБАВИТЬ**, чтобы сохранить изменения и закрыть окно.

11.6. Что делать в случае обнаружения Bitdefender вируса в заведомо надежном файле?

Это может произойти, когда Bitdefender ошибочно помечает легитимные файлы как угрозы (ложноположительное обнаружение). Чтобы исправить эту ошибку, добавьте файл в "Область исключений" Bitdefender:

1. Отключение антивирусной защиты Bitdefender в режиме реального времени:
   a. Нажмите **Защита** в меню навигации интерфейса Bitdefender.
   b. На панели **АНТИВИРУС** нажмите **Настройки**.
   c. В окне **Защита** отключите **Защита Bitdefender**.

      Появится окно предупреждения. Необходимо подтвердить выбор. Для этого в меню следует выбрать период, на который требуется отключить защиту в режиме реального времени. Вы можете отключить защиту в реальном времени на 5, 15 или 30 минут, на час, навсегда или до следующей перезагрузки системы.
2. Отображать скрытые объекты в Windows. Чтобы узнать, как это сделать, обратитесь к *«Как отобразить скрытые объекты в Windows?»* (p. 72).

3. Восстановление файла из области карантина:
   a. Нажмите **Защита** в меню навигации интерфейса Bitdefender.
   b. В области **АНТИВИРУС** нажмите **карантина**.
   c. Выберите файл и затем нажмите **ВОССТАНОВИТЬ**.
4. Добавить файл в "Список исключений". Чтобы узнать, как это сделать, обратитесь к *«Порядок исключения папки из сканирования.»* (p. 61).
5. Включить антивирусную защиту Bitdefender в режиме реального времени.
6. Свяжитесь с нашими представителями службы поддержки, чтобы мы могли удалить обнаруженное обновление сведений об угрозе. Чтобы узнать, как это сделать, обратитесь к *«Обращение за помощью»* (p. 173).

11.7. Как проверить, какие угрозыобнаружил Bitdefender?

Каждый раз, при выполнении сканирования, ведется журнал сканирования и Bitdefender ведет запись обнаруженных проблем.

Журнал сканирования содержит подробные сведения о регистрируемом процессе сканирования, такие как параметры сканирования, цель сканирования, найденные угрозы и действия, предпринятые в отношении этих угроз.

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

Чтобы позже посмотреть журналы сканирования или любые другие обнаруженные инфицированные объекты:

1. Нажмите **Уведомления** в меню навигации интерфейсBitdefender.
2. На вкладке **ВСЕ**, выберите уведомления относительно последнего сканирования.

   Здесь можно просмотреть все события сканирования на наличие угорз, включая угрозы, обнаруженные при доступе, сканировании по инициативе пользователя, а также изменения статуса автоматического сканирования.

3. В списке уведомлений вы можете проверить какие сканирования были выполнены в последнее время. Нажмите на уведомление, чтобы просмотреть сведения о нем.
4. Чтобы открыть журнал сканирования, нажмите **View log**.

12. ЗАЩИТА ДАННЫХ

12.1. Как убедиться, что моя транзакция в Интернете безопасна?

Чтобы убедиться, что ваши онлайн-операции остаются приватными, вы можете использовать браузер, предоставленный Bitdefender для защиты ваших транзакций и приложений для домашнего банкинга.

Bitdefender Safepay™ является защищенным браузером, предназначенным для защиты информации о вашей кредитной карте, номере счета или любых других конфиденциальных данных, которые вы можете ввести при доступе к различным онлайн-локациям.

Чтобы сохранить безопасность и конфиденциальность ваших он-лайн действий:

1. Нажмите **Приватность** в меню навигации интерфейса Bitdefender.
2. На панели **Safepay** нажмите **Открыть Safepay**.
3. Нажмите кнопку для доступа к **Виртуальной клавиатуре**.

   Используйте **Виртуальную клавиатуру** при вводе конфиденциальной информации, например паролей.

12.2. Как удалить файл навсегда с Bitdefender?

Если вы хотите навсегда удалить файл из системы, необходимо удалить данные физически с жесткого диска.

Файловый шредер Bitdefender поможет вам быстро уничтожить файлы или папки с вашего компьютера с помощью контекстного меню Windows выполнив следующие действия:

1. Щелкните правой кнопкой мыши по файлу или папке, которые требуется удалить навсегда в Bitdefender, и выберите **Файловый шредер**.
2. Нажмите **УДАЛИТЬ НАВСЕГДА** и подтвердите, что Вы хотите продолжить процесс.

   Дождитесь завершения процедуры уничтожения файлов Bitdefender.

3. Отобразятся результаты. Нажмите **ЗАВЕРШИТЬ** для выхода из мастера

12.3. Как можно вручную восстановить зашифрованные файлы при сбое процесса восстановления?

Если зашифрованные файлы не могут быть восстановлены автоматически, их можно восстановить вручную, выполнив следующие действия:

1. Нажмите **Уведомления** в меню навигации интерфейсBitdefender.
2. На вкладке **Все** выберите уведомление о последнем обнаруженном поведении программы-вымогателя, затем нажмите **Зашифрованные файлы**.
3. Отобразится список зашифрованных файлов.

   Нажмите **ВОССТАНОВИТЬ ФАЙЛЫ**, чтобы продолжить.
4. В случае сбоя процесса восстановления или его части необходимо выбрать место, в котором следует сохранить расшифрованные файлы. Нажмите **ВОССТАНОВИТЬ РАСПОЛОЖЕНИЕ**, затем выберите расположение на вашем компьютере.
5. Появится окно подтверждения.

   Нажмите **ЗАВЕРШИТЬ** для завершения процесса восстановления.

Файлы со следующими расширениями могут быть восстановлены в случае их шифрования:

.3g2; .3gp; .7z; .ai; .aif; .arj; .asp; .aspx; .avi; .bat; .bin; .bmp; .c; .cda; .cgi; .class; .com; .cpp; .cs; .css; .csv; .dat; .db; .dbf; .deb;.doc; .docx; .gif; .gz; .h264; .h; .flv; .htm; .html;.ico; .jar; .java; .jpeg; .jpg;.js; .jsp; .key; .m4v; .mdb; .mid; .midi; .mkv; .mp3; .mp4; .mov; .mpg; .mpeg; .ods; .odp;.odt; .ogg; .pdf; .pkg; .php; .pl; .png; .pps; .ppt; .pptx; .ps; .psd; .py; .rar; .rm; .rtf; .sav; .sql; .sh; .svg; .swift; .swf; .tar; .tex; .tif; .tiff; .txt; .xlr; .xls; .xlsx; .xml; .wmv; .vb; .vob; .wav; .wks; .wma; .wpl; .wps; .wpd; .wsf; .z; .zip;

13. ПОЛЕЗНАЯ ИНФОРМАЦИЯ

13.1. Как проверить решение безопасности?

Для того, чтобы проверить работоспособность продукта Bitdefender, мы рекомендуем воспользоваться инструментом "Eicar test".

Тест Eicar позволяет проверить антивирусную защиту с помощью безопасного файла, разработанного для этой цели.

Чтобы проверить решение безопасности:

1. Загрузите тестовый файл с официального веб-сайта организации EICAR http://www.eicar.org/.
2. Нажмите вкладку **Антивирусный тест-файл**.
3. Нажмите **Загрузить** в левой части меню.
4. Нажмите на тест-файл **eicar.com** в **Зоне загрузки, используя стандартный протокол http**.
5. Вы получите уведомление о том, что страница, к которой вы пытаетесь получить доступ, содержит файл EICAR-Test (не угроза).

   Если вы нажмете **Я осознаю риски, войти в любом случае**, начнется загрузка теста и появится всплывающее окно Bitdefender, информирующее об обнаружении угрозы.

   Нажмите **Подробнее**, чтобы посмотреть более подробную информацию об этом действии.

Если вы не получили оповещения Bitdefender, рекомендуем связаться с Bitdefender для поддержки, как описано в разделе «*Обращение за помощью*» (p. 173).

13.2. Как удалить Bitdefender?

Если вы хотите удалить Bitdefender Antivirus Plus:

- В **Windows 7**:
  1. Нажмите **Пуск**, перейдите в раздел **Панель управления** и дважды щелкните мышью по элементу **Программы и функции**.
  2. Найдите из списка **Bitdefender Antivirus Plus** и выберите **Удалить**.
  3. Нажмите кнопку **УДАЛИТЬ** в появившемся окне.

4. Дождитесь завершения процесса удаления, после чего выполните перезагрузку системы.

- В **Windows 8 и Windows 8.1**:

1. На стартовом экране Windows найдите **Панель управления** (например, можно начать ввод "Панель управления" непосредственно на начальном экране), а затем щелкните его значок.
2. Нажмите **Удалить программу** или **Программы и компоненты**.
3. Найдите из списка **Bitdefender Antivirus Plus** и выберите **Удалить**.
4. Нажмите кнопку **УДАЛИТЬ** в появившемся окне.
5. Дождитесь завершения процесса удаления, после чего выполните перезагрузку системы.

- В **Windows 10**:

1. Нажмите **Пуск**, выберите Настройки.
2. Нажмите иконку **Система** в области Настройки, затем выберите **Установленные приложения**.
3. Найдите из списка **Bitdefender Antivirus Plus** и выберите **Удалить**.
4. Нажмите **Удалить** снова, чтобы подтвердить выбор.
5. Нажмите кнопку **УДАЛИТЬ** в появившемся окне.
6. Дождитесь завершения процесса удаления, после чего выполните перезагрузку системы.

Примечание
Эта процедура переустановки навсегда удалит настроенные параметры.

13.3. Как удалить BitdefenderVPN?

Процедура удаления Bitdefender VPN аналогична процедуре удаления других программ с Вашего компьютера:

- В **Windows 7**:

1. Нажмите **Пуск**, перейдите в раздел **Панель управления** и дважды щелкните мышью по элементу **Программы и функции**.
2. Найдите **BitdefenderVPN** и выберите **Удалить**.

Дождитесь завершения процесса удаления.

- В **Windows 8 и Windows 8.1**:
  1. На стартовом экране Windows найдите **Панель управления** (например, можно начать ввод "Панель управления" непосредственно на начальном экране), а затем щелкните его значок.
  2. Нажмите **Удалить программу** или **Программы и компоненты**.
  3. Найдите **BitdefenderVPN** и выберите **Удалить**.

     Дождитесь завершения процесса удаления.
- В **Windows 10**:
  1. Нажмите **Пуск**, выберите Настройки.
  2. Нажмите иконку **Система** в области Настройки, затем выберите **Установленные приложения**.
  3. Найдите **BitdefenderVPN** и выберите **Удалить**.
  4. Нажмите **Удалить** снова, чтобы подтвердить выбор.

     Дождитесь завершения процесса удаления.

13.4. Как автоматически выключить компьютер после завершения сканирования?

Чтобы убедиться, что ваша система не подвержена угрозам, Bitdefender предлагает к использованию несколько задач проверки. Сканирование всего компьютера может занять больше времени,в зависимости от вашей системы, аппаратной и программной конфигурации.

По этой причине Bitdefender позволяет настроить продукт на завершение работы системы сразу после завершения сканирования.

Рассмотрим этот пример: вы закончили работу за компьютером. Вы хотите, чтобы вся система проверялась на наличие угроз при помощи Bitdefender.

Это аналогично тому,как настроить Bitdefender для завершения работы системы в конце сканирования:

1. Нажмите **Защита** в меню навигации интерфейса Bitdefender.
2. В области **АНТИВИРУС** нажмите **УПРАВЛЕНИЕ СКАНИРОВАНИЕМ**.

3. В окне **Управление задачами сканирования**, нажмите **НОВАЯ ЗАДАЧА ПОЛЬЗОВАТЕЛЯ**, введите имя сканирования и выберите места для сканирования.
4. Если вы хотите настроить дополнительный параметры сканирования, выберите вкладку **Расширенное**.
5. Выберите завершение работы компьютера после завершения сканирования, если угрозы не найдены.
6. Нажмите **ОК**, чтобы сохранить изменения, и закройте окно.
7. Нажмите **НАЧАТЬ СКАНИРОВАНИЕ**, чтобы сканировать систему.

Если угрозы не найдены, компьютер завершит работу.

Если после сканирования все еще остались угрозы, вам будет предложено выбрать действия, которые следует предпринять по отношению к ним. Для получения более подробной информации, обратитесь к «*Мастер антивирусного сканирования*» (p. 89).

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

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

Чтобы настроить параметры прокси-сервера:

1. Нажмите **Настройки** в меню навигации интерфейс Bitdefender.
2. Выберите вкладку **Advanced**.
3. Включить **Прокси-сервер**.
4. Нажмите **Изменение прокси**.
5. Параметры прокси-сервера можно задать двумя способами:

- **Импортировать параметры прокси-сервера из браузера по умолчанию** — параметры прокси-сервера для текущего пользователя, извлеченные из браузера по умолчанию. Если прокси-сервер запрашивает имя пользователя и пароль, укажите их в соответствующих полях.

  Примечание
  Bitdefenderможет импортировать настройки прокси из самых популярных браузеров, включая последние версии Microsoft Edge, Internet Explorer, Mozilla Firefox и Google Chrome.

- **Пользовательские настройки прокси-сервера** — настройки прокси-сервера, которые вы можете настроить самостоятельно. Необходимо указать следующие параметры:
  - **Адрес** — введите IP-адрес прокси-сервера.
  - **Порт** — введите порт, используемый Bitdefender для подключения к прокси-серверу.
  - **Пользователь** — введите имя пользователя, распознаваемого прокси-сервером.
  - **Пароль** — введите действующий пароль указанного ранее пользователя.

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

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

13.6. Определение используемой версии Windows (32- или 64-разрядная)

Чтобы узнать о наличии 32 бит или 64 бит операционной системы:

- В **Windows 7**:
  1. Нажмите **Пуск**.
  2. Найдите элемент **Компьютер** в меню **Пуск**.
  3. Щелкните правой кнопкой мыши по **Компьютер** и выберите **Свойства**.
  4. Войдите в раздел **Система** для просмотра сведений о системе.
- В **Windows 8**:

1. Введите **Компьютер** в Стартовом окне Windows,(например, можно вводить «Компьютер» непосредственно в Стартовом окне) и затем щелкните правой кнопкой мыши по его значку.

   В **Windows 8.1**, найдите **Этот компьютер**.

2. Выберите **Свойства** в нижнем меню.
3. Посмотрите в системной области, чтобы увидеть ваш тип системы.

- В **Windows 10**:

1. Введите "Система" в поле поиска на панели задач и щелкните значок.
2. Найдите в системной области сведения о типе системы.

13.7. Как отобразить скрытые объекты в Windows?

Эти действия полезны в тех случаях, когда столкнулись с угрозой и вам нужно найти и удалить скрытые зараженные файлы.

Для отображения скрытых объектов в Windows выполните следующие действия:

1. Нажмите **Пуск** и перейдите в **Панель управления**.

   В **Windows 8 и Windows 8.1**: В стартовом окне, находится **Панель управления** (например, можно вводить "Панель управления" непосредственно в Стартовом окне) и затем нажмите на его значок.

2. Выберите **Свойства папки**.
3. Перейдите на вкладку **Просмотр**.
4. Выберите **Отображать скрытые файлы и папки**.
5. Снимите флажок **Скрывать расширение известных типов файлов**.
6. Снимите флажок **Скрывать защищенные файлы операционной системы**.
7. Нажмите **Применить**, затем нажмите **ОК**.

В **Windows 10**:

1. Введите "Показать скрытые файлы и папки" в поле поиска на панели задач и нажмите на его значок.
2. Выберите **Показать скрытые файлы, папки и диски**.

3. Снимите флажок **Скрывать расширение известных типов файлов**.
4. Снимите флажок **Скрывать защищенные файлы операционной системы**.
5. Нажмите **Применить**, затем нажмите **ОК**.

13.8. 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 Antivirus Plus автоматически распознает другое программное обеспечение безопасности и предлагает удалить его.

Если другие решения безопасности не были удалены во время исходной установки, выполните следующие действия:

- В **Windows 7**:
  1. Нажмите **Пуск**, перейдите в раздел **Панель управления** и дважды щелкните мышью по элементу **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.
- В **Windows 8 и Windows 8.1**:
  1. На стартовом экране Windows найдите **Панель управления** (например, можно начать ввод "Панель управления" непосредственно на начальном экране), а затем щелкните его значок.
  2. Нажмите **Удалить программу** или **Программы и компоненты**.
  3. Подождите несколько секунд, пока не отобразится список установленного программного обеспечения.

4. Найдите имя программы, которую следует удалить, и выберите **Удалить**.
5. Дождитесь завершения процесса удаления, после чего выполните перезагрузку системы.

- В **Windows 10**:

1. Нажмите **Пуск**, выберите Настройки.
2. Нажмите иконку **Система** в области Настройки, затем выберите **Установленные приложения**.
3. Найдите имя программы, которую следует удалить, и выберите **Удалить**.
4. Нажмите **Удалить** снова, чтобы подтвердить выбор.
5. 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.

13.9. Как перезагрузить компьютер 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 угроз, 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 угроз неактивны при работе Windows в Безопасном режиме и их можно легко удалить.

Запуск Windows в безопасном режиме:

- В **Windows 7**:

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 **ОК** для подтверждения.
6. Для запуска Windows в нормальном режиме просто перезагрузите систему.

- In **Windows 8, Windows 8.1 и Windows 10**:

1. Запустите **Конфигурация системы** в Windows одновременно нажав клавиши на клавиатуре **Windows + R**.
2. Напишите **msconfig** в открывшемся диалоговом окне **Открыть** и затем нажмите **ОК**.
3. Выберите вкладку **Загрузка**.
4. В разделе **Параметры загрузки** поставьте флажок **Безопасная загрузка**.
5. Выберите **Сеть** и затем **ОК**.
6. Выберите **ОК** в окне **Конфигурация системы**, которое информирует вас о том, что система должна быть перезапущена для того, чтобы иметь возможность внести изменения, которые вы внесли.

   Ваша система перезагрузится в безопасном режиме с доступом к сети.

Для перезагрузки в обычном режиме, переключите настройки, снова запустив **Работа системы** и снимите флажок с **Безопасная загрузка**. Нажмите **ОК** и затем нажмите **ПЕРЕЗАПУСК**. Подождите, пока будут применены новые параметры.

УПРАВЛЕНИЕ БЕЗОПАСНОСТЬЮ

14. АНТИВИРУСНАЯ ЗАЩИТА

Bitdefender защищает ваш компьютер от всех типов угроз (вирусов, троянов, программ-шпионов, руткитов и т. д.). Предложения по защите Bitdefender делятся на две категории:

- Проверка при доступе — предотвращает попадание новых угроз в вашу систему. К примеру, Bitdefender будет сканировать документ Word на наличие известных угроз при его открытии и сообщение электронной почты при его получении.

  Сканирование при доступе обеспечивает постоянную защиту от угроз и является важным компонентом любой программы компьютерной безопасности.

  Важно
  Чтобы предотвратить заражение компьютера, необходимо включить функцию **Сканирование при доступе**.

- Сканирование по требованию — обнаруживает и удаляет угрозы, уже находящиеся в системе. Это классический тип проверки по желанию пользователя: вы выбираете диск, папку или файл для проверки Bitdefender, а Bitdefender проверяет их по вашему требованию.

Bitdefender автоматически сканирует все съемные носители, подключенные к компьютеру, для проверки их безопасности. Для получения более подробной информации, обратитесь к «*Автоматическое сканирование съемных носителей* » (p. 93).

Если не требуется сканирование определенных файлов или их типов, опытные пользователи могут настроить исключения сканирования. Для получения более подробной информации, обратитесь к «*Настройка исключений для сканирования*» (p. 96).

В случае обнаружения угроз 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 более подробной информации, обратитесь к «*Управление файлами в карантине*» (p. 98).

В случае угрозы см. информацию в «*Удаление угроз из системы*» (p. 161). Чтобы помочь вам очистить компьютер от угроз, которые невозможно

удалить из операционной системы Windows, Bitdefender представляет режим«*Bitdefender Режим Восстановления (Rescue Environment в Windows 10)*» (p. 161). Это доверенная среда, предназначена для удаления угроз, позволяет загружать компьютер без запуска Windows. Если компьютер запущен в Режиме Спасения (Rescue Environment в Windows 10), угрозы, находящиеся в системе Windows, становятся неактивны, что упрощает их удаление.

14.1. Резидентное сканирование (защита в реальном времени)

Bitdefender обеспечивает непрерывную защиту в режиме реального времени от широкого спектра угроз, сканируя все доступные файлы и сообщения электронной почты.

14.1.1. Включение или отключение защиты в реальном времени

Для включения или выключения защиты от угроз в режиме реального времени:

1. Нажмите **Защита** в меню навигации интерфейса Bitdefender.
2. На панели **АНТИВИРУС** нажмите **Настройки**.
3. В окне **Защита** включите или отключите **Защиту Bitdefender**.
4. Если вы захотите отключить защиту в реальном времени, то появится окно с предупреждением. Необходимо подтвердить выбор. Для этого в меню следует выбрать период, на который требуется отключить защиту в режиме реального времени. Вы можете отключить защиту в реальном времени на 5, 15 или 30 минут, на час, навсегда или до следующей перезагрузки системы. Защита в реальном времени автоматически включается по истечении выбранного времени.

Предупреждение
Это критическая проблема безопасности. Рекомендуется отключить защиту в режиме реального времени на максимально короткий промежуток времени. Если защита в реальном времени отключена, вы не будете защищены от угроз.

14.1.2. Настройка дополнительных параметров защиты в режиме реального времени

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

Чтобы настроить дополнительные параметры защиты в режиме реального времени:

1. Нажмите **Защита** в меню навигации интерфейса Bitdefender.
2. На панели **АНТИВИРУС** нажмите **Настройки**.
3. В окне **Защита** нажмите в соответствующем меню **Показать дополнительные настройки**.

   Отобразится новая панель
4. Прокрутите страницу вниз, чтобы настроить параметры сканирования по мере необходимости.

Информация о параметрах сканирования

Эти сведения могут быть полезными:

- **Сканировать только приложения.** Вы можете настроить Bitdefender для сканирования только доступных приложений.
- **Сканирование потенциально нежелательных приложений.** Выберите эту опцию для сканирования нежелательных приложений. Потенциально нежелательные приложения или потенциально нежелательные программы представляют собой программу, которая обычно поставляется в комплекте с бесплатным программным обеспечением и отображает всплывающие окна или устанавливает панель инструментов в браузере по умолчанию. Некоторые из них изменяют домашнюю страницу или поисковую систему, запускают несколько процессов в фоновом режиме, замедляя работу устройства, или отображают многочисленные объявления. Такие программы (также называются рекламными) могут быть установлены без согласия или включены по умолчанию в комплект экспресс-установки (с поддержкой рекламы).

- **Сканировать общие сетевые ресурсы.** Для безопасного доступа к удаленной сети рекомендуется включить опцию "Сканирование сетевых ресурсов".
- **Сканирование 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. Угрозы могут повлиять на систему только в том случае, если зараженный файл извлечен из архива и выполнен при выключенной защите в режиме реального времени.

  Если Вы решите использовать эту опцию, включите ее и перетащите ползунок по шкале, чтобы установить максимально допустимый размер (в МБ) архивов, которые будут проверяться при доступе.
- **Сканировать сообщения электронной почты.** Чтобы предотвратить проникновение угроз на ваш компьютер, Bitdefender автоматически сканирует входящие и исходящие сообщения электронной почты.

  В целях повышения производительности системы можно отключить сканирование электронной почты на наличие угроз (не рекомендуется). Если вы отключите соответствующие параметры сканирования, то полученные письма и файлы не будут сканироваться, что позволит сохранить зараженные файлы на вашем компьютере. Это не самая серьезная опасность, поскольку защита в режиме реального времени блокирует угрозы при доступе (открытии, перемещении, копировании или исполнении) к зараженным файлам.
- **Сканирование загрузочных секторов.** Bitdefender можно настроить для сканирования загрузочных секторов жесткого диска. Этот сектор жесткого диска содержит компьютерный код, необходимый для запуска процесса загрузки. Поражение загрузочного сектора может привести к тому, что диск станет недоступен и вы не сможете загрузить систему и получить доступ к своим данным.
- **Сканировать только новые и измененные файлы.** Сканируя только новые и измененные файлы, можно значительно повысить работу системы с минимальными потерями в безопасности.
- **Сканирование на наличие клавиатурных шпионов.** Выберите эту опцию для сканирования вашей системы на предмет кейлоггер-приложений. Кейлоггеры (клавиатурные перехватчики)

записывают то, что вы набираете на клавиатуре и отправляют отчеты хакерам через интернет. В украденных данных хакер может найти личную информацию, такую как номера банковских счетов и пароли, и использовать ее в личных целях.

- **Сканирование при загрузке системы.** Выберите опцию **Сканирование начальной загрузки** для сканирования системы при загрузке, как только все его критические услуги будут загружены. Назначением данной функции является улучшение обнаружения угроз при запуске системы и времени загрузки вашей системы.

Действия, выполненные в отношении обнаруженных угроз

Вы можете настроить функции в режиме реального времени выполнив следующие действия:

1. Нажмите **Защита** в меню навигации интерфейса Bitdefender.
2. На панели **АНТИВИРУС** нажмите **Настройки**.
3. В окне **Защита** нажмите в соответствующем меню **Показать дополнительные настройки**.

   Отобразится новая панель
4. Прокрутите вниз, пока не увидите опцию **Действия с угрозами**.
5. Настройте параметры сканирования по своему выбору.

Следующие действия могут быть предприняты в режиме реального времени защиты в Bitdefender:

Выполнить соответствующие действия

Bitdefender выполнит рекомендуемые действия в зависимости от типа обнаруженного файла:

- **Инфицированные файлы.** Обнаруженные инфицированные файлы соответствуют базе данных угроз 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. Файлы, помещенные в карантин, не могут быть выполнены или открыты; таким образом, не возникает риск заражения. Для получения

более подробной информации, обратитесь к «*Управление файлами в карантине*» (р. 98).

Важно
Для определенных типов угроз лечение невозможно, поскольку обнаруженный файл является полностью вредоносным. В таких случаях выполняется удаление зараженного файла с диска.

- **Подозрительные файлы.** Файлы помечены эвристическим анализом как подозрительные. Лечение подозрительных файлов невозможно, поскольку процедура лечения недоступна. Такие файлы будут перемещены в карантин во избежание потенциального заражения.

  По умолчанию, файлы из карантина автоматически отправляются в лабораторию Bitdefender для дальнейшего анализа специалистами по угрозам Bitdefender. Если подтверждено присутствие угрозы, будет выпущено обновление сведений об угрозе для ее устранения.

- **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.

Перемещение файлов в карантин

Зараженные файлы перемещаются в карантин. Файлы, помещенные в карантин, не могут быть выполнены или открыты; таким образом, не возникает риск заражения. Для получения более подробной информации, обратитесь к «*Управление файлами в карантине*» (р. 98).

Запретить доступ

В случае обнаружения зараженного файла, доступ к нему будет запрещен.

14.1.3. Восстановление настроек по умолчанию

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

Восстановление настроек по умолчанию для защиты в режиме реального времени:

1. Нажмите **Защита** в меню навигации интерфейса Bitdefender.
2. На панели **АНТИВИРУС** нажмите **Настройки**.
3. В окне **Защита** нажмите в соответствующем меню **Показать дополнительные настройки**.

   Отобразится новая панель
4. Прокрутите вниз, пока не увидите параметр **Сброс настроек**. Выберите этот параметр, чтобы сбросить настройки антивируса по умолчанию.

14.2. Сканирование по запросу

Главное назначение программного продукта Bitdefender - защита вашего компьютера от угроз. Это делается путем сохранения новых угроз с компьютера, сканирования сообщений электронной почты и любых новых файлов, загруженных или скопированных в вашу систему.

Существует риск того, что угроза уже находилась в вашей системе до установки Bitdefender. Поэтому полезно проверить ваш компьютер на наличие угроз после установки программы Bitdefender. И это, безусловно, хорошая идея - часто сканировать компьютер на наличие угроз.

Сканирование по требованию основывается на задачах сканирования. Задачи сканирования определяют параметры сканирования и проверяемые объекты. 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.

14.2.1. Сканирование файла или папки на наличие угроз.

Рекомендуется выполнять сканирование файлов и папок каждый раз при подозрении на заражение их вирусом. Щелкните правой кнопкой мыши по файлу или папке, которые необходимо проверить **Bitdefender** и выберите **Сканировать с Bitdefender**. Появится Мастер сканирования и проведет вас через процесс сканирования. На этапе завершения сканирования отобразится сообщение, предлагающее выбрать действия, которые будут выполняться для обнаруженных файлов (если есть).

14.2.2. Запуск быстрого сканирования

Функция быстрого сканирования использует технологию "облачного" сканирования для распознавания угроз, запущенных в системе. Запуск Быстрого сканирования обычно занимает меньше минуты и использует часть системных ресурсов, необходимых в процессе стандартного сканирования на наличие угроз.

Для запуска быстрого сканирования:

1. Нажмите **Защита** в меню навигации интерфейса Bitdefender.
2. В области **АНТИВИРУС** нажмите **Быстрое сканирование**.
3. 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.

14.2.3. Запуск проверки системы

Задача Сканирования системы проверяет компьютер на наличие всех типов угроз, например, шпионские программы, руткиты и другие.

Примечание

Поскольку **Системное сканирование** выполняет тщательную проверку всей системы, сканирование может занять некоторое время. Поэтому рекомендуется запускать эту задачу, когда компьютер не используется.

Перед запуском сканирования системы рекомендуется выполнить следующие действия:

- Убедитесь, что Bitdefender и база данных угроз обновлены. Сканирование компьютера с использованием устаревшей базы данных угроз может помешать Bitdefender обнаружить новые угрозы, выявленные с момента последнего обновления. Для получения более подробной информации, обратитесь к «*Поддержка Bitdefender в обновленном состоянии*» (p. 40).
- Закройте все открытые программы.

Чтобы выполнить сканирование отдельных папок на компьютере или настроить параметры сканирования, создайте и запустите пользовательское сканирование. Для получения более подробной информации, обратитесь к «*Настройка пользовательского сканирования*» (p. 85).

Чтобы запустить сканирование системы:

1. Нажмите **Защита** в меню навигации интерфейса Bitdefender.
2. В области **АНТИВИРУС** нажмите **Системное сканирование**.
3. При первом запуске "Сканирования системы" вы пройдете через эту функцию. Для продолжения нажмите **ОК**.
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.

14.2.4. Настройка пользовательского сканирования

Чтобы подробно настроить пользовательское сканирование и затем запустить его:

1. Нажмите **Защита** в меню навигации интерфейса Bitdefender.
2. В области **АНТИВИРУС** нажмите **УПРАВЛЕНИЕ СКАНИРОВАНИЕМ**.
3. Нажмите **НОВАЯ ЗАДАЧА ПОЛЬЗОВАТЕЛЯ**. В окне **Основное** введите имя для сканирования и выберите сканируемые местоположения.

4. Если вы хотите настроить дополнительный параметры сканирования, выберите вкладку **Расширенное**. Появится новое окно. Следуйте инструкции:

   a. Настроить параметры сканирования можно легко, с помощью регулировки уровня сканирования. Перетащите ползунок по шкале, чтобы задать требуемый 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** режим. Информацию о них вы можете найти в конце этого раздела.

   b. Вы также можете настроить эти основные параметры:

   - **Выполнение задачи с низким приоритетом .** Понизить приоритет для выбранного правила. Таким образом вы ускоряете работу других программ, но увеличиваете время, необходимое для завершения процесса проверки.
   - **Свернуть Мастер сканирования в область уведомлений .** Сворачивает окно сканирования в область уведомлений. Дважды щелкните значок Bitdefender, чтобы открыть его.
   - Задать действие, выполняемое при отсутствии обнаруженных угроз.

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

5. Если вы хотите задать расписание для задачи сканирования, используйте**Расписание** в окне **Основное**. Выберите один из предложенных вариантов, чтобы установить расписание:

   - При запуске системы
   - Один раз
   - Периодически

6. Нажмите **НАЧАТЬ СКАНИРОВАНИЕ** 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).

7. При желании можно быстро перезапустить предыдущее пользовательское сканирование, щелкнув соответствующую запись в доступном списке.

Информация о параметрах сканирования

Эти сведения могут быть полезными:

- Значение незнакомых терминов можно посмотреть в глоссарии. Также вы можете найти полезную информацию в Интернете.
- **Сканирование 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 файлы программ) более подвержены угрозам, 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. Угрозы могут повлиять на систему только в том случае, если зараженный файл извлечен из архива и выполнен при выключенной защите в режиме реального времени. Тем не менее, рекомендуется использовать этот параметр для обнаружения и удаления всех угроз, даже тех, которые не представляют собой непосредственной опасности для системы.

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

- **Сканирование загрузочных секторов.** Bitdefender можно настроить для сканирования загрузочных секторов жесткого диска. Этот сектор жесткого диска содержит компьютерный код, необходимый для запуска процесса загрузки. Поражение загрузочного сектора может привести к тому, что диск станет недоступен и вы не сможете загрузить систему и получить доступ к своим данным.
- **Сканирование памяти.** Выберите этот параметр, чтобы выполнить сканирование программ, запущенных в системной памяти.
- **Сканирование 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.
- **Сканирование файлов cookie.** Выберите этот параметр, чтобы включить сканирование файлов cookie, сохраненных браузером на компьютере.
- **Сканирование только новых/измененных файлов.** Сканируя только новые и измененные файлы, можно значительно повысить работу 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.
- **Сканирование на наличие руткитов.** Выберите этот параметр для сканирования на наличие руткитов и объектов, скрытых с помощью такого программного обеспечения.
- **Сканирование потенциально нежелательных приложений.** Выберите эту опцию для сканирования нежелательных приложений. Потенциально нежелательные приложения или потенциально нежелательные программы представляют собой программу, которая обычно поставляется в комплекте с бесплатным программным

обеспечением и отображает всплывающие окна или устанавливает панель инструментов в браузере по умолчанию. Некоторые из них изменяют домашнюю страницу или поисковую систему, запускают несколько процессов в фоновом режиме, замедляя работу устройства, или отображают многочисленные объявления. Такие программы (также называются рекламными) могут быть установлены без согласия или включены по умолчанию в комплект экспресс-установки (с поддержкой рекламы).

14.2.5. Мастер антивирусного сканирования

Всякий раз, когда вы инициируете сканирование по запросу (например, щелкните правой кнопкой мыши папку, наведите указатель на Bitdefender и выберите **Сканирование с Bitdefender**), появится Мастер антивирусного сканирования Bitdefender. Следуйте инструкциям мастера для завершения процесса сканирования.

Примечание

Если Мастер сканирования не отображается, сканирование может быть настроено на запуск в фоновом режиме. Найдите значок состояния сканирования в область уведомлений. Вы можете щелкнуть этот значок, чтобы открыть окно сканирования и просмотреть ход сканирования.

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).

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

Остановка или приостановка сканирования. Вы можете прервать сканирование в любое время, нажав **Стоп**. При этом вы перейдете к последнему шагу 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 параметров сканирования). Защищенные паролем архивы нельзя сканировать без предоставления пароля. Доступны следующие опции:

- **Пароль.** Если вы хотите, чтобы Bitdefender просканировал архив, выберите этот вариант и введите пароль. Если вы не знаете пароля, выберите любую другую опцию.
- **Не спрашивать пароль и пропустить эти объекты без сканирования.** Выберите этот параметр, чтобы пропустить сканирование этого архива.
- **Пропустить все защищенные паролем элементы без сканирования.** Выберите этот параметр, если вы не хотите беспокоиться о защищенных паролем архивах. Bitdefender не сможет их сканировать, но запись будет сохранена 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).

Примечание

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 угрозы, которой они были инфицированы. Нажмите на ссылку, соответствующую угрозе, чтобы узнать больше информации о зараженных объектах.

Можно выбрать общее действие, которое необходимо предпринять для всех проблем, или выбрать отдельные действия для каждой группы проблем. В меню могут появиться один или несколько из следующих параметров:

Выполнить соответствующие действия

Bitdefender выполнит рекомендуемые действия в зависимости от типа обнаруженного файла:

- **Инфицированные файлы.** Обнаруженные инфицированные файлы соответствуют базе данных угроз 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. Файлы, помещенные в карантин, не могут быть выполнены или открыты; таким образом, не возникает риск заражения. Для получения более подробной информации, обратитесь к «*Управление файлами в карантине*» (p. 98).

  > **Важно**
  > Для определенных типов угроз лечение невозможно, поскольку обнаруженный файл является полностью вредоносным. В таких случаях выполняется удаление зараженного файла с диска.

- **Подозрительные файлы.** Файлы помечены эвристическим анализом как подозрительные. Лечение подозрительных файлов невозможно, поскольку процедура лечения недоступна. Такие файлы будут перемещены в карантин во избежание потенциального заражения.

  По умолчанию, файлы из карантина автоматически отправляются в лабораторию Bitdefender для дальнейшего анализа специалистами по угрозам Bitdefender. Если подтверждено присутствие угрозы, будет выпущено обновление сведений об угрозе для ее устранения.

- **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 предпринимать никаких действий

Для обнаруженных файлов не будет выполняться никаких действий. После завершения сканирования можно открыть журнал сканирования для просмотра сведений об этих файлах.

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

Шаг 3. Сводка

Когда Bitdefender завершит исправление проблем, результаты проверки будут отображены в новом окне. Если вы хотите получить исчерпывающую информацию о процессе сканирования, нажмите **Показать журнал**, для просмотра журнала сканирования. Журнал предоставляется в формате xml и может быть локально сохранен, нажатием кнопки **Сохранить журнал** , после чего необходимо выбрать местоположение.

Важно

В большинстве случаев Bitdefender успешно лечит зараженные файлы, которые обнаруживает, или изолирует инфекцию. Тем не менее, существуют проблемы, которые невозможно устранить автоматически. При необходимости перезагрузите систему, чтобы завершить процесс очистки. Для получения дополнительных сведений и инструкций по удалению угрозы вручную обратитесь к разделу «*Удаление угроз из системы*» (p. 161).

14.2.6. Просмотр журналов сканирования

Каждый раз при выполнении сканирования создается журнал сканирования и Bitdefender записывает обнаруженные неполадки в

окне Антивируса. Журнал сканирования содержит подробные сведения о регистрируемом процессе сканирования, такие как параметры сканирования, цель сканирования, найденные угрозы и действия, предпринятые в отношении этих угроз.

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

Чтобы позже посмотреть журналы сканирования или любые другие обнаруженные инфицированные объекты:

1. Нажмите **Уведомления** в меню навигации интерфейсBitdefender.
2. На вкладке **ВСЕ**, выберите уведомления относительно последнего сканирования.

   Здесь можно просмотреть все события сканирования на наличие угорз, включая угрозы, обнаруженные при доступе, сканировании по инициативе пользователя, а также изменения статуса автоматического сканирования.
3. В списке уведомлений вы можете проверить какие сканирования были выполнены в последнее время. Нажмите на уведомление, чтобы просмотреть сведения о нем.
4. Чтобы открыть журнал сканирования, нажмите **View log**.

14.3. Автоматическое сканирование съемных носителей

Bitdefender автоматически обнаруживает съемное запоминающее устройство к вашему компьютеру и сканирует его в фоновом режиме, когда включена опция Автосканирование. Это рекомендуется для того, чтобы предотвратить заражение компьютера.

Обнаруженные устройства относятся к одной из следующих категорий:

- CD/DVD
- Запоминающие устройства, 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.

14.3.1. Как это работает?

При обнаружении съемного носителя Bitdefender запускает в фоновом режиме процесс его сканирования на наличие угроз (если включена функция автоматического сканирования для этого типа устройств). Откроется всплывающее окно с уведомлением о том, что новое устройство было обнаружено и выполняется его сканирование.

Значок сканирования Bitdefender появится в области уведомлений. Вы можете щелкнуть этот значок, чтобы открыть окно сканирования и просмотреть ход сканирования.

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

В большинстве случаев Bitdefender автоматически удаляет обнаруженные угрозы 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.

Примечание

Обратите внимание на то, что в отношении инфицированных или подозрительных файлов, обнаруженных на CD/DVD, никакие действия не выполняются. Аналогичным образом, если у вас нет соответствующих привилегий, никакие действия не могут быть предприняты для зараженных или подозрительных файлов, обнаруженных на подключенных сетевых дисках.

Следующая информация может оказаться вам полезной:

- Соблюдайте осторожность при использовании зараженных CD/DVD, так как удалить угрозы с дисков невозможно (носители доступны только для чтения). Чтобы предотвратить распространение угроз в системе, убедитесь в том, что включена защита в режиме реального времени. Рекомендуется скопировать любые ценные данные с диска в систему, а затем утилизировать диск.

- В некоторых случаях Bitdefender не может удалить угрозы из определенных файлов из-за юридических или технических ограничений. Таким примером являются файлы, архивированные с использованием запатентованной технологии (это происходит потому, что архив не может быть создан правильно).

  О борьбе с угрозами можно узнать в разделе *«Удаление угроз из системы»* (p. 161).

14.3.2. Управление сканированием съемных носителей

Для управления автоматической проверкой съемных носителей:

Для наилучшей защиты рекомендуется выбрать опцию **Автосканирование** для всех типов съемных запоминающих устройств.

1. Нажмите **Защита** в меню навигации интерфейса Bitdefender.
2. На панели **АНТИВИРУС** нажмите **Настройки**.
3. Выберите вкладку **Диски и устройства**.

Опции сканирования предварительно настроены для достижения наилучших результатов обнаружения. При обнаружении зараженных файлов, Bitdefender попытается вылечить их (удалить вредоносный код) или переместить их в карантин. Если оба действия завершаются ошибкой, Мастер антивирусного сканирования позволит указать другие действия, которые должны быть предприняты для зараженных файлов. Параметры сканирования являются стандартными и их нельзя изменить.

14.4. Сканирование хост-файлов

Файл host поставляется по умолчанию с установкой операционной системы и используется для сопоставления имен хостов с IP-адресами каждый раз при обращении к новой веб-странице, подключении к FTP или к другим Интернет-серверам. Это обычный текстовый файл и вредоносные программы могут изменять его. Продвинутые пользователи знают, как использовать его для блокирования назойливой рекламы, баннеров, сторонних куки или угонщиков или перехватчиков.

Для настройки сканирования хост-файлов:

1. Нажмите **Настройки** в меню навигации интерфейс Bitdefender.

2. Выберите вкладку **Advanced**.
3. Включить или отключить **Сканирование файла hosts**.

14.5. Настройка исключений для сканирования

Bitdefender допускает исключение из сканирования определенных файлов, папок и расширений файлов. Эта функция предназначена для предотвращения помех в работе, а также может помочь повысить производительность системы. Исключения могут быть использованы пользователями, которые имеют большой опыт работы с компьютерами, или в случае получения соответствующих рекомендаций от представителя Bitdefender.

Можно настроить исключения только для применения сканирования по требованию или запросу, а также в обоих случаях. Объекты не будут проверяться, если они исключены из списка сканирования при доступе, независимо от того, используются ли они вами или приложением.

Примечание

Исключения НЕ применяются для системного и контекстного сканирования. Сканирование системы, используемое по запросу, позволяет анализировать всю систему на наличие вредоносных угроз, которые могут угрожать безопасности Ваших данных. Контекстное сканирование — это тип сканирования по запросу: щелкните правой кнопкой мыши файл или папку, которую необходимо сканировать, и выберите **Сканировать с Bitdefender**.

14.5.1. Исключение файлов или папок из сканирования

Чтобы исключить определенные файлы или папки из сканирования:

1. Нажмите **Защита** в меню навигации интерфейса Bitdefender.
2. На панели **АНТИВИРУС** нажмите **Настройки**.
3. Выберите вкладку **Исключения**.
4. Нажмите в соответствующем меню **Список исключенных из сканирования файлов и папок**. В открывшемся окне можно управлять файлами и папками, исключенными из сканирования.
5. Добавьте исключения, выполнив следующие действия:
   a. Нажмите **Добавить**.

b. Нажмите **ОБЗОР**, выберите файл или папку для исключения из сканирования, затем нажмите **ДОБАВИТЬ**. Также путь к файлу или папке можно ввести (или скопировать и вставить) в поле редактирования.

c. По умолчанию указанный файл или папка исключаются из сканирования в режиме реального времени и сканирования по запросу. Чтобы изменить время применения исключения, выберите один из других параметров.

d. Нажмите **Добавить**.

14.5.2. Исключение расширений файлов из сканирования

Если расширение файла исключено из сканирования, Bitdefender больше не будет сканировать файлы с подобным 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 угроз.

Чтобы исключить расширения файлов из сканирования:

1. Нажмите **Защита** в меню навигации интерфейса Bitdefender.
2. На панели **АНТИВИРУС** нажмите **Настройки**.
3. Выберите вкладку **Исключения**.
4. Нажмите в меню **Список расширений, исключенных из сканирования** В открывшемся окне можно управлять расширениями файлов, исключенных из сканирования.
5. Добавьте исключения, выполнив следующие действия:
   a. Нажмите **Добавить**.
   b. Введите расширения, которые требуется исключить из сканирования, разделив их символом "точка с запятой" (;). Пример:

      txt;avi;jpg

c. По умолчанию все файлы с указанными расширениями исключаются из сканирования при доступе и сканирования по запросу. Чтобы изменить время применения исключения, выберите один из других параметров.

d. Нажмите **ДОБАВИТЬ**.

14.5.3. Управление исключениями сканирования

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

Управление исключениями сканирования:

1. Нажмите **Защита** в меню навигации интерфейса Bitdefender.
2. На панели **АНТИВИРУС** нажмите **Настройки**.
3. Выберите вкладку **Исключения**.
4. Используйте опции в **Списке файлов и папок, исключенных из сканирования** в меню управления исключениями сканирования.
5. Чтобы удалить или изменить исключения сканирования, нажмите на одну из доступных ссылок. Выполните следующие действия:
   - Чтобы удалить запись из списка, выделите ее и нажмите **Удалить**.
   - Чтобы исправить запись в таблице, дважды щелкните по ней (или выберите и нажмите кнопку **ИСПРАВИТЬ**). Появится новое окно, в котором вы сможете изменить расширение или путь к исключению, а также тип сканирования, из которого вы хотите его исключить. Внесите необходимые изменения и нажмите **ИЗМЕНИТЬ**.

14.6. Управление файлами в карантине

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

По умолчанию, файлы из карантина автоматически отправляются в лабораторию Bitdefender для дальнейшего анализа специалистами по угрозам Bitdefender. Если подтверждено присутствие угрозы, будет выпущено обновление сведений об угрозе для ее устранения.

Кроме того, Bitdefender сканирует файлы, помещенные в карантин после каждого обновления базы данных угроз. Вылеченные файлы автоматически возвращаются на свое место.

Чтобы проверить и управлять файлами на карантине:

1. Нажмите **Защита** в меню навигации интерфейса Bitdefender.
2. В области **АНТИВИРУС** нажмите **карантина**.

   Здесь можно просмотреть имя помещенных на карантин файлов, их исходное расположение и имя обнаруженных угроз.
3. Bitdefender автоматически управляет файлами в карантине в соответствии с настройками параметров карантина по умолчанию.

   Не смотря на то, что это действие не рекомендуется выполнять, вы можете изменить настройки параметров карантина в соответствии со своими потребностями, нажав **Обзор настроек**.

   Нажмите на переключатели, чтобы включить или отключить:

   Повторное сканирование карантина после обновления сведений об угрозах
   Оставьте этот параметр включенным, чтобы сканирование файлов в карантине выполнялось автоматически после обновления базы данных угроз. Вылеченные файлы автоматически возвращаются на свое место.

   Удалить контент старше 30 дней
   Файлы, находящиеся на карантине более 30 дней, автоматически удаляются.

   Создать исключение для восстановленных файлов
   Файлы, которые вы восстанавливаете из карантина, перемещаются обратно в исходное местоположение без восстановления и автоматически исключаются из последующих сканирований.
4. 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**.

15. АКТИВНЫЙ КОНТРОЛЬ УГРОЗ

Bitdefender Активный Контроль Угроз - это инновационная технология проактивного обнаружения, использующая расширенные эвристические методы выявления новых потенциальных угроз в режиме реального времени.

Активный Контроль Угроз беспрерывно отслеживает приложения, запущенные на компьютере, на наличие угроз. Для всех вышеперечисленных действий присваивается определенный балл и для каждого процесса подсчитывается общий рейтинг.

В качестве меры безопасности вы будете уведомлены при каждом обнаружении и блокировании угроз и потенциально вредоносных процессов.

15.1. Включение и выключение Активный Контроль Угроз:

Чтобы включить или выключить Активный Контроль Угроз:

1. Нажмите **Защита** в меню навигации интерфейса Bitdefender.
2. В области **АКТИВНЫЙ КОНТРОЛЬ УГРОЗ** включите или выключите переключатель.

> **Примечание**
> Для защиты системы от вымогательств и других угроз, рекомендуется производить отключение опции Активный Контроль Угроз на как можно меньшее время.

15.2. Проверка обнаруженных вредоносных атак

При каждом обнаружении угроз или потенциально вредоносных процессов Bitdefender будет блокировать их, чтобы предотвратить заражение компьютера программами-вымогателями или другими вредоносными программами. Вы можете в любой момент проверить список обнаруженных вредоносных атак, выполнив следующие действия:

1. Нажмите **Защита** в меню навигации интерфейса Bitdefender.
2. На панели **Активный Контроль Угроз** щелкните **Защита от угроз**.

3. При первом обращении к параметру "Защита от программ-вымогателей" вы перейдете к этой опции. Для продолжения нажмите **ОК**.

   Отображаются атаки, обнаруженные за последние 90 дней. Чтобы найти информацию о типе обнаруженного вымогателя, пути к вредоносному процессу или успешного обеззараживания, просто нажмите на него.

15.3. Добавление процессов к исключениям

Вы можете настроить правила исключения для доверенных приложений, чтобы "Активный контроль угроз" не блокировал их, когда они выполняют действия, подобные угрозам.

Чтобы начать добавление процессов в список исключений "Активного контроля угроз":

1. Нажмите **Защита** в меню навигации интерфейса Bitdefender.
2. В области **АКТИВНЫЙ КОНТРОЛЬ УГРОЗ** нажмите **Настройки**.
3. В окне **Исключения** нажмите **Добавить приложения в исключения**.
4. Найдите и выберите приложение, которое хотите исключить, затем нажмите **ОК**.

   Чтобы удалить запись из списка, нажмите кнопку **Удалить**, расположенную рядом с ней.

16. ПРЕДОТВРАЩЕНИЕ СЕТЕВЫХ УГРОЗ

Bitdefender "Предотвращение угроз" обеспечивает безопасный просмотр, предупреждая вас о потенциальных вредоносных веб-страницах.

Bitdefender обеспечивает предотвращение угроз в режиме реального времени для:

- Internet Explorer
- Microsoft Edge
- Mozilla Firefox
- Google Chrome
- Safari
- Bitdefender Safepay™
- Opera

Чтобы задать настройки для параметра "Предотвращение угроз":

1. Нажмите **Защита** в меню навигации интерфейса Bitdefender.
2. На панели **ПРЕДОТВРАЩЕНИЕ УГРОЗ** нажмите **Настройки**.

В окне **Веб-защита** нажмите на соответствующие переключатели, чтобы включить или выключить:

- "Предотвращение веб-атак" блокирует угрозы, поступающие из Интернета, включая загружаемые файлы.
- Поисковый советник, компонент, который оценивает результаты поиска запросов и ссылки, размещеные на сайтах социальных сетей, поставив значок рядом с каждым результатом:

  Эту веб-страницу посещать не следует.

  Данная веб-страница может содержать опасную информацию. Соблюдайте осторожность, если вы решите ее посетить.

  Эта страница безопасна для посещения.

  Поисковый советник оценивает результаты поиска следующих поисковых систем:
  - Google
  - Yahoo!
  - Bing
  - Baidu

Поисковый советник оценивает результаты ссылок, размещенных на следующих социальных сетях:
- Facebook
- Twitter

- Зашифрованное веб-сканирование.

  При более сложных атаках, для ввода пользователей в заблуждение, может использоваться защищенный интернет-трафик. Поэтому мы рекомендовали вам включить параметр «Зашифрованное веб-сканирование».

- Защита от мошенничества.

- Защита от фишинга.

В окне **Предотвращение сетевых угроз** находится параметр **Предотвращение сетевых угроз**. Чтобы защитить ваш компьютер от атак сложных вредоносных программам, использующих уязвимости (например, вымогатели), оставьте этот параметр включенным.

Вы можете создать список веб-сайтов, для которых не будет выполняться сканирование на предмет угроз, мошенничества и фишинга при помощи механизмов Bitdefender. Список должен содержать только веб-сайты, которым вы полностью доверяете. Например, добавьте веб-сайты, где вы совершаете покупки в Интернете.

Чтобы настроить и управлять веб-сайтами с помощью функции "Предотвращения угроз" Bitdefender:

1. Нажмите **Защита** в меню навигации интерфейса Bitdefender.
2. На панели **ПРЕДОТВРАЩЕНИЕ УГРОЗ** нажмите **Исключения**.
3. В соответствующем поле введите название веб-сайта, который хотите добавить в белый список, и нажмите **ДОБАВИТЬ**.

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

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

16.1. 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 решения для дальнейших действий. Доступны следующие опции:

- Покинуть веб-страницу, нажав кнопку **СНОВА ЗАЩИЩАТЬ**.
- Игнорируя предупреждение, перейдите на веб-страницу, нажав кнопку **Я осознаю риск. Перейти все равно.**
- Если вы уверены в безопасности обнаруженной веб-страницы, нажмите **ОТПРАВИТЬ**, чтобы добавить ее в белый список. Рекомендуется добавлять только те веб-страницы, которым вы полностью доверяете.

17. УЯЗВИМОСТИ

Важный шаг в защите вашего компьютера от злоумышленников и вредоносного ПО состоит в том, чтобы держать операционную систему и используемые приложения в обновленном состоянии. Кроме того, чтобы предотвратить несанкционированный физический доступ к вашему компьютеру, надежные пароли (пароли, которые не могут быть легко угаданы) должны быть настроены как для каждой учетной записи пользователя Windows, так и для сетей Wi-Fi, к которым вы подключаетесь.

Bitdefender автоматически проверяет вашу систему на наличие уязвимостей и предупреждает вас о них. Он сканирует для следующих:

- устаревшие приложения на вашем компьютере.
- отсутствующие обновления Windows;
- ненадежные пароли учетных записей Windows.
- ненадежные беспроводные сети и маршрутизаторы.

Bitdefender предоставляет два простых способа устранения уязвимостей системы:

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

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

17.1. Сканирование системы на наличие уязвимостей

Для того, чтобы устранить уязвимости системы, используя опцию Сканирование уязвимостей, выполните следующие действия:

1. Нажмите **Защита** в меню навигации интерфейса Bitdefender.
2. В области **УЯЗВИМОСТЬ** нажмите **Сканирование уязвимостей**.

3. Подождите, пока Bitdefender завершит проверку системы на наличие уязвимостей. Чтобы остановить процесс сканирования, нажмите кнопку **Пропустить** в верхней части окна.

   - **Критические обновления Windows**

     Нажмите **Подробнее** , чтобы просмотреть список критических обновлений Windows, которые не установлены на вашем компьютере.

     Для того, чтобы начать установку выбранных обновлений, нажмите **Установить обновления**. 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.

   - **Обновления приложения**

     Если приложение нуждается в обновлении, щелкните на ссылку **Загрузить новую версию**, чтобы загрузить последнюю версию.

     Нажмите **Подробнее** для просмотра информации о приложении, которое необходимо обновить.

   - **Слабые пароли учетных записей Windows**

     Вы можете увидеть список учетных записей пользователей Windows, настроенных на вашем компьютере, и уровень защиты, который обеспечивает пароль.

     Нажмите **Изменить пароль при входе**, чтобы установить новый пароль для вашей системы.

     Нажмите **Подробнее**, 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. Для того, чтобы пароль был сильным, используйте комбинации символов в верхнем и нижнем регистре, числа и специальные символы (такие как, #, $ или @).

   - **Сети Wi-Fi**

     Нажмите **Подробнее** чтобы узнать больше о беспроводной сети, к которой вы подключены. Если рекомендуется установить

надежный пароль для вашей домашней сети, нажмите на соответствующую ссылку.

Когда другие рекомендации доступны, следуйте инструкциям, чтобы убедиться, что ваша домашняя сеть остается в безопасности от любопытных глаз хакеров.

В правом верхнем углу окна вы можете фильтровать результаты в соответствии с вашими предпочтениями.

17.2. Использование автоматического мониторинга уязвимостей

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

Чтобы проверить и исправить обнаруженные проблемы:

1. Нажмите **Уведомления** в меню навигации интерфейсBitdefender.
2. На вкладке **ВСЕ** выберите уведомления относительно сканирования на наличие уязвимостей.
3. Вы можете просмотреть подробные сведения об обнаруженных уязвимостях системы. В зависимости от проблемы, чтобы устранить конкретную уязвимость, выполните следующие действия:
   - Если доступны обновления для Windows, нажмите **Установить**.
   - Если автоматическое обновление Windows отключено, нажмите **Enable**.
   - Если приложение устарело, нажмите **Обновить сейчас**, чтобы найти ссылку на веб-страницу поставщика, с которой можно установить последнюю версию приложения.
   - Если для учетной записи Windows установлен слабый пароль, нажмите **Change password**, чтобы принудить пользователя сменить пароль при следующем входе в систему, или смените его сами. Для того, чтобы пароль был сильным, используйте комбинации символов в верхнем и нижнем регистре, числа и специальные символы (такие как, #, $ или @).
   - Если функция автозапуска Windows включена, нажмите **Fix**, чтобы отключить ее.

- Если на настроенном маршрутизаторе установлен ненадежный пароль, нажмите **Изменить пароль**, чтобы перейти к интерфейсу, где можно установить надежный пароль.
- Если подключенная сеть имеет уязвимости, которые могут подвергнуть вашу систему риску, нажмите **Изменить настройки WI-FI**.

Для настройки параметров мониторинга уязвимостей:

1. Нажмите **Защита** в меню навигации интерфейса Bitdefender.
2. На панели **УЯЗВИМОСТИ** нажмите **Настройки**.

> **Важно**
> Для автоматического получения уведомлений об уязвимостях системы или приложений, параметр **Уязвимости** должен быть включен.

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

   Обновления Windows

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

   Обновления приложения

   Проверьте актуальны ли версии приложений, установленные на вашей системе. Устаревшие приложения могут быть использованы вредоносными программами, что делает компьютер уязвимым для атак извне.

   Пользовательские пароли

   Проверьте, насколько легко угадать пароли учетных записей Windows и маршрутизаторов, настроенных в системе. 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 @).

Автовоспроизведение

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

Некоторые типы угроз используют функцию автозапуска, с целью автоматической передачи угрозы со съемного носителя на компьютер. Поэтому рекомендуется отключить данную функцию в Windows.

Защита Wi-Fi

Проверьте, является ли беспроводная домашняя сеть, к которой вы подключены, безопасной или нет, и имеются ли уязвимости. Кроме того, проверьте насколько надежен пароль доступа домашнего маршрутизатора и как можно сделать его более безопасным.

Большинство незащищенных беспроводных сетей не являются безопасными, что позволяет хакерам получит доступ к Вашим приватным действиям.

Примечание

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

17.3. Советник безопасности Wi-Fi

Система принимает самые быстрые решения, в то время пока Вы находитесь в пути, работаете в кафе, или ждете в аэропорту, подключаетесь к публичной сети для осуществления платежей, проверяете электронные письма или учетные записи в социальных сетях. Но там могут быть любопытные глаза хакеров, которые могут попытаться похитить ваши личные данные.

Личные данные - это пароли и имена пользователей, которые вы используете, чтобы получить доступ к учетным записям в Интернете, не только к электронной почте, банковским счетам, учетным записям средств массовой информации, но и к сообщениям, которые вы посылаете.

Как правило, публичные сети, в большинстве случаев, небезопасны, так как они не требуют пароля при входе в систему, а если и требуют, то пароль может быть доступен для всех, кто хочет подключится. Кроме того, они могут быть вредоносными или сетями "ловушками", представляющие собой цель для кибер-преступников.

Чтобы защитить Вас от опасности использования ненадежных или незашифрованных публичных точек доступа, Советник по Wi-Fi безопасности Bitdefender проанализирует, насколько безопасна беспроводная сеть и, при необходимости, порекомендует Вам использовать параметр Bitdefender VPN.

Bitdefender Wi-Fi Советник безопасности предоставляет информацию о:

- Домашние сети Wi-Fi
- Публичные сети Wi-Fi

17.3.1. Включение/отключение уведомлений Wi-Fi Советника безопасности

Чтобы включить или выключить уведомления Советника Безопасности:

1. Нажмите **Защита** в меню навигации интерфейса Bitdefender.
2. На панели **УЯЗВИМОСТИ** нажмите **Настройки**.
3. В окне **Настройки** включите или отключите параметр **Безопасность Wi-Fi**.

17.3.2. Настройка домашней сети Wi-Fi

Для того, чтобы приступить к настройке домашней сети:

1. Нажмите **Защита** в меню навигации интерфейса Bitdefender.
2. На панели **УЯЗВИМОСТЬ** нажмите **Безопасность Wi-Fi**.
3. На вкладке **ДОМАШНИЙ Wi-Fi** нажмите **ВЫБРАТЬ ДОМАШНИЙ WI-FI**

   Будет отображен список беспроводных сетей, к которым вы подключались ранее.
4. Выберите вашу домашнюю сеть и затем нажмите **ВЫБРАТЬ**.

Если домашняя сеть считается ненадежной или небезопасной, то отобразятся рекомендации по конфигурации, для повышения ее безопасности.

Чтобы удалить беспроводную сеть, которую вы установили в качестве домашней сети, нажмите кнопку **УДАЛИТЬ**.

17.3.3. Публичные Wi-Fi

При подключении к незащищенной или небезопасной беспроводной сети будет активирован профиль Публичный Wi-Fi. Во время работы в этом профиле, Bitdefender Antivirus Plus автоматически применяет следующие настройки программы:

- Активный Контроль Угроз включен
- Включены следующие настройки для параметра "Предотвращение угроз":
  - Зашифрованное веб-сканирование
  - Защита от мошенничества
  - Защита от фишинга
- Кнопка, открывающая Bitdefender Safepay™, доступна. В этом случае по умолчанию включена защита HotSpot для незащищенных сетей.

17.3.4. Проверка информации о сетях Wi-Fi

Чтобы проверить информацию о беспроводных сетях, к которым вы обычно подключаетесь:

1. Нажмите **Защита** в меню навигации интерфейса Bitdefender.
2. На панели **УЯЗВИМОСТЬ** нажмите **Безопасность Wi-Fi**.
3. В зависимости от необходимой информации выберите одну из двух вкладок: **ДОМАШНИЙ Wi-Fi** или **ОБЩЕСТВЕННЫЙ Wi-Fi**.
4. Затем нажмите **Подробнее** рядом с сетью, о которой вы хотите узнать больше информации.

Ниже приведены три типа беспроводных сетей, отфильтрованных по степени важности. Каждый тип обозначается специальным значком:

Небезопасный Wi-Fi - указывает на то, что уровень безопасности сети низкий. Это означает, что существует высокий риск для вас при

использовании ее, и не рекомендуется производить платежи или проверять банковские счета без дополнительной защиты. В таких ситуациях, рекомендуется использовать Bitdefender Safepay™ с защитой HotSpot для незащищенных сетей.

Умеренный Wi-Fi - указывает на то, что уровень безопасности сети умеренный. Это означает, что она может иметь уязвимости и не рекомендуется производить платежи или проверять банковские счета без дополнительной защиты. В таких ситуациях, рекомендуется использовать Bitdefender Safepay™ с защитой HotSpot для незащищенных сетей.

Безопасный Wi-Fi - указывает на то, что используемая сеть безопасна. В этом случае, вы можете использовать конфиденциальные данные для осуществления онлайн-операций.

При переходе по ссылке **Подробнее** в разделе каждой сети, отображаются следующие сведения:

- **Защищенный** - здесь вы можете посмотреть является или нет выбранная сеть безопасной. Незашифрованные сети могут оставлять данные, которые вы использовали, открытыми в сети.
- **Тип шифрования** - здесь вы можете просмотреть тип шифрования, используемый в выбранной сети. Некоторые типы шифрования могут быть небезопасны. Поэтому мы настоятельно рекомендуем вам проверить информацию о типе шифрования, чтобы быть уверенным в защите во время серфинга в Интернете.
- **Канал/Частота** - здесь вы можете просмотреть частоту канала, используемого в выбранной сети.
- **Надежность пароля** - здесь вы можете посмотреть надежность пароля. Обратите внимание, что сети, в которых используются слабые пароли, представляют собой мишень для кибер-преступников.
- **Тип входа** - здесь вы можете посмотреть защищена ли выбранная сеть с помощью пароля или нет. Настоятельно рекомендуется подключаться только к сетям, которые используют надежные пароли.
- **Тип аутентификации** - здесь вы можете просмотреть тип аутентификации, используемый в выбранной сети.

Держите параметр **Уведомлять** включенным для получения уведомлений каждый раз, когда ваша система подключается к этой сети.

18. SAFE FILES

Вирус-Вымогатель - это вредоносное программное обеспечение, которое атакует уязвимые системы, блокируя их, и просит денег, чтобы вернуть пользователю контроль над системой. Это вредоносное ПО действует хитро, показывая ложные сообщения чтобы убедить пользователя приступить к оплате.

Инфекция может распространяться через спам электронной почты, с помощью загрузки вложений, посещение зараженных веб-сайтов и установки вредоносных приложений, при этом никак не проявляя себя.

Вирус-Вымогатель может предпринять одно из следующих действий, препятствующих пользователю доступ к его системе:

- Шифрует конфиденциальные и личные файлы, не давая возможности расшифровки до тех пор, пока жертва не выплатит выкуп.
- Блокирует экран компьютера и выводит сообщение с просьбой о деньгах. В этом случае, файл не зашифрован, только пользователь об этом не знает и вынужден приступить к оплате.
- Блокирует запуск приложений.

С помощью Bitdefender Безопасные файлы Вы можете защитить от атак вируса-вымогателя личные файлы, например,документы, фотографии или фильмы.

Примечание

Активный контроль угроз и Безопасные файлы - два уровня защиты от вымогательства. Активный Контроль Угроз- средство, которое полностью останавливает атаки программ-вымогателей, при этом функция Безопасные файлы гарантирует, что ни один важный файл на вашем компьютере не зашифрован.

18.1. Включение или выключение Безопасных Файлов

Чтобы включить или отключить функцию Безопасные Файлы:

1. Нажмите **Защита** в меню навигации интерфейса Bitdefender.
2. На панели **БЕЗОПАСНЫЕ ФАЙЛЫ** включите или выключите переключатель.

Каждый раз, когда приложение будет пытаться получить доступ к защищенным файлам, Bitdefender будет отображать всплывающее окно. Вы можете разрешить или запретить доступ.

Примечание
Функция «Безопасные файлы» не включена по умолчанию.

18.2. Защита личных файлов от атак вымогателей

Если вы хотите хранить личные файлы под защитой:

1. Нажмите **Защита** в меню навигации интерфейса Bitdefender.
2. На панели **БЕЗОПАСНЫЕ ФАЙЛЫ** нажмите **Защищенные папки**.
3. При первом обращении к параметру "Защищенные папки" вы перейдете к этой опции. Чтобы продолжить, нажмите **ЗАЩИТИТЬ БОЛЬШЕ ПАПОК**
4. Выберите папку, которую Вы хотите защитить и нажмите **ОК** .

   Чтобы добавить новые папки, нажмите ссылку **Защитить больше папок** . Или перетащите папки в это окно.

Папки «Изображения», «Видео», «Музыка» и «Документы» защищены от атак угроз по умолчанию. Персональные данные, хранящиеся в Интернет-службах размещения файлов, таких как Box, Dropbox, Google Drive и OneDrive, также включаются в среду защиты при условии, что их приложения установлены в системе.

Во избежание замедления работы системы, мы рекомендуем Вам добавлять максимум 30 папок или сохранять несколько файлов в одной папке.

Примечание
Настраиваемые папки могут быть защищены только для текущих пользователей. Системные файлы не могут быть добавлены в исключения.

18.3. Настройка доступа к приложениям

Те приложения, которые попытаются изменить или удалить защищенные файлы могут быть помечены как потенциально опасные и будут добавлены в список Заблокированных приложений. Если такое

приложение блокируется, но Вы уверены в безопасности его поведения, Вы можете исключить его, выполнив следующие действия:

1. Нажмите **Защита** в меню навигации интерфейса Bitdefender.
2. На панели **БЕЗОПАСНЫЕ ФАЙЛЫ** нажмите **Доступ к приложению**.
3. В списке указаны приложения, которые запросили изменить файлы в ваших защищенных папках. Включите переключатель рядом с приложением, в безопасности которого вы уверенны.

В этом же окне можно отключить для некоторых приложений защиту от программ-вымогателей, отключив соответствующий переключатель.

Если Вы хотите добавить новые приложения в список, нажмите ссылку **Добавить новое приложение в список** .

18.4. Защита при запуске

Известно, что многие вредоносные приложения устанавливаются при запуске системы, что может серьезно повредить машину. Bitdefender Защита во время загрузки сканирует все критические системные области до загрузки всех файлов, с нулевым воздействием на систему.

Чтобы отключить "Защиту при запуске":

1. Нажмите **Защита** в меню навигации интерфейса Bitdefender.
2. На панели **БЕЗОПАСНЫЕ ФАЙЛЫ** нажмите **Настройки**.
3. Отключите **Защиту при запуске**.

Примечание
Приложения, добавленные к исключениям, будут сканироваться и обрабатываться соответствующим образом.

19. RANSOMWARE REMEDIATION

Bitdefender Ransomware Remediation создает резервные копии ваших файлов (например, документов, фотографий, видео или музыки), чтобы гарантировать их защиту от повреждения или потери в случае шифрования вымогателями. При каждом обнаружении атаки программы-вымогателя Bitdefender будет блокировать все процессы, затронутые атакой, и запустит процесс восстановления. Таким образом, вы сможете восстановить содержимое всех ваших файлов без требующегося в таких случаях выкупа.

19.1. Включение или отключение функции Ransomware Remediation

Чтобы включить или отключить функции Ransomware Remediation:

1. Нажмите **Защита** в меню навигации интерфейса Bitdefender.
2. На панели **RANSOMWARE REMEDIATION** включите или выключите переключатель.

> **Примечание**
> Для защиты файлов от программ-вымогателей, рекомендуется включить функцию Ransomware Remediation.

19.2. Включение и выключение автоматического восстановления

"Автоматическое восстановление" принимает меры для автоматического восстановления файлов в случае их шифрования программой-вымогателем.

Чтобы включить или отключить автоматическое восстановление:

1. Нажмите **Защита** в меню навигации интерфейса Bitdefender.
2. На панели **RANSOMWARE REMEDIATION** нажмите **Настройки**.
3. Чтобы включить или отключить **Автоматическое восстановление**.

19.3. Обзор автоматически восстановленных файлов

Если включена опция **Автоматическое восстановление**, Bitdefender автоматически восстановит файлы, зашифрованные программой-вымогателем. Таким образом, вы можете спокойно работать за компьютером, не беспокоясь за безопасность ваших файлов.

Для просмотра автоматически восстановленных файлов:

1. Нажмите **Уведомления** в меню навигации интерфейсBitdefender.
2. На вкладке **Все** выберите уведомление о последнем обнаруженном поведении программы-вымогателя, затем нажмите **Восстановленные файлы**.

   Отобразится список восстановленных файлов. Здесь также можно просмотреть расположение восстановленных файлов.

19.4. Ручное восстановление зашифрованных файлов

В том случае, если необходимо вручную восстановить файлы, зашифрованные программой-вымогателем, выполните следующие действия:

1. Нажмите **Уведомления** в меню навигации интерфейсBitdefender.
2. На вкладке **Все** выберите уведомление о последнем обнаруженном поведении программы-вымогателя, затем нажмите **Зашифрованные файлы**.
3. Отобразится список зашифрованных файлов.

   Нажмите **ВОССТАНОВИТЬ ФАЙЛЫ**, чтобы продолжить.
4. В случае сбоя процесса восстановления или его части необходимо выбрать место, в котором следует сохранить расшифрованные файлы. Нажмите **ВОССТАНОВИТЬ РАСПОЛОЖЕНИЕ**, затем выберите расположение на вашем компьютере.
5. Появится окно подтверждения.

   Нажмите **ЗАВЕРШИТЬ** для завершения процесса восстановления.

Файлы со следующими расширениями могут быть восстановлены в случае их шифрования:

.3g2; .3gp; .7z; .ai; .aif; .arj; .asp; .aspx; .avi; .bat; .bin; .bmp; .c; .cda; .cgi; .class; .com; .cpp; .cs; .css; .csv; .dat; .db; .dbf; .deb;.doc; .docx; .gif; .gz; .h264; .h; .flv; .htm; .html;.ico; .jar; .java; .jpeg; .jpg;.js; .jsp; .key; .m4v; .mdb; .mid; .midi; .mkv; .mp3; .mp4; .mov; .mpg; .mpeg; .ods; .odp;.odt; .ogg; .pdf; .pkg; .php; .pl; .png; .pps; .ppt; .pptx; .ps; .psd; .py; .rar; .rm; .rtf; .sav; .sql; .sh; .svg; .swift; .swf; .tar; .tex; .tif; .tiff; .txt; .xlr; .xls; .xlsx; .xml; .wmv; .vb; .vob; .wav; .wks; .wma; .wpl; .wps; .wpd; .wsf; .z; .zip;

19.5. Добавление приложений в исключения

Можно настроить правила исключений для надежных приложений, чтобы функция Ransowmare Remediation не блокировала их в том случае, если они выполняют действия, подобные программам-вымогателям.

Чтобы добавить приложения в список исключений функции Ransomware Remediation:

1. Нажмите **Защита** в меню навигации интерфейса Bitdefender.
2. На панели **RANSOMWARE REMEDIATION** нажмите **Исключения**.
3. Чтобы начать добавлять приложения в список, нажмите **Добавить новое приложение в список**.

20. ЗАЩИТА ВАШИХ УЧЕТНЫХ ДАННЫХ ПРИ ПОМОЩИ ПАРАМЕТРА "МЕНЕДЖЕР ПАРОЛЕЙ"

Мы используем компьютеры для покупки товаров или оплаты счетов в интернете, подключения к социальным медиа-платформам или пользуемся приложениями для обмена сообщениями.

Но известно, что не всегда удается легко запомнить пароль!

И если мы не будем осторожны при просмотре онлайн, наша личная информация, например, адрес электронной почты, идентификатор мгновенного обмена сообщениями или данные кредитной карты могут быть скомпрометированы.

Хранить пароли или личную информацию на бумажном носителе или в компьютере может быть опасно, потому что ею могут воспользоваться посторонние люди. Запомнить все пароли к учетным записям в интернете или любимым веб-сайтам нелегко.

Таким образом, встает вопрос: "А можем ли мы быть уверены в том, что найдем пароли, когда нам это необходимо?". И можем ли мы быть уверены в том, что наши секретные пароли всегда находятся в безопасности?

"Менеджер паролей" помогает отслеживать ваши пароли, защищать вашу конфиденциальность и обеспечивать безопасную работу в Интернете.

Используя единый мастер-пароль для доступа к учетным данным, "Менеджер паролей" упрощает хранение паролей в Кошельке.

В целях обеспечения наилучшей защиты конфиденциальной информации, параметр "Менеджер паролей" был интегрирован в Bitdefender Safepay™, и обеспечивает единое решение защиты при различных способах взлома конфиденциальных данных.

"Менеджер паролей" обеспечивает защиту следующей конфиденциальной информации:

- Личные данные, такие как адрес электронной почты или номер телефона
- Учетные данные для входа на веб-сайты
- Банковские реквизиты или номер кредитной карты

- Получать доступ к учетным записям электронной почты
- Пароли для приложений
- Пароли к сетям Wi-Fi

20.1. Создание новой базы данных Кошелька

Bitdefender Кошелек-это место, где вы можете хранить ваши персональные данные. Для упрощения работы с браузером необходимо создать базу данных Кошелька следующим образом:

1. Нажмите **Приватность** в меню навигации интерфейса Bitdefender.
2. На панели **МЕНЕДЖЕР ПАРОЛЕЙ** нажмите **Создать новый Кошелек**.
3. Нажмите **Создать новый**.
4. Введите необходимую информацию в соответствующих полях.
   - Этикетка Кошелька - введите уникальное имя для вашей базы данных Кошелька.
   - Мастер Пароль - введите пароль для вашего Кошелька.
   - Повторно введите пароль - введите пароль, который вы установили.
   - Подсказка - введите подсказку, чтобы запомнить пароль.
5. Нажмите **CONTINUE**.
6. На этом шаге вы можете выбрать хранение информации в облаке. Если вы выберите Да, банковская информация будет храниться локально на вашем устройстве. Выберите желаемый параметр и нажмите **ПРОДОЛЖИТЬ**.
7. Выберите веб-браузер, из которого вы хотите импортировать учетные данные.
8. Нажмите **ЗАВЕРШИТЬ**.

20.2. Импортировать существующую базу данных

Чтобы импортировать базу данных кошелька, хранящуюся локально:

1. Нажмите **Приватность** в меню навигации интерфейса Bitdefender.
2. На панели **МЕНЕДЖЕР ПАРОЛЕЙ** нажмите **Создать новый Кошелек**.
3. Нажмите **"ОТ ЦЕЛИ"**.

4. Перейдите к местоположению на устройстве, где требуется сохранить базу данных кошелька, а затем выберите имя для него.
5. Нажмите **Открыть**.
6. Укажите имя Вашего Кошелька и введите пароль, заданный при первоначальной установке.
7. Нажмите **ИМПОРТ**.
8. Выберите программы, из которых требуется импортировать учетные данные для "Кошелька", а затем кнопку **Завершить**.

20.3. Экспорт базы данных Кошелька

Чтобы экспортировать базу данных Кошелька:

1. Нажмите **Приватность** в меню навигации интерфейса Bitdefender.
2. На панели **МЕНЕДЖЕР ПАРОЛЕЙ** нажмите **Мои Кошельки**.
3. Нажмите на значок ⋮ желаемого кошелька, затем выберите **Экспорт**.
4. Выполните поиск местоположения базы данных кошелька и выберите ее (файл. db).
5. Нажмите **Сохранить**.

Примечание
Кошелек должен быть открыт для того, чтобы опция **Экспорт** была доступна.
Если кошелек, который необходимо экспортировать, заблокирован, нажмите кнопку **АКТИВИРОВАТЬ КОШЕЛЕК**, затем введите пароль, назначенный при создании кошелька.

20.4. Синхронизация ваших Кошельков в облаке

Чтобы включить или выключить синхронизацию бумажника с облаком:

1. Нажмите **Приватность** в меню навигации интерфейса Bitdefender.
2. На панели **МЕНЕДЖЕР ПАРОЛЕЙ** нажмите **Мои Кошельки**.
3. Нажмите значок ⋮ желаемого кошелька, затем выберите **Настройки**.

4. Выберите нужную опцию в появившемся окне, а затем нажмите **Сохранить**.

> **Примечание**
> Кошелек должен быть открыт для того, чтобы опция **Экспорт** была доступна.
> Если кошелек, который необходимо синхронизировать, заблокирован, нажмите кнопку **АКТИВИРОВАТЬ КОШЕЛЕК**, затем введите пароль, назначенный при создании кошелька.

20.5. Управление учетными данными Кошелька

Для управления вашими паролями:

1. Нажмите **Приватность** в меню навигации интерфейса Bitdefender.
2. На панели **МЕНЕДЖЕР ПАРОЛЕЙ** нажмите **Мои Кошельки**.
3. Выберите нужную базу данных для "Кошелька" и нажмите **АКТИВИРОВАТЬ КОШЕЛЕК**.
4. Введите мастер-пароль, а затем нажмите кнопку **ОК**.

Появится новое окно. Выберите необходимую категорию в верхней части окна:

- Личные
- Сайты
- Онлайн-банкинг
- Адреса электронной почты
- Приложения
- Сети Wi-Fi

Добавление/редактирование учетных записей

- Для того, чтобы добавить пароль, выберите необходимую категорию в верхней части окна, нажмите **+ Добавить элемент**, введите информацию в соответствующее поле и нажмите кнопку Сохранить.
- Для того, чтобы отредактировать запись в таблице, выберите соответствующую запись и нажмите кнопку **Редактировать**.
- Чтобы удалить запись, выберите ее, нажмите кнопку **Удалить**.

20.6. Включение и отключение защиты Менеджера паролей

Чтобы включить или отключить защиту Менеджера Паролей:

1. Нажмите **Приватность** в меню навигации интерфейса Bitdefender.
2. На панели **МЕНЕДЖЕР ПАРОЛЕЙ** включите или выключите переключатель.

20.7. Управление настройками Менеджера паролей

Чтобы детально настроить мастер-пароль:

1. Нажмите **Приватность** в меню навигации интерфейса Bitdefender.
2. На панели **МЕНЕДЖЕР ПАРОЛЕЙ** нажмите **Настройки**.
3. Выберите вкладку **Security Settings**.

Доступны следующие опции:

- **Спрашивать мастер-пароль при включении компьютера** - при выполнении входа на устройство вам будет предложено ввести мастер-пароль.
- **Запрашивать мастер-пароль при открытии браузера и приложений** - система предложит вам ввести мастер-пароль при входе в браузер или приложение.
- **Не спрашивать мастер-пароль** - ввод мастер-пароля при доступе к компьютеру, браузеру или приложению запрашиваться не будет.
- **Автоматически блокировать Кошелек, когда я оставляю устройство без присмотра** - вам будет предложено ввести мастер-пароль, когда вы вернетесь к устройству через 15 минут.

> **Важно**
> Обязательно запомните свой мастер-пароль или храните его в надежном месте. Если вы забыли пароль, вам придется переустановить программу или обратиться в службу поддержки Bitdefender.

Улучшение навигации

Чтобы выбрать браузеры или приложения, в которые вы хотите интегрировать "Менеджер паролей":

1. Нажмите **Приватность** в меню навигации интерфейса Bitdefender.
2. На панели **МЕНЕДЖЕР ПАРОЛЕЙ** нажмите **Настройки**.
3. Выберите вкладку **Plugins**.

   Проверьте приложение, чтобы использовать "Менеджер паролей" и улучшить Вашу навигацию:

   - Internet Explorer
   - Mozilla Firefox
   - Google Chrome
   - Безопасный платеж

Настройка "Автозаполнение"

Функция автозаполнения упрощает подключение к любимым веб-сайтам или вход с помощью учетных записей в Интернете. При первом вводе учетных данных для входа и персональных данных в веб-браузер они автоматически заносятся в Кошелек.

Чтобы сконфигурировать настройки **Автозаполнение**:

1. Нажмите **Приватность** в меню навигации интерфейса Bitdefender.
2. На панели **МЕНЕДЖЕР ПАРОЛЕЙ** нажмите **Настройки**.
3. Выберите вкладку **Autofill settings**.
4. Настройте следующие опции:

   - **Настроить, как Password Manager будет обеспечивать защиту учетных данных**:
     - **Сохранить данные в кошельке автоматически** -логин и другие идентифицируемые сведения, такие как личные данные и сведения о кредитной карте, автоматически сохраняются и обновляются в Кошельке.
     - **Спрашивать всегда** - система будет спрашивать вас каждый раз, как захотите добавить свои регистрационные данные в Кошелек.

- Функция **Не сохранять. Я обновлю информацию вручную** - регистрационные данные можно добавить в Кошелек только вручную.

- **Автозаполнение учетных данных**:
  - Функция **Автозаполнение учетных данных всегда** - учетные данные вводятся автоматически в браузере.
- **Автозаполнения форм**:
  - **Подсказать мои варианты заполнения когда я посещаю страницу с формами** - всплывающее окно с вариантами заполнения появится всегда, когда Bitdefender обнаруживает что вы хотите произвести платеж или выполнить вход.

Управление информацией Менеджера паролей из вашего браузера

Вы можете легко управлять информацией Менеджера паролей непосредственно из вашего браузера, чтобы иметь все важные данные под рукой. Надстройка Bitdefender Кошелька поддерживается следующими браузерами: Google Chrome, Internet Explorer и Mozilla Firefox.

Чтобы получить доступ к расширению Кошелька Bitdefender, откройте веб-браузер, разрешите установку надстройки и щелкните значок на панели инструментов.

BitdefenderКошелек содержит следующие параметры:

- Открыть Кошелек - открывает кошелек.
- Заблокировать кошелек - блокирует Кошелек.
- Веб-страницы - открывает подменю со всеми логинами веб-сайтов, хранящихся в "Кошельке". Нажмите **Добавить веб-страницу**, чтобы добавить новые веб-сайты в список.
- Заполнить формы - открывает подменю, содержащее информацию, добавленную для определенной категории. Отсюда вы можете добавлять новые данные в ваш Кошелек.
- Генератор паролей - позволяет генерировать случайные пароли, которые вы можете использовать для новых или существующих

учетных записей. Нажмите **Показать дополнительные настройки**, чтобы настроить сложность пароля.

- Настройки-открывает окно настройки Менеджера паролей.
- Сообщить о проблеме-сообщите о любых неполадках, возникающих в Менеджере паролей Bitdefender.

21. VPN

Приложение VPN можно установить из Вашего Bitdefender и использовать каждый раз, когда Вы хотите добавить дополнительный уровень защиты к Вашему соединению. VPN служит в качестве туннеля между устройством и подключенной сетью для защиты соединения, шифрования данных с помощью банковского шифрования и сокрытия IP-адреса, где бы Вы ни находились. Ваш трафик перенаправляется через отдельный сервер, что гарантирует невозможность идентификации Вашего устройства через множество других средств, используемых нашими сервисами. Кроме того, при подключении к Интернету через Bitdefender VPN Вы можете получить доступ к контенту, который обычно ограничен в определенных областях.

Примечание
Некоторые страны практикуют интернет-цензуру, поэтому использование VPN на их территории запрещено законом. Во избежание юридических последствий при первом использовании функции Bitdefender VPN появится предупреждающее сообщение. Продолжая использовать эту функцию, Вы подтверждаете, что знаете о применимых правилах страны и понимаете риски, с которыми можете столкнуться.

21.1. Установка VPN

Приложение VPN можно установить из интерфейса Bitdefender следующим образом:

1. Нажмите **Приватность** в меню навигации интерфейса Bitdefender.
2. В области **VPN** нажмите **Установить VPN**.
3. В окне с описанием приложения VPN ознакомьтесь с **Соглашением о Подписке**, затем нажмите **УСТАНОВИТЬ BITDEFENDER VPN**.

   Подождите несколько минут, пока файлы загрузятся и установятся
4. Нажмите **ОТКРЫТЬ BITDEFENDER VPN** для завершения процесса установки.

Примечание
Для установки Bitdefender VPN требуется Net Framework 4. 5. 2 или выше. В том случае, если Вы не установите этот пакет, появится окно оповещения. Нажмите **установить. Net Framework** , для перехода на

страницу, откуда можно загрузить новейшую версию этого программного обеспечения.

21.2. Открытие VPN

Чтобы получить доступ к основному интерфейсу VPN Bitdefender, используйте один из следующих способов:

- Из области уведомлений
  1. Щелкните правой кнопкой мыши значок в области уведомлений, затем нажмите **Показать**.
- Из интерфейса Bitdefender:
  1. Нажмите **Приватность** в меню навигации интерфейса Bitdefender.
  2. На панели **VPN** нажмите **Открыть VPN**.

21.3. Интерфейс VPN

Интерфейс VPN отображает состояние приложения, подключенного или отключенного. Расположение сервера для пользователей с бесплатной версией автоматически устанавливается Bitdefender на более подходящий сервер, в то время как у премиум-пользователей есть возможность изменить местоположение сервера, к которому они хотят подключиться. Для получения дополнительной информации о лицензировании VPN см. «*Подписки*» (p. 129).

Чтобы подключиться или отключиться, просто нажмите на статус, отображаемый в верхней части экрана, или щелкните правой кнопкой мыши значок области уведомлений. Значок в области уведомлений отображает зеленую галочку при подключении VPN и красную галочку при отключении VPN.

При подключении, истекшее время и IP-адрес, автоматически назначенные Вашему устройству, отображаются в нижней части интерфейса.

Чтобы получить доступ к дополнительным параметрам, зайдите в область **Меню**, нажав в верхней левой части. Здесь доступны следующие варианты:

- В области **Моя учетная запись** - отображаются сведения о вашей учетной записи Bitdefender и подписке VPN. Нажмите **Переключить учетную запись**, если вы хотите войти с другой учетной записью.

- **Настройки** - Вы можете настроить поведение Вашего продукта исходя из Ваших потребностей:
  - получать уведомления, когда VPN автоматически соединяется или отключается
  - автоматически запускать приложение VPN при загрузке Windows
  - Автозапуск приложения VPN во время подключения устройства к небезопасной сети.
- **Обновить до Premium** - если вы используете бесплатную версию, вы можете перейти на премиум-план отсюда.
- **Техническая поддержка** - переход в Центр поддержки, где можно ознакомиться со статьей об использовании Bitdefender VPN.
- **Информация** - отображение информации об установленной версии.

21.4. Подписки

Bitdefender VPN предлагает бесплатную ежедневную квоту трафика на 200 МБ на каждое устройство для защиты Вашего подключения каждый раз, когда Вам понадобится, и автоматически подключается к оптимальному местоположению сервера.

Чтобы получить неограниченный трафик и доступ к контенту во всем мире, выбирая расположение сервера по своему усмотрению, обновите до премиум-версии.

Вы можете обновить продукт до версии Bitdefender Premium VPN в любое время, нажав кнопку **ПОЛУЧИТЬ НЕОГРАНИЧЕННЫЙ ТРАФИК**, доступную в интерфейсе продукта.

Подписка Bitdefender Premium VPN не зависит от подписки Bitdefender Antivirus Plus, это значит,что вы можете пользоваться ее возможностями, независимо от вашего решения безопасности. В случае истечения срока действия подписки Bitdefender Premium VPN при активной Bitdefender Antivirus Plus, Вы вернетесь к бесплатной версии.

Bitdefender VPN представляет собой кроссплатформенное средство, доступное в Bitdefender, совместимых с Windows, Mac OS, Android и iOS. После того, как Вы перейдете на премиум-план, Вы получите возможность пользоваться всеми продуктами при том условии, что вход в систему будет осуществляться под той же учетной записью Bitdefender.

22. БЕЗОПАСНЫЙ ПЛАТЕЖ - БЕЗОПАСНОСТЬ ДЛЯ ОНЛАЙН-ТРАНЗАКЦИЙ

Компьютер быстро становится основным инструментом для покупок и банковских операций. Оплата счетов, перевод денег, покупка товаров и все остальное становится проще и быстрее.

Это включает отправку личной информации, данных счетов и кредитных карт, пароли и другие виды частной информации через Интернет, иными словами, именно тот тип потока информации, в котором кибер-преступники очень заинтересованы. Хакеры неустанны в своих попытках украсть эту информацию, так что вы никогда не сможете быть в полной безопасности при выполнении онлайн-транзакций.

Bitdefender Safepay™ это, прежде всего, защищенный браузер, изолированная среда, которая призвана сохранить ваш онлайн-банкинг, электронные покупки и любой другой тип интернет-транзакций приватными и безопасными.

Для лучшей защиты конфиденциальности, Bitdefender "Менеджер паролей" был интегрирован в Bitdefender Safepay ™ для защиты ваших учетных данных, когда вы хотите получить доступ к приватным местам в сети. Для получения более подробной информации, обратитесь к «*Защита ваших учетных данных при помощи параметра "Менеджер паролей"*» (p. 119).

Bitdefender Safepay™ предлагает следующие возможности:

- Он блокирует доступ к рабочему столу и любые попытки делать снимки экрана.
- Он защищает ваш секретный пароль, когда вы просматриваете информацию в интернете через параметр "Менеджер паролей".
- Он поставляется с виртуальной клавиатурой, которая, при использовании, делает невозможным для хакеров считывать ваши нажатия клавиш.
- Полностью независим от других браузеров.
- Он поставляется со встроенной защитой Hotspot, которая будет использоваться, когда ваш компьютер подключен к незащищенным сетям Wi-Fi.

- Он поддерживает закладки и позволяет перемещаться между любимыми банковскими/торговыми сайтами.
- Это не ограничивается банковскими операциями и онлайн-шопингом. Любой веб-сайт может быть открыт в Bitdefender Safepay™.

22.1. Использование Bitdefender Safepay™

По умолчанию Bitdefender определяет, когда вы переходите к Интернет-банкингу или Интернет-магазину в любом браузере на вашем компьютере, и предлагает вам запустить его в Bitdefender Safepay™.

Чтобы получить доступ к основному интерфейсу Bitdefender Safepay™, используйте один из следующих способов:

- Из интерфейса Bitdefender:
  1. Нажмите **Приватность** в меню навигации интерфейса Bitdefender.
  2. На панели **Safepay** нажмите **Открыть Safepay**.
- Из Windows:
  - В **Windows 7**:
    1. Нажмите **Пуск** и перейдите в **Все программы**.
    2. Нажмите **Bitdefender**.
    3. Нажмите **Bitdefender Safepay™**.
  - В **Windows 8 и Windows 8.1**:

    Введите Bitdefender Safepay™ в Стартовом окне Windows (например, можно вводить "Bitdefender Safepay™" непосредственно в Стартовом окне) и затем щелкните по его значку.
  - В **Windows 10**:

    Введите "Bitdefender Safepay™" в поле поиска на панели задач и щелкните ее значок.

Примечание

Если плагин Adobe Flash Player не установлен или устарел, то Bitdefender выведет на экран сообщение. Нажмите соответствующую кнопку, чтобы продолжить.
После того, как процесс установки завершен, необходимо заново открыть браузер Bitdefender Safepay™, чтобы продолжить работу.

Если вы ранее пользовались веб-браузерами, то у вас не будет никаких проблем с Bitdefender Safepay™ - он выглядит, как обычный браузер:

- введите URL-адрес в адресной строке.
- Добавьте вкладки для посещения нескольких веб-сайтов в окнеBitdefender Safepay™, нажав
- перемещайтесь назад и вперед, а также обновляйте страницы с помощью соответственно.
- войдите в Bitdefender Safepay™ настройки нажав и выберите **Настройки**.
- защитите ваши пароли с помощью Менеджера паролей нажатием на .
- управлять ваши Закладками, нажав рядом с адресной строкой.
- откройте виртуальную клавиатуру, нажав .
- чтобы увеличить или уменьшить размер браузера, нажмите одновременно **Ctrl** и **+/-** на цифровой клавиатуре.
- чтобы просмотреть информацию о Bitdefender нажмите и выберите **О продукте**.
- чтобы распечатать важную информацию, нажмите .

Примечание
Чтобы переключиться между Bitdefender Safepay ™ и рабочим столом Windows, нажмите клавиши **Alt+Tab** или в верхней левой части окна нажмите **Переключиться на рабочий стол**.

22.2. Настройка параметров

Нажмите и выберите **Настройки**, чтобы настроить Bitdefender Safepay™:

Список доменов

Выберите режим работы Bitdefender Safepay™ для посещения веб-сайтов из конкретных доменов в обычных веб-браузерах, добавив их в список доменов и выбрав режим работы для каждого из них:

- Автоматически открывать в Bitdefender Safepay™.
- Предлагать Bitdefender выбор действий каждый раз.

- Никогда не используйте Bitdefender Safepay™ при посещении страницы домена в обычном браузере.

Блокировка всплывающих окон

Вы можете заблокировать всплывающие окна, щелкнув соответствующий переключатель.

Вы также можете создать список сайтов, в которых будут разрешены всплывающие окна. Список должен содержать только веб-сайты, которым вы полностью доверяете.

Для того, чтобы добавить сайт в белый список, введите его адрес в соответствующем поле и нажмите **Добавить домен**.

Чтобы удалить веб-сайт из списка, выберите X, соответствующий нужному содержимому.

Управление плагинами

Вы можете включить или отключить определенные плагины в модуле Bitdefender Safepay™.

Управление сертификатами

Вы можете импортировать сертификаты из вашей системы в хранилище сертификатов.

Выберите **Импортировать сертификаты** и следуйте инструкциям мастера, чтобы использовать сертификаты в Bitdefender Safepay™.

Автоматический запуск виртуальной клавиатуры в полях пароля

Виртуальная Клавиатура автоматически появится при выборе поля пароля.

Используйте соответствующий переключатель, чтобы включить или отключить эту функцию.

Запросить подтверждение перед печатью

Включите эту опцию, если Вы даете свое подтверждение до начала процесса печати.

22.3. Управление закладками

Если вы отключили автоматическое обнаружение некоторых или всех веб-сайтов, или Bitdefender просто не обнаруживает определенные веб-сайты, вы можете добавить закладки в Bitdefender Safepay™, чтобы в дальнейшем можно было легко запускать избранные веб-сайты.

Выполните следующие действия для добавления URL-адрес в закладки Bitdefender Safepay™:

1. Нажмите значок рядом с адресной строкой, чтобы открыть страницу закладки.

   Примечание
   Страница Закладок открывается по умолчанию при запуске Bitdefender Safepay™.

2. Нажмите **+** кнопку для добавления новой закладки.
3. Введите URL-адрес и название закладки и нажмите **Создать**. Выберите опцию **Автоматически открывать в Безопасном платеже**, если вы хотите чтобы закладки открывались с Bitdefender Safepay™ каждый раз при обращении к ним. Также URL добавляется в список доменов на странице параметры.

22.4. Отключение уведомлений Safepay

Продукт Bitdefender настроен на уведомления через всплывающее окно при обнаружении банковского сайта.

Чтобы отключить уведомления Safepay:

1. Нажмите **Приватность** в меню навигации интерфейса Bitdefender.
2. На панели **Safepay** нажмите **Настройки**.
3. Отключите **Уведомления Safepay**.

22.5. Использование VPN с браузером Safepay

Можно настроить продукт Bitdefender на автоматический запуск приложения VPN одновременно с Safepay для проведения онлайн-платежей в безопасной среде при подключении к незащищенным сетям.

Чтобы начать использовать приложение VPN совместно с Safepay:

1. Нажмите **Приватность** в меню навигации интерфейса Bitdefender.
2. На панели **Safepay** нажмите **Настройки**.
3. Включите **Использовать VPN с Safepay**.

23. ЗАЩИТА ДАННЫХ

23.1. Окончательное удаление файлов

При удалении файла он больше не может быть доступен с помощью обычных средств. Однако файл продолжает храниться на жестком диске до тех пор, пока он не будет перезаписан при копировании новых файлов.

Bitdefender Файловый шредер позволяет окончательно удалить данные, физически удалив их с жесткого диска.

Файлы и папки на компьютере можно быстро уничтожить через контекстное меню Windows выполнив следующие действия:

1. Щелкните правой кнопкой мыши по файлу или папке, которую хотите удалить.
2. Выберите **Bitdefender** > **Файловый шредер** в появившемся контекстном меню.
3. Нажмите **УДАЛИТЬ НАВСЕГДА** и подтвердите, что Вы хотите продолжить процесс.

   Дождитесь завершения процедуры уничтожения файлов Bitdefender.
4. Отобразятся результаты. Нажмите **ЗАВЕРШИТЬ** для выхода из мастера

Кроме того, Вы можете удалить файлы с интерфейса Bitdefender следующим образом:

1. Нажмите **Приватность** в меню навигации интерфейса Bitdefender.
2. На панели **ЗАЩИТА ДАННЫХ** выберите **Файловый шредер**.
3. Следуйте инструкциям мастера Файлового шредера:
   a. Нажмите кнопку **ДОБАВИТЬ ПАПКИ**, чтобы добавить файлы или папки, которые вы хотите удалить навсегда.

      Также можно перетащить эти файлы или папки в это окно.
   b. Нажмите **УДАЛИТЬ НАВСЕГДА** и подтвердите, что Вы хотите продолжить процесс.

      Дождитесь завершения процедуры уничтожения файлов Bitdefender.

c. **Сводка результатов**

Отобразятся результаты. Нажмите **ЗАВЕРШИТЬ** для выхода из мастера

24. USB IMMUNIZER

Функция автозапуска, встроенная в операционные системы Windows, является очень полезным инструментом, который позволяет компьютерам автоматически выполнять файл с носителя, подключенного к нему. Например, установка программного обеспечения может запускаться автоматически при вводе компакт-диска в оптический дисковод.

К сожалению эта функция также может быть использована угрозами для автоматического запуска и проникновения в ваш компьютер с перезаписываемых носителей, таких как USB-накопитель и карты памяти, подключенные через устройства чтения карт памяти. В последние годы были созданы многочисленные атаки, основанные на автозапуске.

С USB-иммунизатором вы можете предотвратить автоматический запуск угроз на дисках с файловой системой NTFS, FAT32 или FAT. После того как USB-устройство будет иммунизировано, угрозы больше не смогут настроить его для запуска определенного приложения при подключении устройства к компьютеру под управлением Windows.

Чтобы иммунизировать USB-устройство:

1. Подключите флэш-накопитель к компьютеру.
2. Откройте ваш компьютер, чтобы найти съемное запоминающее устройство и щелкните правой кнопкой мыши по его значку.
3. В контекстном меню выберите пункт **Bitdefender** и выберите **Иммунизировать этот диск**.

> **Примечание**
> Если диск уже был иммунизирован, то вместо опции Иммунизация появится сообщение **Устройство USB защищено от угроз на основе автозапуска**.

Во избежание проникновения угроз с неиммунизированных устройств отключите функцию автозапуска мультимедиа. Для получения более подробной информации, обратитесь к «*Использование автоматического мониторинга уязвимостей*» (p. 107).

ОПТИМИЗАЦИЯ СИСТЕМЫ

25. ПРОФИЛИ

Ежедневная работа, просмотр фильмов или игр может привести к снижению скорости работы системы, особенно если они работают одновременно с процессами обновления Windows и задачами обслуживания. Теперь с Bitdefender вы можете выбрать и применить нужный профиль, который вносит коррективы системы, которые повышают производительность определенных установленных приложений.

Bitdefender предоставляет следующие профили:

- Профиль Работа
- Профиль "Фильм"
- Профиль Игры
- Профиль публичный Wi-Fi
- Профиль Режим работы от батарей

Если вы решили не использовать **Профили**, то профиль по умолчанию, называемый **Стандартный** включен и не вносит никакую оптимизацию в систему.

В зависимости от ваших действий, следующие настройки продукта применяются при активации профилей Работа, Фильм или Игра:

- Все оповещения Bitdefender и всплывающие окна отключены.
- Автоматическое обновление отложено.
- Плановое сканирование отложено.
- Поисковый советник отключен.
- Уведомления о специальных предложениях отключены.

В зависимости от ваших действий, при активации профилей Работа, Фильм или Игра применяются следующие системные настройки:

- Автоматические обновления Windows отложены.
- Предупреждения и всплывающие окна Windows будут отключены.
- Ненужные фоновые программы приостановлены.

- Визуальные эффекты корректируется для лучшей производительности.
- Задачи технического обслуживания отложены.
- Параметры плана питания корректируется.

Во время работы в профиле Публичный Wi-Fi, Bitdefender Antivirus Plus устанавливается для автоматического выполнения следующих настроек программы:

- Активный Контроль Угроз включен
- Включены следующие настройки для параметра "Предотвращение угроз":
  - Зашифрованное веб-сканирование
  - Защита от мошенничества
  - Защита от фишинга

25.1. Профиль Работа

Запуск нескольких задач к работе, таких как отправка электронных писем, видео-общение с коллегами, работающими удаленно или использование дизайнерских приложений, может повлиять на производительность системы. Профиль Работа был разработан, чтобы помочь вам повысить эффективность работы, отключив некоторые из ваших фоновых служб и задач обслуживания.

Настройка профиля Работа

Чтобы настроить действия, которые должны быть выполнены во время работы в профиле Работа:

1. Нажмите **Настройки** в меню навигации интерфейс Bitdefender.
2. Выберите вкладку **Profiles**.
3. Нажмите кнопку **НАСТРОИТЬ** в области профиля Работа.
4. Выберите настройки системы, которые вы хотите применить, установив следующие параметры:
   - Повышение производительности работающих приложений
   - Оптимизация настроек продукта для профиля Работа

- Отложить фоновые программы и задачи по обслуживанию
- Отложить автоматические обновления Windows

5. Нажмите **СОХРАНИТЬ**, чтобы сохранить изменения и закрыть окно.

Добавление приложений в список профиля Работа вручную

Если при запуске определенного рабочего приложения Bitdefender не входит автоматически в профиль "Работа", вы можете вручную добавить приложение в **Список рабочих приложений**.

Чтобы вручную добавить приложения в "Список рабочих приложений" в профиле "Работа":

1. Нажмите **Настройки** в меню навигации интерфейс Bitdefender.
2. Выберите вкладку **Profiles**.
3. Нажмите кнопку **НАСТРОИТЬ** в области профиля Работа.
4. В окне **Настройки профиля Работа** нажмите **Список приложений**.
5. Нажмите **ДОБАВИТЬ**.

   Появится новое окно. Найдите исполняемый файл приложения, выделите его и нажмите **ОК**, чтобы добавить его в список.

25.2. Профиль "Фильм"

Отображение видео контента высокого качества, таких как фильмов высокой четкости, требует значительных системных ресурсов. Профиль "Фильм" регулирует настройки системы и продукта, чтобы вы могли наслаждаться бесперебойным просмотром фильма.

Настройка профиля "Фильм"

Чтобы настроить действия, выполняемые в профиле "Фильм":

1. Нажмите **Настройки** в меню навигации интерфейс Bitdefender.
2. Выберите вкладку **Profiles**.
3. Нажмите кнопку **НАСТРОИТЬ** в области профиля "Фильм".
4. Выберите настройки системы, которые вы хотите применить, установив следующие параметры:

- Повышение производительности видео-проигрывателей
- Оптимизация параметров продукта для профиля "Фильм"
- Отложить фоновые программы и задачи по обслуживанию
- Отложить автоматические обновления Windows
- Настройка параметров питания для просмотра кино

5. Нажмите **СОХРАНИТЬ**, чтобы сохранить изменения и закрыть окно.

Добавление видео-проигрывателей вручную в список профиля "Фильм"

Если при запуске определенного приложения видео-проигрывателя Bitdefender автоматически не переходит в профиль "Фильм", можно вручную добавить приложение в **Список приложений профиля Фильм**.

Чтобы вручную добавить видео-проигрыватели в список профиля "Фильм":

1. Нажмите **Настройки** в меню навигации интерфейс Bitdefender.
2. Выберите вкладку **Profiles**.
3. Нажмите кнопку **НАСТРОИТЬ** в области профиля "Фильм".
4. В окне **Настройки профиля Фильм** нажмите **Список видео-проигрывателей**.
5. Нажмите **ДОБАВИТЬ**.

   Появится новое окно. Найдите исполняемый файл приложения, выделите его и нажмите **ОК**, чтобы добавить его в список.

25.3. Профиль Игры

Наслаждайтесь бесперебойной игрой без нагрузки на систему и замедления. С помощью поведенческой эвристики вместе со списком известных игр, Bitdefender может автоматически обнаруживать запущенные игры и оптимизировать системные ресурсы, чтобы вы могли наслаждаться игрой беспрерывно.

Настройка профиля Игра

Настройка действий, выполняемых в профиле Игра:

1. Нажмите **Настройки** в меню навигации интерфейс Bitdefender.
2. Выберите вкладку **Profiles**.
3. Нажмите кнопку **НАСТРОИТЬ** в области профиля Игра.
4. Выберите настройки системы, которые вы хотите применить, установив следующие параметры:
   - Повышение производительности игр
   - Оптимизация параметров продукта для профиля Игра
   - Отложить фоновые программы и задачи по обслуживанию
   - Отложить автоматические обновления Windows
   - Настройка параметров плана питания для игр
5. Нажмите **СОХРАНИТЬ**, чтобы сохранить изменения и закрыть окно.

Добавление игры вручную в Список игр

Если при запуске определенного приложения или игры Bitdefender не переходит автоматически в профиль "Игра", вы можете вручную добавить приложение в **Список приложений для игр**.

Чтобы вручную добавить игры в "Список игр" в профиле "Игра":

1. Нажмите **Настройки** в меню навигации интерфейс Bitdefender.
2. Выберите вкладку **Profiles**.
3. Нажмите кнопку **НАСТРОИТЬ** в области профиля Игра.
4. В окне **Настройки профиля "Игра"** нажмите **Список игр**.
5. Нажмите **ДОБАВИТЬ**.

   Появится новое окно. Найдите исполняемый файл игры, выделите его и нажмите **ОК**, чтобы добавить его в список.

25.4. Профиль публичный Wi-Fi

Отправка электронных писем, ввод конфиденциальных учетных данных или совершение покупок в Интернете при подключении к небезопасным беспроводным сетям может подвергнуть риску ваши персональные данные. Профиль Публичный Wi-Fi регулирует настройки продукта,

чтобы у вас была возможность совершать платежи в Интернете и использовать конфиденциальную информацию в защищенной среде.

Настройка профиля Публичный Wi-Fi

Чтобы настроить Bitdefender на применение параметров продукта при подключении к небезопасной беспроводной сети:

1. Нажмите **Настройки** в меню навигации интерфейс Bitdefender.
2. Выберите вкладку **Profiles**.
3. Нажмите кнопку **НАСТРОИТЬ** в области профиля Публичный Wi-Fi.
4. Оставьте флажок **Регулировать настройки продукта для повышения защиты при подключении к небезопасной публичной сети Wi-Fi** включенным.
5. Нажмите **Сохранить**.

25.5. Профиль Режим работы от батарей

Профиль Режим батареи разработан специально для пользователей ноутбуков и планшетных ПК. Его целью является минимизация воздействия как системы, так и Bitdefender на потребление электроэнергии, когда уровень заряда батареи ниже уровня по умолчанию или ниже чем вы установили.

Настройка профиля Режим Батареи

Чтобы настроить профиль Режим батареи:

1. Нажмите **Настройки** в меню навигации интерфейс Bitdefender.
2. Выберите вкладку **Profiles**.
3. Нажмите кнопку **НАСТРОИТЬ** в области профиля Режим батареи.
4. Выберите настройки системы для применения, установив следующие параметры:
   - Оптимизация настроек продукта для Режима Батарей.
   - Отложить фоновые программы и задачи по обслуживанию.
   - Отложить автоматические обновления Windows
   - Настройка параметров плана питания для Режима Батареи.

- Отключите внешние устройства и сетевые порты.

5. Нажмите **СОХРАНИТЬ**, чтобы сохранить изменения и закрыть окно.

Введите допустимое значение в поле Счетчик или выберите его, используя клавиши со стрелками вверх и вниз, чтобы указать, когда система должна начать работать в Режиме батареи. По умолчанию режим активируется, когда уровень заряда аккумулятора опускается ниже 30%.

Следующие параметры продукта применяются, когда Bitdefender работает в профиле Режим батареи:

- Bitdefender Автоматическое обновление отложено.
- Плановое сканирование отложено.
- Виджет безопасности выключен.

Bitdefender определяет, когда ваш ноутбук переключился на питание от аккумулятора и на основе уровня заряда аккумулятора он автоматически переходит в Режим Батареи. Аналогично, Bitdefender автоматически выходит из Режима батареи, когда он обнаруживает, что ноутбук больше не работает от аккумулятора.

25.6. Оптимизация в режиме реального времени

Bitdefender Оптимизация в режиме реального времени — это плагин, который улучшает производительность вашей системы молча, в фоновом режиме, убедившись, что вы не прерываетесь, пока находитесь в профиле режима. В зависимости от нагрузки процессора, плагин отслеживает все процессы, ориентируясь на те, которые занимают более высокую нагрузку, чтобы настроить их на ваши потребности.

Чтобы включить или выключить Оптимизацию в реальном времени:

1. Нажмите **Настройки** в меню навигации интерфейс Bitdefender.
2. Выберите вкладку **Profiles**.
3. Прокрутите вниз, пока не увидите параметр оптимизации в режиме реального времени, затем используйте соответствующий переключатель, чтобы включить или выключить его.

УСТРАНЕНИЕ НЕПОЛАДОК

26. РЕШЕНИЕ ОБЩИХ ВОПРОСОВ.

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.

- «*Система работает медленно*» (p. 147)
- «*Сканирование не начинается*» (p. 149)
- «*Я больше не могу использовать приложение*» (p. 151)
- «*Что делать, если Bitdefender блокирует безопасный веб-сайт или онлайн приложение*» (p. 152)
- «*Что делать, если Bitdefender определяет безопасное приложение в качестве программы-вымогателя*» (p. 153)
- «*Обновление Bitdefender при низкой скорости подключения к Интернету*» (p. 154)
- «*Службы Bitdefender не отвечают*» (p. 154)
- «*Функция "Автозаполнение" в Кошельке не работает*» (p. 155)
- «*Сбой удаления Bitdefender*» (p. 156)
- «*Моя система не загружается после установки Bitdefender*» (p. 157)

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) «*Обращение за помощью*» (p. 173).

26.1. Система работает медленно

Как правило, после установки программного обеспечения безопасности допускается незначительное снижение быстродействия системы.

Если вы заметили значительное замедление, эта проблема может появиться по следующим причинам:

- **В системе установлены другие решения безопасности, помимо Bitdefender.**

Несмотря на то, что Bitdefender выполняет поиск и удаление программ безопасности, обнаруженных во время установки, рекомендуется заранее удалить остальные решения безопасности перед установкой Bitdefender. Для получения более подробной информации, обратитесь к «*Как удалить другие решения безопасности?*» (p. 73).

- **Не соблюдены минимальные системные требования для запуска Bitdefender.**

  Если компьютер не соответствует минимальным системным требованиям, это может стать причиной медленной работы системы, особенно при одновременной работе нескольких приложений. Для получения более подробной информации, обратитесь к «*Минимальные системные требования*» (p. 3).

- **У вас установлены неиспользуемые приложения**.

  На любом компьютере имеются программы или приложения, которые не используются. И многие нежелательные программы работают в фоновом режиме, занимая место на диске и в памяти. Если программа не используется, удалите ее. Это также допустимо для любого другого предварительно установленного программного обеспечения или пробного приложения, которое вы забыли удалить.

  > **Важно**
  > Если вы подозреваете, что программа или приложение являются неотъемлемой частью вашей операционной системы, не удаляйте ее и не обращайтесь за помощью в службу поддержки клиентов Bitdefender.

- **ваша система может быть заражена**.

  Угрозы могут негативно повлиять на производительность системы и ее общее поведение. Шпионские программы, вирусы, трояны и рекламные ПО - все это сказывается на производительности компьютера. Регулярно выполняйте сканирование системы (не реже одного раза в неделю). Рекомендуется использовать Сканирование системы Bitdefender, поскольку оно проверяет на наличие всех типов угроз, подвергающих опасности вашу систему.

  Чтобы запустить Сканирование Системы:

  1. Нажмите **Защита** в меню навигации интерфейса Bitdefender.

2. В области **АНТИВИРУС** нажмите **Системное сканирование**.
3. Следуйте инструкциям мастера.

26.2. 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 переустановите Bitdefender:

  - В **Windows 7**:
    1. Нажмите **Пуск**, перейдите в раздел **Панель управления** и дважды щелкните мышью по элементу **Программы и функции**.
    2. Найдите из списка **Bitdefender Antivirus Plus** и выберите **Удалить**.
    3. Нажмите **ПЕРЕУСТАНОВИТЬ** в появившемся окне.
    4. Дождитесь завершения процесса удаления, после чего выполните перезагрузку системы.
  - В **Windows 8 и Windows 8.1**:
    1. На стартовом экране Windows найдите **Панель управления** (например, можно начать ввод "Панель управления" непосредственно на начальном экране), а затем щелкните его значок.
    2. Нажмите **Удалить программу** или **Программы и компоненты**.
    3. Найдите из списка **Bitdefender Antivirus Plus** и выберите **Удалить**.
    4. Нажмите **ПЕРЕУСТАНОВИТЬ** в появившемся окне.
    5. Дождитесь завершения процесса удаления, после чего выполните перезагрузку системы.
  - В **Windows 10**:
    1. Нажмите **Пуск**, выберите Настройки.
    2. Нажмите иконку **Система** в области Настройки, затем выберите **Установленные приложения**.
    3. Найдите из списка **Bitdefender Antivirus Plus** и выберите **Удалить**.

4. Нажмите **Удалить** снова, чтобы подтвердить выбор.
5. Нажмите **ПЕРЕУСТАНОВИТЬ** в появившемся окне.
6. Дождитесь завершения процесса удаления, после чего выполните перезагрузку системы.

Примечание
Следуя этой процедуре переустановки, настраиваемые параметры сохраняются и доступны в новом установленном продукте. Другие настройки могут быть возвращены к их конфигурации по умолчанию.

- **В системе установлены другие решения безопасности, помимо Bitdefender**.

  В этом случае:

  1. Удалите другое решение безопасности. Для получения более подробной информации, обратитесь к *«Как удалить другие решения безопасности?»* (p. 73).
  2. Переустановите Bitdefender:
     - В **Windows 7**:
       a. Нажмите **Пуск**, перейдите в раздел **Панель управления** и дважды щелкните мышью по элементу **Программы и функции**.
       b. Найдите из списка **Bitdefender Antivirus Plus** и выберите **Удалить**.
       c. Нажмите **ПЕРЕУСТАНОВИТЬ** в появившемся окне.
       d. Дождитесь завершения процесса удаления, после чего выполните перезагрузку системы.
     - В **Windows 8 и Windows 8.1**:
       a. На стартовом экране Windows найдите **Панель управления** (например, можно начать ввод "Панель управления" непосредственно на начальном экране), а затем щелкните его значок.
       b. Нажмите **Удалить программу** или **Программы и компоненты**.
       c. Найдите из списка **Bitdefender Antivirus Plus** и выберите **Удалить**.

d. Нажмите **ПЕРЕУСТАНОВИТЬ** в появившемся окне.

e. Дождитесь завершения процесса удаления, после чего выполните перезагрузку системы.

- В **Windows 10**:

a. Нажмите **Пуск**, выберите Настройки.

b. Нажмите иконку **Система** в области Настройки, затем выберите **Установленные приложения**.

c. Найдите из списка **Bitdefender Antivirus Plus** и выберите **Удалить**.

d. Нажмите **Удалить** снова, чтобы подтвердить выбор.

e. Нажмите **ПЕРЕУСТАНОВИТЬ** в появившемся окне.

f. Дождитесь завершения процесса удаления, после чего выполните перезагрузку системы.

Примечание

Следуя этой процедуре переустановки, настраиваемые параметры сохраняются и доступны в новом установленном продукте. Другие настройки могут быть возвращены к их конфигурации по умолчанию.

Если эта информация не была полезной, вы можете связаться с Bitdefender для поддержки, как описано в разделе *«Обращение за помощью»* (p. 173).

26.3. Я больше не могу использовать приложение

Возникает проблема при попытке использовать программу, которая до установки Bitdefender работала нормально.

После установки Bitdefender 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.

Такой тип ситуации возникает, когда Активный контроль угроз ошибочно обнаруживает некоторые приложения как вредоносные.

Активный контроль угроз - это функция Bitdefender, которая постоянно отслеживает приложения, выполняющиеся в вашей системе, и сообщает о потенциально злонамеренном поведении. Поскольку эта функция основана на эвристической системе, могут быть случаи, когда легальные приложения распознаются Активным контролем угроз как угрозы.

При возникновении подобной ситуации можно исключить соответствующее приложение из мониторинга посредством "Активного контроля угроз".

Чтобы добавить программу в список исключений:

1. Нажмите **Защита** в меню навигации интерфейса Bitdefender.
2. В области **АКТИВНЫЙ КОНТРОЛЬ УГРОЗ** нажмите **Настройки**.
3. В окне **Исключения** нажмите **Добавить приложения в исключения**.
4. Найдите и выберите приложение, которое хотите исключить, затем нажмите **ОК**.

Если эта информация не была полезной, вы можете связаться с Bitdefender для поддержки, как описано в разделе *«Обращение за помощью»* (p. 173).

26.4. Что делать, если Bitdefender блокирует безопасный веб-сайт или онлайн приложение

Bitdefender обеспечивает безопасный просмотр веб-страниц, фильтруя весь веб-трафик и блокируя любое вредоносное содержимое. Однако, вполне возможно, что Bitdefender считает безопасный веб-сайт или онлайн-приложение небезопасным, что приведет к тому, что сканируя HTTP-трафик, Bitdefender будет блокировать их неправильно.

В случае многократного блокирования одного и того же приложения его можно добавить к "Исключениям", чтобы оно не проверялось механизмами Bitdefender, тем самым обеспечивается плавный просмотр веб-страниц.

Чтобы добавить сайт к **Исключениям**:

1. Нажмите **Защита** в меню навигации интерфейса Bitdefender.

2. На панели **ПРЕДОТВРАЩЕНИЕ УГРОЗ** нажмите **Исключения**.
3. В соответствующем поле укажите адрес заблокированного сайта или интернет-приложения и нажмите **ДОБАВИТЬ**.
4. Нажмите **СОХРАНИТЬ**, чтобы сохранить изменения и закрыть окно.

В этот список следует добавить только те сайты, которым вы полностью доверяете. Они будут исключены из сканирования с применением следующих механизмов: угроза, фишинг и мошенничество.

Если эта информация не была полезной, вы можете связаться с Bitdefender для поддержки, как описано в разделе *«Обращение за помощью»* (p. 173).

26.5. Что делать, если Bitdefender определяет безопасное приложение в качестве программы-вымогателя

Вирус-Вымогатель это вредоносная программа, которая пытается вытягивать деньги из пользователей, заблокировав их уязвимые системы. Для того, чтобы оградить вашу систему от нежелательных ситуаций, Bitdefender дает возможность обезопасить ваши личные файлы.

Когда приложение пытается изменить или удалить один из защищенных файлов, то оно будет рассматриваться как небезопасное и Bitdefender будет блокировать его функционирование.

Если такое приложение добавлено в список ненадежных, но вы уверены в его безопасности, выполните следующие действия:

1. Нажмите **Защита** в меню навигации интерфейса Bitdefender.
2. На панели **БЕЗОПАСНЫЕ ФАЙЛЫ** нажмите **Доступ к приложению**.
3. В списке указаны приложения, которые запросили изменить файлы в ваших защищенных папках. Нажмите **"Разрешить"** и выберите приложение, в безопасности которого вы уверены.

26.6. Обновление Bitdefender при низкой скорости подключения к Интернету

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

Чтобы поддерживать систему в актуальном состоянии с помощью новейшей базы данных угроз Bitdefender:

1. Нажмите **Настройки** в меню навигации интерфейс Bitdefender.
2. Выберите вкладку **Update**.
3. Отключите переключатель **Тихое обновление**.
4. В следующий раз, когда будет доступно обновление, вам будет предложено выбрать, какое обновление вы хотите загрузить. Выберите только **Обновление сигнатур**.
5. Bitdefender будет загружать и устанавливать только базу данных угроз.

26.7. Службы Bitdefender не отвечают

Эта статья поможет устранить неполадки **Bitdefender Службы не отвечают**. Эта ошибка может возникнуть следующим образом:

- Значок Bitdefender в области уведомления отображается серым цветом, информируя о том, что службы Bitdefender не отвечают.
- Окно Bitdefender указывает, что службы Bitdefender не отвечают.

Ошибка может быть вызвана одной из следующих причин:

- временные ошибки связи между службами Bitdefender.
- некоторые из служб Bitdefender остановлены.
- другие средства безопасности работают одновременно с Bitdefender.

Чтобы устранить эту ошибку, попробуйте следующие решения:

1. Несколько минут подождите и просмотрите возможные изменения. 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, установлены ли другие решения безопасности, поскольку они могут нарушить нормальную работу Bitdefender. Если они установлены, мы рекомендуем вам удалить все другие решения безопасности, а затем переустановить Bitdefender.

   Для получения более подробной информации, обратитесь к «*Как удалить другие решения безопасности?*» (p. 73).

Если ошибка продолжает возникать, свяжитесь с нашей службой поддержки, как описано в разделе «*Обращение за помощью*» (p. 173).

26.8. Функция "Автозаполнение" в Кошельке не работает

Вы сохранили свои учетные данные в вашем Менеджере Паролей Bitdefender и обратили внимание, что автозаполнение не работает. Обычно это происходит, когда расширение Bitdefender Wallet в вашем браузере не задано.

Для того, чтобы устранить эту проблему, выполните следующие действия:

- В **Internet Explorer:**
  1. Откройте Internel Explorer.
  2. Зайдите в раздел "Инструменты".
  3. Нажмите "Управление дополнениями".
  4. Нажмите "Панель инструментов" и "Расширения".
  5. Наведите указатель мыши на **Bitdefender Кошелек** и нажмите **Включить**.
- В **Mozilla Firefox:**
  1. Откройте Mozilla Firefox.
  2. Зайдите в раздел "Инструменты".
  3. Нажмите "Управление настройками".
  4. Нажмите "Расширение".
  5. Наведите указатель мыши на **Bitdefender Кошелек** и нажмите **Включить**.
- В **Google Chrome:**

1. Откройте Google Chrome.
2. Перейдите к значку меню.
3. Нажмите «Дополнительные инструменты».
4. Нажмите "Расширение".
5. Наведите указатель мыши на **Bitdefender Кошелек** и нажмите **Включить**.

Примечание
Надстройка будет включена после перезагрузки веб-браузера.

Теперь проверьте, работает ли функция автозаполнения в Кошельке для вашей учетной записи в интернете.

Если эта информация не была полезной, вы можете связаться с Bitdefender для поддержки, как описано в разделе *«Обращение за помощью»* (p. 173).

26.9. Сбой удаления Bitdefender

Если вы хотите удалить продукт Bitdefender и заметили, что процесс или система зависают, нажмите **Отмена**, чтобы прервать действие. Если это не помогло, перезапустите систему.

При сбое удаления некоторые ключи и файлы Bitdefender могут оставаться в системе. Такие остатки могут препятствовать новой установке Bitdefender. Также они могут повлиять на производительность и стабильность системы.

Для того, чтобы полностью удалить Bitdefender из вашей системы:

- В **Windows 7**:
  1. Нажмите **Пуск**, перейдите в раздел **Панель управления** и дважды щелкните мышью по элементу **Программы и функции**.
  2. Найдите из списка **Bitdefender Antivirus Plus** и выберите **Удалить**.
  3. Нажмите кнопку **УДАЛИТЬ** в появившемся окне.
  4. Дождитесь завершения процесса удаления, после чего выполните перезагрузку системы.
- В **Windows 8 и Windows 8.1**:

1. На стартовом экране Windows найдите **Панель управления** (например, можно начать ввод "Панель управления" непосредственно на начальном экране), а затем щелкните его значок.
2. Нажмите **Удалить программу** или **Программы и компоненты**.
3. Найдите из списка **Bitdefender Antivirus Plus** и выберите **Удалить**.
4. Нажмите кнопку **УДАЛИТЬ** в появившемся окне.
5. Дождитесь завершения процесса удаления, после чего выполните перезагрузку системы.

- В **Windows 10**:

1. Нажмите **Пуск**, выберите Настройки.
2. Нажмите иконку **Система** в области Настройки, затем выберите **Установленные приложения**.
3. Найдите из списка **Bitdefender Antivirus Plus** и выберите **Удалить**.
4. Нажмите **Удалить** снова, чтобы подтвердить выбор.
5. Нажмите кнопку **УДАЛИТЬ** в появившемся окне.
6. Дождитесь завершения процесса удаления, после чего выполните перезагрузку системы.

26.10. 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.**

  Чтобы решить эту проблему:

  1. Перезагрузите систему и запустите безопасный режим. Чтобы узнать, как это сделать, обратитесь к «*Как перезагрузить компьютер в безопасном режиме?*» (p. 74).

2. Удалите Bitdefender из системы:
   - В **Windows 7**:
     a. Нажмите **Пуск**, перейдите в раздел **Панель управления** и дважды щелкните мышью по элементу **Программы и функции**.
     b. Найдите из списка **Bitdefender Antivirus Plus** и выберите **Удалить**.
     c. Нажмите кнопку **УДАЛИТЬ** в появившемся окне.
     d. Дождитесь завершения процесса удаления, после чего выполните перезагрузку системы.
     e. Перезагрузите систему в обычном режиме.
   - В **Windows 8 и Windows 8.1**:
     a. На стартовом экране Windows найдите **Панель управления** (например, можно начать ввод "Панель управления" непосредственно на начальном экране), а затем щелкните его значок.
     b. Нажмите **Удалить программу** или **Программы и компоненты**.
     c. Найдите из списка **Bitdefender Antivirus Plus** и выберите **Удалить**.
     d. Нажмите кнопку **УДАЛИТЬ** в появившемся окне.
     e. Дождитесь завершения процесса удаления, после чего выполните перезагрузку системы.
     f. Перезагрузите систему в обычном режиме.
   - В **Windows 10**:
     a. Нажмите **Пуск**, выберите Настройки.
     b. Нажмите иконку **Система** в области Настройки, затем выберите **Установленные приложения**.
     c. Найдите из списка **Bitdefender Antivirus Plus** и выберите **Удалить**.
     d. Нажмите **Удалить** снова, чтобы подтвердить выбор.
     e. Нажмите кнопку **УДАЛИТЬ** в появившемся окне.

f. Дождитесь завершения процесса удаления, после чего выполните перезагрузку системы.

g. Перезагрузите систему в обычном режиме.

3. Заново установите продукт Bitdefender.

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

  Чтобы решить эту проблему:

  1. Перезагрузите систему и запустите безопасный режим. Чтобы узнать, как это сделать, обратитесь к *«Как перезагрузить компьютер в безопасном режиме?»* (p. 74).

  2. Удалить другое решение безопасности из вашей системы:

     - В **Windows 7**:

       a. Нажмите **Пуск**, перейдите в раздел **Панель управления** и дважды щелкните мышью по элементу **Программы и функции**.

       b. Найдите имя программы, которую следует удалить, и выберите **Удалить**.

       c. Дождитесь завершения процесса удаления, после чего выполните перезагрузку системы.

     - В **Windows 8 и Windows 8.1**:

       a. На стартовом экране Windows найдите **Панель управления** (например, можно начать ввод "Панель управления" непосредственно на начальном экране), а затем щелкните его значок.

       b. Нажмите **Удалить программу** или **Программы и компоненты**.

       c. Найдите имя программы, которую следует удалить, и выберите **Удалить**.

       d. Дождитесь завершения процесса удаления, после чего выполните перезагрузку системы.

     - В **Windows 10**:

       a. Нажмите **Пуск**, выберите Настройки.

       b. Нажмите иконку **Система** в области Настройки, затем выберите **Установленные приложения**.

c. Найдите имя программы, которую следует удалить, и выберите **Удалить**.

d. Дождитесь завершения процесса удаления, после чего выполните перезагрузку системы.

Чтобы корректно удалить другие программы, с соответствующего веб-сайта запустите инструмент удаления программы или свяжитесь с разработчиком для получения инструкций по удалению.

3. Перезагрузите систему в нормальном режиме и переустановите Bitdefender.

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

Чтобы решить эту проблему:

1. Перезагрузите систему и запустите безопасный режим. Чтобы узнать, как это сделать, обратитесь к «*Как перезагрузить компьютер в безопасном режиме?*» (p. 74).
2. Используйте функцию восстановления системы Windows, чтобы вернуться к состоянию системы до установки продукта Bitdefender.
3. Перезагрузите систему в нормальном режиме и свяжитесь со службой поддержки, как описано в разделе «*Обращение за помощью*» (p. 173).

27. УДАЛЕНИЕ УГРОЗ ИЗ СИСТЕМЫ

Угрозы могут влиять на работу системы различными способами. Работа Bitdefender зависит от типа атаки угрозы. Вследствие того, что поведение угроз часто изменяется, определить единый шаблон их поведения и действий довольно сложно.

В отдельных случаях Bitdefender не удается автоматически удалить угрозы из системы. В таких случаях требуется вмешательство пользователя.

- «*Bitdefender Режим Восстановления (Rescue Environment в Windows 10)*» (p. 161)
- «*Какие действия предпринять в случае обнаружения Bitdefender угроз на компьютере?*» (p. 165)
- «*Как очистить архив от угрозы?*» (p. 167)
- «*Как очистить архив электронной почты от угрозы?*» (p. 168)
- «*Что делать, если имеются подозрения в том, что файл является опасным?*» (p. 169)
- «*Что представляют собой защищенные паролями файлы в журнале сканирования?*» (p. 170)
- «*Поиск пропущенных элементов в журнале сканирования*» (p. 170)
- «*Поиск файлов с избыточным сжатием в журнале сканирования.*» (p. 170)
- «*Почему Bitdefender автоматически удалил зараженный файл?*» (p. 171)

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) «*Обращение за помощью*» (p. 173).

27.1. Bitdefender Режим Восстановления (Rescue Environment в Windows 10)

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

После того, как Bitdefender Antivirus Plus будет установлен на **Windows 7, Windows 8 и Windows 8. 1** и загружен файл изображения Bitdefender Режим восстановления, можно пользоваться Режимом Восстановления, даже если Вы больше не можете продолжать загрузку в Windows.

В Windows 10 Bitdefender Rescue Environment интегрирована с Windows RE, то есть нет необходимости загружать изображение режима Rescue Mode в этой операционной системе, и эта функция не может использоваться, если есть проблемы с запуском. Чтобы очистить систему перед загрузкой служб Windows, рекомендуется использовать загрузочный компакт-диск Bitdefender.

Bitdefender Rescue CD - это бесплатный инструмент, который сканирует и очищает ваш компьютер всякий раз, когда вы подозреваете, что угроза влияет на его работу. Полезные статьи, содержащие сведения о создании и использовании, доступны на платформе центра поддержки Bitdefender в https://www.bitdefender.com/support/consumer.html.

Загрузка изображения Bitdefender Режима Восстановления

Для того чтобы иметь возможность использовать Режим Восстановления в **Windows 7, Windows 8 и Windows 8.1**, сначала необходимо загрузить архив изображения следующим образом:

1. Нажмите **Защита** в меню навигации интерфейса Bitdefender.
2. В области **АНТИВИРУС** нажмите **Режим Восстановления**.
3. Нажмите **Да** в окне подтверждения, которое появится для перезагрузки компьютера.

   Подождите,Bitdefender пока файл изображения Режима Восстановления будет загружен с серверов Bitdefender. Как только процесс загрузки будет завершен, компьютер перезапустится.

   Появится меню с запросом на выбор операционной системы. На этом этапе вы можете начать работу в системе Режима Восстановления или в обычном режиме.

Примечание

Вследствие интеграции Windows Recovery Environment в **Windows 10** не требуется загружать изображение режима Режима спасения в этой операционной системе.

Запуск системы в Режиме Восстановления в Windows 7, Windows 8 и Windows 8. 1

В Режим спасения можно перейти двумя способами:

Из интерфейса Bitdefender

1. Нажмите **Защита** в меню навигации интерфейса Bitdefender.
2. В области **АНТИВИРУС** нажмите **Режим Восстановления**.
3. Нажмите **Да** в окне подтверждения, которое появится для перезагрузки компьютера.
4. После перезагрузки компьютера появится меню с запросом на выбор операционной системы. Выберите **Bitdefender Режим спасения** для загрузки в среде Bitdefender, откуда можно очистить раздел Windows.
5. При появлении запроса нажмите клавишу **Enter** и выберите разрешение экрана, наиболее близкое к разрешению, которое вы обычно используете. Затем снова нажмите **Enter**.

   Режим Восстановления Bitdefender загрузится в несколько мгновений.

Загрузите компьютер в Режиме спасения

Если Windows больше не запускается, вы можете загрузить компьютер в Режиме спасения Bitdefender, выполнив следующие действия:

- В **Windows 7**:
  1. Нажимайте клавишу **F8** , пока не появится экран **Дополнительные параметры загрузки**.
  2. Используйте клавиши со стрелками, чтобы выбрать Bitdefender Режим Восстановления, затем нажмите **Enter** .

     Режим Rescue Mode Bitdefender будет запущен через несколько минут.
- В **Windows 8 и Windows 8.1**:
  1. Нажимайте клавишу **F8** , пока не появится экран **Дополнительные параметры запуска**.

2. Выберите опцию **Использовать другую операционную систему** , затем режим Bitdefender Rescue Mode.

   Режим Rescue Mode Bitdefender будет запущен через несколько минут.

> **Примечание**
> Можно загрузить Ваш компьютер в Режиме Реанимация только в том случае, если файл изображения Режима Восстановления был загружен ранее, как описано в «Загрузка изображения Bitdefender Режима Восстановления» (p. 162).

Запуск системы в Rescue Environment в Windows 10

Вход в Rescue Environment возможен только с ВашегоBitdefender средства, как показано ниже:

1. Нажмите **Защита** в меню навигации интерфейса Bitdefender.
2. В области **ANTIVIRUS** нажмите **Rescue Environment** .
3. Нажмите кнопку **Перезагрузка** в появившемся окне.

   Bitdefender Rescue Environment загрузится через несколько минут.

Сканирование системы в режиме Rescue (Rescue Environment в Windows 10)

Сканировать систему в Режиме Восстановления (Реанимация):

- В **Windows 7, Windows 8 и Windows 8.1**:
  1. Перейдите в режим Rescue Mode, как описано в разделе «Запуск системы в Режиме Восстановления в Windows 7, Windows 8 и Windows 8. 1» (p. 163).
  2. Появится логотип Bitdefender и начнется копирование механизмов решения безопасности.
  3. Откроется окно приветствия. Нажмите **Продолжить**.
  4. Запускается обновление базы данных угроз.
  5. После завершения обновления появится окно "Bitdefender On-demand Antivirus Scanner".

6. Нажмите **Scan Now**, выберите в появившемся окне объект сканирования, а затем нажмите кнопку **Scan Now**, чтобы начать сканирование.

   Рекомендуется выполнить сканирование всего раздела Windows.

   > **Примечание**
   > При работе в режиме Rescue Mode 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 процесса сканирования. Если обнаружена какая-либо угроза, следуйте инструкциям для ее удаления.
8. Для выхода из режима восстановления щелкните правой кнопкой мыши в пустой области рабочего стола, выберите в появившемся меню **Exit**, а затем выберите перезагрузку или выключение компьютера.

- В **Windows 10**:

  1. Перейдите в Среду восстановления, как описано в «Запуск системы в Rescue Environment в Windows 10» (p. 164).
  2. Процесс сканирования Bitdefender запускается автоматически, как только система загружается в Среде восстановления.
  3. Дождитесь завершения процесса сканирования. Если обнаружена какая-либо угроза, следуйте инструкциям для ее удаления.
  4. Чтобы выйти из Среды, нажмите кнопку **ЗАКРЫТЬ** в окне с результатами сканирования.

27.2. Какие действия предпринять в случае обнаружения Bitdefender угроз на компьютере?

Обнаружить наличие угроз на вашем компьютере можно одним из следующих способов:

- Выполнено сканирование компьютера. Bitdefender обнаружил зараженные элементы.
- Оповещение об угрозе сообщает о том, что Bitdefender заблокировал одну или несколько угроз, проникших в компьютер.

В таких ситуациях необходимо обновить Bitdefender для получения последних данных об угрозах, после чего запустить Сканирование системы.

Как только процесс сканирования будет завершен, примените желаемую меру в отношении зараженного элемента (вылечить, удалить, переместить в карантин).

Предупреждение

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. Нажмите **Защита** в меню навигации интерфейса Bitdefender.
   b. На панели **АНТИВИРУС** нажмите **Настройки**.
   c. В окне **Защита** отключите **Защита Bitdefender**.
2. Отображать скрытые объекты в Windows. Чтобы узнать, как это сделать, обратитесь к *«Как отобразить скрытые объекты в Windows?»* (p. 72).
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 первым способом не удалось удалить инфекцию:

1. Перезагрузите систему и запустите безопасный режим. Чтобы узнать, как это сделать, обратитесь к *«Как перезагрузить компьютер в безопасном режиме?»* (p. 74).

2. Отображать скрытые объекты в Windows. Чтобы узнать, как это сделать, обратитесь к *«Как отобразить скрытые объекты в Windows?»* (p. 72).
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 была полезной, вы можете связаться с Bitdefender для поддержки, как описано в разделе *«Обращение за помощью»* (p. 173).

27.3. Как очистить архив от угрозы?

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 архива являются частично или полностью закрытыми. Bitdefender может только обнаруживать наличие в них угроз, не выполняя каких-либо дополнительных действий.

Если Bitdefender уведомляет о том, что в архиве обнаружена угроза и в ее отношении не доступны никакие действия, это означает, что удаление угрозы невозможно из-за ограничений в настройках разрешения архива.

Очистить архив от угрозы можно следующим образом:

1. Определите архив, в котором находится угроза, выполнив сканирование системы.
2. Отключение антивирусной защиты Bitdefender в режиме реального времени:
   a. Нажмите **Защита** в меню навигации интерфейса Bitdefender.
   b. На панели **АНТИВИРУС** нажмите **Настройки**.
   c. В окне **Защита** отключите **Защита Bitdefender**.
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 Bitdefender антивирусную защиту в режиме реального времени и запустите сканирование системы, чтобы убедиться в отсутствии других инфекций в системе.

Примечание
Обратите внимание на то, что угроза, находящаяся в архиве, не являет собой опасность для системы, так как угроза должна быть распакована и выполнена для того, чтобы заразить систему.

Если эта информация не была полезной, вы можете связаться с Bitdefender для поддержки, как описано в разделе «*Обращение за помощью*» (p. 173).

27.4. Как очистить архив электронной почты от угрозы?

Bitdefender также может распознавать угрозы в базе данных и архиве электронной почты, сохраненных на диске.

В отдельных случаях требуется найти зараженное сообщение, используя данные отчета о сканирования, и удалить его вручную.

Удалить угрозу 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. Нажмите **Защита** в меню навигации интерфейса Bitdefender.
   b. На панели **АНТИВИРУС** нажмите **Настройки**.
   c. В окне **Защита** отключите **Защита Bitdefender**.

3. Откройте отчет о сканировании и выполните поиск инфицированных сообщений в 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 Microsoft Outlook 2007: В меню "Файл" выберите "Управление файлами данных". Выберите файлы личных папок (.pst), которые требуется сжать, и нажмите "Параметры". Нажмите "Сжать сейчас".
   - В Microsoft Outlook 2010 / 2013/ 2016: В меню Файл выберите пункт Информация, а затем параметры учетной записи (Добавление и удаление учетных записей или изменение существующих параметров подключения). Затем щелкните файл данных, выберите файлы личных папок (PST), которые требуется сжать, и нажмите кнопку Параметры. Нажмите "Сжать сейчас".
6. Включить антивирусную защиту Bitdefender в режиме реального времени.

Если эта информация не была полезной, вы можете связаться с Bitdefender для поддержки, как описано в разделе «*Обращение за помощью*» (p. 173).

27.5. Что делать, если имеются подозрения в том, что файл является опасным?

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

Чтобы убедиться, что ваша система защищена:

1. Запустите **Сканирование системы** с помощью Bitdefender. Чтобы узнать, как это сделать, обратитесь к «*Как выполнить сканирование системы?*» (p. 59).
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.

Чтобы узнать, как это сделать, обратитесь к «*Обращение за помощью*» (p. 173).

27.6. Что представляют собой защищенные паролями файлы 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. Для того, 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.

27.7. 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.

27.8. 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 то, 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.

27.9. 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.

Для определенных типов угроз лечение невозможно, поскольку обнаруженный файл является полностью вредоносным. 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.

СВЯЖИТЕСЬ С НАМИ

28. ОБРАЩЕНИЕ ЗА ПОМОЩЬЮ

Bitdefender предоставляет своим потребителям быструю и надежную поддержку, которая не имеет аналогов. Если у вас возникают какие-либо проблемы или вопросы по продукту Bitdefender, вы можете воспользоваться несколькими интерактивными ресурсами, чтобы найти решение проблемы или получить ответ на вопрос. Также вы можете обратиться в службу поддержки Bitdefender. Наши представители службы поддержки своевременно ответят на ваши вопросы и окажут необходимую помощь.

В разделе *«Решение общих вопросов.»* (p. 147) описываются проблемы, с которыми чаще всего может столкнуться пользователь продукта.

Если вы не найдет ответ на свой вопрос в предоставленных ресурсах, то вы можете обратиться непосредственно к нам:

- «Свяжитесь с нами напрямую из Bitdefender Antivirus Plus» (p. 173)
- «Свяжитесь с нами через онлайн-центр поддержки» (p. 174)

Свяжитесь с нами напрямую из Bitdefender Antivirus Plus

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

Следуйте инструкции:

1. Нажмите **Поддержка** в меню навигации интерфейса Bitdefender.
2. Для выбора доступны следующие параметры:
   - **Руководство пользователя**

     Войдите в нашу базу данных и найдите необходимую информацию.
   - **Центр поддержки**

     Доступ к статьям и видео-урокам.
   - **НАПИШИТЕ НАМ**

     Нажмите кнопку **Контакты службы технической поддержки**, чтобы запустить инструмент поддержки Bitdefender и связаться с отделом технической поддержки.

a. Заполните форму отправки, указав необходимые данные:

   i. Выберите тип проблемы, с которой Вы столкнулись.

   ii. Введите описание возникшей проблемы.

   iii. Нажмите **ПОПЫТКА ВОСПРОИЗВЕДЕНИЯ ПРОБЛЕМЫ** в случае возникновения проблемы с продуктом. Воспроизведите проблему, затем нажмите кнопку **Готово** в рамке воспроизведения проблемы.

   iv. Нажмите **ПОДТВЕРЖДЕНИЕ ЗАПРОСА**.

b. Продолжайте заполнять форму заявки с необходимыми данными:

   i. Введите свое полное имя.

   ii. Введите свой адрес электронной почты.

   iii. Установите флажок "Согласие".

   iv. Нажмите **СОЗДАТЬ ПАКЕТ ОТЛАДКИ**.

   Подождите несколько минут, пока Bitdefender выполнит сбор сведений о продукте. Эта информация поможет нашим техническим специалистам найти эффективное решение вашей проблемы.

c. Нажмите **Close**, чтобы выйти из мастера. С Вами свяжется как можно скорее один из наших представителей.

Свяжитесь с нами через онлайн-центр поддержки

Если вы не можете получить доступ к необходимой информации с помощью Bitdefender, обратитесь в наш он-лайн центр поддержки:

1. Перейдите к https://www.bitdefender.com/support/consumer.html.

   В центре поддержки Bitdefender имеется множество статей, содержащих решения проблем, связанных с работой Bitdefender.

2. Воспользуйтесь строкой поиска в верхней части окна, чтобы найти статьи, в которых будет предложено решение вашей проблемы. Для того, чтобы запустить поиск, введите термин в строку поиска и нажмите **Search**.

3. Ознакомьтесь с содержанием соответствующих статей или документов и попробуйте предложенные варианты решений.
4. Если решение не поможет решить проблему, перейдите к

   http://www.bitdefender.com/support/contact-us.htmlи связжитесь с нашими представителями поддержки.

29. ОНЛАЙН-РЕСУРСЫ

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

- Центр поддержки Bitdefender:

  https://www.bitdefender.com/support/consumer.html

- Форум техподдержки Bitdefender:

  https://forum.bitdefender.com

- Портал компьютерной безопасности HOTforSecurity:

  https://www.hotforsecurity.com

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

29.1. 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 о предотвращении угроз, управлению решениями Bitdefender с подробными разъяснениями и другая информация.

Центр поддержки Bitdefender доступен для всех и поиск по нему можно осуществлять без каких-либо ограничений. Bitdefender содержит подробную 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

https://www.bitdefender.com/support/consumer.html.

29.2. Форум техподдержки Bitdefender

Форум техподдержки Bitdefender предоставляет пользователям Bitdefender простой способ не только получить необходимую помощь, но и помочь другим.

В случае некорректной работы продукта Bitdefender (продукт не может удалить отдельные угрозы с компьютера) или при возникновении вопросов, касающихся работы продукта, вы можете опубликовать описание проблемы или задать 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 на форуме.

Форум техподдержки Bitdefender доступен по адресу https://forum.bitdefender.com, на пяти различных языках: английском, немецком, французском, испанском и румынском. Нажмите на ссылку **Home & Home Office Protection**, чтобы перейти в раздел потребительских товаров.

29.3. Портал HOTforSecurity

Портал HOTforSecurity - богатый источник информации по безопасности компьютера. Здесь можно найти сведения о различных угрозах, которым подвергается компьютер при подключении к Интернету (вредоносное ПО, фишинговые атаки, спам, киберпреступность).

Для информирования пользователей о последних угрозах, текущих тенденциях развития систем безопасности и других событиях в отрасли компьютерной безопасности регулярно публикуются новые статьи.

Веб-страница HOTforSecurity: https://www.hotforsecurity.com.

30. КОНТАКТНАЯ ИНФОРМАЦИЯ

Эффективное взаимодействие с клиентами является залогом успешного бизнеса. За последние 16 лет компании BITDEFENDER удалось завоевать внушительный авторитет среди своих клиентов и партнеров за счет предвосхищения их ожиданий и постоянного улучшения связи с ними. Мы будем рады ответить на все ваши вопросы и решить ваши проблемы – не стесняйтесь, обратитесь к нам за помощью.

30.1. Веб-адреса

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

30.2. Местные дистрибьюторы

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

Поиск дистрибутора Bitdefender в вашей стране:

1. Перейдите к http://www.bitdefender.com/partners/partner-locator.html.
2. Выберите страну и город, используя соответствующие опции.
3. Если не удалось найти дистрибутора Bitdefender в вашей стране, свяжитесь с нами по адресу электронной почты sales@bitdefender.com. Укажите адрес электронной почты на английском языке, чтобы мы смогли своевременно обработать ваш вопрос.

30.3. Офисы Bitdefender

Местные дистрибьюторы Bitdefender готовы ответить на все вопросы коммерческого и общего характера, находящиеся в их компетенции. Ниже приведены адреса и контактная информация офисов.

США

Bitdefender, LLC
6301 NW 5th Way, Suite 4300
Fort Lauderdale, Florida 33309
Телефон (office & sales): 1-954-776-6262
Продажи: sales@bitdefender.com
Техническая поддержка: https://www.bitdefender.com/support/consumer.html
Сайт: https://www.bitdefender.com

Великобритания и Ирландия

BITDEFENDER LTD
C/O Howsons Winton House, Stoke Road, Stoke on Trent
Staffordshire, United Kindon, ST4 2RW
E-mail: info@bitdefender.co.uk
Телефон: (+44) 2036 080 456
Продажи: sales@bitdefender.co.uk
Техническая поддержка: https://www.bitdefender.co.uk/support/
Сайт: https://www.bitdefender.co.uk

Германия

Bitdefender GmbH
TechnoPark Schwerte
Lohbachstrasse 12
D - 58239 Schwerte
Офис: +49 2304 9 45 - 162
Факс: +49 2304 9 45 - 169
Продажи: vertrieb@bitdefender.de
Техническая поддержка: https://www.bitdefender.de/support/consumer.html
Сайт: https://www.bitdefender.de

Дания

Bitdefender APS
Agern Alle 24, 2970 Hørsholm, Denmark
Офис: +45 7020 2282
Техническая поддержка: http://bitdefender-antivirus.dk/
Сайт: http://bitdefender-antivirus.dk/

Испания

Bitdefender España, S.L.U.
C/Bailén, 7, 3-D
08010 Barcelona
Факс: +34 93 217 91 28
Телефон: +34 902 19 07 65
Продажи: comercial@bitdefender.es
Техническая поддержка: https://www.bitdefender.es/support/consumer.html
Веб-сайт: https://www.bitdefender.es

Румыния

BITDEFENDER SRL
Orhideea Towers, 15A Orhideelor Street, Sector 6
Bucharest
Факс: +40 21 2641799
Телефон отдела продаж: +40 21 2063470
Электронная почта отдела продаж: sales@bitdefender.ro
Техническая поддержка: https://www.bitdefender.ro/support/consumer.html
Веб-сайт: https://www.bitdefender.ro

Объединенные Арабские Эмираты

Dubai Internet City
Building 17, Office # 160
Dubai, UAE
Телефон отдела продаж: 00971-4-4588935 / 00971-4-4589186
Электронная почта отдела продаж: mena-sales@bitdefender.com
Техническая поддержка: https://www.bitdefender.com/support/consumer.html

Веб-сайт: https://www.bitdefender.com

Глоссарий

ActiveX

ActiveX – это компоненты, которые могут использоваться другими программами и операционными системами вызывающими их. Технология ActiveX используется вместе с программой Microsoft Internet Explorer для создания интерактивных страниц, которые выглядят и работают скорее как компьютерные программы, нежели как простые страницы. С помощью ActiveX пользователь может задавать и отвечать на вопросы, «нажимать» на кнопки и другим способом взаимодействовать с веб-страницей. Элементы ActiveX чаще всего 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.

IP-адрес

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

Photon

Фотон является инновационной ненавязчивой технологией Bitdefender, предназначенной для минимизации влияния вашего решения безопасности на производительность. Контролируя деятельность вашего компьютера в фоновом режиме, он создает модели использования, которые помогают оптимизировать загрузку и сканирование процессов.

Архив

Диск, лента или каталог, содержащие резервные копии файлов.

Файл, содержащий один или несколько файлов в сжатом формате.

Ботнет

Термин «ботнет» состоит из слов «робот» и «сеть». Ботнеты - это устройства, подключенные к Интернету, которые могут использоваться для рассылки спама, кражи данных, удаленного управления уязвимыми устройствами или распространения

шпионских программ, вымогателей и других видов угроз. Их цель - заразить как можно больше подключенных устройств, таких как ПК, серверы, мобильные или IoT-устройства, принадлежащие крупным компаниям или отраслям.

Браузер

Коротко о веб-браузере - программное приложение, используемое для поиска и отображения веб-страниц. Популярными браузерами являются Microsoft Internet Explorer, Mozilla Firefox и Google Chrome. Это графические браузеры, что означает, что они могут отображать графику, а также текст. Кроме того, большинство современных браузеров могут отображать мультимедийную информацию, включая звук и видео изображения, хотя некоторые из них требуют установки дополнительных расширений.

Виртуальная частная сеть (VPN)

Это технология, которая позволяет временное и зашифрованное прямое подключение к определенной сети через менее безопасную сеть. Таким образом, передача и прием данных являются безопасными и зашифрованными, что затрудняет их перехват. Доказательством безопасности является аутентификация, которая обеспечивается только с помощью имени пользователя и пароля.

Вирусы-Вымогатели

Вирус-Вымогатель это вредоносная программа, которая пытается вытягивать деньги из пользователей, заблокировав их уязвимые системы. CryptoLocker, CryptoWall и TeslaWall только некоторые варианты, которые атакуют персональные системы пользователей.

Инфекция может распространяться в виде спама по электронной почте, при загрузке вложений почты или установке приложений, при этом никак не проявляя себя. Таким образом, пользователь не может знать о том, что происходит в системе. Ежедневно пользователи и компании становятся мишенью для хакеров-вымогателей.

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.

Загрузить

Копирование данных (обычно целых файлов) из основного местоположения на внешнее устройство. Обычно этот термин используется по отношению к копированию файла из сетевого источника на свой компьютер. Загрузкой также называют копирование файла с сетевого файлового сервера на компьютер в сети.

Загрузочный вирус

Угроза, поражающая загрузочный сектор жесткого или гибкого диска. Попытка загрузки с дискеты, зараженной вирусом загрузочного сектора, приведет к тому, что угроза активизируется в памяти. Каждый раз, когда вы загружаете систему с этого места, угроза будет активизироваться в памяти.

Загрузочный сектор:

Сектор в начале каждого диска, в котором хранится информация о структуре диска (размер сектора, размер кластера и т.д.) На загрузочном диске загрузочный сектор содержит программу, загружающую операционную систему.

Запакованные программы

Файл в сжатом формате. Многие операционные системы и приложения содержат команды, позволяющие запаковать файл для того, чтобы он занимал меньше места. Например, у вас есть текстовый файл, состоящий из десяти последовательных символов пробела. В нормальном состоянии этот файл занимает десять байт памяти.

Однако программа-архиватор может заменить эти пробелы специальным символом пробелов и количеством замененных пробелов. В этом случае десять пробелов займут всего лишь два байта. И это только один из многих методов архивации файлов.

Клавиатурный шпион (Keylogger)

Кейлогер - это приложение, которое регистрирует все, что вы набираете на клавиатуре.

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 в злонамеренных целях (например, для сбора частных данных, таких как учетные данные и номера карт социального страхования).

Код активации

Является уникальным ключом, который можно купить в розницу и используется для активации конкретного продукта или услуги. Код активации позволяет активировать действительную подписку на определенный период времени и число устройств, а также может быть использован для расширения подписки с условием, что будет сформирован на тот же товар или услугу.

Командная строка

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

Лазейки в системе (Backdoor)

Брешь в защите системы, специально оставленная разработчиками или специалистами по сопровождению. 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.

Ловушка

В системе может быть установлен специальный модуль "приманки", который специально привлекает хакеров, чтобы изучать их действия и выявлять эвристические методы, которые они используют для сбора информации о системе. Наиболее заинтересованы в использовании приманок компании и корпорации, чтобы улучшить общее состояние информационной безопасности.

Ложное срабатывание

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

Макро-вирус

Тип компьютерной угрозы, который кодируется как встроенный в документ макрос. Многие приложения, такие как Microsoft Word и Excel, поддерживают сложные макро-языки.

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

Неэвристический анализ (Non-heuristic)

Этот метод сканирования опирается на определенную базу данных угроз. Преимущество неэвристического сканирования заключается в том, что он не реагирует на ложные угрозы и не создает ложных тревог.

Область уведомлений

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 мышкой на значке.

Обновление информации об угрозах

Двоичный шаблон угрозы, используемый решением безопасности для обнаружения и устранения угрозы.

Обновления

Новая версия программного обеспечения или оборудования, разработанная на замену устаревшей версии этого продукта. Кроме того, многие обновления часто определяют, установлена ли на компьютере старая версия данного программного продукта. Если нет – обновление невозможно.

У Bitdefender есть свой собственный модуль обновления, который позволяет вручную проверять наличие или автоматически обновлять программный продукт.

Подписка

Покупка договоренности, что дает пользователю право на использование конкретного продукта или услуги на определенном количестве устройств и в течение определенного периода времени. Подписка, с истекшим сроком действия, может быть автоматически продлена с помощью информации, предоставленной пользователем при первой покупке.

Полиморфный вирус

Угроза, которая изменяет свою форму с каждым зараженным файлом. Поскольку у них 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.

Постоянные угрозы повышенной сложности (Advanced persistent threat)

Advanced persistent threat (APT) использует уязвимости систем, чтобы украсть важную информацию для доставки ее к источнику. Крупные организации, компании или органы управления являются мишенью этой угрозы.

Цель advanced persistent threat - оставаться незамеченными в течение длительного времени с возможностью мониторинга и собора важной информации, не повреждая целевые машины. Метод, используемый для введения угрозы в сеть через PDF-файл или документ Office. Данные файлы выглядят безвредными и любой пользователь может запустить их.

Почтовый клиент

Клиент электронной почты - это приложение, которое позволяет отправлять и получать электронную почту.

Прикладная минипрограмма Java апплет

Программа, написанная на языке Java, которая работает только на веб-страницах. Чтобы использовать апплет на странице, Вы должны указать его название и размер (длину и ширину в пикселях), которые он может использовать. При открывании страницы браузер загружает эту программу с сервера и запускает ее на компьютере пользователя (который в этом случае называется «клиент»). Апплеты отличаются от приложений, которыми они управляются, более строгим протоколом обеспечения безопасности.

Например, даже если апплет 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

Любого рода программа-шпион, которая тайно и без ведома пользователя - чаще всего в рекламных целях - собирает информацию о пользователе во время его соединения с сетью Интернет. Шпионские программы обычно маскируют как скрытые компоненты бесплатных или условно бесплатных (shareware) приложений, которые можно скачать из сети Интернет, хотя следует отметить, что большинство бесплатных или условно бесплатных приложений не содержит программ-шпионов. Программа-шпион после своей установки отслеживает адреса в сети Интернет, к которым обращается пользователь, и тайно пересылает эту информацию третьим лицам. Программы-шпионы могут собирать информацию об адресах электронной почты, паролях и номерах кредитных карт.

Программы-шпионы аналогичны вирусам-троянам в том смысле, что и те и другие устанавливаются самими пользователями во время установки других программ. Жертвами программ-шпионов обычно становятся при скачивании известных программных продуктов из файлообменных сетей.

Действия программ-шпионов являются не только нарушением этики и конфиденциальности, но и кражей ресурсов компьютерной памяти и ресурсов канала соединения с сетью Интернет, за счет передачи информации программой-шпионом своему источнику при подключении пользователя к сети Интернет. За счет потребления памяти и системных ресурсов программами-шпионами, работа

последних в фоновом режиме может приводить к неустойчивой работе системы и ее сбоям.

Протокол TCP/IP

Протокол управления передачей/интернет-протокол (Transmission Control Protocol/Internet Protocol) — набор сетевых протоколов, широко используемых в сети Интернет. 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 маршрутизации трафика.

Путь

Точное расположение 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 имен файлов. Обычно они состоят из трех букв, потому что устаревшие ОС не имеют поддержки более длинных расширений. 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 adware-программу. Поскольку Adware-приложения обычно устанавливаются только после того, как пользователь принимает условия, содержащиеся в соответствующем лицензионном соглашении с указанием функций данного 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 производительность системы. Кроме того, информация, собираемая некоторыми из этих приложений, может нарушить неприкосновенность частной жизни пользователей, которые не были в полной мере осведомлены об условиях 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, при этом 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 перифирийных устройств, если их встроить в соотвествующее программное обеспечение.

По своей природе руткиты не вредоносны. Например, системы, а также некоторые приложения, скрывают важные файлы при помощи руткитов. Однако они используются для скрытия угроз или присутствия злоумышленника в системе. В сочетании с угрозами руткиты представляют собой серьезную угрозу целостности и безопасности системы. Они могут отслеживать трафик, создавать бреши в системе, изменять файлы и журналы, избегая выявления.

События (Events)

Действие или событие, обнаруженное программой. Событиями могут быть действия пользователя, например щелчок кнопкой мыши, или нажатие клавиши, или системные события, например, переполнение памяти.

Спам

"Мусорная" электронная почта или "мусорная" новостная рассылка. Более известна как нежелательная электронная почта.

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 вредоносных программ и червей, трояны не размножаются, но могут быть столь же разрушительными. Одним из самых коварных типов угроз трояна является программа, которая обещает избавить ваш компьютер от угроз, но вместо этого вводит их на ваш компьютер.

Этот термин взят из поэмы Гомера «Илиада», где в одной из глав описывается как греки подарили своим врагам, жителям Трои, огромного деревянного коня, якобы в знак мира. Но после того, как троянцы втащили статую в город, греческие солдаты выскочили из полости в теле коня и открыли городские врата, после чего их соратники ворвались в Трою и захватили город.

Угроза

Программа или часть кода, которая загружается в ваш компьютер без вашего ведома и запускается без вашего участия. Многие угрозы также могут копировать себя. Все компьютерные угрозы создаются людьми. Сравнительно легко создать простую угрозу, которая копирует себя снова и снова. Даже такая простая угроза очень опасна, так как она быстро использует всю свободную память и система зависает. Еще более опасным типом угрозы является угроза, способная передавать себя через сети и обходить системы безопасности.

Файл отчета

Файл, в котором перечислены совершенные действия. Bitdefender хранит файл отчета с указанием пути сканирования, папок, количества просмотренных архивов и файлов, числа обнаруженных зараженных и подозрительных файлов.

Файлы Cookie

В сфере интернет-технологий под файлами cookie подразумеваются небольшие файлы, содержащие информацию о компьютере, которую можно проанализировать и использовать для того, чтобы выяснить

ваши интересы и предпочтения. Поэтому технология создания таких файлов набирает обороты и сейчас вы можете получать рекламу товаров, основанную на ваших интересах. Но это "палка о двух концах" - с одной стороны вы видите именно то, что может вам пригодиться. Но с другой – за вами постоянно следят и знают, на какой странице вы находитесь и на какой кнопке щелкаете мышкой. Понятно, почему сейчас так широко обсуждается конфиденциальность данных пользователей и многие чувствуют себя ущемленными в своих правах, будучи уверенными, что их «считывают» как кассир в магазине считывает штрих-код на этикетке. Порой эта точка зрения кажется крайностью, но иногда она полностью отражает действительность.

Фишинг

Это действие, заключающееся в отправке пользователю электронного письма, якобы от имени реально существующей организации с целью получения обманным путем конфиденциальной информации, которая будет использоваться для кражи личных данных. В получаемом сообщении электронной почты пользователя, с помощью вложенной ссылки, приглашают посетить якобы официальный веб-сайт реально существующей организации, где его просят подтвердить или обновить личные данные (например, пароли и номера банковских счетов, кредитной карточки, карточки социального обеспечения). 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 анализ (Heuristic)

Метод обнаружения новых угроз, основанный на правилах. Этот метод сканирования не зависит от определенной базы данных угроз. Преимущество эвристической проверки состоит в том, что новый вариант угрозы не может "обмануть" фильтр. Однако он может принять подозрительный код в обычных программах за вирус и вызвать так называемое «ложное срабатывание».

Эл. почта

Электронная почта. Сервис, отправляющий сообщения на другие компьютеры через локальную или глобальную сеть.

Элементы запуска

Все файлы, помещенные в эту папку будут открываться при запуске компьютера. Элементами автозагрузки могут быть 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 оперативная память или RAM.